BIT.271.1.7.2025 *Załącznik nr 10 do SWZ*

Wykaz oferowanych urządzeń

Zakup sprzętu informatycznego i urządzeń bezpieczeństwa wraz z licencjami, dostawą i montażem, w ramach projektu „Cyberbezpieczny Urząd”

Wykonawca:

.....

(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)

1. Serwer – 1sztuka

Lp.	Nazwa komponentu	Oferowane parametry (podpowiedzi dla oferenta)
1.	Typ	Podaj, czy serwer jest typu Rack i czy spełnia wymagania dotyczące zabudowy w szafie RACK.
2.	Płyta główna	Podaj, czy płyta główna pozwala na instalację co najmniej jednego fizycznego procesora i czy ma minimum 6 slotów na pamięć. Czy obsługuje wymagane zabezpieczenia pamięci (ECC, SDDC, Memory Mirroring, SBEC)?
3.	Procesor	Podaj model procesora, liczbę rdzeni, wynik w teście SPECint_rate_base2017 oraz potwierdzenie, że procesor jest zgodny z wymaganiami Zamawiającego.
4.	Pamięć operacyjna	Podaj ilość pamięci RAM (w GB) oraz typ modułów (dwu- lub czterobankowe).
5.	Sloty PCI Express/Porty	Podaj liczbę i typ slotów PCIe (w tym liczbę slotów x16 generacji 5), liczbę portów USB (w tym liczbę portów 3.0), liczbę portów RS-232 oraz obecność portu video.
6.	Wewnętrzna Pamięć masowa	Podaj liczbę i pojemność zainstalowanych dysków NVMe (w TB), liczbę i pojemność dysków bootowalnych (w GB), oraz informację o konfiguracji RAID.

Lp.	Nazwa komponentu	Oferowane parametry (podpowiedzi dla oferenta)
7.	Kontroler Dysków	Podaj, czy zainstalowano sprzętowy kontroler dyskowy i czy obsługuje konfiguracje RAID 5.
8.	Grafika	Podaj, czy karta graficzna jest zintegrowana i czy obsługuje rozdzielczość minimum 1280x1024 pikseli.
9.	Interfejsy sieciowe	Podaj liczbę i przepustowość interfejsów sieciowych (w Gb/s), oraz informację o obecności dwuportowej karty sieciowej 10Gb/s.
10.	Obudowa	Podaj, czy obudowa jest typu Rack, jej wysokość (w U), oraz czy zawiera komplet szyn montażowych i organizator kabli.
11.	Zasilacze i Wentylatory	Podaj moc zainstalowanych zasilaczy (w W), czy pracują w trybie redundancji Hot-Plug, oraz liczbę wentylatorów i ich tryb pracy.
12.	Bezpieczeństwo i system diagnostyczny	Podaj, czy obecny jest panel informacyjny na froncie obudowy, oznaczenie fabryczne, moduł TPM, czujnik otwarcia obudowy.
13.	Karta zarządzająca	Podaj, czy karta zarządzająca jest niezależna od systemu operacyjnego, jakie protokoły obsługuje (IPMI 2.0, SNMP, VLAN tagging), oraz jakie ma dodatkowe funkcje (np. wirtualna konsola, integracja z Active Directory).

Lp.	Nazwa komponentu	Oferowane parametry (podpowiedzi dla oferenta)
14.	Certyfikaty i dokumenty	Podaj, czy posiadasz certyfikat PN-EN ISO 9001 lub równoważny, deklarację zgodności UE lub równoważną, oraz wyniki testu procesora.
15.	Dokumentacja	Podaj, czy dostarczana jest dokumentacja w języku polskim lub angielskim, oraz czy dostępny jest nośnik ze sterownikami lub link do strony producenta.
16.	Warunki gwarancji	Podaj czas trwania gwarancji (w latach), czas reakcji na zgłoszenie (w godzinach), oraz dostępność wsparcia technicznego (w godzinach i dniach).

2. Przełącznik sieciowy 24 Porty SFP – 2 sztuki

Lp.	Nazwa komponentu	Oferowane parametry (podpowiedzi dla oferenta)
1.	Parametry fizyczne	Podaj wymiary urządzenia (szerokość, wysokość w jednostkach U), czy jest zgodne z montażem w szafie rack 19", czy posiada zasilanie redundantne 230V, maksymalny pobór mocy (w W), oraz średni czas bezawaryjnej pracy MTBF (w latach).

