Opis Przedmiotu Zamówienia

„Podniesienie odporności na zagrożenia cybernetyczne w Gminie Golina, realizowana w ramach Grantu Fundusze Europejskie na Rozwój Cyfrowy (FERC), II Zaawansowane Usługi Cyfrowe, 2.2 Wzmocnienie Krajowego Systemu Cyberbezpieczeństwa, nr naboru FERC.02,02-CS.01-001/23”

Golina, listopad 2024

Spis treści

Wstęp ***3***

Ogólny zarys projektu *3*

Słownik pojęć *3*

Ogólne zasady równoważności rozwiązań ***5***

Wymagania ogólne ***7***

Harmonogram realizacji przedmiotu zamówienia ***8***

Dostawa sprzętu ***9***

Urządzenie UTM – 5 sztuk *9*

Macierz dyskowa *20*

Serwer *28*

NAS – 5 sztuk *30*

Dostawa oprogramowania ***32***

System SIEM *32*

Platforma e-learning w zakresie cyberbezpieczeństwa *36*

System wirtualizacyjny ..... ***Błąd! Nie zdefiniowano zakładki.***

Oprogramowanie kopii zapasowych *44*

Konfiguracja i uruchomienie sprzętu oraz oprogramowania sprzętowego ***48***

Wdrożenie i konfiguracja elementów bezpieczeństwa ***49***

System SIEM *49*

Platforma szkoleniowa *49*

Wsparcie eksperckie w zakresie cyberbezpieczeństwa ***51***

Przygotowanie oraz przeprowadzenie szkoleń ***53***

Przeprowadzenie audytu bezpieczeństwa ***55***

Aktualizacja Systemu Zarządzania Bezpieczeństwem Infromacji ***57***

Wstęp

Niniejszy dokument stanowi Opis Przedmiotu Zamówienia w zakresie dostawy i wdrożenia sprzętu i oprogramowania zwiększającego poziom bezpieczeństwa cybernetycznego Urzędu Gminy Golina oraz Miejski Ośrodek Pomocy Społecznej, Szkoła Podstawowa w Radolinie, Szkoła Podstawowa w Przyjmie, Szkoła Podstawowa w Kawnicach oraz Szkoła Podstawowa w Golinie.

Zadanie realizowane jest w ramach Grantu Fundusze Europejskie na Rozwój Cyfrowy (FERC), II Zaawansowane Usługi Cyfrowe, 2.2 Wzmocnienie Krajowego Systemu Cyberbezpieczeństwa, nr naboru FERC.02,02-CS.01-001/23.

Ogólny zarys projektu

W ramach zadania planowana jest realizacja kompleksowego projektu zwiększenie bezpieczeństwa informatycznego tj.

- przeprowadzenia audytów (wstępny i powdrożeniowy),
- dostawa i konfiguracja sprzętu,
- dostawa i konfiguracja zaawansowanych systemów bezpieczeństwa,
- przeprowadzenia szkoleń z zakresu bezpieczeństwa dla wszystkich pracowników,
- opracowanie i dostosowanie do wdrożonych rozwiązań dokumentów Systemu Zarządzania Bezpieczeństwem Informacji,
- świadczenie rozszerzonej usługi serwisowej, aktualizacji oprogramowania do najnowszych wersji i wsparcia na okres 24 miesięcy.

Słownik pojęć

Na potrzeby niniejszego postępowania stosuje się następujące pojęcia i definicje:

API - (ang. Application Programming Interface) interfejs programowania aplikacji, umożliwiający komunikację z biblioteką, systemem operacyjnym lub innym systemem zewnętrznym w stosunku do tej aplikacji;

JST – Jednostka Samorządu Terytorialnego – Zamawiający;

LMS – system elearningowy;

PBI – Polityka Bezpieczeństwa Informacji;

PZ – Przedmiot Zamówienia;

SZBI – System Zarządzania Bezpieczeństwem Informacji;

Wykonawca – Oferent, podmiot, który złoży zwycięską ofertę w postępowaniu przetargowym i podpisze umowę z Zamawiającym;

Zamawiający – Gmina Golina.

Ogólne zasady równoważności rozwiązań

W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega znacząco od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym, przy czym nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób, za rozwiązanie równoważne nie można uznać rozwiązania identycznego (tożsamego), a jedynie takie, które w porównywanych cechach wykazuje dokładnie tą samą lub bardzo zbliżoną wartość użytkową. Przez bardzo zbliżoną wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic niewpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są dedykowane. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego. Dostarczenie przez Wykonawcę rozwiązania równoważnego musi być zrealizowane w taki sposób, aby wymiana oprogramowania na równoważne nie zakłóciła bieżącej pracy Urzędu. W tym celu Wykonawca musi do oprogramowania równoważnego przenieść wszystkie dane niezbędne do prawidłowego działania nowych systemów, przeszkolić użytkowników, skonfigurować oprogramowanie, uwzględnić niezbędną asystę pracowników Wykonawcy w operacji uruchamiania oprogramowania w środowisku produkcyjnym itp.

Dodatkowo, wszędzie tam, gdzie zostało wskazane pochodzenie (marka, znak towarowy, producent, dostawca itp.) materiałów lub normy, aprobaty, specyfikacje i systemy, o których mowa w ustawie Prawo Zamówień Publicznych, Zamawiający dopuszcza oferowanie sprzętu lub rozwiązań równoważnych pod warunkiem, że zapewnią uzyskanie parametrów

technicznych nie gorszych niż wymagane przez Zamawiającego w dokumentacji przetargowej. Zamawiający informuje, że w takiej sytuacji przedmiotowe zapisy są jedynie przykładowe i stanowią wskazanie dla Wykonawcy jakie cechy powinny posiadać składniki użyte do realizacji przedmiotu zamówienia. Zamawiający, zgodnie z ustawą Prawo zamówień publicznych, dopuszcza oferowanie materiałów lub urządzeń równoważnych. Materiały lub urządzenia pochodzące od konkretnych producentów określają minimalne parametry jakościowe i cechy użytkowe, a także jakościowe (m.in.: wymiary, skład, zastosowany materiał, kolor, odcień, przeznaczenie materiałów i urządzeń, estetyka itp.) jakim muszą odpowiadać materiały lub urządzenia oferowane przez Wykonawcę, aby zostały spełnione wymagania stawiane przez Zamawiającego. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Posługiwanie się nazwami producentów/produktów ma wyłącznie charakter przykładowy (poza wyjątkami gdzie nie ma możliwości zastosowania rozwiązań równoważnych). Zamawiający, wskazując oznaczenie konkretnego producenta (dostawcy), konkretny produkt lub materiały przy opisie przedmiotu zamówienia, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych lub lepszych parametrach. Zamawiający opisując przedmiot zamówienia przy pomocy określonych norm, aprobat czy specyfikacji technicznych i systemów odniesienia, dopuszcza rozwiązania równoważne opisywanym. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy spełniają wymagania określone przez Zamawiającego. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów, uwiarygodniających te rozwiązania.

Wymagania ogólne

Zamawiający wymaga, aby sprzęt będący przedmiotem dostawy był wyprodukowany nie wcześniej niż 9 miesięcy od dnia dostawy. Oprogramowanie musi być dostarczone i zainstalowane w wersji aktualnej (stabilnej) na dzień jego instalacji. W ramach realizacji przedmiotu zamówienia Wykonawca ma obowiązek przeprowadzić analizę przedwdrożeniową, podczas której zostaną zebrane wymagania techniczne dotyczące realizacji konfiguracji bezpieczeństwa systemów.

Zamawiający oczekuje wdrożenia wszystkich zaleceń audytu bezpieczeństwa, dotyczących technicznych komponentów systemu teleinformatycznego.

W ramach prowadzonych prac, a w szczególności prac konfiguracyjnych, Zamawiający oczekuje utrzymania funkcjonalności wszystkich posiadanych przez siebie systemów i aplikacji. Prace wdrożeniowe muszą być przeprowadzone w taki sposób, aby nie zakłócić normalnej pracy urzędu. Jeżeli podczas prowadzonych prac zaistnieje konieczność rekonfiguracji posiadanych przez Zamawiającego systemów, Wykonawca jest zobowiązany dokonać takich rekonfiguracji na własną odpowiedzialność oraz własny koszt.

