Załącznik nr 1 do Specyfikacji Warunków Zamówienia - opis przedmiotu zamówienia (OPZ).

Biblioteka taśmowa – 1 sztuka

Informacje ogólne	- Dostarczone urządzenie i użyte części powinny być fabrycznie nowe, pochodzące z oficjalnego kanału dystrybucji w Polsce. - Urządzenie i napęd taśmowy powinny być wyprodukowane przez tego samego producenta.
Obudowa	- Urządzenie musi być przystosowane do montażu w szafie 19” - Wysokość urządzenia ma wynosić maksymalnie 1U
Napęd	- Zaoferowane urządzenie musi posiadać jeden napęd LTO8 połówkowej wysokości z interfejsem SAS, z mechanizmem automatycznie dostosowującym prędkość przesuwu taśmy magnetycznej do wartości strumienia danych przekazywanego do napędu. - Urządzenie musi być wyposażone w automatyczny układ dla przenoszenia kaset z taśmami LTO pomiędzy slotami a napędem oraz czytnik kodów kreskowych.
Interfejsy	Urządzenie musi posiadać minimum jeden interfejs SAS.
Liczba slotów	Zaoferowane urządzenie musi posiadać sloty na 9 kaset LTO z możliwością zdefiniowania 1 slotu wejścia-wyjścia.
Taśmy	Do biblioteki powinny być dołączone 3 sztuki taśm LTO8 z kodami kreskowymi oraz 1 kaseta czyszcząca LTO.
Wymagania funkcjonalne	- Urządzenie musi umożliwiać zarządzanie zdalne poprzez interfejs przeglądarki www (GUI) oraz lokalnie poprzez panel sterujący z wyświetlaczem LCD. Dla potrzeb zarządzania, obsługi SNMP oraz powiadomień e-mail biblioteka musi być wyposażona w co najmniej 1 port 10/100/1000 Mbps Ethernet. - Urządzenie musi umożliwiać szyfrowanie danych i musi być kompatybilne z oprogramowaniem do zarządzania kluczami szyfrującymi Guardium Key Lifecycle Manager. - Urządzenie musi wspierać systemy operacyjne: Windows Server 2016 i nowsze, Red Hat 7,8,9, SLES 12 i 15, Ubuntu LTS 18 i 20.
Zasilanie	Urządzenie musi posiadać minimum jeden zasilacz.
Szyny montażowe i okablowanie	- Zestaw do montażu w szafie RACK, - Wraz z urządzeniem musi być dostarczony kabel SAS ze złączami miniSAS-miniSAS HD o długości nie mniejszej niż 3m.
Warunki Gwarancji	Dla oferowanego urządzenia wymagana jest gwarancja na okres 36 miesięcy ze zgłaszaniem awarii w trybie 24x7 i reakcją tego samego dnia.

Przełącznik sieciowy (switch) – 2 sztuki

Ilość i typ portów przełącznika (obudowa/chassis)	- Przełącznik wyposażony w minimum 20 portów 10 Gb/s (SFP+) oraz minimum 4 porty 10 Gb/s Base-T. - Dostarczony z szynami rack umożliwiającym zamontowanie w standardowej szafie 42U.
Interfejs użytkownika	- Web oraz CLI. - Wsparcie dla łączności przez SSH, SSH-2, HTTP, HTTPS, Telnet.
Wsparcie łączenia w stosy	Możliwość konfigurowania i zarządzania wszystkimi przełącznikami w stosie jako pojedynczą jednostką, z jednym adresem IP. Możliwość łączenia minimum 8 przełączników w stos.
Zdolność przełączania	Nie mniej niż 480 Gb/s
Wymagania sprzętowe	- Minimum 512 MB pamięci flash - Minimum 1GB pamięci RAM - Procesor ARM z taktowaniem minimum 1,4 GHz
Kontrola dostępu i bezpieczeństwo	- Wsparcie dla RADIUS, TACACS+, Secure Shell v.2 (SSH2) - Wsparcie dla protokołu 802.1x - Wsparcie dla Secure Core Technology (SCT), zabezpieczenia źródła IP, Secure Copy (SCP), Secure Sensitive Data (SSD)
Realizowane funkcje	- Link Aggregation Group (LAG) - z rozszerzeniem wspierającym agregację interfejsów wielu urządzeń/przełączników). - Obsługa ramek Jumbo 9KB - Wsparcie dla SNMP 1, RMON, SNMP 3,SNMP 2c, TFTP, ICMP, DHCP, RSTP - Multicast VLAN Registration (MVR) - IGMP Snooping - Voice Services Discovery Protocol (VSDP) - Link Layer Discovery Protocol (LLDP) - Access Control List (ACL) - Quality of Service (QoS) - DHCP Relay
VLAN	- Wsparcie dla minimum 4093 VLAN-ów jednocześnie - VLAN do zarządzania - Dynamiczne przydzielanie sieci VLAN za pośrednictwem serwera RADIUS wraz z uwierzytelnianiem klienta - Private VLAN Edge (PVE) - Auto surveillance VLAN (ASV)

Zgodność z normami	IEEE 802.3 10BASE-T Ethernet, , IEEE 802.3z, IEEE 802.1D (STP, GARP, and GVRP), IEEE 802.1Q/p VLAN, IEEE 802.3ab 1000BASE-T Gigabit Ethernet, IEEE 802.3x Flow Control, IEEE 802.3ad (LACP), IEEE 802.1w Rapid STP, IEEE 802.1X Port Access Authentication, IEEE 802.3ae 10 Gbps Ethernet over fiber for LAN, IEEE 802.1ab (LLDP), IEEE 802.3an 10GBASE-T 10 Gbps Ethernet over copper twisted pair cable, IEEE 802.3az Energy Efficient Ethernet
Wsparcie techniczne i gwarancja	- 5-letnia gwarancja producenta. - Czas reakcji w miejscu instalacji - kolejny dzień roboczy - Wsparcie techniczne realizowane przez serwis producenta

