

Znak sprawy: ZP.272.2.2024

OPIS PRZEDMIOTU ZAMÓWIENIA

w postępowaniu o udzielenie zamówienia publicznego w trybie podstawowym bez negocjacji o wartości zamówienia mniejszej niż kwoty określone w obwieszczeniu Prezesa Urzędu Zamówień Publicznych, ogłoszonym na podstawie art. 3 ust. 3 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz.U. 2023 poz. 1605 ze zm.), pod nazwą:

Dostawa sprzętu i oprogramowania informatycznego

realizowanego w ramach projektu

„Cyberbezpieczny Samorząd”

Zamawiający: Powiat Proszowski, ul. 3 Maja 72, 32-100 Proszowice

Projekt finansowany ze środków Funduszy Europejskich na Rozwój Cyfrowy (FERC) 2021-2027 Priorytet II „Zaawansowane usługi cyfrowe” Działanie 2.2 „Wzmocnienie krajowego systemu cyberbezpieczeństwa”

L.P.	WYMAGANE MINIMALNE PARAMETRY JAKOŚCIOWE	PARAMETR WYMAGANY / P OŻĄDANY	PUNKTACJA	DT ¹	PARAMETR OFEROWANY – WYKONAWCA WINIEN OPISAĆ/PODAĆ OFEROWANE PARAMETRY
I.	Rozbudowa systemu UTM				
1	INFORMACJE OGÓLNE				
1)	Producent/Nazwa rozwiązania/Model	WYMAGANY	NIE DOTYCZY		<i>Podać producenta, nazwę oraz model</i>
2)	Rok produkcji 2024	WYMAGANY	NIE DOTYCZY		<i>Podać rok produkcji</i>
3)	Zamawiający obecnie używa zapory sieciowej UTM StotmShield SN510 wraz z modułem pasywnego skanera badającego podatności sieci. Należy rozbudować istniejące rozwiązanie w zakresie obejmującym utworzenie klastra wysokiej dostępności pracującego co najmniej w trybie active/passive oraz w zakresie dodatkowej funkcjonalności obejmującej rozszerzenie filtra URL o dodatkowe kategorie tematyczne, oraz o funkcjonalność obejmującą analizę nieznanych plików w wyizolowanym, wirtualnym środowisku (sandbox).	WYMAGANY	NIE DOTYCZY		<i>Nie dotyczy</i>
4)	Urządzenie tworzące klaster wysokiej dostępności musi posiadać parametry funkcjonalne zgodnie z pkt. 2 – pkt.21	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
5)	W ramach niniejszego postępowania istnieje możliwość zaoferowania rozwiązania równoważnego o parametrach minimalnych opisanych poniżej. Zamawiający zastrzega, że w przypadku oferowania rozwiązania równoważnego należy uwzględnić wdrożenie systemu, wraz z przeniesieniem całej konfiguracji i odzwierciedlenie usług na nowym rozwiązaniu – bez przerwy w dostępie do usług po stronie Zamawiającego i poza godzinami pracy urzędu.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
2	WYMAGANIA OGÓLNE				
1)	Rozwiązanie musi tworzyć klaster wysokiej dostępności HA co najmniej w trybie Active-Pasive	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
2)	Komunikacja klastra wysokiej dostępności musi być utworzona za pomocą redundantnych połączeń światłowodowych i odbywać się poprzez dwa interfejsy SFP	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
3)	Rozwiązanie musi zapewnić monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
3	INTERFEJSY				
1)	minimum 8 interfejsów 2,5Gb	WYMAGANY	NIE DOTYCZY	DT	<i>Opisać oferowane parametry</i>
2)	minimum 2 interfejsy SFP 1Gb	WYMAGANY	NIE DOTYCZY	DT	<i>Opisać oferowane parametry</i>

3)	minimum 2 interfejsy SFP+ 10Gb	WYMAGANY	NIE DOTYCZY	DT	Opisać oferowane parametry
4)	Możliwość tworzenia minimum 128 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1q.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
5)	Do interfejsów SFP oraz SFP+ należy dostarczyć kompatybilne wkładki SX oraz SR	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
4 PAMIĘĆ					
1)	Dysk SSD o pojemności minimum 200GB	WYMAGANY	NIE DOTYCZY	DT	Opisać oferowane parametry
5 ZASILANIE					
1)	Redundantny zasilacz o mocy dopasowanej do samodzielnego zapewnienia zasilania urządzenia, pracujące w sieci 230V 50/60Hz.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
6 FUNKCJE BEZPIECZEŃSTWA					
1)	System ochrony musi realizować wszystkie z poniższych funkcjonalności. Poszczególne funkcjonalności systemu bezpieczeństwa mogą być realizowane w postaci osobnych platform sprzętowych lub programowych: <ul style="list-style-type: none"> – kontrola dostępu – zaporą ogniową klasy Stateful Inspection – kontrola stron Internetowych – Web Filter [WF] – kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3) – kontrola pasma oraz ruchu [QoS i Traffic shaping] – kontrola aplikacji oraz rozpoznawanie ruchu P2P – ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, HTTP, FTP, HTTPS). Skanowanie AV dla plików typu: rar, zip; – ochrona przed atakami - Intrusion Prevention System [IPS/IDS] – poufność danych - IPsec VPN oraz SSL VPN – analiza ruchu szyfrowanego protokołem SSL 	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
2)	Wbudowany moduł TPM	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
7 FIREWALL					
1)	Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
2)	Obsługa translacji NAT oraz PAT.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
3)	Ochrona przed atakami DoS oraz DDoS (flood protection).	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
4)	Ochrona przed skanowaniem portów.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
5)	Blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP).	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
6)	Filtrowanie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów MAC.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry

7)	Możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
8)	Możliwość uwierzytelnienia i autoryzacji użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
9)	Musi posiadać wbudowany posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
10)	Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
8	VPN				
1)	Tworzenie połączeń w topologii Site-to-site oraz możliwość definiowania połączeń Client-to-site.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
2)	Wsparcie sieci VPN typu, minimum: PPTP VPN, IPSec VPN, SSL VPN	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
3)	Klient VPN producenta rozwiązania współpracujący z dostarczonym rozwiązaniem.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
4)	Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
5)	Możliwość przełączania tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover)	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
6)	Praca w topologii Hub and Spoke oraz Mesh lub równoważnej.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
7)	Obsługa mechanizmów minimum IPSec NAT Traversal, DPD, Xauth.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
8)	Obsługa SSL VPN w trybach portal oraz tunel.	WYMAGANY	NIE DOTYCZY	DT	Opisać oferowane parametry
9	IPS				
1)	Wykrywanie włamań oraz anomalii w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
2)	Usuwanie szkodliwej zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej bez blokowania dostępu do tej strony po usunięciu zagrożenia	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
3)	Baza wykrywanych ataków musi zawierać co najmniej 1000 wpisów.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
4)	Wykrywanie anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDoS.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
10	ANTYWIRUS				
1)	Silnik antywirusowy musi zapewniać skanowanie ruchu w obu kierunkach	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry

	komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).				
2)	Możliwość pracy w trybie przezroczystego serwera poczty (Transparent Email Proxy)	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
3)	Automatyczna aktualizacja sygnatur zagrożeń.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
4)	Ochrona przed spamem i szkodliwym oprogramowaniem w trakcie transakcji SMTP.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
5)	Inspekcja komunikacji email realizowanej przy użyciu protokołów SMTP, SMTPS, POP3, POP3S.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
6)	Wykrywanie, blokowanie i skanowanie załączników poczty email.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
7)	Tworzenie białych i czarnych list adresów email.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
8)	Wykrywanie spamu niezależnie od stosowanego języka.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
9)	Musi korzystać minimum z dwóch różnych serwerów publikujących listy RBL.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
11 FILTR STRON WWW					
1)	Wbudowany filtr URL oparty o technologię w chmurze, obsługujący minimum 65 kategorii z możliwością tworzenia własnych kategorii.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
2)	Filtr URL musi mieć możliwość korzystania z adresów WWW dostępnych w chmurze.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
3)	Musi udostępniać kategorie minimum spam, hacking, malware, botnets.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
4)	Baza filtra WWW musi umożliwiać grupowanie w kategorie tematyczne.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
5)	Filtrowanie treści oraz szkodliwego oprogramowania w obrębie protokołów HTTP i HTTPS.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
6)	Możliwość blokowania i wysyłania treści poprzez HTTP i HTTPS.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
7)	Inspekcja z obsługą protokołu TLS 1.3.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
8)	Filtrowanie plików na podstawie MIME.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
12 KONTROLA APLIKACJI					
1)	Kontrola ruchu na podstawie głębokiej analizy pakietów, nie bazującej jedynie na wartościach portów TCP/UDP.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
2)	Wykrywanie i kontrolę mikroaplikacji (np. Gry portalu Facebook).	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
3)	Identyfikacja aplikacji niezależnie od wykorzystywanego portu, protokołu, szyfrowania.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
13 BADANIE PODATNOŚCI					

1)	Wykrywanie typu i wersji oprogramowania sieciowego, którego ruch jest filtrowany przez urządzenie.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
2)	Wykrywanie i informowanie o lukach i podatnościach występujących w wykrytym oprogramowaniu.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
3)	Rozwiązanie musi weryfikować czy wykryta aplikacja jest wrażliwa na ataki lub posiada inne luki bezpieczeństwa.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
4)	Prezentacja szczegółowej listy aplikacji sieciowych, pracujących na stacjach roboczych, jak np. przeglądarki internetowe, aplikacje do multimediów (streamingu audio/video), programy antywirusowe, itp.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
5)	Kliknięcie na wskazaną przez narzędzie aplikację musi powodować wyświetlenie wszystkich komputerów, na których dany program został wykryty, a także pozwala sprawdzić wersję tej aplikacji.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
6)	Wyszukiwanie nieaktualnych wersji oprogramowania na stacjach roboczych i serwerach.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
7)	Automatyczne wysyłanie powiadomień o zagrożeniach wskazując zagrożone stacje robocze.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
14	ANALIZA NIEZNANYCH PLIKÓW				
1)	Detekcja złośliwych plików poprzez wykrywanie ataków oraz zagrożeń, realizowane poza siecią firmową, w odrębnym i bezpiecznym środowisku.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
2)	Ochrona przed zagrożeniami ukierunkowanymi oraz ransomware.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
3)	Inspekcja plików wykonywalnych np., .exe	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
4)	Inspekcja plików dokumentów w tym .doc, .docx, .rtf	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
5)	Inspekcja plików .pdf	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
6)	Inspekcję plików archiwów w tym zip, arj, lha, rar, cab	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
7)	Dynamiczna analiza behawioralna kodu uruchamianego w realnych środowiskach testowych Windows.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
15	OBSŁUGA ROUTINGU				
1)	Obsługa Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły minimum: RIPv2, OSPF, BGP.	WYMAGANY	NIE DOTYCZY	DT	Opisać oferowane parametry
2)	Możliwość realizacji routingu statycznego w oparciu o polityki automatycznego wyboru łącza w trybie failover.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
3)	Trasowanie pakietów z poziomu wybranej reguły firewall (Policy Based Routing)	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry

4)	Trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
5)	Możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP).	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
6)	Możliwość wykorzystania mechanizmu SD-WAN poprzez analizę stanu łącza w czasie rzeczywistym i dynamicznym wyborze najkorzystniejszego łącza.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
16 WYDAJNOŚĆ					
1)	Wydajność systemu Firewall minimum 10 Gbps	WYMAGANY	NIE DOTYCZY	DT	Opisać oferowane parametry
2)	Wydajność ochrony przed atakami (IPS) minimum 5 Gbps	WYMAGANY	NIE DOTYCZY	DT	Opisać oferowane parametry
3)	Wydajność VPN IPSec minimum 2,5 Gbps	WYMAGANY	NIE DOTYCZY	DT	Opisać oferowane parametry
4)	Minimalna liczba jednoczesnych połączeń: 500.000.	WYMAGANY	NIE DOTYCZY	DT	Opisać oferowane parametry
5)	Minimum 25.000 nowych połączeń na sekundę	WYMAGANY	NIE DOTYCZY	DT	Opisać oferowane parametry
17 RAPORTOWANIE					
1)	System realizujący funkcję Firewall musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
2)	Rozwiązanie musi udostępniać predefiniowane raporty dla ruchu WWW, modułu IPS, skanera antywirusowego i antyspamowego.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
3)	Musi umożliwiać generowanie różnych typów raportów.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
4)	System raportowania i przeglądania logów wbudowany w system bezpieczeństwa nie może wymagać dodatkowej licencji do swojego działania.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
18 BEZPIECZEŃSTWO					
1)	Uwierzytelnianie tożsamości użytkowników za pomocą haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
2)	Uwierzytelnianie tożsamości użytkowników za pomocą haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
3)	Uwierzytelnianie tożsamości użytkowników za pomocą haseł dynamicznych (RADIUS) w oparciu o zewnętrzne bazy danych.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
4)	Możliwość budowy architektury uwierzytelniania typu Single Sign On w środowisku Active Directory bez konieczności instalowania jakiegokolwiek oprogramowania na kontrolerze domeny.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
5)	Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP,	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry

	interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety).				
6)	Możliwość uwierzytelniania dwuetapowego 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
19	AKTUALIZACJA				
1)	Automatyczne ściąganie sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
20	ZARZĄDZANIE				
1)	Elementy systemu muszą zapewniać lokalne zarządzanie (HTTPS, SSH) jak i współpracować z dedykowanymi platformami do centralnego zarządzania i monitorowania.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
2)	Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
3)	Konfiguracja urządzenia z wykorzystaniem GUI minimum w polskiej wersji językowej.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
4)	Możliwość zarządzania z poziomu konsoli (SSH)	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
5)	Interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
6)	Interfejs administracyjny musi umożliwiać generowanie skryptów z czynności wykonywanych przez administratora.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
7)	Interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
8)	Możliwość eksportowania logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
9)	Możliwość budowania reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
10)	Możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry

21	CERTYFIKATY I DEKLARACJE				
1)	Element oferowanego systemu bezpieczeństwa realizujący zadanie Firewall musi posiadać certyfikat ICSA lub EAL4+ lub równoważny dla rozwiązań kategorii Network Firewall.	WYMAGANY	NIE DOTYCZY		Opisać oferowane certyfikaty i deklaracje
2)	Deklaracja zgodności UE (certyfikat CE) potwierdzająca spełnienie wymagań dyrektywy „Nowego Podejścia”. Urządzenie musi posiadać oznakowanie CE.	WYMAGANY	NIE DOTYCZY		Opisać oferowane certyfikaty i deklaracje
3)	Certyfikat zgodności z dyrektywą RoHS lub dokument wystawiony przez niezależną, akredytowaną jednostkę potwierdzający spełnienie kryteriów środowiskowych zgodnych z dyrektywą RoHS o eliminacji substancji niebezpiecznych.	WYMAGANY	NIE DOTYCZY		Opisać oferowane certyfikaty i deklaracje
4)	Deklaracja zgodności z dyrektywą WEEE lub oświadczenie producenta o spełnieniu obowiązków w zakresie postępowania z odpadami WEEE i zgodności z Ustawą z 11 września 2015 o zużyтым sprzęcie elektrycznym i elektronicznym. Urządzenie musi być oznaczone etykietą WEEE.	WYMAGANY	NIE DOTYCZY		Opisać oferowane certyfikaty i deklaracje
II.	Rozbudowa zabezpieczeń logicznych				
1	INFORMACJE OGÓLNE				
1)	Producent/Nazwa rozwiązania/Model	WYMAGANY	NIE DOTYCZY		Podać producenta, nazwę oraz model
2)	Rok produkcji 2024	WYMAGANY	NIE DOTYCZY		Podać rok produkcji
3)	Zamawiający dostarczenia 3 routerów VPN dla jednostek organizacyjnych, współpracujących z systemem UTM Zamawiającego	WYMAGANY	NIE DOTYCZY		Nie dotyczy
2	WYMAGANIA OGÓLNE				
1)	Elementy systemu przenoszące ruch użytkowników muszą dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub transparent.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
2)	Urządzenie musi być wyposażone w wewnętrzną pamięć do przechowywania danych minimum 200GB	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
3	INTERFEJSY				
1)	minimum 5 interfejsów miedzianych 1GbE	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
4	VPN				
1)	Wydajność połączenia IPSec throughput - AES128/SHA1 / AES256/SHA2 minimum 200 Mbps	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
2)	Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
3)	Klient VPN producenta rozwiązania współpracujący z dostarczonym rozwiązaniem.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry

4)	Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
5)	Praca w topologii Hub and Spoke oraz Mesh lub równoważnej.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
6)	Obsługa mechanizmów minimum IPSec NAT Traversal, DPD, Xauth.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
7)	Obsługa SSL VPN w trybach portal oraz tunel.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
8)	Obsługa bezpłatnego mechanizmu uwierzytelniania dwuskładnikowego do generowania kodów jednorazowych np. Google Authenticator	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
5	BEZPIECZEŃSTWO				
1)	Uwierzytelnianie tożsamości użytkowników za pomocą haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
2)	Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety).	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
6	ZARZĄDZANIE				
1)	Elementy systemu muszą zapewniać lokalne zarządzanie (HTTPS, SSH) jak i współpracować z dedykowanymi platformami do centralnego zarządzania i monitorowania.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
2)	Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
7	CERTYFIKATY I DEKLARACJE				
1)	Deklaracja zgodności UE (Certyfikat CE). Urządzenie musi posiadać oznakowanie CE.	WYMAGANY	NIE DOTYCZY		Opisać oferowane certyfikaty i deklaracje
2)	Certyfikat zgodności z dyrektywą RoHS lub dokument wystawiony przez niezależną, akredytowaną jednostkę potwierdzający spełnienie kryteriów środowiskowych zgodnych z dyrektywą RoHS o eliminacji substancji niebezpiecznych.	WYMAGANY	NIE DOTYCZY		Opisać oferowane certyfikaty i deklaracje
3)	Deklaracja zgodności z dyrektywą WEEE lub oświadczenie producenta o spełnieniu obowiązków w zakresie postępowania z odpadami WEEE i zgodności z Ustawą z 11 września 2015 o zużytych sprzęcie elektrycznym i elektronicznym. Urządzenie musi być oznaczone etykietą WEEE.	WYMAGANY	NIE DOTYCZY		Opisać oferowane certyfikaty i deklaracje
4)	Certyfikat ICSA Labs dla funkcji VPN IPSec lub urządzenie musi znajdować się na liście produktów kryptograficznych zatwierdzonych przez Radę UE	WYMAGANY	NIE DOTYCZY		Opisać oferowane certyfikaty i deklaracje
5)	Certyfikat Common Criteria lub oświadczenie producenta potwierdzające bezpieczeństwo systemu zgodnie z wymaganiami normy ISO 15408.	WYMAGANY	NIE DOTYCZY		Opisać oferowane certyfikaty i deklaracje