Lp.	Nazwa komponentu	Oferowane parametry (podpowiedzi dla oferenta)
2.	Interfejsy sieciowe	Podaj liczbę portów GE RJ45 SFP (w tym typ wkładek, np. 1GE SFP+ long range), liczbę portów 10GE SFP+ (w tym typ wkładek, np. 10GE SFP+ short range).
3.	Zarządzanie	Podaj, czy dostępny jest dedykowany interfejs do zarządzania, port konsoli szeregowej, czy obsługuje zarządzanie przez SSH i graficzny interfejs webowy. Czy istnieje możliwość zarządzania przez kontroler przełączników, automatycznej konfiguracji Spanning Tree, tagowania 802.1q, aktualizacji oprogramowania, oraz sprawdzenia informacji o urządzeniach na wybranym porcie?
4.	Parametry wydajnościowe	Podaj przepustowość urządzenia (w Gbps), liczbę pakietów na sekundę (Mpps), maksymalną liczbę adresów MAC, opóźnienie (w mikrosekundach), rozmiar bufora pakietów (w MB), rozmiar pamięci DRAM (w GB) i FLASH (w MB).
5.	Wymagane funkcje	Podaj, czy obsługuje automatyczną negocjację prędkości i duplexu, protokoły Spanning Tree (802.1d, 802.1w, 802.1s), agregację portów (802.3ad), liczbę obsługiwanych VLANów (802.1Q), routing statyczny i dynamiczny (OSPFv2, RIPv2), funkcje DHCP Relay, DHCP Snooping, Dynamic ARP Inspection, IGMP Snooping, port-mirroring, sFlow, listy kontrolne ACL, MCLAG, kontrolę dostępu 802.1x, zarządzanie Telnet/SSH, HTTP/HTTPS, SNTP, LLDP, SNMP, integrację z NGFW, Captive Portal, białe i czarne listy MAC, stateful firewall, routing statyczny i dynamiczny (co najmniej OSPF).
6.	Gwarancja oraz wsparcie	Podaj czas trwania gwarancji (w latach), czas trwania wsparcia serwisowego (w latach), oraz czy serwis jest realizowany na terenie Polski.

Lp.	Nazwa komponentu	Oferowane parametry (podpowiedzi dla oferenta)
7.	Dodatkowe wymagania	Podaj, czy dostawca posiada dokument potwierdzający zgodność z przepisami dotyczącymi produktów podwójnego zastosowania, oraz czy posiada certyfikowany system zarządzania jakością.

3. Urządzenie bezpieczeństwa sieciowego – 2 sztuki połączone w klaster

Lp.	Nazwa komponentu	Oferowane parametry (podpowiedzi dla oferenta)
1.	Typ	Podaj, czy urządzenie jest typu Firewall i czy jest przeznaczone do zabudowy w szafie RACK.
2.	Redundancja, monitoring i wykrywanie awarii	Podaj, czy urządzenie obsługuje tryby pracy Active-Active lub Active-Passive, synchronizację sesji firewall, monitoring sprzętu, oprogramowania i łączy sieciowych, oraz monitorowanie stanu połączeń VPN.
3.	Interfejsy	Podaj liczbę portów Gigabit Ethernet RJ-45, gniazd SFP 1 Gbps, gniazd SFP+ 10 Gbps, obecność portu konsoli szeregowej oraz gniazda USB.

Lp.	Nazwa komponentu	Oferowane parametry (podpowiedzi dla oferenta)
4.	Parametry wydajnościowe	Podaj liczbę obsługiwanych jednoczesnych połączeń (w milionach), liczbę nowych połączeń na sekundę (w tysiącach), przepustowość Stateful Firewall (w Gbps), przepustowość Firewall z włączoną funkcją Kontroli Aplikacji (w Gbps), wydajność szyfrowania IPSec VPN (w Gbps), wydajność skanowania ruchu dla IPS (w Gbps), wydajność skanowania ruchu z włączonymi funkcjami IPS, Application Control, Antywirus (w Gbps), oraz wydajność inspekcji komunikacji szyfrowanej SSL dla ruchu http (w Gbps).
5.	Funkcje systemu bezpieczeństwa	Podaj, czy urządzenie obsługuje kontrolę dostępu, kontrolę aplikacji, szyfrowanie IPSec VPN i SSL VPN, ochronę przed malware, ochronę przed atakami (IPS), kontrolę stron WWW, kontrolę zawartości poczty (Antyspam), zarządzanie pasmem (QoS, Traffic shaping), mechanizmy DLP, uwierzytelnianie dwuskładnikowe, analizę ruchu szyfrowanego SSL, lokalny serwer DNS z obsługą DoT i DoH, oraz filtrowanie zapytań DNS.
6.	Polityki - Firewall	Podaj, czy polityka Firewall uwzględnia adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje, reakcje zabezpieczeń, rejestrowanie zdarzeń, translację adresów NAT, translację PAT, dedykowany ALG dla protokołu SIP, tworzenie stref bezpieczeństwa, integrację z rozwiązaniami SDN (AWS, Azure, GCP, OpenStack, VMware NSX).
7.	Połączenia VPN	Podaj, czy urządzenie obsługuje konfigurację połączeń IPSec VPN i SSL VPN, wsparcie dla IKE v1 i v2, szyfrowanie AES 128/256 bitów, obsługę protokołu Diffie-Hellman grup 19 i 20, topologie Hub and Spoke oraz Mesh, tworzenie połączeń Site-to-Site i Client-to-Site, monitorowanie tuneli VPN, mechanizmy IPSec NAT Traversal, DPD, Xauth, oraz funkcję „Split tunneling” dla połączeń Client-to-Site.