Przełącznik sieciowy (switch) – 1 sztuka

Ilość i typ portów przełącznika (obudowa/chassis)	- Przełącznik wyposażony w minimum 24 portów Base-T 10/100/1000 Mb/s oraz minimum 4 porty 10 Gb/s (SFP+). - Dostarczony z szynami rack umożliwiającym zamontowanie w standardowej szafie 42U.
Interfejs użytkownika	- Web oraz CLI. - Wsparcie dla łączności przez SSH, SSH-2, HTTP, HTTPS, Telnet.
Wsparcie łączenia w stosy	Możliwość konfigurowania i zarządzania wszystkimi przełącznikami w stosie jako pojedynczą jednostką, z jednym adresem IP. Możliwość łączenia minimum 8 przełączników w stos.
Zdolność przełączania	Nie mniej niż 128 Gb/s
Wymagania sprzętowe	- Minimum 512 MB pamięci flash - Minimum 1GB pamięci RAM - Procesor ARM z taktowaniem minimum 1,4 GHz
Kontrola dostępu i bezpieczeństwo	- Wsparcie dla RADIUS, TACACS+, Secure Shell v.2 (SSH2). - Wsparcie dla protokołu 802.1x. - Wsparcie dla Secure Core Technology (SCT), zabezpieczenia źródła IP, Secure Copy (SCP), Secure Sensitive Data (SSD)
Realizowane funkcje	- Link Aggregation Group (LAG) - z rozszerzeniem wspierającym agregację interfejsów wielu urządzeń/przełączników) - Obsługa ramek Jumbo 9KB - Wsparcie dla SNMP 1, RMON, SNMP 3,SNMP 2c, TFTP, ICMP, DHCP, RSTP - Multicast VLAN Registration (MVR) - IGMP Snooping - Voice Services Discovery Protocol (VSDP) - Link Layer Discovery Protocol (LLDP) - Access Control List (ACL) - Quality of Service (QoS) - DHCP Relay
VLAN	- Wsparcie dla minimum 4093 VLAN-ów jednocześnie - VLAN do zarządzania - Dynamiczne przydzielanie sieci VLAN za pośrednictwem serwera RADIUS wraz z uwierzytelnianiem klienta - Private VLAN Edge (PVE) - Auto surveillance VLAN (ASV)
Zgodność z normami	IEEE 802.3 10BASE-T Ethernet, , IEEE 802.3z, IEEE 802.1D (STP, GARP, and GVRP), IEEE 802.1Q/p VLAN, IEEE

	802.3ab 1000BASE-T Gigabit Ethernet, IEEE 802.3x Flow Control, IEEE 802.3ad (LACP), IEEE 802.1w Rapid STP, IEEE 802.1X Port Access Authentication, IEEE 802.3ae 10 Gbps Ethernet over fiber for LAN, IEEE 802.1ab (LLDP), IEEE 802.3an 10GBASE-T 10 Gbps Ethernet over copper twisted pair cable, IEEE 802.3az Energy Efficient Ethernet
Wsparcie techniczne i gwarancja	- 5-letnia gwarancja producenta. - Czas reakcji w miejscu instalacji - kolejny dzień roboczy. - Wsparcie techniczne realizowane przez serwis producenta.

Przełącznik sieciowy (switch) – 1 sztuka

Ilość i typ portów przełącznika (obudowa/chassis)	- Przełącznik wyposażony w minimum 48 portów Base-T 10/100/1000 Mb/s oraz minimum 4 porty 10 Gb/s (SFP+). - Dostarczony z szynami rack umożliwiającym zamontowanie w standardowej szafie 42U.
Interfejs użytkownika	- Web oraz CLI. - Wsparcie dla łączności przez SSH, SSH-2, HTTP, HTTPS, Telnet.
Wsparcie łączenia w stosy	Możliwość konfigurowania i zarządzania wszystkimi przełącznikami w stosie jako pojedynczą jednostką, z jednym adresem IP. Możliwość łączenia minimum 8 przełączników w stos.
Zdolność przełączania	Nie mniej niż 176 Gb/s
Wymagania sprzętowe	- Minimum 512 MB pamięci flash - Minimum 1GB pamięci RAM - Procesor ARM z taktowaniem minimum 1,4 GHz
Kontrola dostępu i bezpieczeństwo	- Wsparcie dla RADIUS, TACACS+, Secure Shell v.2 (SSH2). - Wsparcie dla protokołu 802.1x. - Wsparcie dla Secure Core Technology (SCT), zabezpieczenia źródła IP, Secure Copy (SCP), Secure Sensitive Data (SSD)
Realizowane funkcje	- Link Aggregation Group (LAG) - z rozszerzeniem wspierającym agregację interfejsów wielu urządzeń/przełączników) - Obsługa ramek Jumbo 9KB - Wsparcie dla SNMP 1, RMON, SNMP 3,SNMP 2c, TFTP, ICMP, DHCP, RSTP - Multicast VLAN Registration (MVR) - IGMP Snooping - Voice Services Discovery Protocol (VSDP) - Link Layer Discovery Protocol (LLDP) - Access Control List (ACL) - Quality of Service (QoS) - DHCP Relay
VLAN	- Wsparcie dla minimum 4093 VLAN-ów jednocześnie - VLAN do zarządzania - Dynamiczne przydzielanie sieci VLAN za pośrednictwem serwera RADIUS wraz z uwierzytelnianiem klienta - Private VLAN Edge (PVE) - Auto surveillance VLAN (ASV)

Zgodność z normami	IEEE 802.3 10BASE-T Ethernet, , IEEE 802.3z, IEEE 802.1D (STP, GARP, and GVRP), IEEE 802.1Q/p VLAN, IEEE 802.3ab 1000BASE-T Gigabit Ethernet, IEEE 802.3x Flow Control, IEEE 802.3ad (LACP), IEEE 802.1w Rapid STP, IEEE 802.1X Port Access Authentication, IEEE 802.3ae 10 Gbps Ethernet over fiber for LAN, IEEE 802.1ab (LLDP), IEEE 802.3an 10GBASE-T 10 Gbps Ethernet over copper twisted pair cable, IEEE 802.3az Energy Efficient Ethernet
Wsparcie techniczne i gwarancja	- 5-letnia gwarancja producenta. - Czas reakcji w miejscu instalacji - kolejny dzień roboczy. - Wsparcie techniczne realizowane przez serwis producenta.

