Postępowanie numer: GUM2024ZP0105

Załącznik nr 3 do SWZ

Załącznik nr … do umowy

OPIS PRZEDMIOTU ZAMÓWIENIA

po zmianie zapisów z dnia 31.10.2024 r.

WYMAGANIA OGÓLNE

1. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej Wykonawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
2. Element systemu realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
3. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania co najmniej 9 administratorów do poszczególnych instancji systemu.
4. W ramach postępowania wymaganym jest dostarczenie licencji wsparcia dla wszystkich oferowanych urządzeń.
5. W niniejszym dokumencie przedstawiono minimalne parametry urządzeń. W przypadku, gdy nie określono, że parametr określa maksymalną wartość jest to jego wartość minimalna. Wartości te należy zawsze rozumieć jako ograniczone z bezsporną korzyścią dla Zamawiającego.
6. Przedmiot zamówienia musi pochodzić z oficjalnego kanału dystrybucyjnego producenta zaoferowanego rozwiązania.
7. Przedmiot zamówienia musi być fabrycznie nowy (wyprodukowany po 01 stycznia 2024 r.), kompletny, wolny od wszelkich wad i uszkodzeń, nigdy wcześniej nie używany i nie będący przedmiotem praw osób trzecich, dopuszczony do obrotu.

DODATKOWE WYMAGANIA:

8. Przedmiot zamówienia musi spełniać wszystkie normy stawiane takim towarom przez prawo polskie.
9. Nie dopuszcza się urządzeń typu refurbished (zwróconych do producenta i później odsprzedawanych ponownie przez producenta).
10. Urządzenia muszą być oznakowane przez producentów w taki sposób, aby możliwa była identyfikacja zarówno produktu, producenta, jak i daty produkcji.
11. Do każdego urządzenia musi być dostarczony niezbędny sprzęt eksploatacyjny (przewody zasilające, przewody sygnałowe, szyny i elementy montażowe itp.) niezbędny do uruchomienia danego urządzenia w budowanym rozwiązaniu w miejscu dostawy wskazanym przez Zamawiającego. Sprzęt, o którym mowa powyżej jest integralną częścią oferty i przechodzi na własność Zamawiającego.

12. Oferowany sprzęt musi posiadać oznakowanie CE.
13. Wszystkie dostarczane urządzenia na dzień złożenia oferty nie mogą być w fazie end-of-life (EOL) lub nie może być wskazana data wejścia urządzenia w EOL (brak wsparcia producenta lub wycofanie urządzenia z oficjalnej dystrybucji).
14. Wszystkie zestawy komputerowe, laptopy, drukarki oraz sprzęt zasilany przez zasilacze pośrednie muszą współpracować z siecią energetyczną o parametrach: 230V±10%, 50Hz.
15. Zamawiający wymaga, aby wszystkie dostarczane urządzenia i pakiety oprogramowania były sprawdzone w praktyce rynkowej. Oznacza to, iż oprogramowanie systemowe (firmware urządzeń) realizujące wszystkie wymagane funkcje jak też samo urządzenie musiało być dostępne na rynku co najmniej 6 miesięcy przed terminem składania ofert.
16. Urządzenie i powiązane z nim oprogramowanie systemowe musi być objęte pełnym serwisem producenta w chwili, i co najmniej w okresie 6 miesięcy przed złożeniem ofert. Niedopuszczalne jest proponowanie oprogramowanie np. w wersji Beta. Za datę jego dostępności Zamawiający przyjmuje publikację konkretnej oferowanej wersji oprogramowania (wersji z pełnym wsparciem) na stronie Producenta rozwiązania.
17. Zamawiający wymaga, aby zaoferowane urządzenia były dostępne i serwisowane przez Producenta oraz nie będą przez niego przewidziane do wycofania ze sprzedaży i wsparcia (ogłoszone tzw. dokumenty End-of-Sale lub End-of-Life lub równoważne) - na dzień składania oferty.