Lp.	Nazwa komponentu	Oferowane parametry (podpowiedzi dla oferenta)
8.	Routing i obsługa połączeń WAN oraz zarządzanie pasmem	Podaj, czy urządzenie obsługuje routing statyczny, Policy Based Routing, dynamiczny routing (RIPv2, OSPF, BGP, PIM), równoważenie obciążenia łączy WAN, reguły SD-WAN, zarządzanie pasmem (maksymalna, gwarantowana ilość pasma, oznaczanie DSCP, priorytet ruchu), oraz zarządzanie pasmem dla wybranych kategorii URL.
9.	Ochrona przed atakami i wirusami	Podaj, czy urządzenie obsługuje analizę sygnaturową i analizę anomalii w protokołach sieciowych, ochronę przed atakami na aplikacje na niestandardowych portach, automatyczne aktualizacje bazy sygnatur, definiowanie wyjątków i własnych sygnatur, wykrywanie anomalii protokołów i ruchu sieciowego, ochronę przed atakami DoS i DDoS, ochronę dla aplikacji Web'owych, wykrywanie i blokowanie komunikacji C&C do sieci botnet, skanowanie ruchu w obu kierunkach dla protokołów na niestandardowych portach, skanowanie archiwów (zip, RAR), sygnatury do ochrony urządzeń mobilnych (co najmniej dla systemu Android), usuwanie aktywnej zawartości plików PDF i Microsoft Office, oraz wykorzystanie silnika AI.
10.	Kontrola aplikacji i www	Podaj, czy urządzenie obsługuje kontrolę ruchu na podstawie głębokiej analizy pakietów, kontrolę aplikacji chmurowych (Facebook, Google Docs, Dropbox), bazę kategorii aplikacji (proxy, P2P), definiowanie wyjątków i własnych sygnatur, bazę adresów URL (40 milionów), kategorie istotne z punktu widzenia bezpieczeństwa (malware, phishing, spam, Dynamic DNS, proxy), kategorię stron zabronionych (Hazard), nadpisywanie kategorii i tworzenie wyjątków (białe/czarne listy dla adresów URL), funkcję Safe Search, definiowanie komunikatów dla użytkowników, oraz określanie kategorii url lub wskazanych url dla których system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Lp.	Nazwa komponentu	Oferowane parametry (podpowiedzi dla oferenta)
11.	Uwierzytelnianie użytkowników	Podaj, czy urządzenie obsługuje uwierzytelnianie za pomocą haseł statycznych, LDAP, haseł dynamicznych (RADIUS, RSA SecurID), uwierzytelnianie dwuskładnikowe, integrację z Active Directory, RADIUS lub API, oraz uwierzytelnianie SAML dla ruchu HTTP.
12.	Zarządzanie	Podaj, czy urządzenie obsługuje zarządzanie lokalne (HTTPS, SSH), centralne zarządzanie i monitorowanie, szyfrowaną komunikację, uwierzytelnianie dwuskładnikowe, współpracę z rozwiązaniami monitorowania (SNMP, netflow, sflow), zarządzanie przez API, wbudowane narzędzia diagnostyczne (ping, traceroute, podgląd pakietów, monitorowanie procesowania sesji i stanu sesji firewall).
13.	Logowanie	Podaj, czy dostarczony jest komercyjny system logowania i raportowania, przekazywanie danych o ruchu, aktywności administratorów, zużyciu zasobów i stanie pracy systemu, oraz możliwość wysyłania logów do wielu serwerów logowania i serwera SYSLOG.
14.	Gwarancja, serwis i licencje	Podaj, czy dostarczone są licencje na aktualne bazy funkcji ochronnych, serwis gwarancyjny na okres co najmniej 48 miesięcy, oraz dostęp do aktualizacji oprogramowania i wsparcie techniczne.
15.	Certyfikaty i dokumenty	Podaj, czy poszczególne elementy systemu bezpieczeństwa posiadają certyfikacje ICSA lub EAL4 dla funkcji Firewall, deklarację zgodności UE lub równoważną, oraz dokumenty potwierdzające zaoferowane parametry.