Zasilacz UPS 15 kVA – 1 sztuka

Minimalne wymagania techniczne	- Moc znamionowa jednostki nie mniej niż 15000VA / 15000W - Technologia Podwójnej konwersji (online) - Temperatura eksploatacji 0 - 40 °C - Wilgotność względna podczas pracy 0 - 95 % - Wysokość n.p.m. podczas pracy 0-3000 m - Hałas słyszalny w odległości 1 m od powierzchni urządzenia 58,0 dBA - Rozpraszanie ciepła w trybie online ≤ 3821,00 BTU/h - Sprawność: praca on-line ≥ 94,7% przy pełnym obciążeniu - Klasa ochrony IP 20 - Klasa energetyczna sprzętu przeciwprzepięciowego 600J
Parametry wejściowe	- Nominalne napięcie wejściowe 230V, 400V 3PH - Częstotliwość wejściowa 38–72 Hz (wykrywanie automatyczne) - Typ gniazda wejściowego: Hard wire 3-wire (1P + N + E), Hard wire 5 wire (3P + N + E) - Zmienny zakres napięcia wejściowego w trybie podstawowym 160 – 285V, 100 – 160V (połowa obciążenia) - Inne napięcia wejściowe 220, 240, 380, 415 V (nastawa z wyświetlacza)
Parametry wyjściowe	- Napięcie wyjściowe 230VAC - Możliwość konfiguracji znamionowego trójfazowego napięcia wyjściowego 400 V - Zniekształcenia napięcia wyjściowego ≤5% - Częstotliwość na wyjściu (zsynchronizowana z siecią zasilającą) 50/60Hz ± 4 Hz - Inne napięcia wyjściowe 220, 240, 380, 415 V - Współczynnik szczytu 3:1 - Typ przebiegu sinusoida - Złącza wyjściowe: - 1 szt. IEC 320 C19 - 1 szt. Hard wire 5-wire (3P + N + E) - Układ obejściowy (bypass) wewnętrzny tor obejściowy (automatyczny lub ręczny)
Akumulatory i czas podtrzymania	- Typ akumulatora bezobsługowy szczelny akumulator kwasowo-ołowiowy z elektrolitem w postaci żelu - Czas autonomii z jednym dodatkowym modułem akumulatorowym: - 15 minut 57 sekund dla pełnego obciążenia - 37 minut dla połowy obciążenia - Typowy czas ładowania 4 godziny - Oczekiwana żywotność akumulatora (lata) 3 – 5 - Rozszerzalny czas podtrzymania za pomocą dodatkowych modułów

	- Baterie wymieniane na gorąco - Opcje przedłużonego podtrzymania zasilania: do 4 zewnętrznych modułów bateryjnych
Komunikacja i zarządzanie	- (Smart Slot x1) Wbudowana karta sieciowa WEB/SNMP obsługująca protokoły komunikacyjne: IP v.6, SNMP v.3, Modbus TCP, HTTPS/SSL, SSH z kluczem do 2048 bit, SMTP, NTP, FTP, Telnet - Port uniwersalny do podłączenia np. czujnika temperatury - Porty komunikacyjne: RJ-45, RS-232, 10/100 Base-T ,USB - Panel sterowania: wielofunkcyjna konsola sterownicza i informacyjna LCD - Alarm dźwiękowy: alarmy dźwiękowe i wizualne według priorytetu ważności zdarzenia - Awaryjny wyłącznik zasilania (EPO)
Parametry fizyczne	- Możliwość zastosowania w wersji wolnostojącej i do montażu w szafie przemysłowej (szyny do montażu opcjonalnie). - Wysokość w szafie: 7U
Certyfikaty, zgodności oraz gwarancja	- CE, Znak CE, CB, EAC, EN/IEC 62040-1, EN/IEC 62040-2, EN/IEC62040-3, EN/IEC 61000-4-2, IRAM, RCM, VDE - 3 lata gwarancji naprawy lub wymiany (bez akumulatora) i 2 lata na akumulatory
Oprogramowanie	Dostępne oprogramowanie do zarządzania/monitorigu (niektóre wersje odpłatne) z VMware® ESXi (VMware® ESXi Server 6.5 Update 3 (vMA 6.5), VMware® ESXi Server 6.5 Update 2 (vMA 6.5)); Microsoft® Hyper-V (Windows® Hyper-V Server 2019, 2012 R2); Windows® Server 2019, 2016, 2012; Windows® 10, 7; Red Hat® Enterprise Linux; SuSE® Linux®.
Dodatkowe parametry	- Wyświetlacz LCD musi sygnalizować stany ostrzegawcze i alarmowe poprzez zmianę koloru podświetlenia ekranu - tryb ECO - możliwość zimnego startu - możliwość pracy równoległej do 4 jednostek - automatyczny test akumulatora - automatyczne włączenie UPS-a po powrocie zasilania

Zasilacz UPS 8 kVA – 1 sztuka

Minimalne wymagania techniczne	- Moc znamionowa jednostki nie mniej niż 8000VA / 8000W - Montaż w szafie rack (wysokość: 6U) - Technologia Podwójnej konwersji (online) - Klasa VFI-SS-111 zgodnie z PN-EN62040-1 - Temperatura eksploatacji 0 - 40 °C - Wilgotność względna podczas pracy 0 - 95 % - Wysokość n.p.m. podczas pracy 0-3000 metry - Hałas słyszalny w odległości 1 m od powierzchni urządzenia 55,0dBA - Rozpraszanie ciepła w trybie online ≤1497,00 BTU/h - Sprawność: praca on-line ≥ 94% przy pełnym obciążeniu - Klasa ochrony IP 20 - Klasa energetyczna sprzętu przeciwprzepięciowego 480J
Parametry wejściowe	- Nominalne napięcie wejściowe 220 V/380 V, 230 V/400 V, 240 V/ 415 V - Częstotliwość wejściowa 40–70 Hz (wykrywanie automatyczne) - Typ gniazda wejściowego: Hard Wire 3 wire (1PH+N+G), Hard Wire 5-wire (3PH + N + G) - Zmienny zakres napięcia wejściowego w trybie podstawowym 160/277 – 275/476 VV_{AC} - połowa obciążenia 100/173 – 275/476 V_{AC} - Inne napięcia wejściowe 220, 240, 380, 415 (nastawa z wyświetlacza)
Parametry wyjściowe	- Napięcie wyjściowe 230VAC - Zniekształcenia napięcia wyjściowego ≤2% - Częstotliwość na wyjściu (zsynchronizowana z siecią zasilającą) 50/60Hz ±3Hz - Inne napięcia wyjściowe 220, 240 V - Współczynnik szczytu 3:1 - Typ przebiegu sinusoida - Złącza/gniazda wyjściowe: - 6 IEC 320 C13 (Zasilanie gwarantowane) - 4 IEC 320 C19 (Zasilanie gwarantowane) - 1 Hard wire 3-wire (H N + E) - Układ obejściowy (bypass) wewnętrzny tor obejściowy (automatyczny lub ręczny)
Akumulatory i czas podtrzymania	- Typ akumulatora bezobsługowy szczelny akumulator kwasowo-ołowiowy z elektrolitem w postaci żelu - Czas autonomii z jednym dodatkowym zestawem akumulatorów: 14 minut 42 sekundy dla pełnego obciążenia 34 minuty dla połowy obciążenia - Typowy czas ładowania 1,5 godziny - Oczekiwana żywotność akumulatora 3 – 5 lat

