*ABR.272.14.2024.MŚ Załącznik nr 2 do SWZ*

**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**

w ramach projektu

**„Cyberbezpieczny Samorząd Powiat Brzeski”**

**Zamawiający**: Powiat Brzeski, ul. Bartosza Głowackiego 51, 32-800 Brzesko

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 / pożądany** | | | | **Punktacja** | | **DT1** | | | **Parametr oferowany –**  *Wykonawca winien opisać/podać oferowane parametry* |
|  | ***Macierz dyskowa*** | | | | | | | | | | |
|  | **Informacje ogólne** | | | | | | | | | | |
|  | Producent / Model | wymagany | | | | nie dotyczy | | **DT** | | *Podać producenta i model* | |
|  | Rok produkcji 2024 | wymagany | | | | nie dotyczy | |  | | *Podać rok produkcji* | |
|  | **Wymagania ogólne** | | | | | | | | | | |
|  | Macierz dyskowa musi współpracować z posiadanymi przez Zamawiającego serwerami – ProLiant DL380Gen10, 2 x Huawei RH2288H V3. | wymagany | | | | nie dotyczy | |  | | *Opisać oferowane parametry* | |
|  | Możliwość rozbudowy macierzy do co najmniej 100 szt. oferowanego typu napędów dyskowych bez wymiany kontrolerów.  Dla zapewnienia obsługi dysków gwarantujących uzyskanie wymaganej przestrzeni dyskowej, Zamawiający dopuszcza zastosowanie do jednostki głównej modułu rozszerzeń. | wymagany | | | | nie dotyczy | | **DT** | | *Opisać oferowane parametry* | |
|  | Obudowa jednostki kontrolerowej muszą zawierać układ nadmiarowy dla modułów zasilania i chłodzenia umożliwiający wymianę tych elementów (tego elementu) bez konieczności wyłączania macierzy. | wymagany | | | | nie dotyczy | |  | | *Opisać oferowane parametry* | |
|  | **Obudowa jednostki kontrolerowej** | | | | | | | | | | |
|  | Obudowa typu RACK do instalacji w standardowej szafie 19” | wymagany | | | | nie dotyczy | |  | | *Opisać oferowane parametry* | |
|  | Obudowa musi umożliwiać instalację minimum 24 dysków 2,5” Hot Plug. | wymagany | | | | nie dotyczy | | **DT** | | *Podać oferowane parametry* | |
|  | **Kontrolery** | | | | | | | | | | |
|  | Minimum 2 kontrolery pracujące w układzie nadmiarowym typu active‐active.  Możliwość rozbudowy do minimum 4 kontrolerów bez konieczności wymiany istniejących kontrolerów | wymagany | | | | nie dotyczy | | **DT** | | *Opisać oferowane parametry* | |
|  | Możliwość konfiguracji poziomów RAID minimum: 5, 6 lub równoważnych zapewniających taki sam poziom ochrony danych. | wymagany | | | | nie dotyczy | | **DT** | | *Opisać oferowane parametry* | |
|  | Zabezpieczenia RAID realizowane za pomocą sprzętowego, dedykowanego układu, z możliwością ich kombinacji w/w typów w ramach oferowanej macierzy. | wymagany | | | | nie dotyczy | |  | | *Opisać oferowane parametry* | |
|  | Macierz musi umożliwiać konfigurację RAID tolerującą awarię 3 dysków bez utraty danych. | wymagany | | | | nie dotyczy | |  | | *Opisać oferowane parametry* | |
|  | **Cache** | | | | | | | | |  | |
|  | Minimum 64 GB na każdy kontroler. | wymagany | | | | nie dotyczy | | **DT** | | *Opisać oferowane parametry* | |
|  | Możliwość rozbudowy pamięci do minimum 256GB | wymagany | | | | nie dotyczy | |  | | *Opisać oferowane parametry* | |
|  | Pamięć Cache musi być zabezpieczona przed utratą danych w przypadku awarii zasilania poprzez funkcję zapisu zawartości pamięci Cache na dysk lub posiadać podtrzymywanie bateryjne. | wymagany | | | | nie dotyczy | |  | | *Opisać oferowane parametry z podaniem sposobu zabezpieczenia przed utratą danych* | |
|  | **Obsługa dysków** | | | | | | | | | | |
|  | Macierz musi wspierać dyski SSD SAS. | wymagany | | | | nie dotyczy | | **DT** | | *Opisać oferowane parametry* | |
|  | Do obsługi każdego zainstalowanego dysku macierz musi wykorzystywać redundantne połączenia SAS 12Gbps. | wymagany | | | | nie dotyczy | | **DT** | | *Opisać oferowane parametry* | |
|  | Możliwość definiowania dysków SPARE lub odpowiedniej przestrzeni dyskowej. | wymagany | | | | nie dotyczy | |  | | *Opisać oferowane parametry* | |
|  | **Przestrzeń dyskowa** | | | | | | | | | | |
|  | Macierz musi być dostarczona z dyskami SSD SAS o pojemności zapewniającej przestrzeń roboczą minimum 30TB w RAID6. | wymagany | | | | nie dotyczy | |  | | *Opisać oferowane parametry* | |
|  | **Interfejsy** | | | | | | | | | | |
|  | Minimum 8 portów FC+ pracujących z prędkością, co najmniej 16Gb/s. | wymagany | | | | nie dotyczy | |  | | *Opisać oferowane parametry* | |
|  | Minimum 4 porty Ethernet pracujące z prędkością, co najmniej 10Gb/s. | wymagany | | | | nie dotyczy | |  | | *Opisać oferowane parametry* | |
|  | **Zasilacze** | | | | | | | | | | |
|  | Redundantne zasilacze Hot Plug o każdy mocy dopasowanej do samodzielnego zapewnienia zasilania urządzenia, pracujące w sieci 230V 50/60Hz. | wymagany | | | | nie dotyczy | |  | | *Opisać oferowane parametry* | |
|  | **Funkcjonalność** | | | | | | | | | | |
|  | Tworzenie i prezentacja dysków logicznych (LUN) o pojemności większej niż zajmowana fizyczna przestrzeń dyskowych (ang. ThinProvisioning). | wymagany | | | | nie dotyczy | | **DT** | | *Opisać oferowane parametry* | |
|  | Zwrot skasowanej przestrzeni dyskowej do puli zasobów wspólnych. | wymagany | | | | nie dotyczy | | **DT** | | *Opisać oferowane parametry* | |
|  | Możliwość tworzenia lustrzanych zasobów LUN z możliwością automatycznego i bezprzerwowego przełączenia na kopię lustrzaną LUN w przypadku awarii podstawowego zasobu LUN. | wymagany | | | | nie dotyczy | |  | | *Opisać oferowane parametry* | |
|  | Migracja danych ze źródłowego LUNa do docelowego LUNa bezprzerwowo dla hostów. | wymagany | | | | nie dotyczy | |  | | *Opisać oferowane parametry* | |
|  | Tworzenie na żądanie migawkowej kopii danych (ang. snapshot) w ramach macierzy do wykorzystania w celu np. wykonywania kopii zapasowych lub testów systemów komputerowych.  Wymagana minimalna liczba snapshotów 2000. | wymagany | | | | nie dotyczy | | **DT** | | *Opisać oferowane parametry* | |
|  | Tworzenie na żądanie pełnej fizycznej kopii danych (klon) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. | wymagany | | | | nie dotyczy | | **DT** | | *Opisać oferowane parametry* | |
|  | Kopiowanie pomiędzy obszarami danych zabezpieczonych różnymi poziomami RAID. | wymagany | | | | nie dotyczy | |  | | *Opisać oferowane parametry* | |