Zamawiający oczekuje, aby wszystkie wdrożone usługi były zgodne z ITIL (Information Technology Infrastructure Library) w zakresie najlepszych praktyk zarządzania usługami IT w celu zwiększenia efektywności, skuteczności oraz bezpieczeństwa operacji IT, w szczególności w efektywnym zarządzaniu ryzykiem, reagowaniu na incydenty bezpieczeństwa, a także w zapewnieniu zgodności z przepisami prawnymi i standardami branżowymi.

Harmonogram realizacji przedmiotu zamówienia

Harmonogram rzeczowo-finansowy z podziałem na etapy wraz z wartością, kolejność realizacji zakresów, kamienie milowe zostanie ustalony opracowany przez Wykonawcę w porozumieniu z Zamawiającym i zaakceptowany przez Zamawiającego w ciągu 7 dni od daty podpisania Umowy.

Dostawa sprzętu

Urządzenie UTM – 5 sztuk

Cecha	Wymagania minimalne
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 4 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 podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
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 Enterprise Traffic Mix - minimum 1 Gbps. 6. 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 oraz SSL VPN. 4. Ochrona przed malware. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. 13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa)
Polityki, Firewall	1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu.

	• Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP. 5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. 7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu. • Amazon Web Services (AWS). • Microsoft Azure. • Cisco ACI. • Google Cloud Platform (GCP). • OpenStack. • VMware NSX. • Kubernetes.
Połączenia VPN	1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: • Wsparcie dla IKE v1 oraz v2. • Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19, 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.

	• Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. • Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. • Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. • Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling" dla połączeń Client-to-Site. 2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia: • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0. • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta. • Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.
Routing i obsługa łączy WAN	W zakresie routingu rozwiązanie zapewnia obsługę: 1. Routingu statycznego. 2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).

	3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection). 7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
Funkcje SD-WAN	1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
Zarządzanie pasmem	1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System daje możliwość określania pasma dla poszczególnych aplikacji. 3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system

	będzie próbował zdekompresować w celu przeskanowania zawartości. 4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. 5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze. 8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. 10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.
Ochrona przed atakami	1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach. 3. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. 4. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.

	5. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). 6. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. 8. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
Kontrola aplikacji	1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 3. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 4. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. 5. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 6. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).
Kontrola WWW	1. 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 dwuskładnikowego.

	3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. 4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. 3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

	8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). 9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
Logowanie	1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. 4. Możliwość włączenia logowania per reguła w polityce firewall. 5. System zapewnia możliwość logowania do serwera SYSLOG. 6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
Certyfikaty	Poszczególne elementy systemu bezpieczeństwa posiadają następujące certyfikacje: • ICSA lub EAL4 dla funkcji Firewall.
Gwarancja oraz wsparcie	1. Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres co najmniej 12 miesięcy, polegającym na naprawie. W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Macierz dyskowa

Cecha	Wymaganie minimalne
Obudowa	Obudowa o wysokości 2U do montażu w szafie rack 19” za pomocą dostarczonych dedykowanych elementów. Obudowa w ramach cache musi posiadać zainstalowane minimum 4 dyski 1.92TB SSD SAS każdy.
Architektura	Oferowany deduplikator musi być zbudowany w oparciu o architekturę active-active tj. posiada minimum dwa kontrolery do obsługi danych, pracujące nadmariowo w trybie active-active
Kontrolery	Deduplikator musi być wyposażona w minimum 2 kontrolery pracujące w trybie active-passive lub active-active. Deduplikator nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. W przypadku awarii kontrolera wszystkie procesy musi przejąć drugi kontroler.
Wydajność kopii zapasowych	Oferowany model deduplikatora musi osiągać w maksymalnej konfiguracji zagregowaną wydajność backupu co najmniej 5 TB/h (dane podawane przez producenta). Wydajność podawana bez uwzględnienia deduplikacji na źródle.
Wydajność odtworzenia kopii zapasowych	Oferowany model deduplikatora w oferowanej konfiguracji musi osiągać zagregowaną wydajność odtworzenia backupu co najmniej 0.8 TB/h. Wymagane oświadczenia producenta lub wydruk z oryginalnego estymatora producenta.
Wymagana przestrzeń	Przestrzeń użytkowa HDD po zbudowaniu RAID 6 (z min. dyskiem hot-spare lub przestrzenią hot-spare) musi wynosić min 16 TB. Ze względów wydajnościowych oraz niezawodnościowych pojemność RAW pojedynczego dysku nie może być większa niż 4 TB. Wymagana pojemność użytkowa rozumiana jest jako pojemność dostępna po konfiguracji RAID i odliczeniu rezerwy na dyski/przestrzeń hot-*spare* i

	dostępna dla hostów bez uwzględnienia jakichkolwiek mechanizmów kompresji, czy deduplikacji.
Zabezpieczenie RAID	Dane przechowywane w obrębie urządzenia na dyskach HDD muszą być chronione za pomocą technologii RAID 6 lub równoważnej tolerującej jednoczesną awarię 3 dysków bez utraty danych. Urządzenie musi umożliwiać bezpieczne usuwanie danych zgodnie ze standardem DoD 5220.22-M poprzez mechanizm nadpisywania danych.
Pamięc cache	Co najmniej 256GB pamięci cache zbudowanej z pamięci RAM (nie dopuszcza się zbudowania 256GB pamięci cache w ramach dysków SSD) na cały deduplikator (dwa kontrolery). Pamięć cache musi być zabezpieczona przed utratą danych w przypadku awarii zasilania.
Dostępne interfejsy	Urządzenie musi posiadać minimum: 8 portów Ethernet 10Gb/s SFP+ z możliwością obsługi każdym portem Ethernet protokołów iSCSI, CIFS, NFS, wszystkie porty wyposażone we wkładki optyczne. 4 portów Ethernet 10Gb/s SFP+ wszystkie porty wyposażone we wkładki optyczne oraz 8 portów Ethernet Gb/s RJ45. Minimum 12 przewodów każdy o długości minimum 3 metry dla powyższych portów Ethernet 10Gb/s SFP+.
Obsługiwane protokoły	Wymagane wsparcie dla FC, iSCSI, NFS, CIFS.
Szyfrowanie	Deduplikator musi zapewniać szyfrowanie zasobów w ramach zastosowania algorytmu AES.

Zarządzanie	Zarządzanie deduplikatorem (wszystkimi kontrolerami) z poziomu pojedynczego interfejsu graficznego. Wymagane jest stałe monitorowanie stanu deduplikatora w tym monitorowanie wydajności obiektów takich jak: - cały deduplikator - kontrolery - CPU - porty front-end - porty logiczne - dyski - file systemy Pod kątem parametrów takich jak: - operacje wejścia/wyjścia IOPS - przepustowość (KB/s lub MB/s) - czas odpowiedzi (latency) - średnie użycie (w % dla CPU) Wymagana możliwość dostępu do historycznych danych wydajnościowych z poziomu GUI urządzenia do co najmniej 2 lat wstecz lub jako równoważne dostarczenie fizycznego serwera z oprogramowaniem umożliwiającym zbieranie i przeglądanie danych historycznych. Wymagany dostęp do prognozy zużycia przestrzeni. Wymagana możliwość tworzenia wielu użytkowników deduplikatora w oparciu o wbudowane role. Rozwiązanie musi umożliwiać tworzenie własnych ról.

	Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.
Redukcja danych	Urządzenie musi deduplikować dane inline przed zapisem na nośnik dyskowy. Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym bloku. Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych. Proces deduplikacji musi odbywać się inline – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Dane muszą być poddane także procesowi kompresji. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej oczekiwanej pojemności. Wymagana także obsługa deduplikacji na źródle, co pozwala ograniczyć zużycie sieci.