LP.	OPIS WYMAGANEGO PARAMETRU:
I.	**Wymagania ogólne dotyczące wszystkich elementów systemu**
1.	Gwarancja i wsparcie: a. Wszystkie urządzenia zostaną objęte serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości; b. W ramach tego serwisu producent zapewnia również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7;
2.	Zasilanie – dwa redundantne zasilacze AC 240V
3.	Realizacja sprzętowa lub programowa
4.	Zarządzanie - Interfejs – GUI, shell & API
5.	Dostarczone urządzenia umożliwiają ich montaż w szafie rack 19”. Wraz z urządzeniami wykonawca dostarczy wszystkie niezbędne elementy montażowe.
6.	Udzielenie wsparcia przy wdrożeniu inżyniera w wymiarze 30 godzin przez okres roku od dostarczenia przedmiotu zamówienia (1 roboczogodzina = 60 minut)
II.	**Zapora UTM:**
1.	System realizujący funkcję firewall udostępnia możliwość pracy w jednym z trzech trybów: router z funkcją NAT, transparentnym i monitorowania na porcie SPAN
2.	System wspiera protokoły IPv4 oraz IPv6 w zakresie: firewall, ochrony w warstwie aplikacji oraz protokołów routingu dynamicznego;
3.	System dostarczony w formie klastra składającego się z dwóch urządzeń, umożliwiający tryb pracy Active-Active lub Active-Passive dla ról firewall, IPsec, kontrola aplikacji oraz IPS z funkcją synchronizacji sesji firewall; awaria jednego z urządzeń nie wywiera negatywnego wpływu na działanie klastra

Postępowanie numer: GUM2024ZP0105

4.	System umożliwia wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych oraz monitoring stanu realizowanych połączeń VPN
5.	System realizujący funkcję firewall dysponuje minimum: 16 portami Gigabit Ethernet (RJ-45), 8 gniazdami SFP, 4 gniazdami SFP+ i 4 gniazdami SFP28 oraz umożliwia agregację połączeń (statyczną oraz w oparciu o protokół LACP) i tworzenie interfejsów redundantnych
6.	System posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB
7.	W ramach systemu firewall istnieje możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych – definiowanych jako VLAN-y w oparciu o standard 802.1Q
8.	Parametry wydajnościowe: a. Obsługa nie mniej niż 16 milionów jednoczesnych połączeń oraz 720 tysięcy nowych połączeń na sekundę w zakresie usługi firewall; b. Przepustowość Statefull Firewall nie mniejsza niż 163Gbps dla pakietów 512B; c. Przepustowość Firewall przy włączonej funkcji Kontroli Aplikacji nie mniejsza niż 74Gbps; d. Wydajność szyfrowania IPSec VPN nie mniej niż 55Gbps; e. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla typowego ruchu z włączonymi aplikacjami nie mniej niż 26 Gbps; ~~f.~~ f. Wydajność skanowania ruchu z włączonymi funkcjami: IPS, Application Control, Antywirus nie mniej niż 20 Gbps", z zastrzeżeniem, iż wydajność skanowania ruchu z włączonymi funkcjami IPS i Application Control nie będzie mniejsza niż 22 Gbps. ~~Wydajność skanowania ruchu z włączonymi funkcjami: IPS, Application Control, Antywirus nie mniej niż 22 Gbps;~~ g. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http minimum 16Gbps;
9.	System umożliwia realizację następujących funkcji bezpieczeństwa: a. Kontrola dostępu – zapora ogniowa klasy Statefull Inspection; b. Kontrola aplikacji; c. Poufność transmisji danych – szyfrowane połączenia IPSec VPN oraz SSL VPN; d. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP/HTTPS oraz FTP; e. Ochrona przed atakami – Intrusion Prevention System; f. Kontrola dostępu do stron WWW; g. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3; h. Zarządzenia pasmem (QoS, Traffic shaping); i. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP); j. Dwuskładnikowe uwierzytelnienie z wykorzystaniem tokenów (sprzętowych lub programowych); k. Analiza ruchu szyfrowanego z wykorzystaniem protokołów SSL i SSH;
10.	Zapora ogniowa umożliwia: a. Tworzenie polityk uwzględniających adresy IP, użytkowników, protokoły, usługi sieciowe aplikacje lub ich zbiory, reakcje zabezpieczeń rejestrowanie zdarzeń; b. Translację adresów NAT: źródłowego i docelowego, translację PAT oraz translację jeden do jeden oraz jeden do wielu; c. Tworzenie wydzielonych stref bezpieczeństwa np.: DMZ, LAN, WAN; d. Integrację z rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych w celu wykorzystania ich przy budowaniu polityk kontroli dostępu dla: Amazon Web Services, Microsoft Azure, Google Cloud Platform, OpenStack i Vmware vCenter;