|  | Obsługa deduplikacji i kompresji danych w trybie in-line. | wymagany | | | | nie dotyczy | | **DT** | | *Opisać oferowane parametry* | |
|  | Możliwość zdalnej replikacji danych typu on-line (bez przerywania prezentacji wolumenów dyskowych) do macierzy tej samej rodziny w trybie synchronicznym i asynchronicznym, dla całej przestrzeni dyskowej. | wymagany | | | | nie dotyczy | |  | | *Opisać oferowane parametry* | |
|  | Dynamicznie przydzielanie zasobów macierzy w celu spełnienia określonych celów wydajnościowych aplikacji bez przerywania pracy systemu. | wymagany | | | | nie dotyczy | |  | | *Opisać oferowane parametry* | |
|  | Możliwość ustawiania priorytetów wydajności dla aplikacji w oparciu o zdefiniowane profile wolumenowe, dla wydajności w IOPS i przepustowości danych. | wymagany | | | | nie dotyczy | |  | | *Opisać oferowane parametry* | |
|  | Wsparcie dla technologii klastrowania macierzy dyskowych (ang. Storage Metro Cluster). | wymagany | | | | nie dotyczy | |  | | *Opisać oferowane parametry* | |
|  | Musi zapewniać bezprzerwowe działanie środowiska (aplikacja/system operacyjny/serwer) podłączonego do macierzy w przypadku wystąpienia awarii logicznego połączenia z tą macierzą bądź awarii samej macierzy powodujących dla danego środowiska brak dostępu do zasobów macierzy preferowanej, z wykorzystaniem synchronicznej replikacji danych po protokołach FC lub IP. | wymagany | | | | nie dotyczy | |  | | *Opisać oferowane parametry* | |
|  | Możliwość podłączenia macierzy innych producentów i udostępnienie zasobów wirtualnego urządzenia jako własne. | wymagany | | | | nie dotyczy | |  | | *Opisać oferowane parametry* | |
|  | Wszystkie wyszczególnione i wymagane funkcjonalności muszą być realizowane przez kontrolery dostarczonej macierzy dyskowej. Nie dopuszcza się realizowania w/w funkcjonalności z użyciem oprogramowania firm trzecich lub komponentów sprzętowych firm trzecich. | wymagany | | | | nie dotyczy | |  | | *Opisać oferowane parametry* | |
|  | **Wsparcie dla systemów i technologii** | | | | | | | | | | |
|  | Microsoft® Windows®, VMware®, Hyper-V®, SLES, RHES, Oracle VM | wymagany | | | | nie dotyczy | | **DT** | | *Opisać oferowane parametry* | |
|  | | **Certyfikaty i Deklaracje** | | | | | | | | | | |
|  | | Deklaracja zgodności UE (certyfikat CE) potwierdzająca spełnienie wymagań dyrektywy „Nowego Podejścia”. Urządzenie musi posiadać oznakowanie CE. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane certyfikaty i deklaracje* |
|  | | 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* |
|  | | 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 (Dz.U. 2015 poz.1688). Urządzenie musi być oznaczone etykietą WEEE. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane certyfikaty i deklaracje* |
|  | ***Utworzenie klastra UTM HA*** ***+ konsola zarządzająca*** | | | | | | | | | | |
|  | **Informacje ogólne** | | | | | | | | | | |
|  | Producent/Nazwa rozwiązania/Model | wymagany | | | | nie dotyczy | |  | | | *Podać producenta, nazwę oraz model* |
|  | Rok produkcji 2024 | wymagany | | | | nie dotyczy | |  | | | *Podać rok produkcji* |
|  | Zamawiający obecnie używa zapory sieciowej UTM StotmShield SN510 wraz z modułem pasywnego skanera badającego podatności sieci. Nr licencji obecnie posiadanego systemu SN510A27C5038A7. Ważność licencji do 18 kwietnia 2027.  Należy rozbudować istniejące rozwiązanie w zakresie obejmującym utworzenie klastra wysokiej dostępności oraz w zakresie dodatkowej funkcjonalności obejmującej rozbudowę filtra URL o dodatkowe kategorie tematyczne i analizę nieznanych plików w wyizolowanym, wirtualnym środowisku. | wymagany | | | | nie dotyczy | |  | | | *Nie dotyczy* |
|  | | Urządzenie tworzące klaster wysokiej dostępności musi posiadać parametry funkcjonalne zgodnie z pkt. 2 – pkt.21 | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | **Wymagania ogólne** | | | | | | | | | | |
|  | | Rozwiązanie musi tworzyć klaster wysokiej dostępności HA co najmniej w trybie Active-Pasive | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Komunikacja klastra wysokiej dostępności musi być utworzona za pomocą redundantnych połączeń światłowodowych i odbywać się poprzez dwa interfejsy SFP | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Rozwiązanie musi zapewnić monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | **Interfejsy** | | | | | | | | | | |
|  | | minimum 8 interfejsów 2,5Gb | wymagany | | | | nie dotyczy | **DT** | | | | *Opisać oferowane parametry* |
|  | | minimum 2 interfejsy SFP 1Gb | wymagany | | | | nie dotyczy | **DT** | | | | *Opisać oferowane parametry* |
|  | | minimum 2 interfejsy SFP+ 10Gb | wymagany | | | | nie dotyczy | **DT** | | | | *Opisać oferowane parametry* |
|  | | Możliwość tworzenia minimum 128 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1q. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Do interfejsów SFP oraz SFP+ należy dostarczyć kompatybilne wkładki SX oraz SR | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | **PAMIĘĆ** | | | | | | | | | | |
|  | | Dysk SSD o pojemności minimum 200GB | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | **Zasilanie** | | | | | | | | | | |
|  | | Redundantny zasilacz o mocy dopasowanej do samodzielnego zapewnienia zasilania urządzenia, pracujące w sieci 230V 50/60Hz. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | **Funkcje bezpieczeństwa** | | | | | | | | | | |
|  | | System ochrony musi realizować wszystkie z poniższych funkcjonalności. Poszczególne funkcjonalności systemu bezpieczeństwa mogą być realizowane w postaci osobnych platform sprzętowych lub programowych:   * kontrola dostępu – zapora ogniowa 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* |
|  | | Wbudowany moduł TPM | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | **Firewall** | | | | | | | | | | |
|  | | Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Obsługa translacji NAT oraz PAT. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Ochrona przed atakami DoS oraz DDoS (flood protection). | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Ochrona przed skanowaniem portów. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP). | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Filtrowanie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów MAC. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | 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* |