4. Urządzenie bezpieczeństwa sieciowego – 18 sztuk

Lp.	Nazwa komponentu	Oferowane parametry (podpowiedzi dla oferenta)
1.	Typ	Podaj, czy urządzenie jest typu Firewall i czy jest przeznaczone do zabudowy w szafie RACK w każdej z 18 lokalizacji.
2.	Redundancja, monitoring i wykrywanie awarii	Podaj, czy urządzenie obsługuje tryby pracy Active-Active lub Active-Passive, synchronizację sesji firewall, monitoring sprzętu, oprogramowania i łączy sieciowych, oraz monitorowanie stanu połączeń VPN.
3.	Interfejsy	Podaj liczbę portów Gigabit Ethernet RJ-45, portów SFP 1 Gbps, obecność portu konsoli szeregowej oraz gniazda USB.
4.	Parametry wydajnościowe	Podaj liczbę obsługiwanych jednoczesnych połączeń (w milionach), liczbę nowych połączeń na sekundę (w tysiącach), przepustowość Stateful Firewall (w Gbps), przepustowość Firewall z włączoną funkcją Kontroli Aplikacji (w Gbps), wydajność szyfrowania IPSec VPN (w Gbps), wydajność skanowania ruchu dla IPS (w Gbps), wydajność skanowania ruchu z włączonymi funkcjami IPS, Application Control, Antywirus (w Gbps), oraz wydajność inspekcji komunikacji szyfrowanej SSL dla ruchu http (w Gbps).
5.	Funkcje systemu bezpieczeństwa	Podaj, czy urządzenie obsługuje kontrolę dostępu, kontrolę aplikacji, szyfrowanie IPSec VPN i SSL VPN, ochronę przed malware, ochronę przed atakami (IPS), kontrolę stron WWW, kontrolę zawartości poczty

Lp.	Nazwa komponentu	Oferowane parametry (podpowiedzi dla oferenta)
		(Antyspam), zarządzanie pasmem (QoS, Traffic shaping), mechanizmy DLP, uwierzytelnianie dwuskładnikowe, analizę ruchu szyfrowanego SSL.
6.	Polityki - Firewall	Podaj, czy polityka Firewall uwzględnia adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje, reakcje zabezpieczeń, rejestrowanie zdarzeń, translację adresów NAT, translację PAT, dedykowany ALG dla protokołu SIP, tworzenie stref bezpieczeństwa (np. DMZ, LAN, WAN).
7.	Połączenia VPN	Podaj, czy urządzenie obsługuje konfigurację połączeń IPSec VPN i SSL VPN, wsparcie dla IKE v1 i v2, szyfrowanie AES 128/256 bitów, obsługę protokołu Diffie-Hellman grup 19 i 20, topologie Hub and Spoke oraz Mesh, tworzenie połączeń Site-to-Site i Client-to-Site, monitorowanie tuneli VPN, mechanizmy IPSec NAT Traversal, DPD, Xauth, oraz funkcję „Split tunneling” dla połączeń Client-to-Site.
8.	Routing i obsługa połączeń WAN oraz zarządzanie pasmem	Podaj, czy urządzenie obsługuje routing statyczny, Policy Based Routing, dynamiczny routing (RIPv2, OSPF, BGP, PIM).
9.	Uwierzytelnianie użytkowników	Podaj, czy urządzenie obsługuje uwierzytelnianie za pomocą haseł statycznych, LDAP, haseł dynamicznych (RADIUS, RSA SecurID), uwierzytelnianie dwuskładnikowe, integrację z Active Directory, RADIUS lub API.

Lp.	Nazwa komponentu	Oferowane parametry (podpowiedzi dla oferenta)
10.	Zarządzanie	Podaj, czy urządzenie obsługuje zarządzanie lokalne (HTTPS, SSH), centralne zarządzanie i monitorowanie, szyfrowaną komunikację, uwierzytelnianie dwuskładnikowe, współpracę z rozwiązaniami monitorowania (SNMP, netflow, sflow), zarządzanie przez API, wbudowane narzędzia diagnostyczne (ping, traceroute, podgląd pakietów, monitorowanie procesowania sesji i stanu sesji firewall).
11.	Logowanie	Podaj, czy dostarczony jest komercyjny system logowania i raportowania, przekazywanie danych o ruchu, aktywności administratorów, zużyciu zasobów i stanie pracy systemu, oraz możliwość wysyłania logów do wielu serwerów logowania i serwera SYSLOG.
12.	Gwarancja, serwis i licencje	Podaj, czy system jest objęty serwisem gwarancyjnym producenta lub Wykonawcy przez okres co najmniej 48 miesięcy, dostęp do aktualizacji oprogramowania i wsparcie techniczne.
13.	Certyfikaty i dokumenty	Podaj, czy poszczególne elementy systemu bezpieczeństwa posiadają certyfikacje ICSA lub EAL4 dla funkcji Firewall, deklarację zgodności UE lub równoważną, oraz dokumenty potwierdzające zaoferowane parametry.