III. Przetłacznik szkieletowy 24 x SFP+					
1	INFORMACJE OGÓLNE				
1)	Producent / Model	WYMAGANY	NIE DOTYCZY	DT	<i>Podać producenta i model</i>
2)	Rok produkcji 2024	WYMAGANY	NIE DOTYCZY		<i>Podać rok produkcji</i>
2	OBUDOWA				
1)	Obudowa typu RACK 19"	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
2)	Wysokości maksymalnej 1U	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
3	ZASILANIE				
1)	Wbudowany zasilacz o mocy dopasowanej do samodzielnego zapewnienia zasilania urządzenia, pracujący w sieci 230V 50/60Hz prądu zmiennego	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
4	PAMIĘĆ				
1)	Wbudowana pamięć RAM minimum 4 GB	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
2)	Wbudowana pamięć flash o pojemności minimum 1 GB.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
5	INTERFEJSY				
1)	Minimum 24 portów SFP+	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
2)	Minimum 6 portów QSFP+	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
3)	Minimum 1 port USB lub RJ45 do zarządzania	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
4)	Minimum 1 port USB umożliwiający podłączenie zewnętrznej pamięci flash	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
5)	Możliwość skonfigurowania min. 1000 interfejsów vlan interface SVI	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
6	WYDAJNOŚĆ				
1)	Matryca przełączająca o wydajności minimum 1,44 Tbps	WYMAGANY	NIE DOTYCZY	DT	<i>Opisać oferowane parametry</i>
2)	Wydajność przełączania przynajmniej 490 Mpps	WYMAGANY	NIE DOTYCZY	DT	<i>Opisać oferowane parametry</i>
3)	Obsługa minimum 64 000 adresów MAC	WYMAGANY	NIE DOTYCZY	DT	<i>Opisać oferowane parametry</i>
4)	Obsługa minimum 4090 sieci VLAN jednocześnie	WYMAGANY	NIE DOTYCZY	DT	<i>Opisać oferowane parametry</i>
5)	Obsługa 802.1Q tunneling (QinQ)	WYMAGANY	NIE DOTYCZY	DT	<i>Opisać oferowane parametry</i>
6)	Możliwość skonfigurowania min. 512 interfejsów vlan interface SVI	WYMAGANY	NIE DOTYCZY	DT	<i>Opisać oferowane parametry</i>
7)	Obsługa ramek jumbo o wielkości minimum 9216 bajtów	WYMAGANY	NIE DOTYCZY	DT	<i>Opisać oferowane parametry</i>
8)	Wydajność połączenia w stos minimum 40 Gb/s	WYMAGANY	NIE DOTYCZY	DT	<i>Opisać oferowane parametry</i>
7	ROUTING				
1)	Obsługa min. 64 000 tras dla routingu Ipv4;	WYMAGANY	NIE DOTYCZY	DT	<i>Opisać oferowane parametry</i>

2)	Obsługa min. 32 000 tras dla routingu Ipv6;	WYMAGANY	NIE DOTYCZY	DT	Opisać oferowane parametry
3)	Obsługa min. 25 wirtualnych tablic routingu-forwardingu (VRF)	WYMAGANY	NIE DOTYCZY	DT	Opisać oferowane parametry
8	PROTOKOŁY				
1)	Obsługa protokołu GVRP;	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
2)	Wsparcie dla protokołów IEEE 802.1w Rapid Spanning Tree oraz IEEE 802.1s Multi-Instance Spanning Tree. Wymagane wsparcie dla min. 64 instancji protokołu MSTP;	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
3)	Obsługa protokołów LLDP i LLDP-MED	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
4)	Obsługa protokołu UDLD lub równoważnego	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
9	OBŚŁUGA KOLEJEK				
1)	Implementacja co najmniej ośmiu kolejek sprzętowych QoS na każdym porcie wyjściowym z możliwością konfiguracji dla obsługi ruchu o różnych klasach;	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
2)	Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy adres MAC, docelowy adres MAC, źródłowy adres IP, docelowy adres IP, źródłowy port TCP, docelowy port TCP.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
10	ŁĄCZENIE W STOS				
1)	Zarządzanie stosem poprzez jeden adres IP	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
2)	Możliwość łączenia minimum 8 jednostek w stosie	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
3)	Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (ang. Cross-stack link aggregation);	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
4)	Stos przełączników musi być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree;	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
5)	Wymagane są moduły stackujące lub licencje umożliwiające łączenie urządzeń w stos jeżeli dotyczy. Dopuszcza się możliwość łączenia w stosy za pomocą portów typu uplink.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
11	BEZPIECZEŃSTWO				
1)	Minimum 3 poziomy dostęp administracyjny poprzez konsolę	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
2)	Autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz dynamicznego przypisania listy ACL	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
3)	Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC oraz poprzez portal WWW	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
4)	Zarządzanie przez HTTPS, SNMP i SSH za pomocą protokołów Ipv4 i Ipv6	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry

5)	Możliwość filtrowania ruchu w oparciu o adresy MAC, Ipv4, Ipv6, porty TCP/UDP	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
6)	Obsługa mechanizmów Port Security, Dynamic ARP Inspection, IP Source Guard, voice VLAN oraz private VLAN (lub równoważny)	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
7)	Możliwość synchronizacji czasu zgodnie z NTP	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
12	ZARZĄDZANIE I MONITORING				
1)	Możliwość lokalnej i zdalnej obserwacji ruchu na określonym porcie, polegająca na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu oraz poprzez określony VLAN	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
2)	Plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC)	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
3)	Dedykowany port konsoli oraz dedykowany port zarządzający out-of-band 10/100Base-T Ethernet	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
4)	Mechanizm do badania jakości połączeń (IP SLA) z możliwością badania takich parametrów jak: jitter, opóźnienie, straty pakietów dla wygenerowanego strumienia testowego UDP	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
5)	Możliwość pracy jako generator / odbiornik pakietów testowych IP SLA	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
6)	Możliwość konfiguracji liczby wysyłanych pakietów UDP w ramach pojedynczej próbki oraz odstępu czasowego pomiędzy kolejnymi wysłanymi pakietami UDP w ramach pojedynczej próbki	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
13	CERTYFIKATY I DEKLARACJE				
1)	Deklaracja zgodności UE (certyfikat CE) potwierdzająca spełnienie wymagań dyrektywy „Nowego Podejścia”. Urządzenie musi posiadać oznakowanie CE.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane certyfikaty i deklaracje</i>
2)	Certyfikat zgodności z dyrektywą RoHS lub dokument wystawiony przez niezależną, akredytowaną jednostkę potwierdzający spełnienie kryteriów środowiskowych zgodnych z dyrektywą RoHS o eliminacji substancji niebezpiecznych.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane certyfikaty i deklaracje</i>
3)	Deklaracja zgodności z dyrektywą WEEE lub oświadczenie producenta o spełnieniu obowiązków w zakresie postępowania z odpadami WEEE i zgodności z Ustawą z 11 września 2015 o zużyтым sprzęcie elektrycznym i elektronicznym). Urządzenie musi być oznaczone etykietą WEEE.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane certyfikaty i deklaracje</i>
IV.	Rozbudowa systemu backup				
1	INFORMACJE OGÓLNE				

1)	Producent / Model	WYMAGANY	NIE DOTYCZY		<i>Podać producenta i model oferowanych urządzeń</i>
2)	Rok produkcji 2024	WYMAGANY	NIE DOTYCZY		<i>Podać rok produkcji</i>
3)	Rozbudowa systemu kopii zapasowych obejmuje zakup pamięci masowej RDX	WYMAGANY	NIE DOTYCZY		<i>Nie dotyczy</i>
2	OBUDOWA				
1)	Obudowa typu RACK 19" o wysokości maksymalnej 1U	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
2)	Wypożyczona w minimum 4 zintegrowane napędy na wymienne kasety dyskowe	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
3	ZASILANIE				
2)	Wbudowany zasilacz o mocy dopasowanej do samodzielnego zapewnienia zasilania urządzenia, pracujący w sieci 230V 50/60Hz prądu zmiennego	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
4	INTERFEJSY				
1)	Minimum 4 porty 1 GbE	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
2)	Minimum 1 x IPMI	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
3)	Minimum 2 porty USB	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
5	TRANSFER DANYCH				
1)	Minimum 400 MB/s	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
6	PAMIĘĆ MASOWA				
1)	Minimum 4 wymienne kasety dyskowe, każda o pojemności minimum 4 TB bez kompresji	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
2)	Kaseta dyskowa musi być zabezpieczona przed otwarciem i wyciągnięciem nośnika.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
3)	Kaseta dyskowa musi być odporna na upadki.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
7	ZARZĄDZANIE				
7)	Możliwość zarządzania z przeglądarki internetowej minimum Edge, Chrome	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
8)	Możliwość konfiguracji urządzenia w trybie tworzenia kopii zapasowych, archiwizacji, dystrybucji oraz udostępniania danych.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
9)	Możliwość szyfrowania danych.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
8	CERTYFIKATY I DEKLARACJE				
1)	Deklaracja zgodności UE (certyfikat CE) potwierdzająca spełnienie wymagań dyrektywy „Nowego Podejścia”. Urządzenie musi posiadać oznakowanie CE.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane certyfikaty i deklaracje</i>
2)	Certyfikat zgodności z dyrektywą RoHS lub dokument wystawiony przez niezależną,	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane certyfikaty i deklaracje</i>

	akredytowaną jednostkę potwierdzający spełnienie kryteriów środowiskowych zgodnych z dyrektywą RoHS o eliminacji substancji niebezpiecznych.				
3)	Deklaracja zgodności z dyrektywą WEEE lub oświadczenie producenta o spełnieniu obowiązków w zakresie postępowania z odpadami WEEE i zgodności z Ustawą z 11 września 2015 o zużytym sprzęcie elektrycznym i elektronicznym. Urządzenie musi być oznaczone etykietą WEEE.	WYMAGANY	NIE DOTYCZY		Opisać oferowane certyfikaty i deklaracje
V. Rozbudowa systemu ochrony urządzeń					
1 INFORMACJE OGÓLNE					
1)	Producent / Nazwa	WYMAGANY	NIE DOTYCZY		Podać producenta i nazwę oprogramowania
2)	Istniejący system ochrony urządzeń ESET należy rozbudować w zakresie modułu posiadającego narzędzia wykrywania incydentów i automatycznego reagowania umożliwiającego korelację zdarzeń (XDR), mechanizmy uwierzytelniania wieloskładnikowego (MFA) oraz w zakresie proaktywnej ochrony przed zagrożeniami zero-day z analizą w odizolowanym chmurowym środowisku.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
3)	W wyniku rozbudowy systemu o nowe moduły funkcjonalne przy zachowaniu dotychczasowej funkcjonalności w zakresie ochrony stacji roboczych, ochrony serwerów, ochrony urządzeń mobilnych. Nowe moduły muszą być kompatybilne z istniejącym systemem, a całe rozwiązanie musi zapewniać minimum funkcjonalność określoną w pkt. 2 - 8	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
4)	Zamawiający dopuszcza wymianę istniejącego rozwiązania na rozwiązanie równoważne do istniejącego systemu ochrony urządzeń, realizującego minimum funkcjonalności opisane w pkt.2-8, Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, iż 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 systemu na równoważne nie zakłóciła bieżącej pracy Zamawiającego. 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.	WYMAGANY	NIE DOTYCZY		Opisać jeżeli dotyczy
5)	Rozwiązanie musi zapewniać jednoczesną ochronę 56 stacji komputerowych .	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry

	Rozwiązanie musi być dostarczone z wymaganą ilością licencji na w/w ilość stacji.				
2	WYMAGANIA OGÓLNE				
1)	Rozwiązanie musi być zarządzane z jednej centralnej konsoli administracyjnej dostępnej z poziomu interfejsu WWW zabezpieczonego protokołem SSL. Wymagana jest autoryzacja dwuetapowa do konsoli administracyjnej.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
2)	Serwer administracyjny dostępny w chmurze musi pozwalać na centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, zaporą osobista, kontrola dostępu do stron internetowych, które działają na stacjach roboczych w sieci oraz musi umożliwiać tworzenie polityk dla programów zabezpieczających i komponentów środowiska serwera centralnego zarządzania.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
3)	Konsola administracyjna musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
4)	Moduł XDR musi być oparty o motor baz danych SQL celem zapewnienia maksymalnej wydajności pracy i maksymalnej ochrony danych. Motor bazy SQL należy dostarczyć wraz z modułem XDR.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
5)	Rozwiązanie musi zapewnić uwierzytelnianie użytkownika zanim zostanie uruchomiony system operacyjny.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
3	XDR				
1)	Automatyczna wizualizacja zdarzeń, incydentów i ataków ukierunkowanych	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
2)	Możliwość wyszukiwania zagrożeń na podstawie definiowanych filtrów	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
3)	Wbudowany zestaw reguł zapewniający reagowanie na wykryte incydenty z możliwością budowania własnych reguł oraz edycji istniejących.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
4)	Możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
5)	Możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
6)	Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>

7)	Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry jeżeli dotyczy
8)	Możliwość uruchomienia reguł w oparciu o dane historyczne.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry jeżeli dotyczy
9)	Możliwość blokowania plików po sumach kontrolnych.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry jeżeli dotyczy
10)	Możliwość ustawiania priorytetu zdarzeń.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry jeżeli dotyczy
11)	Możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry jeżeli dotyczy
12)	Możliwość oznaczenia plików DLL jako bezpieczne, pobrania do analizy oraz ich zablokowania.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry jeżeli dotyczy
13)	Weryfikacja uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry jeżeli dotyczy
14)	Dla wykonanego skryptu lub pliku exe, weryfikacja powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry jeżeli dotyczy
15)	Możliwość bezpośredniego sprawdzenia SHA-1 pliku, na portalach służących do weryfikacji bezpieczeństwa (np. VirusTotal).	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry jeżeli dotyczy
16)	Możliwość włączenia izolacji komputera od sieci.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry jeżeli dotyczy
4	UWIERZYTELNIANIE WIELOSKŁADNIKOWE (MFA)				
1)	Wbudowany serwer RADIUS umożliwiający uwierzytelnianie użytkowników dla rozwiązań VPN, które wspierają protokół RADIUS.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry jeżeli dotyczy
2)	Możliwość integracji minimum z systemem operacyjnym Windows Server poprzez konsolę zarządzającą systemem operacyjnego.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry jeżeli dotyczy
3)	Moduł zarządzania uwierzytelnianiem się użytkowników musi integrować się minimum z wbudowanym w systemie operacyjnym Windows Server modułem do zarządzania kontami użytkowników w postaci dodatkowej zakładki we właściwościach użytkownika.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry jeżeli dotyczy
4)	Możliwość określenia metody uwierzytelniania dwuskładnikowego użytkowników, minimum wiadomość SMS, aplikacja mobilna	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry jeżeli dotyczy
5)	Do wysyłania wiadomości SMS nie może być wymagane posiadanie własnej	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry jeżeli dotyczy

	bramy SMS i centrali GSM. Wysyłanie wiadomości SMS z hasłami jednorazowymi musi odbywać się z infrastruktury producenta rozwiązania.				
6)	Możliwość wysyłania wiadomości na telefony pracujące w roamingu.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
7)	Możliwość wyboru użytkowników uwierzytelniania dwuskładnikowego.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
8)	Możliwość ograniczenia dostępu przy uwierzytelnianiu metodą RADIUS do grupy użytkowników wskazanych w konfiguracji.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
9)	Rozwiązanie musi posiadać mechanizm zabezpieczający przed atakiem typu brute-force, które po określonej liczbie prób nieudanego logowania musi automatycznie zablokować możliwość uwierzytelnienia się dla danego użytkownika.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
10)	W ramach modułu musi być zapewniony dostęp do dedykowanej aplikacji mobilnej działającej pod kontrolą Android i iOS	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
11)	Dostępne API pozwalające programistom na zintegrowanie rozwiązania z serwisem web lub oprogramowaniem wykorzystującym uwierzytelnianie w oparciu minimum o usługę Active Directory. Dla środowisk nie wykorzystujących usług Active Directory musi być dostępny pakiet SDK umożliwiający implementację w tych środowiskach, dwuskładnikowego uwierzytelniania do autoryzacji użytkowników.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
5 SANDBOXING W CHMURZE					
1)	Wbudowany serwer RADIUS umożliwiający uwierzytelnianie użytkowników dla rozwiązań VPN, które wspierają protokół RADIUS.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
2)	Możliwość integracji minimum z systemem operacyjnym Windows Server poprzez konsolę zarządzającą systemem operacyjnego.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
3)	Moduł zarządzania uwierzytelnianiem się użytkowników musi integrować się minimum z wbudowanym w systemie operacyjnym Windows Server modułem do zarządzania kontami użytkowników w postaci dodatkowej zakładki we właściwościach użytkownika.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
4)	Ochrona przed zagrożeniami 0-day.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
5)	Możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
6)	Możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>