|  | | 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* |
|  | | Musi posiadać wbudowany posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | **VPN** | | | | | | | | | | |
|  | | Tworzenie połączeń w topologii Site-to-site oraz możliwość definiowania połączeń Client-to-site. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Wsparcie sieci VPN typu, minimum: PPTP VPN, IPSec VPN, SSL VPN | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Klient VPN producenta rozwiązania współpracujący z dostarczonym rozwiązaniem. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Możliwość przełączania tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover) | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Praca w topologii Hub and Spoke oraz Mesh lub równoważnej. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Obsługa mechanizmów minimum IPSec NAT Traversal, DPD, Xauth. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Obsługa SSL VPN w trybach portal oraz tunel. | wymagany | | | | nie dotyczy | **DT** | | | | *Opisać oferowane parametry* |
|  | | **IPS** | | | | | | | | | | |
|  | | Wykrywanie włamań oraz anomaliów w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | 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* |
|  | | Baza wykrywanych ataków musi zawierać co najmniej 1000 wpisów. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Wykrywanie anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDoS. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | **Antywirus** | | | | | | | | | | |
|  | | Silnik antywirusowy musi zapewniać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Możliwość pracy w trybie przezroczystego serwera poczty (Transparent Email Proxy) | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Automatyczna aktualizacja sygnatur zagrożeń. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Ochrona przed spamem i szkodliwym oprogramowaniem w trakcie transakcji SMTP. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Inspekcja komunikacji email realizowanej przy użyciu protokołów SMTP, SMTPS, POP3, POP3S. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Wykrywanie, blokowanie i skanowanie załączników poczty email. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Tworzenie białych i czarnych list adresów email. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Wykrywanie spamu niezależnie od stosowanego języka. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Musi korzystać minimum z dwóch różnych serwerów publikujących listy RBL. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | **Filtr stron WWW** | | | | | | | | | | |
|  | | Wbudowany filtr URL oparty o technologię w chmurze, obsługujący minimum 65 kategorii z możliwością tworzenia własnych kategorii. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Filtr URL musi mieć możliwość korzystania z adresów WWW dostępnych w chmurze. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Musi udostępniać kategorie minimum spam, hacking, malwere, botnets. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Baza filtra WWW musi umożliwiać grupowanie w kategorie tematyczne. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Filtrowanie treści oraz szkodliwego oprogramowania w obrębie protokołów HTTP i HTTPS. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Możliwość blokowania i wysyłania treści poprzez HTTP i HTTPS. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Inspekcja z obsługą protokołu TLS 1.3. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Filtrowanie plików na podstawie MIME. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | **Kontrola Aplikacji** | | | | | | | | | | |
|  | | Kontrola ruchu na podstawie głębokiej analizy pakietów, nie bazującej jedynie na wartościach portów TCP/UDP. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Wykrywanie i kontrolę mikroaplikacji (np. Gry portalu Facebook). | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Identyfikacja aplikacji niezależnie od wykorzystywanego portu, protokołu, szyfrowania. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | **Badanie podatności** | | | | | | | | | | |
|  | | Wykrywanie typu i wersji oprogramowania sieciowego, którego ruch jest filtrowany przez urządzenie. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry* |
|  | | Wykrywanie i informowanie o lukach i podatnościach występujących w wykrytym oprogramowaniu. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry* |
|  | | Rozwiązanie musi weryfikować czy wykryta aplikacja jest wrażliwa na ataki lub posiada inne luki bezpieczeństwa. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry* |
|  | | 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* |
|  | | 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* |
|  | | Wyszukiwanie nieaktualnych wersji oprogramowania na stacjach roboczych i serwerach. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry* |
|  | | Automatyczne wysyłanie powiadomień o zagrożeniach wskazując zagrożone stacje robocze. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry* |
|  | | **Analiza nieznanych plików** | | | | | | | | | | |
|  | | Detekcja złośliwych plików poprzez wykrywanie ataków oraz zagrożeń, realizowane poza siecią firmową, w odrębnym i bezpiecznym środowisku. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry* |
|  | | Ochrona przed zagrożeniami ukierunkowanymi oraz ransomware. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry* |
|  | | Inspekcja plików wykonywalnych np., .exe | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry* |
|  | | Inspekcja plików dokumentów w tym .doc, .docx, .rtf | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry* |
|  | | Inspekcja plików .pdf | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry* |
|  | | Inspekcję plików archiwów w tym zip, arj, lha, rar, cab | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry* |
|  | | Dynamiczna analiza behawioralna kodu uruchamianego w realnych środowiskach testowych Windows. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry* |