5. Urządzenie bezpieczeństwa sieciowego – 4 sztuki

Lp.	Nazwa komponentu	Oferowane parametry (podpowiedzi dla oferenta)
1.	Typ	Podaj, czy urządzenie jest typu Firewall i czy jest przeznaczone do zabudowy w szafie RACK w każdej z 4 lokalizacji.
2.	Ochrona przed atakami i wirusami	Podaj, czy urządzenie obsługuje ochronę IPS opartą na analizie sygnaturowej i anomalii w protokołach sieciowych, ochronę przed atakami na aplikacje na niestandardowych portach, automatyczne aktualizacje bazy sygnatur, definiowanie wyjątków i własnych sygnatur, wykrywanie anomalii protokołów i ruchu sieciowego, ochronę przed atakami DoS i DDoS, ochronę dla aplikacji Web'owych (co najmniej przed CSS, SQL Injection, Trojany, Exploity, Roboty), kontrolowanie długości nagłówka, ilości parametrów URL, Cookies, wykrywanie i blokowanie komunikacji C&C do sieci botnet, skanowanie ruchu w obu kierunkach dla protokołów na niestandardowych portach (np. FTP na porcie 2021), skanowanie archiwów (zip, RAR), sygnatury do ochrony urządzeń mobilnych (co najmniej dla systemu Android), usuwanie aktywnej zawartości plików PDF i Microsoft Office, oraz wykorzystanie silnika AI wytrenowanego przez laboratoria producenta.
3.	Kontrola aplikacji i www	Podaj, czy urządzenie obsługuje kontrolę ruchu na podstawie głębokiej analizy pakietów, kontrolę aplikacji chmurowych (Facebook, Google Docs, Dropbox), bazę kategorii aplikacji (proxy, P2P), definiowanie wyjątków i własnych sygnatur, bazę adresów URL (40 milionów), kategorie istotne z punktu widzenia bezpieczeństwa (malware, phishing, spam, Dynamic DNS, proxy), kategorię stron zabronionych (Hazard), nadpisywanie kategorii i tworzenie wyjątków (białe/czarne listy dla adresów URL), funkcję Safe Search, definiowanie komunikatów dla użytkowników, oraz określanie kategorii url lub wskazanych url dla których system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Lp.	Nazwa komponentu	Oferowane parametry (podpowiedzi dla oferenta)
4.	Gwarancja, serwis i licencje	Podaj, czy dostarczone są licencje na aktualne bazy funkcji ochronnych, serwis gwarancyjny na okres co najmniej 48 miesięcy, dostęp do aktualizacji oprogramowania i wsparcie techniczne, oraz czy serwis jest świadczony przez 8 godzin na dobę przez 5 dni w tygodniu.
5.	Certyfikaty i dokumenty	Podaj, czy poszczególne elementy systemu bezpieczeństwa posiadają certyfikacje ICSA lub EAL4 dla funkcji Firewall, deklarację zgodności UE lub równoważną, oraz dokumenty potwierdzające zaoferowane parametry.

6. Urządzenie służące do kompleksowej analizy i raportowania oraz zarządzania dziennikami zabezpieczeń – 1 sztuka

Lp.	Nazwa komponentu	Oferowane parametry (podpowiedzi dla oferenta)
1.	Typ	Podaj, czy urządzenie jest przeznaczone do zabudowy w szafie RACK w lokalizacji Urzędu Miasta Żywiec, Rynek 2. Czy dopuszcza się montaż na specjalnej półce RACK i czy dostawa półki jest częścią oferty.
2.	Przeznaczenie	Podaj, czy urządzenie jest przeznaczone do analizy zdarzeń w sieci obejmującej 22 lokalizacje wyniesione oraz lokalizację główną UM Żywiec (Rynek 2).