	- Rozszerzalny czas podtrzymania za pomocą dodatkowych modułów - Baterie wymieniane na gorąco - Opcje przedłużonego podtrzymania zasilania: do 10 zewnętrznych modułów akumulatorowych
Komunikacja i zarządzanie	- Gniazdo do montażu karty WEB/SNMP - Smart Slot x1 - Moduł WEB/SNMP obsługiwane protokoły komunikacyjne: IP v.6, SNMP v.3, HTTPS/SSL, SSH z kluczem do 2048 bit, TLS, SMTP, NTP, FTP, Telnet, Modbus TCP - Port uniwersalny do podłączenia np. czujnika temperatury (jeden czujnik temperatury dostarczyć w komplecie z UPS) - Porty komunikacyjne: RJ-45 10/100/1000 Base-T, RJ-45 Serial Port, USB, Console Port - Panel sterowania: Wielofunkcyjna konsola sterownicza i informacyjna LCD - Alarm dźwiękowy: Alarmy dźwiękowe i wizualne według priorytetu ważności zdarzenia - Awaryjny wyłącznik zasilania (EPO)
Certyfikaty, zgodności oraz gwarancja	- CE, EAC, EN/IEC 62040-1, EN/IEC 62040-2, RCM, VDE - 3 lata gwarancji naprawy lub wymiany (bez akumulatora) i 2 lata na akumulatory, z możliwością przedłużenia o 3 lata.
Oprogramowanie	Dostępne oprogramowanie do zarządzania/monitorigu (niektóre wersje odpłatne) z VMware® ESXi (VMware® ESXi Server 6.5 Update 3 (vMA 6.5), VMware® ESXi Server 6.5 Update 2 (vMA 6.5)); Microsoft® Hyper-V (Windows® Hyper-V Server 2019, 2012 R2); Windows® Server 2019, 2016, 2012; Windows® 10, 7; Red Hat® Enterprise Linux; SuSE® Linux®.
Dodatkowe parametry	- Wyświetlacz LCD musi sygnalizować stany ostrzegawcze i alarmowe poprzez zmianę koloru podświetlenia ekranu - Zasilacz UPS musi być wyposażony w sterowane programowo gniazda wyjściowe (co najmniej dwie grupy gniazd). Sterowanie gniazd musi umożliwiać sekwencyjne wyłączanie / załączanie odbiorów w zaprogramowanym interwale czasowym. Sterowanie gniazdami musi umożliwiać również powiązanie ze zdarzeniami.

Zewnętrzny moduł bateryjny UPS – 1 sztuka

Minimalne wymagania techniczne	- Montaż w szafie rack (wysokość: 4U) - Rodzaj akumulatora: kwasowo-ołowiowy - Ilość wstępnie zainstalowanych baterii: 4 - Napięcie akumulatora: 192V - 2 lata gwarancji naprawy lub wymiany

Urządzenie sieciowe NGFW – 2 sztuki

Interfejs	- Urządzenie musi posiadać interfejs WWW, z poziomu którego administrator może wykonać wszystkie czynności administracyjne - Urządzenie musi posiadać możliwość podpięcia go do systemu centralnego zarządzania i zarządzania nim poprzez dedykowaną aplikacje dostępną na urządzenia mobilne z systemem Android i IOS. - Urządzenie musi posiadać możliwość zarządzania nim z poziomu chmurowego portalu centralnego zarządzania. Dostęp do portalu chmurowego musi być dostarczony w ramach podstawowej licencji. - Z poziomu interfejsu WWW administrator musi mieć możliwość szybkiego przeglądu stanu urządzenia widząc na pierwszej stronie minimum następujące informacje: • wersja oprogramowania układowego, • nazwa urządzenia, • adres sprzętowy urządzenia, • czas pracy urządzenia od ostatniego restartu, • status sieci Internet, • ostatnio wykryte urządzenia w sieci wraz z alertami, • aktywność sieci zawierającą wykres ilości pakietów i ilości danych przepływających w czasie rzeczywistym przez urządzenie. - Urządzenie musi możliwość wyświetlenie wszystkich aktywnych urządzeń pracujących w sieci, w postaci listy dostępnej bezpośrednio z interfejsu WWW. Lista musi zawierać minimum następujące informacje: • nazwa urządzenia, • adres IP urządzenia, • adres MAC urządzenia, • typ urządzenia. - Urządzenie musi umożliwiać generowanie raportów ogólnych zawierających status urządzenia minimum w odstępach: • ostatnia godzina, • ostatni dzień, - Urządzenie musi umożliwiać generowanie raportów z aktywności użytkowników i komputerów minimum w odstępach: • ostatnia godzina, • ostatni dzień, • ostatni tydzień, • ostatni miesiąc, - Urządzenie musi zezwalać na wydruk raportów z aktywnością użytkowników bezpośrednio z poziomu interfejsu WWW rozwiązania. - Urządzenie musi umożliwiać przegląd i wyszukiwanie logów sieciowych bezpośrednio z interfejsu WWW.

	- Urządzenie musi umożliwiać przegląd i wyszukiwanie logów systemowych bezpośrednio z interfejsu WWW. - Urządzenie musi mieć możliwość wyświetlenia: • stanu zasobów sprzętowych, • tablicy routingu, • stanu połączenia z usługami chmurowymi, bezpośrednio z poziomu interfejsu WWW - Urządzenie musi posiadać funkcje pozwalające na wykonanie testów działania sieci dostępne bezpośrednio z interfejsu WWW. Wymagane są minom narzędzia takie jak: • ping, • traceroute, • dns lookup, • tcpdump, - Urządzenie musi umożliwiać wygenerowanie plików diagnostycznych z działania systemu urządzenia, bezpośrednio z interfejsu WWW. - Interfejs WWW musi umożliwiać zalogowanie się wielu administratorom jednocześnie.
Funkcje	- Urządzenie musi pracować jako sonda współpracująca raportująca do systemów minimum następujących producentów: Armis, Claroty, Medigate. - Urządzenie musi mieć możliwość pracy zarówno w trybie monitorowania, jak i w trybie inline. - Urządzenie musi być minimalnie wyposażone w następujące moduły funkcjonalne: • Firewall, • Kontrola aplikacji i URL Filtering, • Rozpoznawanie użytkowników, • QoS, • IPS, • Anti-Virus, • Anti-Bot, • Emulacja zagrożeń, • Antyspam, • VPN Site-to-Site, • VPN Client-to-Site, - Urządzenie musi mieć możliwość monitorowania dostępu do Internetu poprzez weryfikacje podanych przez administratora hostów. - Urządzenie musi monitorować minimum następujące parametry sieciowe: • Utrata pakietów, • Średnie opóźnienie, • Minimalne opóźnienie, • Maksymalne opóźnienie, • Jitter,