Postępowanie numer: GUM2024ZP0105

11.	System umożliwia konfigurację połączeń typu IPSec VPN i cechuje się funkcjami: a. Wsparcie dla IKE v1 oraz v2; b. Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode (GCM); c. Obsługa protokołu Diffie-Hellman grup 19 i 20; d. Wsparcie dla pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE; e. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site; f. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności; g. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego; h. Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth; i. Mechanizm „Split tunneling" dla połączeń Client-to-Site;
12.	System umożliwia konfigurację połączeń typu SSL VPN i cechuje się funkcjami: a. Praca w trybie Portal, w którym dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki internetowej; system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0; b. Praca w trybie Tunnel z możliwością włączenia funkcji Split tunneling przy zastosowaniu dedykowanego klienta; c. Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN;
13.	W zakresie routingu rozwiązanie zapewnia obsługę: a. Routingu statycznego; b. Policy Based routingu; c. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.;
14.	W zakresie zarządzania pasmem zapora umożliwia: a. Określenie maksymalnej, gwarantowanej ilości pasma, oznaczenie DSCP oraz wskazania priorytetu ruchu; b. Określenie pasma dla poszczególnych aplikacji; c. Zarządzanie pasmem dla wybranych kategorii URL;
15.	Rozwiązanie zapewnia ochronę przed malware: a. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021); b. System umożliwia skanowanie archiwów, minimum ZIP oraz RAR; c. System dysponuje sygnaturami do ochrony urządzeń mobilnych, minimum dla systemu operacyjnego Android; d. System współpracuje z dostarczoną platformą typu Sandbox; wymagania dotyczące platformy zostały opisane w dalszej części dokumentu; e. System umożliwia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików;
16.	System zapewnia ochronę przed atakami, w tym: a. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych; b. System chroni przed atakami na aplikacje pracujące na niestandardowych portach; c. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora;

	d. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur; e. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS; f. Mechanizmy ochrony dla aplikacji Webowych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz zapewnia możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies; g. Wykrywanie i blokowanie komunikacji C&C do sieci botnet;
17.	System zapewnia kontrolę aplikacji, realizowaną poprzez: a. Kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP; b. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora; c. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików; d. Baza zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P; e. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur;
18.	Rozwiązanie umożliwia kontrole WWW, w szczególności: a. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne; b. W ramach filtra www są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy; c. Filtr WWW dostarcza kategorię stron zabronionych prawem: Hazard; d. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL; e. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo; f. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania; g. W ramach systemu istnieje możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji;
19.	System umożliwia weryfikację tożsamości w ramach sesji za pomocą: a. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu; b. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP; c. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych; d. Jest możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego; e. Rozwiązanie umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API;
20.	Zarządzaniem rozwiązaniem odbywa się poprzez: a. Elementy systemu bezpieczeństwa dające możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i dające możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania; b. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów; c. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego;

Postępowanie numer: GUM2024ZP0105

	d. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow; e. System ma możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację; f. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall;
21.	Rozwiązanie umożliwia logowanie i raportowanie zdarzeń poprzez: a. Logowanie do dostarczonego w ramach postępowania systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej; b. W ramach logowania system pełniący funkcję Firewall zapewnia przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Została zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania; c. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu; d. Istnieje możliwość logowania do serwera SYSLOG;
22.	W ramach postępowania zostaną dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów, obejmujące kontrolę aplikacji, IPS, antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), analiza typu sandbox, antyspam;
23.	System jest objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent zapewnia również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7, a także subskrypcję;
IV	**System logowania**
1.	System logowania, raportowania i korelacji, umożliwia centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach infrastruktury zabezpieczeń
2.	Rozwiązanie zostanie dostarczone w postaci komercyjnej platformy sprzętowej lub programowej. W przypadku implementacji programowej dostawca zapewnia niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym
3.	System jest w stanie przyjmować minimum 200GB logów dziennie
4.	System jest w stanie przeanalizować minimum 4000 logów na sekundę
5.	System umożliwia gromadzenie logów z co najmniej 800 systemów/urządzeń
6.	System umożliwia przeglądanie zbieranych logów w czasie rzeczywistym
7.	System umożliwia przeglądanie zgromadzonych logów z funkcją filtrowania
8.	System umożliwia dostosowanie widoku wyświetlanych logów przez dodanie, usunięcie oraz zmianę kolejności kolumn zawierających elementy logowanych zdarzeń
9.	System musi prezentować informacje na temat ilości przestrzeni dyskowej wykorzystywanej na przechowywanie logów
10.	System oferuje konfigurację oraz predefiniowane raporty graficzne lub tekstowe obrazujące stan pracy urządzenia UTM oraz ogólne informację dotyczące statystyk ruchu sieciowego oraz zdarzeń bezpieczeństwa na przestrzeni wskazanego wycinka czasu. Raporty obejmują: a. listę najczęściej wykrywanych ataków; b. listę najbardziej aktywnych użytkowników lub innych źródeł ruchu sieciowego;