	Musi być oficjalne wsparcie producenta dla oferowanego deduplikatora maksymalnego stopnia redukcji danych min. 60:1.
Kontrola zasobów plikowych	Wymagana możliwość skonfigurowania tzw. quoty ograniczającej wystawione zasoby plikowe. Wymagana możliwość ograniczenia użytkownikom przestrzeni z której mogą korzystać lub liczby plików jakie mogą być przechowywane na udostępnionej przestrzeni. Wymagana możliwość skonfigurowania polityki filtrowania zapisywanych plików poprzez wykluczenie ich konkretnych rozszerzeń. Wymagana możliwość ograniczenia dostępu do udostępnionych udziałów CIFS/NFS poprzez zdefiniowanie adresów IP lub ich przedziałów, które będą miały do nich dostęp. Dostarczenie powyższych funkcjonalności jest wymagane wraz z dostawą przedmiotu zamówienia.
Ochrona zasobów plikowych	Tworzenie na żądanie tzw. migawkowej kopii danych (ang. snapshot) file system'ów w ramach deduplikatora do wykorzystania w celu np. wykonywania kopii zapasowych. Wymagana jest możliwość utworzenia harmonogramu snapshotów. Deduplikator musi umożliwiać utworzenie min 8000 snapshotów. Musi być możliwość utworzenia snapshotów których nie można modyfikować ani usunąć przez wybrany okres czasu bez odpowiednich uprawnień celem przywrócenia danych w przypadku ataku ransomware. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania na całą oczekiwaną pojemność i na maksymalną liczbę snapshotów obsługiwanych przez oferowany model deduplikatora.

	Wymagana możliwość zablokowania plików przed modyfikacją lub usunięciem (WORM). Dostarczenie licencji na tą funkcjonalność jest wymagane wraz z dostawą przedmiotu zamówienia. Tworzenie na żądanie tzw. migawkowej kopii danych (ang. snapshot) file system'ów w ramach deduplikatora do wykorzystania w celu np. wykonywania kopii zapasowych. Wymagana jest możliwość utworzenia harmonogramu snapshotów. Deduplikator musi umożliwiać utworzenie min 8000 snapshotów. Musi być możliwość utworzenia snapshotów których nie można modyfikować ani usunąć przez wybrany okres czasu bez odpowiednich uprawnień celem przywrócenia danych w przypadku ataku ransomware. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania na całą oczekiwaną pojemność i na maksymalną liczbę snapshotów obsługiwanych przez oferowany model deduplikatora. Wymagana możliwość zablokowania plików przed modyfikacją lub usunięciem (WORM). Dostarczenie licencji na tą funkcjonalność jest wymagane wraz z dostawą przedmiotu zamówienia. Tworzenie na żądanie tzw. migawkowej kopii danych (ang. snapshot) file system'ów w ramach deduplikatora do wykorzystania w celu np. wykonywania kopii zapasowych. Wymagana jest możliwość utworzenia harmonogramu snapshotów. Deduplikator musi umożliwiać utworzenie min 8000 snapshotów. Musi być możliwość utworzenia snapshotów których nie można modyfikować ani usunąć przez wybrany okres czasu bez odpowiednich uprawnień celem przywrócenia danych w przypadku ataku ransomware. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania na całą oczekiwaną pojemność i na maksymalną liczbę snapshotów obsługiwanych przez oferowany model deduplikatora.

	Wymagana możliwość zablokowania plików przed modyfikacją lub usunięciem (WORM). Dostarczenie licencji na tą funkcjonalność jest wymagane wraz z dostawą przedmiotu zamówienia.
Replikacja danych	Urządzenie musi umożliwiać replikację danych do drugiego takiego samego urządzenia. Replikacja musi się odbywać w trybie asynchronicznym. Wymagana możliwość ograniczenia ilości przesyłanych danych poprzez ich deduplikację oraz kompresję. Deduplikator musi umożliwiać konfigurację harmonogramu replikacji poprzez określenie interwału (np. replikacja co 60min) lub konkretnych okien czasowych (np. w każdą sobotę o godz 20:00). Wymagana możliwość zastosowania funkcjonalności typu AirGap czyli fizyczne wyłączanie portów dedykowanych do replikacji w czasie kiedy replikacja nie jest wykonywana. Dopuszcza się realizację tej funkcjonalności poprzez zastosowanie dodatkowego oprogramowania. Dostarczenie powyższych funkcjonalności nie jest wymagane wraz z dostawą przedmiotu zamówienia.
Wspierana oprogramowania	Urządzenie musi wspierać co najmniej następujące aplikacje do backupu: Commvault, Veritas NetBackup, Veeam.

do kopii zapasowych	
Obsługa serwisowa	Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż w 2024 roku i pochodzić z autoryzowanego kanału dystrybucji producenta, a także musi być objęte serwisem producenta lub autoryzowanego partnera serwisowego na terenie RP. Usługi gwarancyjne muszą być świadczone przez producenta lub autoryzowanego przedstawiciela producenta posiadającego co najmniej certyfikat ISO 9001 na świadczenie usług serwisowych. Urządzenie musi zostać objęte minimum 36 miesięcznym okresem gwarancji w trybie 9x5 NBD onsite z gwarantowanym czasem reakcji najpóźniej w następnym dniu roboczym od momentu zgłoszenia usterki. Deduplikator musi posiadać możliwość upgradeu firmware-u kontrolerów bez przerywania dostępu do danych. Urządzenie przystosowane do napraw w miejscu instalacji oraz wymiany elementów bez konieczności jego wyłączania. Urządzenie musi umożliwiać zdalne zarządzanie. Wymagane jest, aby gwarancja świadczona była z zachowaniem poniższych warunków: • możliwość pobierania najnowszego firmware. • dostęp do bazy wiedzy producenta w zakresie dostarczanych urządzeń. • dostęp do centrum pomocy technicznej producenta.

	• otwieranie zgłoszeń serwisowych w przypadku podejrzenia możliwości błędu w oprogramowaniu/hardware. • otrzymywanie poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z deduplikatorem oraz oprogramowania wewnętrznego deduplikatora. W przypadku awarii dysków uszkodzone nośniki pozostają u Zamawiającego.

Serwer

Obudowa	Rack
Wysokość	Max 2U
Procesor	DWA procesory MIN 16 RDZENI taktowanie rdzenia MIN 2.4 GHz,
Pamięć	32 gniazda DIMM z dwoma procesorami (16 gniazd DIMM na procesor). Każdy procesor ma 8 kanałów pamięci, z 2 modułami DIMM na kanał. ZAINSTALOWANE 128GB W modułach RDIMM 3200 MHz
Maksymalna pamięć	Do 8 TB z 32 modułami 3DS RDIMM 256 GB
Ochrona pamięci	ECC, SDDC, Patrol/Demand Scrubbing, DRAM Address Command Parity with Replay, DRAM Uncorrected ECC Error Retry, Post Package Repair
Kieszenie na dyski	Wymagane min 8 szt. 2,5-calowych wnęk na dyski typu hot-swap, z możliwością wymiany podczas pracy
pamięć wewnętrzna	2 x dysk min 480GB , 6x dysk 1,92 TB ssd

Kontroler pamięci masowej	Wbudowany NVMe (bez RAID) Wbudowane złącze SATA (bez RAID) Adapter SAS/SATA RAID: z 2 GB pamięci podręcznej z obsługą pamięci flash obsługa RAID 0, 1, 10, 5, 50, 6, 60
Interfejsy sieciowe	Wymagane : 2 porty 10/25 GbE
Gniazda rozszerzeń PCI	2 gniazda PCIe 4.0 x16
Porty	Przód: 1x port USB 3.1 G1 (5 Gb/s), 1x port USB 2.0 zewnętrzny port diagnostyczny wraz panelem LCD lub rozwiązanie równoważne Tył: 3 porty USB 3.1 G1 (5 Gb/s), 1 port wideo VGA, 1 port zarządzania systemami RJ-45 1 GbE do zdalnego zarządzania Wewnętrzne: 1x złącze USB 3.1 G1 do systemu operacyjnego lub klucza licencyjnego
Chłodzenie	6 nadmiarowych wentylatorów 60 mm N+1 z możliwością wymiany podczas pracy, w zależności od konfiguracji. Jeden wentylator zintegrowany w każdym zasilaczu.
Zasilacz	Dwa zasilacze sieciowe z możliwością wymiany podczas pracy, certyfikat 80 PLUS Platinum. min 750 W obsługujące 220 V AC. obsługujące również zasilanie wejściowe 110 V.
Wideo	Grafika G200 z 16 MB pamięci z akceleratorem sprzętowym 2D, zintegrowana z kontrolerem XClarity. Maksymalna rozdzielczość to 1920x1200 32 bpp przy 60 Hz.
Części wymieniane podczas pracy serwera	Napędy, zasilacze, wentylatory.
Zarządzanie systemami	Dedykowany port wraz z kontrolerem do monitorowania parametrów serwera z funkcją zdalnego sterowania obsługę montowania zdalnych plików multimedialnych (plików obrazów ISO i IMG)
Funkcjonalność związana z bezpieczeństwem	Przełącznik naruszenia obudowy, hasło włączenia zasilania, hasło administratora, Trusted Platform Module (TPM), obsługa TPM 2.0.