|  | | **Obsługa Routingu** | | | | | | | | | | |
|  | | Obsługa Policy Routingu, routing statyczny i dynamiczny w oparciu o  protokoły minimum: RIPv2, OSPF, BGP. | wymagany | | | | nie dotyczy | **DT** | | | | *Opisać oferowane parametry* |
|  | | Możliwość realizacji routingu statycznego w oparciu o polityki automatycznego wyboru łącza w trybie failover. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Trasowanie pakietów z poziomu wybranej reguły firewall (Policy Based Routing) | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | 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* |
|  | | Możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP). | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Możliwość wykorzystania mechanizmu SD-WAN poprzez analizę stanu łącza w czasie rzeczywistym i dynamicznym wyborze najkorzystniejszego łącza. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | **Wydajność** | | | | | | | | | | |
|  | | Wydajność systemu Firewall minimum 10 Gbps | wymagany | | | | nie dotyczy | **DT** | | | | *Opisać oferowane parametry* |
|  | | Wydajność ochrony przed atakami (IPS) minimum 5 Gbps | wymagany | | | | nie dotyczy | **DT** | | | | *Opisać oferowane parametry* |
|  | | Wydajność VPN IPSec minimum 2,5 Gbps | wymagany | | | | nie dotyczy | **DT** | | | | *Opisać oferowane parametry* |
|  | | Minimalna liczba jednoczesnych połączeń: 500.000. | wymagany | | | | nie dotyczy | **DT** | | | | *Opisać oferowane parametry* |
|  | | Minimum 25.000 nowych połączeń na sekundę | wymagany | | | | nie dotyczy | **DT** | | | | *Opisać oferowane parametry* |
|  | | **Raportowanie** | | | | | | | | | | |
|  | | System realizujący funkcję Firewall musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Rozwiązanie musi udostępniać predefiniowane raporty dla ruchu WWW, modułu IPS, skanera antywirusowego i antyspamowego. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Musi umożliwiać generowanie różnych typów raportów. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | System raportowania i przeglądania logów wbudowany w system bezpieczeństwa nie może wymagać dodatkowej licencji do swojego działania. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | **Bezpieczeństwo** | | | | | | | | | | |
|  | | Uwierzytelnianie tożsamości użytkowników za pomocą haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Uwierzytelnianie tożsamości użytkowników za pomocą haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Uwierzytelnianie tożsamości użytkowników za pomocą haseł dynamicznych (RADIUS) w oparciu o zewnętrzne bazy danych. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | 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* |
|  | | 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* |
|  | | Możliwość uwierzytelniania dwuetapowego 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP). | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | **Aktualizacja** | | | | | | | | | | |
|  | | Automatyczne ściąganie sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | **Zarządzanie** | | | | | | | | | | |
|  | | 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* |
|  | | Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Konfiguracja urządzenia z wykorzystaniem GUI minimum w polskiej wersji językowej. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Możliwość zarządzenia z poziomu konsoli (SSH) | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Interfejs administracyjny musi umożliwiać generowanie skryptów z czynności wykonywanych przez administratora. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Możliwość eksportowania logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS). | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | Możliwość budowania reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane parametry* |
|  | | 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* |
|  | | **Certyfikaty i Deklaracje** | | | | | | | | | | |
|  | | 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* |
|  | | Deklaracja zgodności UE (certyfikat CE) potwierdzająca spełnienie wymagań dyrektywy „Nowego Podejścia”. Urządzenie musi posiadać oznakowanie CE. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane certyfikaty i deklaracje* |
|  | | 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* |
|  | | 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 (Dz.U. 2015 poz.1688). Urządzenie musi być oznaczone etykietą WEEE. | wymagany | | | | nie dotyczy |  | | | | *Opisać oferowane certyfikaty i deklaracje* |
|  | ***Rozbudowa systemu backup*** | | | | | | | | | | |
|  | **Informacje ogólne** | | | | | | | | | | |
|  | Producent / Model | wymagany | | | | nie dotyczy | | **DT** | | | *Podać producenta i model* |
|  | Rok produkcji 2024 | wymagany | | | | nie dotyczy | |  | | | *Podać rok produkcji* |
|  | Rozbudowa systemu kopii zapasowych obejmuje zakup 2 przełączników SAN, pracujących w układzie redundantnym HA | wymagany | | | | nie dotyczy | |  | | | *Nie dotyczy* |
|  | Każde z urządzeń musi być zgodne z funkcjonalnością określoną w pkt.2 -.pkt.8 | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry* |
|  | | **Obudowa** | | | | | | | | | | |
|  | | Obudowa typu RACK 19” | wymagany | | | nie dotyczy | | |  | *Opisać oferowane parametry* | | |
|  | | Wysokości maksymalna 1U | wymagany | | | nie dotyczy | | |  | *Opisać oferowane parametry* | | |
|  | | **Zasilanie** | | | | | | | | | | |
|  | | Wbudowany zasilacz o mocy dopasowanej do samodzielnego zapewnienia zasilania urządzenia, pracujący w sieci 230V 50/60Hz prądu zmiennego | wymagany | | | nie dotyczy | | |  | *Opisać oferowane parametry* | | |
|  | | **Pory** | | | | | | | | | | |
|  | | Minimum 24 porty FC | wymagany | | | nie dotyczy | | |  | *Opisać oferowane parametry* | | |
|  | | Porty FC muszą współpracować z wkładkami 32/16/8/4 Gbps. Wybór prędkości działania portu musi być możliwy w trybie autonegocjacji. | wymagany | | | nie dotyczy | | | **DT** | *Opisać oferowane parametry* | | |
|  | | Minimum 8 portów aktywnych, z wkładkami SFP+ 16Gbps LC do połączeń wielomodowych krótkodystansowych. | wymagany | | | nie dotyczy | | |  | *Opisać oferowane parametry* | | |