	c. listę najczęściej wykorzystywanych aplikacji; d. listę najczęściej odwiedzanych stron www; e. listę krajów, do których nawiązywane są połączenia; f. listę najczęściej wykorzystywanych polityk Firewall; g. informację o realizowanych połączeniach IPSec oraz SSL VPN; h. listę najczęściej występujących zdarzeń systemowych.
11.	Rozwiązanie posiada możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych za pomocą protokołu Syslog i/lub CEF (ang. Common Event Format). System w tym zakresie zapewnia mechanizm filtrowania przesyłanych logów;
12.	System umożliwia cykliczny eksport logów do zewnętrznego systemu w celu przechowywania długoterminowego. Eksport logów jest możliwy z wykorzystaniem protokołu SFTP i/lub SCP. System ma możliwość, kiedy i w jaki sposób ma następować eksport logów;
13.	System zapewnia co najmniej możliwość komunikacji z innymi systemami przesyłającymi logi na portach UDP/514 oraz TCP/514;
14.	W zakresie raportowania system zapewnia: a. generowanie raportów co najmniej w formatach: CSV, HTML, PDF; b. predefiniowane zestawy raportów, w których administrator systemu może modyfikować parametry prezentowanych wyników; c. możliwość definiowania własnych raportów; d. możliwość spolszczenia raportów; e. generowania raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesyłania wyników na określony adres lub adresy email, oraz do automatycznego przesyłania raportu na zewnętrzy serwer za pomocą protokołów SFTP i SCP; f. możliwość automatycznego usuwania raportów po określonym czasie;
15.	W zakresie korelacji zdarzeń system zapewnia: a. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany; b. Możliwość tworzenia własnych reguł korelowania logów; c. Możliwość konfiguracji powiadomień: email, SNMP i API w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa. W treści powiadomienia jest możliwość przekazania informacji o tym jakie zdarzenie wywołało powiadomienie, np. Nazwa wykrytego zagrożenia; d. System koreluje zdarzenia co najmniej dla następujących kategorii: • Malware/AV, • Aplikacje sieciowe, • Email, • IPS, • Web Filter, • Traffic (logi z ruchu sieciowego), • Systemowe (m.in. utracone połączenie VPN, utracone połączenie sieciowe, zdarzenia związane z klastrem niezawodnościowym, zmiana w sieci SD-WAN); e. Możliwość automatycznego, zwrotnego powiadomienia systemu bezpieczeństwa NGFW o wystąpieniu wybranych zdarzeń korelacji na podstawie wskaźników kompromitacji (IoC);