Obsługiwane systemy operacyjne	Microsoft Windows Server, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, VMware ESXi.
Gwarancja	3letnia na miejscu z 9x5 następnego dnia roboczego (NBD)., realizowana przez autoryzowany serwis producenta lub partnera serwisowego
Serwis i wsparcie	Możliwość rozszerzenia usługi gwarancji producenta w trakcie trwania gwarancji o 2-godzinny czas reakcji wraz z 4-godzinnym czasem naprawy w dowolnym momencie w ciągu 5 lat trwania serwisu. W przypadku niesprawności dysków w ramach naprawy gwarancyjnej pozostają one u Zamawiającego.
Wymiary	Dostosowane do szafy 42U o głębokości 80 cm Serwer dostarczony wraz z szynami montażowymi do wysuwania serwera
Dodatkowe	Dostawa urządzenia UPS gwarantującego zasilanie awaryjne urządzenia na czas min. 10 minut

NAS – 5 sztuk

Obudowa	Tower
Pojemność	4 dyski twarde, 4TB, 7200obr. 256MB cache, niezawodność 1 000 000 godzin
Maksymalna pojemność	72TB
Kieszenie na dyski	2,5”/3,5” – 4szt. (Hot swap)
Interfejsy	RJ45, USB 3.2 Gen
Pamięc RAM	Min. 2Gb
Obsługiwane systemy plików	FAT, exFAT, NTFS, EXT3, EXT4
Funkcje dodatkowe	Wake on LAN, dostęp przez web oraz aplikacje mobilne
Gwarancja producenta	Min. 24 miesiące

Dodatkowe	Dostawa urządzenia UPS gwarantującego zasilanie awaryjne urządzenia NAS na czas min. 15 minut

Dostawa oprogramowania

System SIEM

Cecha	Wymagania minimalne
Serwer	System musi być rozwiązaniem klasy SIEM z rozszerzeniem XDR umożliwiającym monitorowanie bezpieczeństwa, wykrywania zagrożeń, monitorowania integralności oraz odpowiedzi na incydenty.
	System musi umożliwiać monitorowanie infrastruktury IT w czasie rzeczywistym. Infrastruktura IT Zamawiającego składa się z: • 4 serwerów • 1 urządzeń UTM • 3 przełączników sieciowych • 45 komputerów
	Komponenty serwerowe systemu muszą być możliwe do zainstalowania na systemie operacyjnym z rodziny Linux.
	System musi być możliwy do zainstalowania w środowisku wirtualizacyjnym opartym o Proxmox VE.
	Instalacja i konfiguracja systemu musi być możliwa do automatyzacji z wykorzystaniem Ansible.
	Wykonawca w ramach postępowania dostarczy wszelkie niezbędne licencje umożliwiające uruchomienie Systemu takie jak np. systemy operacyjne, serwery baz danych, itp.
	System musi być dostarczony w konfiguracji wysokodostępnej (klaster High Availability) dla każdego z komponentów z wyłączeniem agentów.
	System musi umożliwiać monitorowanie agentowe oraz bezagentowe (sieciowe).

	Silnik system musi udostępniać API w technologii REST pozwalające na rejestrację zdarzeń, zarządzanie konfiguracją agentów oraz odczyt stanu każdego z monitorowanych komponentów.
	Logowanie operatorów do systemu musi odbywać się z wykorzystaniem Centralnego Systemu Zarządzania Tożsamością (SSO) co najmniej w zakresie protokołu SAML2.
	System musi posiadać kontrolę dostępu opartą na rolach (RBAC).
	System musi posiadać funkcję wysyłania powiadomień do użytkowników lub grup w odpowiedzi na występujące zagrożenia. System musi wysyłać powiadomienia co najmniej za pomocą email oraz SMS.
	System musi być dostarczony wraz z wbudowanymi regułami detekcji. Musi istnieć możliwość dodawania własnych reguł.
	System musi umożliwiać zaawansowane metody detekcji poprzez integrację z frameworkiem MITRE ATT&CK.
	System musi wykrywać i aktywnie blokować ataki typu brute-force na hasła systemów operacyjnych.
	System musi umożliwiać integrację z oprogramowaniem NIDS tj. Suricata.
	System musi wykrywać i zapobiegać atakom typu SQL Injection.
	System musi wykrywać i blokować ataki typu DDoS.

	System musi umożliwiać wykrywania i usuwanie malware poprzez integrację z zewnętrznymi bazami i narzędziami tj. VirusTotal.
	System musi wykrywać znane podatności na każdym monitorowanym obiekcie z wykorzystaniem baz CVE.
	System musi wykrywać ukryte procesy oraz wykonywanie podejrzanych operacji przez zainstalowane w systemie operacyjnym monitorowanego obiektu aplikacje.
Agent	System musi udostępniać dedykowane pliki instalacyjne agentów dla systemów co najmniej Windows, Linux oraz MacOS.
	Agent musi komunikować się z serwerem systemu za pomocą szyfrowanego i autoryzowanego połączenia.
	Agent musi posiadać funkcjonalność zdalnej konfiguracji oraz zdalnej aktualizacji po podłączeniu się do serwera.
	Agent musi posiadać budowę modułową z możliwością wyłączenia poszczególnych modułów w zależności od wymaganej konfiguracji oraz możliwości wydajnościowych monitorowanego obiektu.
	Agent musi posiadać co najmniej następujące moduły: • Moduł zbierania logów (kolektor logów) • Moduł wykonywania poleceń • Moduł monitorowania integralności plików • Moduł inwentaryzacji zasobów • Moduł oceny konfiguracji bezpieczeństwa (SCA) • Moduł wykrywania podatności • Moduł zgodności ze standardami bezpieczeństwa • Moduł reaktywnej odpowiedzi

	• Moduł wykrywania malware
	Agent musi posiadać kolektor logów wspierający filtry XPath do przetwarzania Dziennika zdarzeń systemu Windows.
	Kolektor logów musi wspierać odczyt wielolinijkowych logów (co najmniej format Linux Audit).
	Monitor integralności plików musi umożliwiać rejestrowania zdarzeń tj. utworzenie pliku, modyfikacja lub usunięcie wraz ze wskazaniem użytkownika oraz czasu zdarzenia. Dodatkowo moduł musi umożliwiać monitorowanie zmian atrybutów, uprawnień, właściciela oraz monitoring zawartości pliku.
	Moduł inwentaryzacji zasobów musi zbierać i udostępniać informacje o obiekcie w zakresie co najmniej: • Rodzaj i wersja systemu operacyjnego, • Lista i rodzaj interfejsów sieciowych, • Lista aktywnych procesów systemu operacyjnego, • Lista zainstalowanych aplikacji, • Lista otwartych portów sieciowych.
	Moduł oceny konfiguracji bezpieczeństwa musi umożliwiać, za pomocą predefiniowanych reguł, skanowanie obiektu w celu wykrycia zagrożeń lub błędnych konfiguracji w zakresie co najmniej: • Siła haseł, • Usunięcie niepotrzebnego lub niebezpiecznego oprogramowania, • Wyłączenie zbędnych usług Moduł musi posiadać predefiniowane reguły SCA dla każdego z wymaganych systemów operacyjnych oraz udostępniać możliwość tworzenia własnych polityk SCA.