	- Na podstawie parametrów z punktu 4 urządzenie musi posiadać funkcjonalność SD-WAN pozwalającą na definiowanie jakie aplikacje mają używać jakiego łącza, oraz na definicje wartości granicznych po których przekroczeniu łącze będzie zmieniane. Moduł SD-WAN musi być zarządzany z poziomu interfejsu urządzenia. Niedopuszczalne jest stosowanie dodatkowej konsoli zarządzania modułem SD-WAN. - Urządzenie musi umożliwiać pełną rekonfigurację interfejsów wewnętrznych, wspierając m.in.: • Stworzenie wirtualnego switch-a z interfejsów, • Stworzenie interfejsów typu bridge, • Agregacji interfejsów m.in. za pomocą LACP. - Rozwiązanie musi posiadać moduł IoT, który wykrywa, kategoryzuje urządzenia IoT, w sieci wewnętrznej, oraz proponuje tworzenie odpowiednich reguł firewall-a dla wykrytych urządzeń. - Moduł IoT musi wykrywać próby połączeń z adresami IP w sieci Internet, niezgodne z wzorcem dla danego typu urządzenia IoT - Moduł IoT musi być zarządzany z poziomu interfejsu urządzenia. Niedopuszczalne jest stosowanie dodatkowej konsoli zarządzania modułem IoT. - Urządzenie musi mieć możliwość filtrowania ruchu sieciowego poprzez filtrowanie adresów MAC. - Urządzenie musi posiadać mechanizm DNS Proxy. - Urządzenie musi posiadać możliwość ograniczenia dostępu administracyjnego tylko z konkretnych podsieci, oraz tylko z konkretnych stref. - Urządzenie musi mieć możliwość synchronizacji czasu poprzez protokół NTP. - Urządzenie musi mieć możliwość uruchomienia serwera NTP bezpośrednio na urządzeniu. - Urządzenie musi wspierać serwisy DDNS, minimum: • DynDNS • no-ip.org - Urządzenie musi posiadać funkcję pozwalającą na zarządzenie urządzeniem z sieci Internet, nawet jeśli znajduje się za NAT-em. Funkcja ta nie może wymagać od administratora uruchomienia tunelu VPN do sieci wewnętrznej, oraz musi zostać dostarczona w ramach podstawowej licencji. - Urządzenie musi mieć możliwość działania w klastrze wysokiej dostępności (High Availability) - minimum w trybie active - passive. - Urządzenie musi posiadać predefiniowane profile pracy Firewall-a, Kontroli aplikacji, URL Filteringu i modułu IPS. - Urządzenie musi umożliwiać ręczne definiowanie reguł działających na: • firewall-u, • module kontroli aplikacji i URL Filteringu, • module IPS,

	- Urządzenie musi umożliwiać logowanie każdej sesji sieciowej dopuszczonej lub zablokowanej na poziomie urządzenia. - Urządzenie musi posiadać dwa osobne zestawy reguł. Jeden dla połączeń wychodzących do Internetu, drugi dla obsługi połączeń wewnętrznych. - Urządzenie musi posiadać predefiniowaną politykę translacji adresów, pozwalającą na jej zastosowanie przy połączeniach wychodzących do Internetu. - Urządzenie musi wspierać filtrowanie protokołów VoIP, oraz pozwalać na konfiguracje filtrowania tych urządzeń za pomocą prostego kreatora konfiguracji. - Urządzenie musi mieć możliwość integrowania się z usługami katalogowymi, minimum Microsoft Active Directory. - Urządzenie musi mieć możliwość inspekcji ruchu SSL. - Urządzenie musi mieć możliwość kategoryzowania stron HTTPS bez inspekcji ruchu SSL. - Urządzenie musi posiadać interfejs, w którym administrator może znaleźć wszystkie zainfekowane urządzenia w sieci. - Urządzenie musi mieć możliwość całkowitego wyłączenia modułu IPS i uruchomienia go tylko w trybie IDS. - Urządzenie musi umożliwiać na stworzenie tuneli VPN typu client-2-site minimum w formie: • dedykowanego klienta VPN dostarczanego przez producenta rozwiązania, • mobilnego klienta VPN dostarczanego przez producenta rozwiązania, • portalu SSL VPN, • klienta wbudowanego w system Windows, - Urządzenie musi posiadać moduł kontroli aplikacji zawierający ponad 9300 różnych aplikacji. - Urządzenie musi umożliwiać inspekcje ponad 70 protokołów przemysłowych w tym minimum: • BACNet, • CIP, • DNP3, • IEC-60870-5-104, • IEC 60870-6 (ICCP), • IEC 61850, • MMS, • ModBus, • OPC DA & UA, • Profinet, • Step7 (Siemens) - Urządzenie musi posiadać funkcjonalność tzw. Virtual Patchingu. Funkcja ta pozwala na zablokowanie ataków kierowanych na podatne

	urządzenie, które z różnych przyczyn nie mogą zostać zaktualizowane przez administratora. - Lista wspieranych przez moduł kontroli aplikacji, aplikacji musi być publicznie dostępna i pozwalać na przeszukiwanie jej z wykorzystaniem różnych filtrów.
Wydajność	- Urządzenie musi być przystosowane do pracy w temperaturach od 0 stopni do 40 stopni Celsiusa. - Urządzenie musi posiadać następujące certyfikacje: CB 62368-1, CE, FCC IC Class B, VCCI, AS/NZS RCM EMC. - Urządzenie musi posiadać następujące porty: • LAN: 5 x 1GbE, • WAN: 1x1GbE • USB typ C do połączenia konsolowego, • Port USB 3.0, - Wymagane przepustowość urządzenia dla: • Ruchu akcelerowanego: 440 Mbps, • Ruchu NGTP: 340 Mbps, • Ruchu NGFW: 600 Mbps, • Ruchu IPS: 670 Mbps, • Ruchu Firewall: 1000 Mbps, • Firewalla i pakietów UDP o wielkości 1518 bajtów: 2000 Mbps, • VPN AES-128: 970 Mbps, • Połączeń na sekundę: 10500 • Jednoczesnych połączeń: 1000000
System centralnej konfiguracji	- Standardowa licencja dostarczana z urządzeniem musi umożliwiać uruchomienie systemu centralnej konfiguracji dostarczanego przez producenta. System centralnej konfiguracji nie może wymagać wykupienia dodatkowej licencji, oraz nie może być dostarczony jako element darmowy, ale zawierający osobną licencję. - System centralnej konfiguracji musi być utrzymywany i dostarczany przez producenta urządzenia jako rozwiązanie SaaS. - System centralnej konfiguracji nie może być dostarczany jako maszyn wirtualna lub obraz OVA hostowany w środowisku zamawiającego. - System centralnej konfiguracji musi umożliwiać na tworzenie grup konfiguracyjnych w ramach, których zarządzane urządzenia będą otrzymywać taką samą konfigurację. - System centralnej konfiguracji musi być wyposażony w moduł proxy oraz DynDNS umożliwiający na podłączenie się do interfejsu administracyjnego do urządzeń: • Posiadających dynamiczny adres IP bez wiedzy jaki w danym momencie urządzenie ma adres. • Znajdujących "za NAT-em" i nie posiadających publicznego adresu IP, bez przekierowania portów administracyjnych. - System centralnej konfiguracji musi posiadać możliwość definiowania administratorów o różnych poziomach dostępu.