Lp.	Nazwa komponentu	Oferowane parametry (podpowiedzi dla oferenta)
3.	Interfejsy, pamięć masowa	Podaj liczbę portów Gigabit Ethernet RJ-45 (minimum 2), pojemność przestrzeni dyskowej (minimum 4 TB) oraz czy zaimplementowano mechanizm zabezpieczający przed utratą danych w przypadku awarii nośnika.
4.	Parametry wydajnościowe	Podaj, czy system jest w stanie przyjmować minimum 25 GB logów na dzień, analizować minimum 500 logów na sekundę, oraz czy umożliwia kolekcjonowanie logów z co najmniej 50 systemów.
5.	Wymagania dla centralnego systemu logowania	Podaj, czy system oferuje podgląd logowanych zdarzeń w czasie rzeczywistym, przeglądanie logów historycznych z funkcją filtrowania, dostosowywanie widoku logów (dodawanie, usuwanie, zmiana kolejności kolumn), predefiniowane lub konfigurowalne raporty graficzne lub tekstowe (np. lista najczęściej wykrywanych ataków, najbardziej aktywnych użytkowników/źródeł ruchu, najczęściej wykorzystywanych aplikacji, najczęściej odwiedzanych stron www, krajów, do których nawiązywane są połączenia, najczęściej wykorzystywanych polityk Firewall, realizowanych połączeń IPSec i SSL VPN, najczęściej występujących zdarzeń systemowych), przesyłanie kopii logów za pomocą Syslog i/lub CEF z mechanizmami filtrowania, komunikację z wykorzystaniem portów UDP/514 oraz TCP/514, eksport logów do zewnętrznego systemu za pomocą SFTP i/lub SCP, prezentację informacji o wykorzystanej przestrzeni dyskowej na przechowywanie logów.
6.	Wymagania dla centralnego systemu raportowania	Podaj, czy system umożliwia generowanie raportów w formatach HTML, PDF, CSV, posiada predefiniowane zestawy raportów z możliwością modyfikacji parametrów, funkcję definiowania własnych raportów, możliwość spolszczenia raportów, generowanie raportów cyklicznie lub na żądanie z automatycznym przesyłaniem wyników na określony adres email lub serwer za pomocą FTP/SCP, filtrowanie danych w raportach

Lp.	Nazwa komponentu	Oferowane parametry (podpowiedzi dla oferenta)
		(np. ograniczenie zakresu raportu do danych z wybranych urządzeń i adresacji IP), oraz automatyczne usuwanie raportów po określonym czasie.
7.	Wymagania dla centralnego systemu korelacji zdarzeń	Podaj, czy system umożliwia korelowanie logów z określeniem urządzeń, tworzenie własnych reguł korelowania, konfigurację powiadomień (e-mail, SNMP, API http) z dodatkowymi informacjami o zdarzeniu (np. nazwa wykrytego zagrożenia), wybór kategorii zdarzeń dla reguł korelacyjnych (m.in. Malware/AV, Aplikacje sieciowe, Email, IPS, Web Filter, Traffic, Systemowe), oraz automatyczne powiadomienie systemu bezpieczeństwa o wystąpieniu wybranych zdarzeń korelacji.
8.	Zarządzanie	Podaj, czy system umożliwia zarządzanie lokalne (HTTPS, SSH) lub za pomocą dedykowanej konsoli zarządzania z wykorzystaniem szyfrowanych protokołów, proces uwierzytelniania administratorów (lokalna baza, Radius, LDAP, Tacacs+, PKI), definiowanie co najmniej 8 administratorów z określeniem praw dostępu do wybranych modułów systemu logowania i raportowania, podział na wirtualne systemy logowania i raportowania (konteksty/domeny) z przypisywaniem praw dostępu do wybranych kontekstów i niezależnym przydzielaniem zasobów dyskowych oraz określaniem maksymalnego czasu przechowywania logów.
9.	Gwarancja, serwis i licencje	Podaj, czy system jest objęty serwisem gwarancyjnym producenta lub Wykonawcy przez okres co najmniej 48 miesięcy, dostęp do aktualizacji oprogramowania i wsparcie techniczne, oraz czy serwis jest świadczony przez 8 godzin na dobę przez 5 dni w tygodniu.

Lp.	Nazwa komponentu	Oferowane parametry (podpowiedzi dla oferenta)
10.	Certyfikaty i dokumenty	Podaj, czy poszczególne elementy systemu bezpieczeństwa posiadają deklarację zgodności UE lub równoważną, oraz dokumenty potwierdzające zaoferowane parametry.

7. System centralnego zarządzania systemami bezpieczeństwa NGFW – 1 sztuka

Lp.	Nazwa komponentu	Oferowane parametry (podpowiedzi dla oferenta)
1.	Typ	Podaj, czy rozwiązanie jest w postaci komercyjnej platformy działającej w środowisku wirtualnym lub na bazie Linux w środowisku wirtualnym. Czy jest kompatybilne z hypervisorami takimi jak VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, KVM, Proxmox.
2.	Przeznaczenie	Podaj, czy system jest przeznaczony do centralnego zarządzania wszystkimi urządzeniami bezpieczeństwa sieciowego dostarczonymi w ramach niniejszego postępowania.
3.	Interfejsy wraz z pozostałymi wymogami technicznymi	Podaj, czy system obsługuje co najmniej 4 interfejsy sieciowe, 4 vCPU, 8 GB pamięci RAM, oraz czy wspiera pracę w klastrze HA.