|  | | Możliwość aktywacji łącznie 24 portów FC obsadzonych wkładkami SFP+ 16Gbps | wymagany | | | nie dotyczy | | |  | *Opisać oferowane parametry* | | |
|  | | Aktywne porty nie mogą być ograniczone czasowo. | wymagany | | | nie dotyczy | | |  | *Opisać oferowane parametry* | | |
|  | | Obsługa trybu NPIV na portach. | wymagany | | | nie dotyczy | | |  | *Opisać oferowane parametry* | | |
|  | | Trunking portów 16Gb na łącze ISP | wymagany | | | nie dotyczy | | |  | *Opisać oferowane parametry* | | |
|  | | **Wydajność** | | | | | | | | | | |
|  | | Matryca przełączająca o wydajności minimum 128 Gbps | wymagany | | | nie dotyczy | | | **DT** | *Opisać oferowane parametry* | | |
|  | | **Bezpieczeństwo** | | | | | | | | | | |
|  | | Możliwość kontroli dostępu na poziomie portu. | wymagany | | | nie dotyczy | | |  | *Opisać oferowane parametry* | | |
|  | | Autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz dynamicznego przypisania listy ACL | wymagany | | | nie dotyczy | | |  | *Opisać oferowane parametry* | | |
|  | | Uwierzytelnianie za pomocą protokołów FCAP | wymagany | | | nie dotyczy | | |  | *Opisać oferowane parametry* | | |
|  | | Wsparcie szyfrowania protokołem SSHv2, SSL/HTTPS, SNMP v1/v3 | wymagany | | | nie dotyczy | | |  | *Opisać oferowane parametry* | | |
|  | | Wsparcie protokołów RADIUD, LDAP, Open LDAP, TACACS+ | wymagany | | | nie dotyczy | | |  | *Opisać oferowane parametry* | | |
|  | | Obsługa QoS oraz izolacja ruchu | wymagany | | | nie dotyczy | | |  | *Opisać oferowane parametry* | | |
|  | | **Zarządzanie** | | | | | | | | | | |
|  | | Konfiguracja i zarządzanie z wykorzystaniem protokołu HTTP/HTTPS, SSH | wymagany | | | nie dotyczy | | |  | *Opisać oferowane parametry* | | |
|  | | Dedykowany port konsoli i port zarządzający 10/100/1000 Base-T Ethernet | wymagany | | | nie dotyczy | | |  | *Opisać oferowane parametry* | | |
|  | | **Certyfikaty i Deklaracje** | | | | | | | | | | |
|  | | Deklaracja zgodności UE (certyfikat CE) potwierdzająca spełnienie wymagań dyrektywy „Nowego Podejścia”. Urządzenie musi posiadać oznakowanie CE. | wymagany | nie dotyczy | | | | |  | *Opisać oferowane certyfikaty i deklaracje* | | |
|  | | 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* | | |
|  | | 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 (Dz.U. 2015 poz.1688). Urządzenie musi być oznaczone etykietą WEEE. | wymagany | nie dotyczy | | | | |  | *Opisać oferowane certyfikaty i deklaracje* | | |
|  | | ***Przełącznik „Enterprise”*** | | | | | | | | | | |
|  | | **Informacje ogólne** | | | | | | | | | | |
|  | | Producent / Model | wymagany | | | nie dotyczy | | | **DT** | *Podać producenta i model* | | |
|  | | Rok produkcji 2024 | wymagany | | | nie dotyczy | | |  | *Podać rok produkcji* | | |
|  | | **Obudowa** | | | | | | | | | | |
|  | | Obudowa typu RACK 19” | wymagany | | | nie dotyczy | | |  | *Opisać oferowane parametry* | | |
|  | | Wysokości maksymalnej 1U | wymagany | | | nie dotyczy | | |  | *Opisać oferowane parametry* | | |
|  | | **Zasilanie** | | | | | | | | | | |
|  | | Wbudowany zasilacz o mocy dopasowanej do samodzielnego zapewnienia zasilania urządzenia, pracujący w sieci 230V 50/60Hz prądu zmiennego | wymagany | | | nie dotyczy | | |  | *Opisać oferowane parametry* | | |
|  | | **Pamięć** | | | | | | | | | | |
|  | | Wbudowana pamięć RAM minimum 64 MB | wymagany | | | nie dotyczy | | |  | *Opisać oferowane parametry* | | |
|  | | Wbudowana pamięć flash o pojemności minimum 16 MB. | wymagany | | | nie dotyczy | | |  | *Opisać oferowane parametry* | | |
|  | | **Pory** | | | | | | | | | | |
|  | | Minimum 24 portów SFP+ | wymagany | | | nie dotyczy | | |  | *Opisać oferowane parametry* | | |
|  | | Minimum 2 porty QSFP+ | wymagany | | | nie dotyczy | | |  | *Opisać oferowane parametry* | | |
|  | | Minimum 1 port USB lub RJ45 do zarządzania | wymagany | | | nie dotyczy | | |  | *Opisać oferowane parametry* | | |
|  | | Minimum 1 port USB umożliwiający podłączenie zewnętrznej pamięci flash | wymagany | | | nie dotyczy | | |  | *Opisać oferowane parametry* | | |
|  | | **Wydajność** | | | | | | | | | | |
|  | | Matryca przełączająca o wydajności minimum 640 Gbps | wymagany | | | nie dotyczy | | | **DT** | *Opisać oferowane parametry* | | |
|  | | Wydajność przełączania przynajmniej 252 Mpps | wymagany | | | nie dotyczy | | | **DT** | *Opisać oferowane parametry* | | |
|  | | Obsługa minimum 32 000 adresów MAC | wymagany | | | nie dotyczy | | | **DT** | *Opisać oferowane parametry* | | |
|  | | Obsługa minimum 4000 sieci VLAN jednocześnie | wymagany | | | nie dotyczy | | | **DT** | *Opisać oferowane parametry* | | |
|  | | Obsługa 802.1Q tunneling (QinQ) | wymagany | | | nie dotyczy | | | **DT** | *Opisać oferowane parametry* | | |
|  | | Możliwość skonfigurowania min. 512 interfejsów vlan interface SVI | wymagany | | | nie dotyczy | | | **DT** | *Opisać oferowane parametry* | | |
|  | | Obsługa ramek jumbo o wielkości minimum 9216 bajtów | wymagany | | | nie dotyczy | | | **DT** | *Opisać oferowane parametry* | | |
|  | | Wydajność połączenia w stos minimum 40 Gb/s | wymagany | | | nie dotyczy | | | **DT** | *Opisać oferowane parametry* | | |
|  | | **Routing** | | | | | | | | | | |
|  | | Obsługa min. 4 000 tras dla routingu Ipv4; | wymagany | | | nie dotyczy | | | **DT** | *Opisać oferowane parametry* | | |
|  | | Obsługa min. 2 000 tras dla routingu Ipv6; | wymagany | | | nie dotyczy | | | **DT** | *Opisać oferowane parametry* | | |
|  | | Obsługa min. 25 wirtualnych tablic routingu-forwardingu (VRF) | wymagany | | | nie dotyczy | | | **DT** | *Opisać oferowane parametry* | | |
|  | | **Protokoły** | | | | | | | | | | |
|  | | Obsługa protokołu GVRP; | wymagany | | | nie dotyczy | | |  | *Opisać oferowane parametry* | | |
|  | | 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* | | |
|  | | Obsługa protokołów LLDP i LLDP-MED | wymagany | | | nie dotyczy | | |  | *Opisać oferowane parametry* | | |
|  | | Obsługa protokołu UDLD lub równoważnego | wymagany | | nie dotyczy | | | |  | *Opisać oferowane parametry* | | |
|  | | **Obsługa kolejek** | | | | | | | | | | |
|  | | 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* | | |
|  | | 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* | | |
|  | | **Łączenie w stos** | | | | | | | | | | |