	- System centralnej konfiguracji musi posiadać możliwość definiowania właścicieli urządzeń zarządzanych przez niego. Poprzez przypisanie właściciela zamawiający ma na myśli możliwość zdefiniowania w ramach obiektu typu urządzenie nazwy oraz adresu email właściciela urządzenia. - System centralnej konfiguracji musi umożliwiać wysyłanie raportów bezpieczeństwa z zarządzanych urządzeń do administratorów systemu, jak i do właścicieli urządzeń. - System centralnej konfiguracji musi posiadać wbudowany serwer syslog umożliwiający przesyłanie wszystkich logów z zarządzanych urządzeń do tego serwera. - System centralnej konfiguracji musi umożliwiać eksport logów ze swojego systemu syslog do innego systemu syslog mogącego znajdować się w infrastrukturze zamawiającego. - System centralnej konfiguracji musi posiadać interfejs WWW. Niedopuszczalne jest zarządzanie systemem z poziomu zewnętrznej aplikacji. - System centralnej konfiguracji musi umożliwiać na integrację z systemami 2FA, oraz serwerem RADIUS.
Wsparcie i licencje	Dostarczone urządzenie musi stanowić całość pochodzącą od jednego producenta (oprogramowanie oraz sprzęt), fabrycznie nowe, pochodzić z oficjalnego kanału sprzedaży. Być serwisowane przez producenta lub autoryzowany serwis producenta ze wsparciem na 5 lat. Dodatkowo musi posiadać licencje na okres 5 lat.

Urządzenie do zbierania i analizowania logów – 1 sztuka

1. Zamawiający wymaga, aby rozwiązanie do zbierania i analizowania logów zostało dostarczone w formie rozwiązania sprzętowego i posiadało dostęp przez interfejs web umożliwiający administratorom i operatorom wykorzystanie wszystkich jego funkcji.
2. Zamawiający wymaga aby rozwiązanie obsługiwało natywnie co najmniej: Eset, Cisco switches, Linux, Microsoft SQL, Microsoft Windows, MySQL, Oracle DB, VMware.
3. Zdarzenia z systemów Windows muszą być zbierane przez dedykowane oprogramowanie (tzw. agent) instalowane bezpośrednio na stacjach końcowych i wysyłające dane do centralnej instancji systemu.
   1) Agent Windows musi umożliwiać zbieranie logów zarówno z systemowego dziennika zdarzeń jak i z plików tekstowych w systemie Windows.
   2) Agent musi zapewniać zbieranie wszystkich danych związanych ze zdarzeniem w oryginalnej, niezmodyfikowanej formie (tzn. całość a nie tylko części zdarzenia).
4. Oferowane rozwiązanie musi umożliwiać filtrowanie zdarzeń (przykładowo odrzucanie nieistotnych) zbieranych przez agenta Windows jeszcze przed wysłaniem do centralnej instancji. Filtrowanie zdarzeń zbieranych przez agenta Windows musi być możliwe do skonfigurowania za pomocą programowania wizualnego.
5. Ilość agentów dla systemu Windows nie może być limitowana licencyjnie. Oferowane rozwiązanie musi być pozbawione limitowania pod kątem ilości zbieranych danych.
6. Wymagania wobec Agenta Windows:
   1) Dostarczenie dokumentacji opisującej proces instalacji i konfiguracji agenta.
   2) Po zainstalowaniu, nie może wymagać interwencji administratora na systemie końcowym - musi być centralnie zarządzany, a jego konfiguracja możliwa do przeprowadzenia z poziomu interfejsu graficznego web, bez konieczności ręcznego edytowania plików systemowych. Aktualizacja konfiguracji agenta musi być automatycznie dystrybuowana bezpośrednio z centralnej konsoli systemu.
   3) Musi automatycznie tłumaczyć kody zdarzeń Windows na postać tekstową wynikającą ze zdefiniowanych słowników (przykładowo: Logon Type 2 = Interactive, Logon Type 3 = Network, etc.).
   4) Musi posiadać bufor lokalny na wypadek utraty połączenia stacji końcowej z centralną instancją systemu. Dane, których nie udało się przekazać do centralnej instancji systemu, muszą zostać przekazane natychmiast po powrocie połączenia, również gdy stacja robocza była w między czasie restartowana.

5) Komunikacja pomiędzy agentem Windows, a centralną instancją systemu musi być zaszyfrowana (min. TLS 1.2).
6) Musi wspierać kolekcjonowanie nie tylko podstawowych zdarzeń z dziennika zdarzeń (Application, Security, Setup, System), ale także umożliwiać zbieranie logów z folderu Applications and Services Logs. Dodatkowo agent Windows musi umożliwiać pobieranie danych logów z plików tekstowych z systemu Windows, konfigurowane z centralnej instancji systemu, w tym możliwość wybrania ich formatu danych (przykładowo: dziennik zdarzeń, plik txt, dhcp, iis).
7) Musi automatycznie dodawać opis tekstowy do wszystkich zbieranych zdarzeń, dokładnie tak jak jest to prezentowane w Dzienniku Zdarzeń systemu Windows.
8) Musi umożliwiać zbieranie logów z płaskich plików w systemie, z którego zbierane są logi poprzez podanie ich ścieżki w systemie plików w menu konfiguracji agenta. Konfiguracja ścieżki musi uwzględniać wykorzystanie tzw. wildcardów (przykładowo: C\Windows\System32\dhcp\logs\Dhcp*.log - pobranie wszystkich plików z wskazanego folderu zaczynających się od "Dhcp" i kończących na ".log").
9) Musi automatycznie odpytywać centralny system w zadanym interwale - tzw. heartbeat - w celu sprawdzenia czy zaszły zmiany w konfiguracji - jeżeli tak, to agent pobiera nową konfigurację, a następnie ją implementuje. Nie jest dopuszczalne "wypychanie" konfiguracji z centralnego systemu do agenta.