Lp.	Nazwa komponentu	Oferowane parametry (podpowiedzi dla oferenta)
4.	Parametry wydajnościowe	Podaj, czy system umożliwia zarządzanie co najmniej 24 systemami bezpieczeństwa NGFW.
5.	Wymagania dla centralnego systemu zarządzania	Podaj, czy system posiada mechanizm zarządzania zmianami konfiguracji z osobnymi rolami administratorów (wykonujących konfigurację i zatwierdzających zmiany), mechanizm audytu i porównywania konfiguracji, powiadamianie o oczekujących zmianach, pełną konfigurację NGFW, harmonogram implementacji zmian, przechowywanie i implementację polityk bezpieczeństwa z dziedziczeniem ustawień, sprawdzanie spójności polityki firewall, tworzenie dynamicznych obiektów (np. adresów IP), wyszukiwanie obiektów i filtrowanie reguł firewall, przypisywanie polityk i profili do wielu systemów NGFW, tworzenie wspólnych bloków polityk firewall, wersjonowanie konfiguracji, zarządzanie wersjami firmware i centralną aktualizację oprogramowania NGFW, aktualizację baz sygnatur bez dostępu do Internetu, podgląd licencji i ich ważności, zdalne wykonywanie skryptów z wykorzystaniem zmiennych, monitoring zarządzanych systemów NGFW (np. routing, DHCP server, SD-WAN, status tuneli VPN IPSec), zarządzanie systemami za NAT, ZTP, optymalizację konfiguracji VPN, pracę w trybie klastra niezawodnościowego, podział na wirtualne systemy zarządzania (konteksty), pracę wielu administratorów jednocześnie z blokadą kontekstu i polityk firewall, definiowanie globalnych obiektów dostępnych w wybranych kontekstach, włączanie/wyłączanie widoczności elementów konfiguracji w GUI, łatwą zamianę urządzenia NGFW na nowe bez konieczności ponownej konfiguracji.
6.	Zarządzanie w trybie pracy lokalnej	Podaj, czy system umożliwia zarządzanie lokalne (HTTPS, SSH), proces uwierzytelniania administratorów (lokalna baza, Radius, LDAP, TACACS+, PKI), definiowanie wielu administratorów z określeniem praw dostępu i wyborem zarządzanych systemów dostępnych dla nich, szyfrowaną komunikację z zarządzanymi systemami NGFW, oraz posiadanie API do zarządzania zarówno urządzeniami jak i systemem centralnego zarządzania.

Lp.	Nazwa komponentu	Oferowane parametry (podpowiedzi dla oferenta)
7.	Gwarancja, serwis i licencje	Podaj, czy system jest objęty serwisem gwarancyjnym producenta lub Wykonawcy przez okres co najmniej 48 miesięcy, dostęp do aktualizacji oprogramowania i wsparcie techniczne, oraz czy serwis jest świadczony przez 8 godzin na dobę przez 5 dni w tygodniu.
8.	Certyfikaty i dokumenty	Podaj, czy poszczególne elementy systemu bezpieczeństwa posiadają deklarację zgodności UE lub równoważną, oraz dokumenty potwierdzające zaoferowane parametry.

8. Centralny system służący do monitorowania bezpieczeństwa w systemach informatycznych (SIEM ang. Security Information and Event Managment) – 1 sztuka / licencja

Lp.	Nazwa komponentu	Oferowane parametry (podpowiedzi dla oferenta)
1.	Typ	Podaj, czy dostarczone platformy sprzętowe są z odpowiednio zabezpieczonym systemem operacyjnym, czy wykorzystany zostanie serwer dostarczony zgodnie z punktem 2.1.SWT
2.	Architektura	Podaj, czy system działa w architekturze klient-serwer, z agentami zbierającymi dane z urządzeń i przesyłającymi je do centralnego serwera (menadżera) do analizy i zarządzania.

Lp.	Nazwa komponentu	Oferowane parametry (podpowiedzi dla oferenta)
3.	Uruchomienie i konfiguracja	Podaj, czy dostawca jest zobowiązany do uruchomienia systemu SIEM w środowisku Zamawiającego oraz przeprowadzenia pełnej konfiguracji systemu, zapewniając jego poprawne działanie.
4.	Główne cechy i funkcje	Podaj, czy system umożliwia: Zbieranie i monitorowanie w czasie rzeczywistym zdarzeń bezpieczeństwa (nieautoryzowane logowania, zmiany plików, ataki sieciowe, inne niebezpieczne zachowania). Zarządzanie zgodnością z regulacjami i standardami (np. GDPR, HIPAA, PCI DSS). Analizę zgodnie z MITRE ATT&CK. Skalowanie rozwiązania. Architekturę klient-serwer z agentami na chronionych urządzeniach. Programowalne akcje "Active response". Pracę bezagentową. Zbieranie logów przy użyciu protokołu syslog. Agenty na systemy Windows, Linux i MacOS. Interaktywny interfejs z przeglądarki bez dodatkowego oprogramowania. Wbudowane reguły analizy.