	Moduł wykrywania podatności musi umożliwiać wykrywania luk w aplikacjach zainstalowanych na obiekcie za pomocą dostawców tj. National Vulnerability Database, Red Hat, Canonical, ALAS, MSU.
	Moduł zgodności ze standardami bezpieczeństwa musi umożliwiać badania obiektu pod katem zgodności ze standardami tj. PCI DSS, HIPAA, NIST 800-53 oraz GDPR.
	Moduł reaktywnej odpowiedzi musi umożliwiać automatyczne (bez udziału operatora SIEM) uruchomienie akcji tj.: • Zablokowanie połączenia sieciowego, • Zatrzymanie aktywnego procesu, • Usunięcie pliku, • Przeskanowanie pliku pod kątem obecności wirusów.
	Moduł wykrywania malware musi posiadać możliwość wykrywania anomalii i na tej podstawie obecności złośliwego oprogramowania. Moduł musi umożliwiać wykrywania ukrytych procesów, ukrytych plików oraz podejrzanych otwartych portów TCP/UDP.

Platforma e-learning w zakresie cyberbezpieczeństwa

Cecha	**Wymagania minimalne**
Ogólne	System musi umożliwiać kompleksowe przeprowadzanie szkoleń przez Internet.
	System musi zapewniać instruktaże krok po kroku.
	System musi umożliwiać dodanie filmów szkoleniowych.
	System udostępniania poradniki i materiały dla uczestnika.
	System musi umożliwiać publikację wykładów wyjaśniających zasady działania systemu, pokazując bezpieczeństwo płatności internetowych i korzyści wynikające z korzystania z EPUAP i cyfrowego urzędu.
	System umożliwia dodanie dwóch rodzajów uczestników szkoleń – urzędnik i mieszkaniec.

	System musi umożliwiać przeszukiwanie bazy szkoleń.
	System musi zapewniać możliwość wystawiania certyfikatów z odbytych szkoleń.
	System generuje raporty pozwalające na kontrolę stopnia wykorzystania narzędzia.
	System zbudowana jest w sposób modułowy i opiera się o architekturę klient-serwer: a) serwer (WWW/Aplikacji LMS/Bazy Danych), b) klient (dowolny system operacyjny, dowolna przeglądarka internetowa);
	System musi zapewniać prowadzenie szkoleń za pośrednictwem Internetu z wykorzystaniem: a) komputerów, b) smartfonów, c) tabletów;
	System umożliwia dostęp on-line do szkoleń z dowolnego systemu operacyjnego i dowolnej przeglądarki internetowej.
	System musi umożliwiać prowadzenie szkoleń z wykorzystaniem kursów multimedialnych, książek elektronicznych, elementów audio/wideo, telewizji internetowej.
	System jest wyposażony w platformę do zarządzania szkoleniami (LMS).
	System posiada narzędzie dla autorów szkoleń do tworzenia kursów e-learning (LCMS).
	System pozwala na modyfikację istniejących szkoleń (edycja m.in. w zakresie opisu kursów i zawartości).
	System posiada mechanizm autoryzacji dostępu z wykorzystaniem Centralnego Systemu Zarządzania Tożsamością.
	System posiada mechanizm określenia dostępności szkoleń (w tym: czas dostępności, sposób zapisu, klucz dostępu, widoczność elementów, itp.).
	System pozwala na dezaktywację szkoleń.
	System udostępnia uprawnionym użytkownikom narzędzia do sprawdzania wiedzy i umiejętności opanowanych przez kursantów/uczniów z możliwością tworzenia bazy pytań kontrolnych różnego rodzaju spośród których tworzony jest test, w tym:

	jednokrotnego/wielokrotnego wyboru, prawda/fałsz, wartość liczbowa, odpowiedź tekstowa, itp.
	System udostępnia narzędzia monitorowania i oceniania aktywności uczestników kursów z możliwością przypisywania oceny do zadań wykonanych przez kursantów.
	System posiada mechanizm dziennika zawierającego wyniki przeprowadzanych testów/sprawdzianów.
Zarządzanie szkoleniami	System posiada interfejs oraz mechanizm pomocy kontekstowej w języku polskim.
	System musi zapewniać nieograniczoną liczbę użytkowników
	System musi zapewniać moduł raportowania.
	System musi zapewniać współpracę z bazami danych.
	System musi zapewniać zarządzanie programami i planowaniem szkoleń.
	System musi zapewniać zarządzanie profilami/kontami użytkowników.
	System musi zapewniać przypisywanie użytkownikom globalnie (w obrębie całego systemu) określonych ról (np. edytor, autor, administrator, itd.) lub lokalnie (w ramach pojedynczego kursu) wskazywanie uczestników kursu.
	System musi zapewniać harmonogram kursu.
	System musi zapewniać mechanizm administracji szkoleniami i kursantami.
	System musi zapewniać mechanizm generowania zadań, pytań testowych i zarządzania testami.
	System musi zapewniać interfejs w języku polskim.
Tworzenie kursów	System musi zapewniać mechanizm pomocy kontekstowej w języku polskim.
	System musi zapewniać dokumentację w języku polskim.
	System musi zapewniać tworzenie scenariuszy lekcji.
	System musi zapewniać możliwość umieszczania na stronach różnego rodzaju interakcji.
	System musi zapewniać możliwość tworzenia kursów on-line.
	System musi zapewniać tworzenie testów.
	System musi zapewniać zarządzanie zawartością szkoleń.
	System musi zapewniać mechanizm generowania zadań, pytań testowych i zarządzania testami.

	System musi zapewniać możliwość eksportu do LMS.
	System musi zapewniać możliwość edycji wyglądu kursów.
	System musi zapewniać interfejs w języku polskim.
	System musi zapewniać mechanizm pomocy kontekstowej w języku polskim.
	System musi zapewniać dokumentację w języku polskim.
Egzaminy	System musi umożliwić tworzenie egzaminów z kursu
	System musi umożliwić dodanie więcej niż jednego egzaminu do kursu.
	Tworzenie pytań do egzaminów powinno być możliwe do wykonania z dwóch miejsc: - z panelu administracyjnego - z poziomu danego egzaminu. Przy czym wszystkie pytania utworzone z poziomu egzaminu również trafiają na listę wszystkich pytań.
	Tworzenie pytania powinno polegać na określeniu: - treści pytania - dodatkowego opisu - typu pytania - prawidłowej odpowiedzi - treści widomości dla poprawnej odpowiedzi - treści widomości dla niepoprawnej odpowiedzi - ilość punktów za prawidłową odpowiedź - wskazówki do odpowiedzi
	System musi umożliwić korzystanie przynajmniej z poniższych typów pytań: - Jednokrotny wybór - jedna prawidłowa odpowiedź - Wielokrotny wybór - wiele prawidłowych odpowiedzi - Pytanie otwarte - należy wpisać odpowiedź - Sortowanie - ułożenie obiektów w prawidłowej kolejności - Sortowanie w macierzy - dopasowywanie elementów do siebie w tabeli dwuwymiarowej - Wypełnij puste miejsce - wypełnienie pustego miejsca znakiem, liczbą lub tekstem

	- Ocena - wskazanie wartości - Esej / Otwarta odpowiedź - dłuższa wypowiedź pisemna
	W przypadku pytania: - Wielokrotny wybór - Pytanie otwarte - Sortowanie - Sortowanie w macierzy - Wypełnij puste miejsce w systemie musi istnieć możliwość określenia przyznanych punktów za każdą odpowiedź.
	W przypadku pytania typu "Esej/Otwarta odpowiedź" musi istnieć możliwość wpisania odpowiedzi bezpośrednio w systemie oraz załączenia pliku.
	System musi umożliwić przypisanie każdego pytania do jednego testu.
	System musi umożliwić zapis każdego pytania jako szkic lub opublikować.
	System musi umożliwić usunięcie każdego pytania lub przeniesienie do kosza oraz opublikowanie w dowolnym momencie.
	System musi umożliwić eksport egzaminów do pliku xml
	System musi umożliwić tworzenie nowego egzaminu poprzez: - manualne wprowadzenie - sklonowanie egzaminu który już istnieje w systemie - import z pliku xml
	W przypadku tworzenie egzaminu manualnie należy wpisać tytuł strony, dodać treść (opcjonalnie) oraz wskazać pytania do egzaminu.
	Wskazanie pytań do egzaminu musi odbywać się poprzez wskazanie pytań z repozytorium lub poprzez utworzenie ich z poziomu budowania testu.
	System musi umożliwić przypisanie egzaminu do kursu
	System musi umożliwić przypisanie egzaminu do konkretnej lekcji kursu
	System musi umożliwić określenie od kiedy egzamin jest dostępny dla użytkowników: - natychmiast - test jest dostępny od momentu zapisania się na kurs