7)	Możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
8)	Tworzenie listy wykluczeń określonych plików lub folderów z przesyłania.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
9)	Możliwość wyświetlenia listy plików, które zostały przesłane do analizy.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
10)	Możliwość analizowania plików, bez względu na lokalizację stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
6 OCHRONA STACJI ROBOCZYCH					
1)	Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
2)	Ochrona przed rootkitami oraz podłączeniem komputera do sieci botnet.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
3)	Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
4)	Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
5)	Skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
6)	Skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
7)	Umieszczenia na liście wykluczeń wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
8)	Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
9)	Skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
10)	Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
11)	Blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: pamięci masowych, optycznych pamięci masowych, pamięci masowych firewalli,	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>

	urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.				
12)	Blokowanie nośników wymiennych, bądź grup urządzeń wraz z możliwością tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
13)	Możliwość generowania raportu dotyczącego stacji, zawierającego informacje dotyczące, minimum: zainstalowanych aplikacji, usług systemowych, systemu operacyjnego, aktywnych procesów, połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
14)	Automatyczna, inkrementalna aktualizacja silnika detekcji.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
15)	Tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
16)	Skaner UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
17)	Zintegrowany moduł bezpiecznej przeglądarki. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez użytkownika.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
18)	Zintegrowany moduł kontroli dostępu do stron internetowych.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
19)	Możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
20)	Ochrona przed zagrożeniami 0-day.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
7 OCHRONA SERWERÓW					
1)	Ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
2)	Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
3)	Skanowania dysków sieciowych typu NAS.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
4)	Wbudowane minimum dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
5)	Automatyczna, inkrementalna aktualizacja silnika detekcji.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
6)	Możliwość wykluczania ze skanowania procesów.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
7)	Możliwość określenia typu podejrzanych plików, jakie będą przesyłane do	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>

	producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.				
8)	System zapobiegania włamaniom działający na hoście (HIPS).	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
9)	Skanowanie magazynu Hyper-V.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
10)	Skaner UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
11)	Możliwość blokowania zewnętrznych nośników danych na serwerze w tym przynajmniej: pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
12)	Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
13)	Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
14)	Ochrona przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
15)	Możliwość uruchomienia lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
8	OCHRONA URZĄDZEŃ MOBILNYCH				
1)	Skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
2)	Automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
3)	Możliwość skonfigurowania zaufanej karty SIM.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
4)	Wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi usunięcie zawartości urządzenia, przywrócenie urządzenia do ustawień fabrycznych, zablokowania urządzenia, uruchomienie sygnału dźwiękowego, lokalizację GPS.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
5)	Wyświetlenie listy zainstalowanych aplikacji.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>
6)	Blokowanie aplikacji w oparciu o nazwę aplikacji, nazwę pakietu, kategorię sklepu Google Play, uprawnienia aplikacji, pochodzenie	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry jeżeli dotyczy</i>

	aplikacji z nieznanego źródła.				
7)	Skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry jeżeli dotyczy
VI. System zarządzania hasłami					
1	INFORMACJE OGÓLNE				
1)	Producent / Nazwa	WYMAGANY	NIE DOTYCZY		Podać producenta i nazwę oprogramowania
2	WYMAGANIA OGÓLNE				
1)	Rozwiązanie musi być dostarczone z licencją na 56 kont użytkowników				
2)	Rozwiązanie musi być dostępne minimum w wersji chmurowej (SaaS) i zapewniać pełne szyfrowanie danych.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
3)	Musi umożliwiać generowanie silnych i unikalnych haseł i nazw użytkownika do witryn internetowych i aplikacji mobilnych oraz ich zapisywanie w kontenerach użytkowników.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
4)	Dostęp do systemu na różnych urządzeniach	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
5)	Logowanie dwuetapowe, minimum FIDO2, aplikacja uwierzytelniająca, klucz sprzętowy.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
6)	Generowanie i automatyczne wypełnianie kodów TOTP dla 2FA	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
7)	Uwierzytelnianie SSO na zaufanych urządzeniach.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
8)	Odszyfrowywanie danych przy użyciu klucza szyfrowania przechowywanego na urządzeniu	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
9)	System musi zapewnić ochronę danych on-line	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
10)	Musi umożliwiać zarządzanie użytkownikami	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
11)	Musi zapewnić kontrolę dostępu do zasobów opartą o role i poziomy uprawnień	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
12)	Możliwość resetowania haseł głównych do kont głównych użytkowników przez wyznaczonych administratorów.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
13)	Integracja z kontami użytkowników Active Directory lub LDAP	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
14)	Musi udostępniać API zgodny z OpenAPI	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
3	RAPORTOWANIE				
1)	Generowanie raportów dotyczących minimum haseł ujawnionych, ponownie użytych oraz słabych.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
2)	Raporty dotyczące danych naruszonych w wyniku znanych naruszeń (np.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry

	adresów e-mail, hasła)				
3)	Dziennik zdarzeń	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
4	CERTYFIKATY				
1)	Certyfikat SOC kategorii minimum 2 lub certyfikat równoważny wydany przez akredytowaną jednostkę certyfikującą, potwierdzający wysoki standard usług obejmujących ochronę danych i bezpieczeństwo przetwarzania.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
VII. Wdrożenie rozwiązań					
1	INSTALACJA I MONTAŻ				
1)	Zamawiający wymaga dostarczenia wszelkich komponentów potrzebnych do zamontowania dostarczonych urządzeń oraz do połączenia urządzeń do infrastruktury pasywnej (np. szyny montażowe, moduły światłowodowe, przewody krosowe, przewody zasilające, osprzęt montażowy).	WYMAGANY	NIE DOTYCZY		Nie dotyczy*
2)	Wymagana instalacja dostarczonych urządzeń posiadających obudowę przeznaczoną do montażu stelażowego, we wskazanej przez Zamawiającego szafie RACK 19".	WYMAGANY	NIE DOTYCZY		Nie dotyczy*
3)	Urządzenia muszą być montowane za pośrednictwem szyn montażowych dostarczonych wraz z urządzeniami.	WYMAGANY	NIE DOTYCZY		Nie dotyczy*
4)	Zamawiający wymaga wykonanie wszystkich połączeń urządzeń, niezbędnych do uruchomienia całości środowiska.	WYMAGANY	NIE DOTYCZY		Nie dotyczy*
5)	Przetłaczniki szkieletowe muszą być zamontowane w szafie RACK wskazanej przez Zamawiającego na etapie realizacji i podłączone. Należy wykonać połączenia pomiędzy przetłacznikami umożliwiające pracę urządzeń w trybie HA za pomocą dostarczonego okablowania.	WYMAGANY	NIE DOTYCZY		Nie dotyczy*
6)	Zamawiający wymaga instalacji dostarczonych systemów na urządzeniach wskazanych przez zamawiającego na etapie realizacji.	WYMAGANY	NIE DOTYCZY		Nie dotyczy*
2	KONFIGURACJA				
1)	Klaster UTM HA musi być skonfigurowany zgodnie z wytycznymi administratora Zamawiającego, z uwzględnieniem minimalnych prac: a) konfiguracja pracy urządzeń w układzie HA b) weryfikacja założeń wdrożenia c) konfiguracja sieci (interfejsy i routing) d) konfiguracja firewalla e) konfiguracja NAT	WYMAGANY	NIE DOTYCZY		Nie dotyczy*