16.	Zarządzanie systemem: a. System logowania i raportowania zapewnia możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania dostarcza dedykowaną konsolę zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów; b. Proces uwierzytelniania administratorów jest realizowany w oparciu o: lokalną bazę, Radius, LDAP, TACACS+, PKI; c. System umożliwia definiowanie co najmniej 8 administratorów z możliwością określenia praw dostępu do wybranych modułów systemu logowania i raportowania; d. System ma możliwość podziału na wirtualne systemy logowania i raportowania (konteksty/domeny). Istnieje możliwość przypisywania administratorom praw dostępu do wybranych kontekstów. Dla każdego kontekstu jest możliwość niezależnego przydzielania zasobów dyskowych oraz określania maksymalnego czasu przechowywania logów;
17.	System dysponuje co najmniej: a. 4 portami Gigabit Ethernet RJ-45; b. 2 portami Gigabit Ethernet SFP;
18.	Rozwiązanie dysponuje powierzchnią dyskową min. 16 TB;
19.	System ma możliwość konfiguracji RAID, minimum 0, 1 lub 10, w celu zabezpieczenia danych w przypadku awarii dysku;
20.	Gwarancja oraz wsparcie: System jest objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
V	**Rozwiązanie typy Sandbox**
1.	Urządzenie wykorzystuje technologię piaskownicy (sandbox) do izolowania i analizy podejrzanych plików i aplikacji w wirtualnym środowisku, chroniąc tym samym sieć przed infekcjami i włamaniami;
2.	System składa się z jednego lub kilku elementów zapewniając opisany poniżej zestaw funkcji;
3.	System umożliwia skanowanie plików zarchiwizowanych (.7z, .ace, .arj, .bz2, .gz, .iso, .jar, .kgb, .lzh, .rar, .swf, .tar, .tgz, .upx, .xz, .z, .zip), wykonywalnych (.exe, .dll, .msi), PDF, Microsoft Office Document, Javascript, AdobeFlash oraz JavaArchive (JAR);
4.	System umożliwia analizę plików powyżej 200MB;
5.	System umożliwia skanowanie zasobów sieciowych SMB/NFS oraz kwarantanny podejrzanych plików;
6.	System umożliwia przesyłanie do analizy plików oraz adresów URL;
7.	System umożliwia szczegółowe raportowanie charakterystyki badanego pliku oraz zachowania: modyfikacji plików w systemie, zachowania uruchomionych procesów, zmian w rejestrze, zachowania sieci. System musi posiadać funkcję generowania raportu z tego zachowania;
8.	System pozwala na analizę min. 10 000 plików na godzinę przy włączonej funkcji prefilteringu, skanowania statycznego oraz dynamicznego;
9.	System umożliwia jednoczesne uruchomienie 10 maszyn wirtualnych w celu analizy różnych próbek oraz analizy behawioralnej;
10.	System umożliwia wgrywanie własnych obrazów systemów operacyjnych;
11.	System realizuje jednoczesną analizę próbek na obrazach/maszynach wirtualnych następujących systemów operacyjnych: a. Co najmniej na 4 maszynach wirtualnych z systemem operacyjnym Windows 10; b. Co najmniej na 4 maszynach wirtualnych z systemem operacyjnym Windows 11;
12.	System realizuje jednoczesną analizę próbek będących dokumentami pakietu Microsoft Office na 4 dedykowanych maszynach wirtualnych, których rodzaje wymieniono w punkcie powyżej;
13.	Wymagane jest dostarczenie niezbędnych licencji dla systemów Microsoft Windows oraz Microsoft Office wymienionych w punktach 11 oraz 12;

Postępowanie numer: GUM2024ZP0105

14.	System umożliwia skanowanie plików na obrazach Android oraz Linux;
15.	System umożliwia analizę w systemach Microsoft Windows: a. sprawdzenie procesów i rejestru; b. sprawdzanie połączenie z Botnet C&C oraz złośliwymi URL; c. sprawdzenie pakietów sieciowych przeprocesowanych przez maszynę wirtualną; d. sprawdzenie działań przeprowadzony przez badane oprogramowania oraz zrzuty ekranu z badanej maszyny wirtualnej;
16.	W ramach postępowania zostaną dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji skanujących oraz analitycznych w okresie obowiązywania gwarancji;
17.	System pozwala na analizę w maszynach wirtualnych minimum 500 plików na godzinę;
18.	System umożliwia interakcję z badaną próbką przez dostęp do konsoli wirtualnej maszyny uruchomionej na potrzeby analizy. Funkcjonalność dostępna przy uruchamianiu skanowania próbki z poziomu interfejsu Webowego Interfejsu Systemu;
19.	Dostęp do analizowanych plików w celu dodatkowego badania: przykładowe pliki, logi z analizy (tracer), zapis pakietów pcap;
20.	System udostępnia interfejs API umożliwiający integracje np. z systemem SIEM lub zgłoszeniowym;
21.	System umożliwia dodanie sum kontrolnych plików do białej lub czarnej listy;
22.	System umożliwia jednokrotne logownaie (Single Sign-On) przez SAML;
23.	System powinien ma możliwość integracji z regułami YARA;
24.	Urządzenie posiada 4 porty Gigabit Ethernet RJ-45 z obsługą agregacji w celi zwiększenia przepustowości i redundancji;
25.	Urządzenie jest wyposażone w przynajmniej jeden dysk o pojemności minimum 960GB;
26.	Licencje upoważniające do korzystania z aktualnych baz funkcji skanujących oraz analitycznych (tzw. threat intelligence) obejmują okres minimum 36 miesięcy;
27.	Bazy sygnatur wykorzystywanych przez funkcje skanujące są systematycznie aktualizowane;
28.	W ramach postępowania zostaną dostarczone licencje niezbędne do uruchomienia wszystkich wymaganych maszyn wirtualnych;