	- na podstawie daty zapisu - test dostępny X dni po zapisaniu się na kurs - konkretna data - test dostępny w konkretnym dniu, od określonej godziny
	System musi umożliwić określenie czy wzięcie udziału w egzaminie wymaga ukończenia wcześniej innego egzaminu. Jeśli tak, należy wskazać jakie konkretnie egzaminy musi zdać użytkownik aby móc przystąpić do tego.
	System musi umożliwić określenie procentowej ilość punktów niezbędną do zdania egzaminu.
	System musi umożliwić wskazanie szablonu dla wydawanego certyfikatu po zdanym egzaminie.
	W systemie musi istnieć możliwość uruchomienia zapisywania egzaminu na serwerze
	W systemie musi istnieć możliwość ograniczenia ilości podejść do egzaminu
	Musi istnieć możliwość wymuszenia uzupełnienia wszystkich pytań w celu zakończenia egzaminu
	Musi istnieć możliwość określenia limitu czasu na przesłanie egzaminu
	Musi istnieć możliwość dodania materiałów dotyczących egzaminu (np. Materiałów edukacyjnych).
	Musi istnieć możliwość uruchomienia egzaminu automatycznie lub po wybraniu startu przez egzaminowanego.
	Musi istnieć możliwość przeglądu tabeli wszystkich pytań z możliwością podglądu podsumowania oraz pominięciem pytania
	Musi istnieć możliwość ustawienia losowej kolejności pytań dla każdego użytkownika
	Musi istnieć możliwość określenia kilku wiadomości na zakończenie egzaminu (w zależności od osiągniętej ilości punktów).
	Musi istnieć możliwość wyświetlenia użytkownikowi ilości zdobytych punktów oraz czasu poświęconego na egzamin.
	System musi wysyłać powiadomienia do użytkownika o odbytym egzaminie
	System musi wysyłać powiadomienia administratorowi o użytkownikach którzy odbyli egzamin

	Musi istnieć możliwość ograniczenia czasu trwania egzaminu. W przypadku przekroczenia czasu przez użytkownika egzaminu zostaje zakończony administracyjnie.
	System musi umożliwiać tworzenie certyfikatów ukończenia egzaminu
	Tworzenie certyfikatu musi się odbywać za pomocą edytora blokowego.
	System musi umożliwić użycie jednego certyfikatu do wielu egzaminów oraz tworzenie certyfikatów dla każdego egzaminu osobno.
	System musi umożliwić przeglądanie statystyk egzaminu.
	Statystyka z egzaminu musi zawierać przynajmniej informacje: - użytkownik egzaminowany - liczba punktów - ilość poprawnych odpowiedzi - ilość niepoprawnych odpowiedzi - ilość użytych wskazówek - czas poświęcony na egzamin - wynik egzaminu
	System musi umożliwić eksport pełnych statystyk z systemu do pliku CSV

System wirtualizacyjny

Cecha	**Wymagania minimalne**
Ogólne	Oprogramowanie musi wspierać zarządzanie wirtualizację w zakresie maszyn wirtualnych oraz konteneryzacji.
	Oprogramowanie musi zarządzać przestrzenią pamięci masowej (storage) oraz wirtualnymi sieciami.
	Wymagane jest wsparcie dla pełnej wirtualizacji za pomocą KVM, umożliwiające tworzenie i zarządzanie wirtualnymi maszynami (VM) z różnymi systemami operacyjnymi.

	Wymagane jest wsparcie dla kontenerów Linux (LXC), pozwalające na uruchamianie izolowanych środowisk aplikacyjnych
Interfejs użytkownika	Platforma musi oferować webowy interfejs użytkownika (UI), który pozwala na zarządzanie wirtualizacją, storage i sieciami w łatwy i intuicyjny sposób za pomocą przeglądarki internetowej.
	Interfejs użytkownika musi zapewniać dostęp do konsoli każdej wirtualnej maszyny i kontenera bezpośrednio z poziomu przeglądarki.
Zarządzanie zasobami	System musi pozwalać na dynamiczne przydzielanie zasobów (CPU, RAM, dysk) wirtualnym maszynom i kontenerom.
	Wymagane jest wsparcie dla różnych typów storage, takich jak NFS, iSCSI, Ceph, ZFS, oraz możliwość ich łatwej integracji i zarządzania.
Wysoka dostępność i klastrowanie	Oprogramowanie musi umożliwiać konfigurację wielu serwerów w klaster, pozwalając na centralne zarządzanie.
	Wymagane jest wsparcie dla konfiguracji wysokiej dostępności, umożliwiającej automatyczne przenoszenie wirtualnych maszyn na inne węzły w przypadku awarii.
Zarządzanie siecią	Oprogramowanie musi umożliwiać tworzenie i zarządzanie wirtualnymi sieciami (VLAN, bridges) dla wirtualnych maszyn i kontenerów.
	Wymagane jest wsparcie dla sieci definiowanych programowo (SDN) w celu bardziej elastycznego zarządzania ruchem sieciowym.
Bezpieczeństwo	Oprogramowanie musi umożliwiać skonfigurowanie uwierzytelniania wielopoziomowego dla zwiększenia bezpieczeństwa dostępu.

	Wymagana jest możliwość izolacji zasobów na poziomie sieci i storage, co zapewnia bezpieczeństwo danych i komunikacji między wirtualnymi maszynami.
Kopie zapasowe	Oprogramowanie musi wspierać automatyczne tworzenie kopii zapasowych wirtualnych maszyn i kontenerów z możliwością planowania zadań backupowych.
	Wymagana jest możliwość tworzenia przyrostowych kopii zapasowych w celu oszczędności miejsca i zwiększenia efektywności backupu.
Monitorowanie	Oprogramowanie musi oferować zintegrowane narzędzia do monitorowania zasobów, takich jak CPU, RAM, storage, i sieć, z opcją generowania raportów i alertów.
	Wymagane jest prowadzenie szczegółowego logowania zdarzeń oraz dostęp do narzędzi analitycznych dla lepszego zarządzania i diagnozowania problemów.
	Oprogramowanie musi współpracować z oprogramowaniem monitoringu oraz systemem SIEM, wdrażanymi w ramach realizacji Przedmiotu Zamówienia.
Integracja	Platforma musi oferować REST API, umożliwiające automatyzację zadań administracyjnych oraz integrację z zewnętrznymi systemami.
	Wymagane jest wsparcie dla integracji z chmurą publiczną, pozwalające na tworzenie hybrydowych środowisk IT.

Oprogramowanie kopii zapasowych

Cecha	Wymagania minimalne
Ogólne	Oprogramowanie musi umożliwiać tworzenia kopii zapasowych i przywracania danych i być ściśle zoptymalizowane z oprogramowaniem do wirtualizacji, wdrażanym w ramach realizacji Przedmiotu Zamówienia.
	System musi umożliwiać tworzenie kopii zapasowych wirtualnych maszyn (VM) oraz kontenerów LXC zarządzanych przez oprogramowanie do wirtualizacji z wykorzystaniem deduplikacji danych na poziomie bloku.
	Musi być dostępna funkcjonalność tworzenia przyrostowych kopii zapasowych, które zapisują jedynie zmiany od ostatniego backupu, co zmniejsza zapotrzebowanie na przestrzeń dyskową i przyspiesza proces tworzenia kopii.
Deduplikacja i kompresja danych	System musi wspierać deduplikację blokową, która identyfikuje i eliminuje duplikaty danych na poziomie bloków, co znacząco redukuje ilość miejsca potrzebnego na przechowywanie kopii zapasowych.
	Musi być dostępna funkcja kompresji danych, która dodatkowo zmniejsza ilość miejsca zajmowanego przez kopie zapasowe.
Weryfikacji integralności danych	System musi posiadać mechanizm automatycznej weryfikacji integralności przechowywanych danych, aby zapewnić, że kopie zapasowe są wolne od błędów i mogą być przywrócone w razie potrzeby.
	Wymagane jest wsparcie dla hashowania danych przy każdej operacji zapisu i weryfikacji, co zapewnia spójność i niezawodność przechowywanych kopii zapasowych.