Lp.	Nazwa komponentu	Oferowane parametry (podpowiedzi dla oferenta)
		Funkcjonalność FIM, rootkit detection. Wsparcie dla „Security Configuration Assessment" z dynamicznie generowanym raportem. Moduł do sprawdzania podatności oprogramowania oparty o bazy NVD dla systemów Windows, Linux. RESTful API. Integrację z innymi rozwiązaniami (np. Virus Total). Możliwość wykonywania aktualizacji Offline. Konfigurację alertów i powiadomień (e-mail, Slack, Webhook-i). Zbieranie i analizę logów z Office 365. Monitorowanie i zabezpieczanie środowisk chmurowych (AWS, Azure, GCP) oraz środowisk opartych o Docker. Brak ograniczeń licencyjnych co do ilości zbieranych danych.

9. Audyt bezpieczeństwa systemów IT, Audyt zerowy zgodności z KRI, Wdrożenie SZBI, Audyt końcowy zgodności z KRI/ISO 27001

Lp.	Nazwa	Oferowane parametry	Wskazówki dla oferenta
1.	Certyfikaty audytorów	Co najmniej 2 audytorów posiadających certyfikaty z listy: CIA, CISA, CISM, CRISC, CGEIT, CISSP, SSCP, Certified Reliability Professional, ISA/IEC 62443 Cybersecurity Expert.	Oferent powinien podać dokładne nazwy certyfikatów posiadanych przez audytorów oraz daty ich uzyskania. Warto również uwzględnić, czy audytorzy posiadają doświadczenie w audytach zgodności z KRI i ISO 27001.
2.	Audyt zerowy zgodności z KRI	Ocena zgodności z KRI/KSC w zakresie: wyznaczenia osoby do kontaktu, przekazania danych osoby wyznaczonej, zarządzania incydentem, zgłaszania i obsługi incydentu, dostępu do wiedzy, SZBI, inwentaryzacji, analizy ryzyka, zarządzania uprawnieniami, szkoleń, monitorowania dostępu, zabezpieczenia przed nieautoryzowanym dostępem, zasad pracy mobilnej, ochrony informacji, aktualizacji oprogramowania, zarządzania podatnościami, audytu bezpieczeństwa.	Oferent powinien opisać, jak zamierza przeprowadzić audyt zerowy, jakie narzędzia i metody zastosuje oraz jakie są jego doświadczenia w przeprowadzaniu podobnych audytów. Warto również uwzględnić, jakie dokumenty zostaną przygotowane na podstawie audytu.

Lp.	Nazwa	Oferowane parametry	Wskazówki dla oferenta
3.	Wdrożenie SZBI	Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z KRI, UoKSC, ISO 27001, ISO 22301. Wdrożenie obejmuje procesy, procedury, dokumenty.	Oferent powinien przedstawić plan wdrożenia SZBI, w tym harmonogram prac, zakres odpowiedzialności, metodykę wdrożenia oraz jakie zasoby ludzkie i techniczne zostaną zaangażowane. Warto również uwzględnić, jakie działania zostaną podjęte w celu zapewnienia ciągłości działania jednostki podczas wdrożenia.
4.	Audyt końcowy zgodności z KRI/ISO 27001	Ocena zgodności z KRI/ISO 27001, opracowanie raportu z audytu, uzupełnienie ankiety dojrzałości cyberbezpieczeństwa.	Oferent powinien opisać, jak zamierza przeprowadzić audyt końcowy, jakie kryteria zostaną użyte do oceny zgodności oraz jakie są jego doświadczenia w przeprowadzaniu audytów końcowych. Warto również uwzględnić, jakie działania zostaną podjęte w celu poprawy wyników audytu, jeśli takie będą potrzebne.
5.	Raport z audytu	Opracowanie raportu z audytu zawierającego wyniki, wnioski i rekomendacje.	Oferent powinien opisać strukturę raportu, jakie informacje zostaną w nim zawarte oraz jakie są jego doświadczenia w przygotowywaniu podobnych raportów. Warto również uwzględnić, jakie działania zostaną podjęte w celu zapewnienia, że raport będzie zrozumiały i użyteczny dla jednostki.

Lp.	Nazwa	Oferowane parametry	Wskazówki dla oferenta
6.	Ankieta dojrzałości cyberbezpieczeństwa	Uzupełnienie ankiety dojrzałości cyberbezpieczeństwa w jednostkach samorządu terytorialnego.	Oferent powinien opisać, jak zamierza przeprowadzić ocenę dojrzałości cyberbezpieczeństwa, jakie kryteria zostaną użyte oraz jakie są jego doświadczenia w przeprowadzaniu podobnych ocen. Warto również uwzględnić, jakie działania zostaną podjęte w celu poprawy wyników ankiety, jeśli takie będą potrzebne.