	<p>f) konfiguracja IPS – zgodnie z wymaganiami klienta</p> <p>g) konfiguracja dodatkowych usług sieciowych tj. DHCP, DNS Proxy</p> <p>h) integracja z AD lub założenie wewnętrznej bazy użytkowników (bez dodawania użytkowników).</p> <p>i) konfiguracja transparentnej autoryzacji w AD – konfiguracja po stronie urządzenia, inżynier nie instaluje agenta SSO a jedynie instruuje klienta jak powinna przebiegać instalacja.</p> <p>j) konfiguracja VPN:</p> <ul style="list-style-type: none"> – IPSec Site-to-Site – zgodnie z parametrami tuneli otrzymanymi na etapie realizacji – IPSec Client-to-Site – konfiguracja urządzenia i jednej wzorcowej stacji klienckiej na kliencie dedykowanym lub ShrewVPN. <p>k) konfiguracja SSL VPN lub PPTP VPN.</p>				
2)	<p>W zakresie rozbudowy systemu bezpieczeństwa, Wykonawca:</p> <p>a) zainstaluje na dostarczonym serwerze i skonfiguruje motor baz danych SQL w sposób zapewniający stabilną pracę modułu XDR. Jeżeli instalacja motoru baz danych będzie wymagała instalacji dodatkowych bibliotek programowych, należy je doinstalować;</p> <p>b) moduł XDR - należy skonfigurować i zoptymalizować reguły reagowania na incydenty oraz przygotować polityki połączeniowej i zaaplikowanie dla stacji końcowych z zainstalowanym konektorem;</p> <p>c) uruchomić możliwość uwierzytelniania dwuskładnikowego MFA dla użytkowników systemu.</p> <p>Dodatkowo w przypadku rozwiązania równoważnego:</p> <ol style="list-style-type: none"> 1) przygotować pakiety instalacyjne i zainstalować system na wszystkich stacjach komputerowych; 2) przygotować wymagane polityki dla organizacji i działu IT; 3) skonfigurować polityki szyfrowania; 4) uruchomić wszystkie moduły; 5) włączenie domyślnych reguł zgodnie z wytycznymi Zamawiającego określonymi na etapie realizacji; 6) wykonać dokumentację zawierającą opis wszystkich modułów, punktów konfiguracji (wraz z rzutami ekranowymi, adresacjami, loginami wraz z hasłami, zalecenia wdrożeniowe; <p>zapewnienie minimum 16 godzin instruktazu stanowiskowego dla administratorów</p>	WYMAGANY	NIE DOTYCZY		Nie dotyczy*

	Zamawiającego zapewniającego pełne zrozumienie administracyjnych, instalacji oprogramowania systemowego i narzędziowego, znajomości i umiejętności realizacji procedur, znajomości wytycznych polityk bezpieczeństwa, potwierdzonego protokołem z wykonania instruktarzu.				
Wdrożenie 802.1x EAP-TLS					
1)	Uruchomienie i konfiguracja serwera certyfikacji wystawiającego certyfikaty dla pracowników Zamawiającego oraz wdrożenie certyfikatu klienta na stacjach roboczych Windows w zakresie: a) Utworzenie polityk GPO; b) utworzenia i wydawania szablonu certyfikatu Uwierzytelniania stacji roboczej dla urzędu certyfikacji; c) konfiguracji automatycznego sporządzania listy szablonów uwierzytelniania stacji roboczej przy użyciu zasady grupy; d) automatyczne rejestrowanie certyfikatu uwierzytelniania stacji roboczej i weryfikowanie jego instalacji na komputerach.	WYMAGANY	NIE DOTYCZY		Nie dotyczy*
2)	Konfiguracja serwera certyfikacji musi umożliwiać autoryzację użytkowników za pomocą wydanych certyfikatów. Administrator musi mieć możliwość rejestracji użytkowników, publikacji oraz unieważniania certyfikatów.	WYMAGANY	NIE DOTYCZY		Nie dotyczy*
3)	Konfiguracja protokołu 802.1x EAP-TLS.	WYMAGANY	NIE DOTYCZY		Nie dotyczy*
4)	Uruchomienie uwierzytelniania użytkowników z wykorzystaniem wygenerowanych certyfikatów zapisanych na kluczu sprzętowym z obsługą FIDO2. Klucze sprzętowe należy dostarczyć w ramach wdrożenia.	WYMAGANY	NIE DOTYCZY		Nie dotyczy*
5)	Wymagana jest konfiguracja 4 przełączników sieciowych oraz zapory UTM w zakresie autoryzacji IEEE 802.1x	WYMAGANY	NIE DOTYCZY		Nie dotyczy*
6)	Przeprowadzenie instruktarzu administratora w zakresie administracji obejmującego zagadnienia związane z konfiguracją i zarządzaniem usługami domenowymi.	WYMAGANY	NIE DOTYCZY		Nie dotyczy*
3	DOKUMENTACJA POWYKONAWCZA				
1)	Po zakończeniu realizacji, Zamawiający wymaga dostarczenia pełnej dokumentacji powykonawczej oraz procedur eksploatacji rozwiązań. Dokumentacja powykonawcza musi zawierać minimum:	WYMAGANY	NIE DOTYCZY		Nie dotyczy*

	a) opis ogólnych informacji o rozwiązaniach; b) schematy połączeń urządzeń i ich adresacje; c) zestawienie loginów i haseł do rozwiązań; d) zestawienie ustawień wszystkich rozwiązań; e) instrukcje instalacji, konfiguracji, uruchomienia; f) zestawienie licencji; g) listę autoryzowanych kontaktów serwisowych;				
--	--	--	--	--	--

** parametr obligatoryjny, Zamawiający nie wymaga potwierdzenia na etapie oferty*

¹ *Parametry oznaczone indeksem DT muszą być potwierdzone dokumentami pochodzącymi od producenta oferowanych urządzeń, zgodnie z Rozdział VIII ust. 2 SWZ.*

Proszowice dnia 26.11.2024 r.

Data; kwalifikowany podpis elektroniczny lub podpis zaufany lub podpis osobisty