Zarządzanie politykami backupu	System musi pozwalać na tworzenie elastycznych harmonogramów dla zadań backupowych, w tym pełnych i przyrostowych kopii zapasowych, z możliwością zdefiniowania częstotliwości i czasu wykonywania kopii.
	Musi być dostępna funkcjonalność zarządzania retencją kopii zapasowych, umożliwiająca automatyczne usuwanie starych lub zbędnych kopii zapasowych na podstawie zdefiniowanych reguł.
Szyfrowanie i wersjonowanie kopii zapasowych	System musi wspierać szyfrowanie kopii zapasowych zarówno podczas tworzenia, jak i przechowywania, aby zapewnić bezpieczeństwo danych, szczególnie w środowiskach o wysokich wymaganiach dotyczących ochrony danych.
	Wymagane jest szyfrowanie transmisji danych podczas przesyłania kopii zapasowych do serwera backupu, aby zabezpieczyć je przed nieautoryzowanym dostępem.
	System musi umożliwiać przechowywanie wielu wersji kopii zapasowych, co pozwala na przywrócenie danych do konkretnego punktu w czasie w przypadku błędów lub innych problemów.
Przywracanie danych	System musi umożliwiać szybkie przywracanie pojedynczych plików lub katalogów bez konieczności przywracania całej maszyny wirtualnej lub kontenera.
	Musi być dostępna funkcjonalność szybkiego przywracania całych maszyn wirtualnych lub kontenerów do określonego stanu z kopii zapasowej.
Obsługa zdalnego backupu	System musi umożliwiać tworzenie kopii zapasowych w zdalnych lokalizacjach, co zwiększa odporność na awarie lokalnej infrastruktury.

	Musi być dostępna możliwość replikacji kopii zapasowych między różnymi serwerami Proxmox Backup Server, aby zapewnić dodatkową redundancję i odporność na awarie.
Monitorowanie	System musi oferować funkcje monitorowania statusu kopii zapasowych, w tym informacje o powodzeniu, błędach i wydajności zadań backupowych.
	Musi być dostępna funkcjonalność powiadamiania administratorów o statusie zadań backupowych oraz o wszelkich problemach za pomocą e-maili lub innych metod.
Interfejs użytkownika	System musi oferować łatwy w użyciu webowy interfejs użytkownika, który umożliwia zarządzanie wszystkimi funkcjami backupu, w tym planowaniem, przywracaniem i monitorowaniem.
	Wymagane jest wsparcie dla API REST, które umożliwia integrację z zewnętrznymi narzędziami i automatyzację procesów backupowych oraz przywracania danych.
Wsparcie dla urządzeń i systemów	System musi wspierać różne systemy plików i urządzenia storage, takie jak ZFS, ext4, XFS, NFS, iSCSI, co zapewnia elastyczność w implementacji.
	Musi być możliwość efektywnego zarządzania i przechowywania dużych wolumenów danych.

Konfiguracja i uruchomienie sprzętu oraz oprogramowania sprzętowego

Konfiguracja dostarczonego sprzętu musi być wykonana na podstawie projektu wykonawczego, opracowanego przez Wykonawcę i zatwierdzonego przez Zamawiającego. Projekt musi być opracowany na podstawie wizji lokalnej i szczegółowych wytycznych Zamawiającego. Przed opracowaniem projektu Zamawiający oczekuje szkolenia wstępnego dotyczącego możliwości konfiguracji sprzętu.

W ramach instalacji deduplikatora danych Wykonawca jest zobowiązany opracować i wdrożyć politykę backupu i retencji danych oraz szczegółowo przeanalizować możliwości techniczne wykonania kopii i jej odtworzenia dla wszystkich maszyn wirtualnych oraz systemów i aplikacji wykorzystywanych przez Zamawiającego.

Wdrożenie i konfiguracja elementów bezpieczeństwa

System SIEM

Wdrożenie oprogramowania SIEM zgodnie z założeniami projektowymi, co najmniej w zakresie:

1. Instalacja oprogramowania SIEM.
2. Integracja z systemem centralnego zarządzania tożsamością.
3. Integracja z oprogramowaniem do zarządzania incydentami.
4. Przygotowanie instrukcji instalacji agentów system SIEM oraz wsparcie przy instalacji pierwszego agenta dla każdego typu wspieranego systemu operacyjnego.
5. Przygotowanie obsługi do 5 niestandardowych źródeł logów (dekodery i reguły).
6. Określenie technik i taktyk ataku zgodnie z MITRE ATT&CK dla wszystkich niestandardowych reguł, które będą tego wymagały.
7. Określenie priorytetów alarmów w celu ograniczenia „szumu informacyjnego” i eskalacji istotnych alertów.
8. Konfiguracja mechanizmów agenta SIEM do czasowego blokowania źródłowych adresów IP wykonujących brute force.
9. Konfiguracja do 2 kokpitów.
10. Konfiguracja powiadomień mailowych.
11. Opracowanie dokumentacji powykonawczej z uwzględnieniem procedur administracyjnych.

Platforma szkoleniowa

W ramach realizacji PZ Wykonawca jest zobowiązany do opracowania i wdrożenia w postaci kursu LMS materiałów szkoleniowych dla pracowników Zamawiającego. Zamawiający planuje wykorzystać system LMS do realizacji wstępnych oraz okresowych szkoleń dla swoich pracowników z tematyki cyberbezpieczeństwa. Zakres wdrożonego kursy musi być tożsamy z wymaganiami dotyczącymi szkoleń dla pracowników nie będących informatykami. Dodatkowo Wykonawca jest zobowiązany przygotować testy wiedzy oraz wdrożyć opcjonalny mechanizm testów w ramach LMS.

Zamawiający oczekuje, aby każdy pracownik, korzystając z Centralnego Systemy Zarządzania Tożsamością, zalogował się w systemie, zrealizował kurs i opcjonalnie zdał egzamin. System musi generować każdorazowo powiadomienia o realizacji kursu przez pracownika i umożliwiać wygenerowanie list zbiorczych.

Wsparcie eksperckie w zakresie cyberbezpieczeństwa

Zamawiający wymaga, aby Wykonawca w ramach oferty zapewnił wsparcie techniczne w ramach drugiej i trzeciej linii wsparcia z zakresu cyberbezpieczeństwa dla wdrażanych i posiadanych przez Zamawiającego rozwiązań IT. Wsparcie techniczne ma być realizowane w ciągu 24 miesięcy od podpisania końcowego protokołu odbioru. Zamawiający wymaga dostępności inżynierów drugiej linii wsparcia w modelu 5x8, w godzinach pracy Urzędu. Zakres wsparcia zawiera:

- Analiza i eskalacja incydentów:
  - Przejęcia incydentów od pierwszej linii wsparcia w celu przeprowadzenia analizy technicznej,
  - Ocena i klasyfikacja incydentów, określenie ich wpływu na organizację oraz priorytetyzacja działań naprawczych,
  - Eskalacja incydentów do CSIRT NASK.
- Zaawansowana analiza techniczna:
  - Analiza logów i śledzenie incydentów z wykorzystaniem narzędzi wdrażanego systemu SIEM,
  - Analiza artefaktów,
  - Odtwarzanie zdarzeń.
- Reakcja na incydenty i wdrażanie środków zaradczych:
  - Izolacja zagrożonych systemów,
  - Usuwanie zagrożeń,
  - Monitorowanie i weryfikacja po wdrożeniu środków zaradczych.
- Zarządzanie podatnościami oraz łatkami:
  - Regularne przeglądanie wyników skanów podatności,
  - Testowanie i wdrażanie poprawek oraz rekomendacja ich wdrożenia.
- Szkolenie i mentoring:
  - Prowadzenie szkoleń i sesji mentoringowych z pracownikami pierwszej linii wsparcia na żądanie Zamawiającego.

- Wsparcie merytoryczne i techniczne w zakresie posiadanych przez Zamawiającego systemów bezpieczeństwa teleinformatycznego.
- Doradztwo w zakresie konfiguracji, rozbudowy lub dodatkowych zakupów elementów systemu bezpieczeństwa teleinformatycznego.