|  | | Zarządzanie stosem poprzez jeden adres IP | wymagany | | | nie dotyczy | | |  | *Opisać oferowane parametry* | | |
|  | | Możliwość łączenia minimum 8 jednostek w stosie | wymagany | | | nie dotyczy | | |  | *Opisać oferowane parametry* | | |
|  | | 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* | | |
|  | | Stos przełączników musi być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree; | wymagany | | | nie dotyczy | | |  | *Opisać oferowane parametry* | | |
|  | | 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* | | |
|  | | **Bezpieczeństwo** | | | | | | | | | | |
|  | | Minimum 3 poziomy dostępu administracyjnego poprzez konsolę | wymagany | | | nie dotyczy | | |  | *Opisać oferowane parametry* | | |
|  | | Autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz dynamicznego przypisania listy ACL | wymagany | | | nie dotyczy | | |  | *Opisać oferowane parametry* | | |
|  | | Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC oraz poprzez portal WWW | wymagany | | | nie dotyczy | | |  | *Opisać oferowane parametry* | | |
|  | | Zarządzanie urządzeniem przez HTTPS, SNMP i SSH za pomocą protokołów Ipv4 i Ipv6 | wymagany | | | nie dotyczy | | |  | *Opisać oferowane parametry* | | |
|  | | Możliwość filtrowania ruchu w oparciu o adresy MAC, Ipv4, Ipv6, porty TCP/UDP | wymagany | | | nie dotyczy | | |  | *Opisać oferowane parametry* | | |
|  | | Obsługa mechanizmów Port Security, Dynamic ARP Inspection, IP Source Guard, voice VLAN oraz private VLAN (lub równoważny) | wymagany | | | nie dotyczy | | |  | *Opisać oferowane parametry* | | |
|  | | Możliwość synchronizacji czasu zgodnie z NTP | wymagany | | | nie dotyczy | | |  | *Opisać oferowane parametry* | | |
|  | | **Zarządzanie i monitoring** | | | | | | | | | | |
|  | | 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 | | |  | *Opisać oferowane parametry* | | |
|  | | 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 | | |  | *Opisać oferowane parametry* | | |
|  | | Dedykowany port konsoli oraz dedykowany port zarządzający out-of-band 10/100Base-T Ethernet | wymagany | | | nie dotyczy | | |  | *Opisać oferowane parametry* | | |
|  | | 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 | | |  | *Opisać oferowane parametry* | | |
|  | | Możliwość pracy jako generator / odbiornik pakietów testowych IP SLA | wymagany | | | nie dotyczy | | |  | *Opisać oferowane parametry* | | |
|  | | Możliwość konfiguracji liczby wysyłanych pakietów UDP w ramach pojedynczej próbki oraz odstępu czasowego pomiędzy kolejnymi wysyłanymi pakietami UDP w ramach pojedynczej próbki | wymagany | | | nie dotyczy | | |  | *Opisać oferowane parametry* | | |
|  | | **Certyfikaty i Deklaracje** | | | | | | | | | | |
|  | | Deklaracja zgodności UE (certyfikat CE) potwierdzająca spełnienie wymagań dyrektywy „Nowego Podejścia”. Urządzenie musi posiadać oznakowanie CE. | wymagany | nie dotyczy | | | | |  | *Opisać oferowane certyfikaty i deklaracje* | | |
|  | | 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* | | |
|  | | 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 (Dz.U. 2015 poz.1688). Urządzenie musi być oznaczone etykietą WEEE. | wymagany | nie dotyczy | | | | |  | *Opisać oferowane certyfikaty i deklaracje* | | |
|  | ***Rozbudowa systemu ochrony stacji w zakresie szyfrowania, XDR*** | | | | | | | | | | |
|  | **Informacje ogólne** | | | | | | | | | | |
|  | Producent / Nazwa | wymagany | | | | nie dotyczy | |  | | | *Podać producenta i nazwę oprogramowania* |
|  | 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.  Nr licencji obecnie posiadanego systemu 3AA-EUD-6NC | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry* |
|  | W wyniku rozbudowy systemu o nowe moduły funkcjonalne przy zachowaniu dotychczasowej funkcjonalność 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* |
|  | Zamawiający dopuszcza wymianę istniejącego rozwiązania na rozwiązanie równoważne do istniejącego systemy 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* |
|  | Rozwiązanie musi zapewniać ochronę 150 stacji komputerowych w poniższym zakresie. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry* |
|  | **Wymagania ogólne** | | | | | | | | | | |
|  | 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 | |  | | | *Opisać oferowane parametry* |
|  | Serwer administracyjny dostępny w chmurze musi pozwalać na centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, zapora 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 | |  | | | *Opisać oferowane parametry* |
|  | 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 | |  | | | *Opisać oferowane parametry* |
|  | 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 | |  | | | *Opisać oferowane parametry* |
|  | Rozwiązanie musi zapewnić uwierzytelnianie użytkownika zanim zostanie uruchomiony system operacyjny. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry* |
|  | **XDR** | | | | | | | | | | |
|  | Automatyczna wizualizacja zdarzeń, incydentów i ataków ukierunkowanych | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Możliwość wyszukiwania zagrożeń na podstawie definiowanych filtrów | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Wbudowany zestaw reguł zapewniający reagowanie na wykryte incydenty z możliwością budowania własnych reguł oraz edycji istniejących. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | 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* |
|  | Możliwość uruchomienia reguł w oparciu o dane historyczne. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Możliwość blokowania plików po sumach kontrolnych. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Możliwość ustawiania priorytetu zdarzeń. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | 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* |
|  | Możliwość oznaczenia plików DLL jako bezpieczne, pobrania do analizy oraz ich zablokowania. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Weryfikacja uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | 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* |
|  | Możliwość bezpośredniego sprawdzenia SHA-1 pliku, na portalach służących do weryfikacji bezpieczeństwa (np. VirusTotal). | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Możliwość włączenia izolacji komputera od sieci. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | **Uwierzytelnianie wieloskładnikowe (MFA)** | | | | | | | | | | |
|  | Wbudowany serwer RADIUS umożliwiający uwierzytelnia-nie użytkowników dla rozwiązań VPN, które wspierają protokół RADIUS. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Możliwość integracji minimum z systemem operacyjnym Windows Server poprzez konsolę zarządzającą systemu operacyjnego. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | 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* |
|  | Możliwość określenia metody uwierzytelniania dwuskładnikowego użytkowników, minimum wiadomość SMS, aplikacja mobilna | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Do wysyłania wiadomości SMS nie może być wymagane posiadanie własnej bramy SMS i centrali GSM. Wysyłanie wiadomości SMS z hasłami jednorazowymi musi odbywać się z infrastruktury producenta rozwiązania. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Możliwość wysyłania wiadomości na telefony pracujące w roamingu. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Możliwość wyboru użytkowników uwierzytelniania dwuskładnikowego. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Możliwość ograniczenia dostępu przy uwierzytelnianiu metodą RADIUS do grupy użytkowników wskazanych w konfiguracji. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | 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 | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | W ramach modułu musi być zapewniony dostęp do dedykowanej aplikacji mobilnej działającej pod kontrolą Android i iOS | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | 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 | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | **Sandboxing w chmurze** | | | | | | | | | | |
|  | Wbudowany serwer RADIUS umożliwiający uwierzytelnia-nie użytkowników dla rozwiązań VPN, które wspierają protokół RADIUS. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Możliwość integracji minimum z systemem operacyjnym Windows Server poprzez konsolę zarządzającą systemu operacyjnego. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | 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* |
|  | Ochrona przed zagrożeniami 0-day. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | 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 | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Tworzenie listy wykluczeń określonych plików lub folderów z przesyłania. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Możliwość wyświetlenia listy plików, które zostały przesłane do analizy. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Możliwość analizowania plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | **Ochrona stacji roboczych** | | | | | | | | | | |
|  | Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Ochrona przed rootkitami oraz podłączeniem komputera do sieci botnet. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Umieszczenia na liście wykluczeń wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | 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 | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | 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 | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: pamięci masowych, optycznych pamięci masowych, pamięci masowych firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | 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 | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | 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 | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Automatyczna, inkrementalna aktualizacja silnika detekcji. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Skaner UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Zintegrowany moduł bezpiecznej przeglądarki. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez użytkownika. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Zintegrowany moduł kontroli dostępu do stron internetowych. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Ochrona przed zagrożeniami 0-day. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | **Ochrona serwerów** | | | | | | | | | | |
|  | Ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Skanowania dysków sieciowych typu NAS. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | 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 | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Automatyczna, inkrementalna aktualizacja silnika detekcji. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Możliwość wykluczania ze skanowania procesów. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | System zapobiegania włamaniom działający na hoście (HIPS). | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Skanowanie magazynu Hyper-V. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Skaner UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | 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 | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Ochrona przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Możliwość uruchomienia lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | **Ochrona urządzeń mobilnych** | | | | | | | | | | |
|  | 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* |
|  | Automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Możliwość skonfigurowania zaufanej karty SIM. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi usunięcie zawartości urządzenia, przywrócenie urządzenie do ustawień fabrycznych, zablokowania urządzenia, uruchomienie sygnału dźwiękowego, lokalizację GPS. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Wyświetlenie listy zainstalowanych aplikacji. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | Blokowanie aplikacji w oparciu o nazwę aplikacji, nazwę pakietu, kategorię sklepu Google Play, uprawnienia aplikacji, pochodzenie aplikacji z nieznanego źródła. | wymagany | | | | nie dotyczy | |  | | | *Opisać oferowane parametry jeżeli dotyczy* |
|  | 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* |
|  | ***Wdrożenie rozwiązań*** | | | | | | | | | | |
|  | **Instalacja i montaż** | | | | | | | | | | |