Przygotowanie oraz przeprowadzenie szkoleń

W ramach realizacji PZ Wykonawca jest zobowiązany do przeprowadzenia szkoleń dotyczących tematyki cyberbezpieczeństwa dla wszystkich pracowników Zamawiającego oraz podmiotów zależnych – w sumie 61 pracowników. Zamawiający oczekuje realizacji szkoleń w swojej siedzibie, szkolenia muszą być przeprowadzone niezależnie dla:

1. Pracowników nie będących informatykami – 4 grupy po 20 osób, czas trwania szkolenia co najmniej 8 godzin zegarowych.
2. Administratorów – 1 grupa 10-osobowa, czas trwania szkolenia co najmniej 16 godzin zegarowych.

Zamawiający przed przeprowadzeniem szkolenia musi otrzymać do akceptacji szczegółowy plan szkolenia, harmonogram z podziałem na grupy oraz CV osoby, która będzie prowadzić szkolenie. Zamawiający zastrzega sobie prawo odrzucenia propozycji szkolenia w przypadku zastrzeżeń do kompetencji i doświadczenia trenera, w takim przypadku Wykonawca będzie musiał przedstawić inną osobę.

Zamawiający wymaga przedstawienia szczegółowej agendy dla szkoleń, która musi spełniać minimalny zakres, odpowiednio:

1. Szkolenie dla pracowników:
    a. Informacje poufne i RODO (hasła, RODO, adresy wysyłka maili, numery telefonów, adresy fizyczne, dane biometryczne),
    b. Przetwarzania danych mieszkańca oraz dane poufne (triada CIA, polityka zero-trust, szyfrowanie dokumentów oraz nośników danych, przechowywanie dokumentów, utylizacja nośników, drukowanie dokumentów, usługi online)
    c. Zagrożenia (blokowanie ekranu, socjotechniki, nieuprawniony dostęp do pomieszczeń, ransomware, kody QR, niebezpieczne nośniki danych)
    d. Zabezpieczenia techniczne (zabezpieczenie pomieszczeń, VPN, menadżer haseł, przekazywanie szyfrowanych dokumentów, kopie zapasowe, aktualizacje, weryfikacja dwuetapowa, bezpieczne hasła)
    e. Higiena pracy (zasady korzystania ze służbowego sprzętu, podejrzane maile, czyste biurko, sieć firmowa, reklamy)

   f. Podejrzane wydarzenia i reagowania (podejrzane pliki, podejrzane zachowania, zgłaszanie incydentów)

2. Szkolenia dla administratorów
   a. Bezpieczeństwo sieci (protokoły komunikacyjne, VLAN, fizyczna separacja sieci, UTM, tworzenie ACL, IDS/IPS, skanowanie sieci, bezpieczeństwo WiFI, ARP Spoofing, DHCP Spoofing, konfiguracja SIEM)
   b. Utwardzanie stacji roboczych (utwardzanie Windows, MacOS, Linux, szyfrowanie dysków, polityka aktualizacji, konfiguracja agentów SIEM)
   c. Monitoring i zarządzania stacjami roboczymi (ruch sieciowy, logi, snmp, konfiguracja systemu ciągłego monitoringu, konfiguracja agentów SIEM, bezpieczny dostęp zdalny do stacji)
   d. Bezpieczeństwo poczty elektronicznej (phishing, szyfrowanej poczty PGP oraz X.509, SPF, DKIM, DMARC)
   e. Kopie zapasowe (polityka kopii zapasowych, przechowywanie, wykorzystanie deduplikacji w celu ochrony przed ransnomware, retencja i utylizacja kopii)
   f. Cyfrowy Usługi Zaufania (podpisy elektroniczne, e-dowód, mObywatel, portfele tożsamości, e-doręczenia).

Dodatkowo, Zamawiający wymaga przygotowanie i przeprowadzenia szkoleń dla administratorów dla dostarczanego sprzętu oraz oprogramowania specjalistycznego. Szczegółowa agenda szkoleń oraz czas ich trwania będzie ustalony na etapie wdrożenia i musi być zgodny z zaleceniami producenta.

Przeprowadzenie audytu bezpieczeństwa

W ramach realizacji PZ Zamawiający oczekuje realizacji dwóch audytów bezpieczeństwa:

1. Wstępnego – według harmonogramu,
2. Powdrożeniowego – według harmonogramu.

Audyt bezpieczeństwa musi każdorazowo obejmować zakres:

1. Polityka i Procedury Bezpieczeństwa
    a. Stosowanie polityki bezpieczeństwa informacji
    b. Przegląd dokumentacji procedur bezpieczeństwa informacji i ich realizacji w praktyce
2. Zarządzanie Ryzykiem i Bezpieczeństwem
    a. Ocena procesów identyfikacji, oceny i zarządzania ryzykiem
    b. Analiza skuteczność podejmowanych działań zapobiegawczych i kontroli ryzyka
3. Zarządzanie Zabezpieczeniem Aktywów
    a. Ocena klasyfikacji aktywów informacyjnych oraz skuteczności ich ochrony
    b. Przegląd procedur związanych z identyfikacją i zabezpieczaniem aktywów
4. Bezpieczne Zarządzanie Dostępem
    a. Sprawdzenie mechanizmów kontroli dostępu do systemów i danych
    b. Ocena skuteczności systemów uwierzytelniania i autoryzacji
5. Kryptografia
    a. Analiza zastosowania kryptografii do ochrony poufności i integralności danych
    b. Ocena zgodności z wymaganiami dotyczącymi stosowania kryptografii
6. Bezpieczeństwo Fizyczne i Środowiskowe
    a. Ocena zabezpieczeń infrastruktury fizycznej i działań zapobiegawczych przeciwko awariom i katastrofom
    b. Przegląd procedur związanych z zapewnieniem bezpieczeństwa środowiskowego
7. Bezpieczeństwo Personelu
    a. Przegląd procesów selekcji, szkolenia i monitorowania personelu pod kątem bezpieczeństwa informacji
    b. Ocena świadomości pracowników na temat polityki bezpieczeństwa informacji

8. Bezpieczne Operacje
    a. Ocena stosowania procedur dotyczących bezpiecznej eksploatacji systemów i usług
    b. Sprawdzenie zgodności z wymaganiami dotyczącymi bezpiecznych operacji
9. Zarządzanie Incydentami Bezpieczeństwa Informacji
    a. Sprawdzenie procedur reagowania na incydenty bezpieczeństwa informacji
    b. Analiza skuteczności działań podejmowanych w przypadku incydentów
10. Monitorowanie, Przeglądy i Audyty
    a. Ocena systemu monitorowania skuteczności zarządzania bezpieczeństwem informacji
    b. Przegląd przeprowadzonych audytów i ich wyników
11. Ciągłe Doskonalenie
    a. Analiza procesów ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji
    b. Ocena działań podejmowanych w celu identyfikacji i eliminacji słabych punktów

Aktualizacja Systemu Zarządzania Bezpieczeństwem Informacji

W ramach realizacji przedmiotu zamówienia Wykonawca musi opracować na podstawie danych od Zamawiającego następujące dokumenty będące podstawą SZBI:

1. Deklaracja najwyższego kierownictwa
2. Polityka Bezpieczeństwa Informacji
3. Procedura zarządzania ciągłością działania
4. Procedura zarządzania incydentami
5. Procedura bezpieczeństwa fizycznego
6. Procedura bezpieczeństwa teleinformatycznego
7. Procedura zarządzania uprawnieniami
8. Procedura zarządzania ryzykiem
9. Procedura realizacji działań naprawczych
10. Procedura klasyfikacji informacji
11. Procedura audytów wewnętrznych
12. Procedura bezpieczeństwa dostępu zdalnego

Dokumenty muszą być opracowane we współpracy z Zamawiającym, z uwzględnieniem otrzymanych od Zamawiającego wytycznych oraz wzorców, wytycznych audytu bezpieczeństwa i zostać zatwierdzone ostatecznie przez Zamawiającego.

Opracowana dokumentacja musi uwzględniać techniczne wytyczne, specyfikę wdrażanego sprzętu i oprogramowania oraz ewentualne ograniczenia. Zamawiający oczekuje otrzymania dokumentów, których stosowanie będzie możliwe wprost przy udziale wdrażanego w ramach PZ systemów. Spójność opracowanej dokumentacji i możliwości realizacji zapisanych w niej postanowień będzie przedmiotem badania audytu powdrożeniowego.