|  | 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\** |
|  | Wymagana instalacja dostarczonych urządzeń posiadających obudowę przeznaczoną do montażu stelażowego, we wskazanej przez Zamawiającego szafie RACK 19”. | wymagany | | | | nie dotyczy | |  | | | *Nie dotyczy\** |
|  | Urządzenia muszą być montowane za pośrednictwem szyn montażowych dostarczonych wraz z urządzeniami. | wymagany | | | | nie dotyczy | |  | | | *Nie dotyczy\** |
|  | Zamawiający wymaga wykonanie wszystkich połączeń urządzeń, niezbędnych do uruchomienia całości środowiska. | wymagany | | | | nie dotyczy | |  | | | *Nie dotyczy\** |
|  | Dostarczona macierz dyskowa musi być połączona z istniejącymi serwerami z wykorzystaniem portów SFP+ i przewodów światłowodowych za pośrednictwem dostarczonego przełącznika SAN. Moduły SFP+ niezbędne do realizacji połączeń należy dostarczyć w ramach zamówienia. | wymagany | | | | nie dotyczy | |  | | | *Nie dotyczy\** |
|  | Przełączniki „Enterprise” muszą być zamontowane w szafir RACK wskazanej przez Zamawiającego na etapie realizacji i podłączone.  Należy wykonać połącznia pomiędzy przełącznikami umożliwiające pracę urządzeń w trybie HA za pomocą dostarczonego okablowania.  Połączenie HA musi być również wykonane pomiędzy przełącznikami a serwerami oraz pomiędzy dostarczonymi przełącznikami a przełącznikami Mikrotik Cloud Router Switch CRS326-24S+2Q+RM zlokalizowanymi w odrębnym budynku za pośrednictwem istniejących przewodów światłowodowych.  W celu wykonania połączeń Zamawiający wymaga dostarczenia wraz z przełącznikami kompatybilnych wkładek 24 x SFP+ 10G SR oraz 24 x SFP+ 10Gbase-T | wymagany | | | | nie dotyczy | |  | | | *Nie dotyczy\** |
|  | Zamawiający wymaga instalacji dostarczonych systemów na urządzeniach wskazanych przez zamawiającego na etapie realizacji. | wymagany | | | | nie dotyczy | |  | | | *Nie dotyczy\** |
|  | **Konfiguracja** | | | | | | | | | | |
|  | Zamawiający wymaga konfiguracji macierzy dyskowej zgodnie z wytycznymi Zamawiającego dostarczonymi na etapie realizacji. | wymagany | | | | nie dotyczy | |  | | | *Nie dotyczy\** |
|  | Przełączniki SAN muszą być zainstalowany, w wskazanej przez Zamawiającego szafie RACK, podłączone za pomocą dostarczonego wraz z przełącznikiem okablowania zasilającego i FC. | wymagany | | | | nie dotyczy | |  | | | *Nie dotyczy\** |
|  | Połączenia FC pomiędzy przełącznikiem a serwerami i macierzą muszą zapewniać komunikację w układzie redundantnym.  Komunikacja musi odbywać się za pomocą kabli typu G.652d ze złączami dostosowanymi do zainstalowanych wkładek w macierzy i serwerach o długości minimum 5 metrów. | wymagany | | | | nie dotyczy | |  | | | *Nie dotyczy\** |
|  | Klaster UTM HA musi być skonfigurowany zgodnie z wytycznymi administratora Zamawiającego, z uwzględnieniem minimalnych prac:   1. konfiguracja pracy urządzeń w układzie HA 2. weryfikacja założeń wdrożenia 3. konfiguracja sieci (interfejsy i routing) 4. konfiguracja firewalla 5. konfiguracja NAT 6. konfiguracja IPS – zgodnie z wymaganiami klienta 7. konfiguracja dodatkowych usług sieciowych tj. DHCP, DNS Proxy 8. integracja z AD lub założenie wewnętrznej bazy użytkowników (bez dodawania użytkowników). 9. konfiguracja transparentnej autoryzacji w AD – konfiguracja po stronie urządzenia, inżynier nie instaluje agenta SSO a jedynie instruuje klienta jak powinna przebiegać instalacja. 10. konfiguracja VPN:  * 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.  1. konfiguracja SSL VPN lub PPTP VPN. | wymagany | | | | nie dotyczy | |  | | | *Nie dotyczy\** |
|  | Konfiguracja dostarczonych przełączników sieciowych „Enterprice” w zakresie   1. sieci VLAN, adresacji IP, interfejsów VLAN; 2. interfejsów fizycznych, funkcjonalności LACP; 3. funkcjonalności routingu; 4. stackowania przełączników; 5. polityk bezpieczeństwa, QoS, mechanizmów STP i ich bezpieczeństwa; 6. mechanizmów zarządzania urządzeniami (np. SSH, telnet, SNMP, HTTPS); 7. autoryzacji IEEE 802.1x.   Należy wykonać rekonfigurację istniejących urządzeń sieciowych (obecnie 4 przełączniki brzegowe Mikrotik 48 x 1GbE zarządzalne w warstwie 2 i 3, zamontowane w 4 szafach, spięte poprzez przełącznik szkieletowy Mikrotik 24xSFP+) poprzez jej segmentacje (rozdzielenie środowisk serwerowych, urządzeń drukujących, stacji komputerowych użytkowników w obrębie 2 budynków połączonych ze sobą) | wymagany | | | | nie dotyczy | |  | | | *Nie dotyczy\** |
|  | W zakresie rozbudowy systemu bezpieczeństwa, Wykonawca:   1. zainstaluje 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; 2. moduł XDR - należy skonfigurować i zoptymalizować reguły reagowania na incydenty oraz przygotować polityki połączeniowej i zaaplikowanie dla stacji końcowych z zainstalowanym konektorem; 3. uruchomić możliwość uwierzytelniania dwuskładnikowego MFA dla użytkowników systemu.   Dodatkowo w przypadku rozwiązania równoważnego:   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;   Zapewnienie minimum 16 godzin instruktarzu stanowiskowego dla administratorów Zamawiającego zapewniającego pełne zrozumienie administracyjnych, instalacji oprogramowania systemowego i narzędziowego, znajomości i umiejętności realizacji procedur, znajomości wytycznych polityk bezpieczeństwa, potwierdzonego protokołem z wykonania instruktarzu. | wymagany | | | | nie dotyczy | |  | | | *Nie dotyczy\** |
|  |  |  | | | |  | |  | | |  |
|  | **Dokumentacja powykonawcza** | | | | | | | | | | |
|  | Po zakończeniu realizacji, Zamawiający wymaga dostarczenia pełnej dokumentacji powykonawczej oraz procedur eksploatacji rozwiązań. Dokumentacja powykonawcza musi zawierać minimum:   1. opis ogólnych informacji o rozwiązaniach; 2. schematy połączeń urządzeń i ich adresacje; 3. zestawienie loginów i haseł do rozwiązań; 4. zestawienie ustawień wszystkich rozwiązań; 5. instrukcje instalacji, konfiguracji, uruchomienia; 6. zestawienie licencji; 7. listę autoryzowanych kontaktów serwisowych; | wymagany | | | | nie dotyczy | |  | | | *Nie dotyczy\** |

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

***Parametry oznaczone indeksem DT muszą być potwierdzone dokumentami pochodzącymi od producenta oferowanych urządzeń, zgodnie z Rozdział XI ust. 3.5 SWZ.***

*……………………………………………………………..(miejscowość)* dnia *………………………… r.*