7. Interfejs graficzny web umożliwiający dostęp do logów, tworzenia alertów i parserów, raportów oraz zarządzania systemem musi być jednolity oraz zunifikowanym tak aby wszystkie operacje konfiguracji, zarządzania i analizy logów były w nim wykonywane.
8. Nie dopuszcza się stosowania wielu różnych interfejsów. Interfejs ten musi być dostępny z poziomu popularnych przeglądarek (przykładowo: Google Chrome, Mozilla Firefox, Opera, Microsoft Edge).
9. Stosowany w rozwiązaniu interfejs graficzny musi umożliwiać łatwe klasyfikowanie danych wejściowych (logów) na potrzeby dalszego procesowania. Klasyfikowanie powinno umożliwiać przypisywanie określonych logów do odpowiednich parserów oraz nadawanie im tagów ułatwiających dalszą pracę z logami (np. wyszukiwanie). Logika klasyfikacji powinna być tworzona przy wykorzystaniu tzw. programowania wizualnego.
10. Oferowane rozwiązanie musi umożliwiać rozbudowywanie natywnie dostępnych funkcjonalności, takich jak klasyfikacja, parsowanie, alertowanie oraz filtrowanie poprzez tak zwane programowanie wizualne, które polega na tworzeniu kodu z graficznych bloków reprezentujących określone instrukcje i funkcje na zasadach WYSIWYG.

11. Zamawiający wymaga, aby programowanie wizualne było możliwe do wykonania przez osoby posiadające podstawową wiedzę programistyczną taką jak znajomość min. instrukcji warunkowych, pętli czy zmiennych, jednakże rozwiązanie musi posiadać możliwość testowania i weryfikowania poprawności logiki stworzonego kodu.
12. Oferowane rozwiązanie musi udostępniać pre-definiowane widoki danych (dashboards) podzielone na kategorie pod względem typu lub producenta urządzenia źródłowego lub aplikacji.
13. Wraz z każdą nową wersją oprogramowania zapisane widoki muszą być automatycznie aktualizowane.
14. Wymagania ogólne wobec rozwiązania:
    1) Filtrowanie nieistotnych zdarzeń na etapie klasyfikacji. Logika filtrowania powinna być tworzona przy wykorzystaniu tzw. programowania wizualnego. Wymagane jest dostarczenie dokumentacji opisującej ten proces.
    2) Zapis oryginalnej wersji odbieranych logów.
    3) Proste wyszukiwanie zapisanych w bazie logów i tworzenie raportów w formie graficznej bez konieczności wykorzystania dedykowanego języka programowania lub zapytań SQL. Wyszukiwanie i raporty muszą być integralną częścią oferowanego rozwiązania i muszą być dostępne przez interfejs graficzny web.
    4) Nie dopuszcza się możliwości modyfikacji bądź manualnego usunięcia logów zapisanych w bazie. Każdy log musi posiadać unikalny identyfikator, który umożliwi jego jednoznaczne rozróżnienie.
    5) Prezentowanie logów ma być realizowane w formie wykresów, zgrupowanych w tzw. widokach (dashboard). Widoki muszą być dynamicznie aktualizowane i interaktywne (tzw. "drill down" - przykładowo: wybranie wartości przedstawionej na jednym wykresie powoduje automatyczne utworzenie filtru wyszukiwania w oparciu o wybraną wartość i dostosowanie pozostałych wykresów).
    6) Tworzenie własnych parserów logów przy wykorzystaniu programowania wizualnego z poziomu interfejsu graficznego web. Wymagane jest dostarczenie dokumentacji zawierającej czytelną instrukcję tworzenia parserów.
    7) Odbieranie wszystkich rodzajów logów. W przypadku braku odpowiedniego parsera dla odbieranego logu, system powinien zapisać go w bazie danych w formie źródłowej (RAW) i umożliwić jego wyszukiwanie.
    8) Automatyczne wzbogacanie logi o tzw. metadane czyli informacje opisujące dany log (przykładowo: typ źródła, protokół transportowy, port docelowy, tagi, nagłówek syslog) i możliwość wyszukiwania wszystkich zapisanych logów w oparciu o te dane. Metadane powinny być dodawane do logu automatycznie nawet jeżeli nie został on poddany parsowaniu.

15. W zakresie parsowania musi być możliwość:
    1) Tworzenia lub modyfikacji parsera - musi istnieć możliwość weryfikacji poprawności utworzonej logiki poprzez zastosowanie jej do przykładowego logu i wyświetlenie ostatecznej wersji w jakiej log zostanie zapisany w bazie, jeżeli testowany parser zostanie użyty. W przypadku wystąpienia błędów w logice parsera, system powinien poinformować o tym użytkownika.
    2) W procesie parsowania oferowane rozwiązanie musi normalizować odbierane logi do ujednoliconego formatu poprzez przypisanie poszczególnych wartości logu do odpowiadających im kluczy (format klucz = wartość). Każdy z utworzonych w procesie parsowania kluczy powinien być oddzielnie indeksowany w bazie danych aby umożliwić szybkie wyszukiwanie wartości skojarzonych z danym kluczem. Zintegrowane w systemie parsery powinny automatycznie wzbogacać procesowane logi o odpowiednią kategorię. Wymagane jest rozróżnianie przynajmniej następujących typów logów: udane logowanie, nieudane logowanie, wylogowanie, zmiana konfiguracji.
    3) Dodania w/w kategorii podczas tworzenia własnych parserów.
    4) Zamiany wybranych elementów logu na podstawowe typy (integer, float), w celu wykonywania na nich operacji matematycznych (suma, średnia, największa/najmniejsza wartość etc.) podczas prezentowania ich na dashboardach.
    5) Wykorzystania operacji matematycznych (dodawanie, odejmowanie, mnożenie, dzielenie) oraz operacji natywnego kodowania/dekodowania URL. Te operacje muszą umożliwiać tworzenie logiki mającej na celu tworzenie linków URL do zewnętrznych systemów oraz połączenie narzędzia z zewnętrznymi aplikacjami.
    6) Dodawania własnych znaczników czasu do odbieranych logów i wykorzystywać go podczas przeglądania danych. Jednocześnie system musi zachowywać oryginalny znacznik czasu z odebranych logów.
    7) Tworzenie własnych parserów musi umożliwiać ustawienie typu wartości jako adres MAC i identyfikację producenta urządzenia sieciowego.
    8) Automatycznego wzbogacania wartości IP wyekstraktowane z pól logu o powiązany rekord DNS i dane GeoIP aby umożliwić ich graficzną reprezentację na widoku mapy świata bez konieczności wykorzystania zewnętrznych usług bądź aplikacji.
    9) Średnią stałą wydajność procesowania min. 2000 EPS (logów na sekundę), przy założeniu średniego rozmiaru logu równego 700 Bajtów. W przypadku wystąpienia większej chwilowej ilości logów na sekundę, rozwiązanie musi być w stanie wykorzystać bufor i umożliwić odbieranie dwukrotnej większej wartości prze co najmniej 5 minut.
16. Oferowane rozwiązanie musi umożliwiać również:

1) Zbieranie logów i zdarzeń z systemów Windows poprzez dedykowanego agenta instalowanego na stacji końcowej/serwerze. Agent musi być centralnie zarządzany z konsoli systemu.
2) Odbieranie logów na przynajmniej 50 różnych portach UDP/TCP w celu ułatwienia rozróżnienia źródeł.
3) Procesowanie (kolekcjonowanie oraz parsowanie) logów z dowolnych źródeł takich jak aplikacje, systemy operacyjne oraz urządzenia sieciowe.
4) Zbieranie logów z platformy Office365 bez konieczności instalacji dodatkowych komponentów. Proszę dostarczyć dokumentację opisującą proces konfiguracji connectora Office365.
5) Monitorowanie źródeł logów i tworzenie reguł mających na celu powiadamianie administratora systemu w przypadku w którym źródło logów zdefiniowane w regule nie wyśle logów w określonym interwale. System musi być dostarczony wraz z parserami do obsługi logów generowanych przez urządzenia najpopularniejszych dostawców rozwiązań IT oraz umożliwiać tworzenie własnej logiki parsowania dla nietypowych źródeł.
6) Odbieranie i procesowanie logów, zdarzeń oraz innych danych przesyłanych przez urządzenia w sposób jawny i ustandaryzowany, wykorzystując co najmniej następujące protokoły: UDP/TCP SYSLOG, TCP RELP (nieszyfrowany), TCP RELP (szyfrowany).
7) Łatwe tworzenie ról definiujących poziom dostępu użytkowników do zapisanych logów oraz poszczególnych elementów systemu. Wymagane jest dostarczenie dokumentacji opisującej sposób tworzenia ról użytkowników.
8) Wzbogacanie logów o dodatkowe informacje z zewnętrznych list (przykład: wzbogacenie nazwy użytkownika o jego adres email i przynależność do grup AD).
9) Integrację z systemem LDAP w celu logowania użytkowników. W przypadku awarii systemu LDAP, Zamawiający wymaga również możliwości logowania lokalnego.
10) Tagowanie indywidualnych źródeł danych, aplikacji, urządzeń czy całych podsieci IP, w celu oznaczania, przykładowo: lokalizacji urządzenia, jego typu, krytyczności etc. Tagi muszą być możliwe do dodania w procesie tworzenia parsera. Wszystkie dodane tagi muszą być przechowywane razem z logiem zapisanym w bazie. System musi umożliwiać filtrowanie i wyszukiwanie logów w oparciu o tagi, a także umożliwiać ograniczenie widoczności logów posiadających określony tag w procesie definiowania ról.
11) Wykorzystanie REST-API do integracji z zewnętrznymi systemami do monitoringu (Zabbix, Nagios, MRTG etc.).

12) Integrację z bazami danych (przynajmniej: MSSQL, MySQL, Oracle i PostgreSQL) poprzez konektor ODBC (integracja rozumiana jako możliwości pobierania całych wierszy wybranych tabel w bazie).
13) Integrację z platformą wirtualizacji Vmware (ESXi, vSphere) poprzez dedykowany konektor pobierający logi i zdarzenia bezpośrednio z platformy.
14) Weryfikację poprawności działania własnych parserów w trakcie ich pisania.
15) Zbieranie danych przynajmniej w formatach RAW, Syslog RFC5424, CEF, LEEF, JSON RFC8259.
16) Wspieranie podstawowych funkcji SIEM - tworzenie tzw. korelacji zdarzeń, umożliwiających wygenerowanie alertu w przypadku przekroczenia określonego limitu lub wystąpienia kilku zdarzeń w zdefiniowanym oknie czasowym. Tworzenie i edycja reguł korelacji musi być możliwa do przeprowadzenia za pomocą interfejsu programowania graficznego wyposażonego w funkcjonalność sprawdzania działania logiki reguły na przykładowych logach.
17) Wdrożenie w trybie wysokiej dostępności, w którym możliwe jest klastrowanie przynajmniej 2 urządzeń. Ustawienia klastra muszą być możliwe do skonfigurowania przez interfejs graficzny web, nie jest dopuszczalne konfigurowanie klastra poprzez ręczne modyfikowanie plików systemu operacyjnego. System musi dostarczać użytkownikom czytelnych informacji o stanie klastra i synchronizacji bazy. Wymaga się dostarczenia dokumentacji opisującej cały proces tworzenia klastra, oraz odzyskiwania danych w przypadku awarii jednego z komponentów klastra. Urządzenia pracujące w klastrze muszą przyśpieszać wyszukiwanie poprzez równoległe współdzielenie obciążenia.
18) Generowanie alertów, jeżeli w procesowanym logu zostaną spełnione zdefiniowane warunki. Alert musi być możliwy do wysłania poprzez wiadomość e-mail, a jego treść możliwa do utworzenia przez użytkownika. Oferowane rozwiązanie musi być również wyposażone w alerty i korelacje utworzone przez producenta.
19) Wykorzystanie pól procesowanego logu do tworzenia treści wiadomość e-mail.
20) Umożliwiać tworzenie alertów i korelacji poprzez wykorzystanie programowania wizualnego. Podobnie jak w przypadku tworzenia parserów, musi istnieć możliwość weryfikacji poprawności utworzonej logiki poprzez wykorzystanie testowego logu w oknie tworzenia alertu oraz powiadamiania o ewentualnych błędach. Wymagane jest dostarczenie dokumentacji opisującej proces tworzenia i testowania poprawności alertu.
21) Wysłanie logu naruszającego zdefiniowaną logikę alertu do zewnętrznych systemów, co najmniej za pomocą protokołu SMPT lub Syslog (TCP). System

musi umożliwiać definiowanie własnego formatu przesyłanego logu w celu łatwiejszego dostosowania go (integracji) do systemu docelowego.

22) Nadawanie alertom nowych tagów.
23) Wspierać tworzenie i odzyskiwanie kopii zapasowej konfiguracji.
24) Tworzenie i odzyskiwanie kopii zapasowej bazy danych. Tworzenie kopii zapasowej musi być możliwe zarówno na żądanie jak i w określonych interwałach czasowych. Tworzenie i odzyskiwanie musi być możliwe do wykonania z poziomu interfejsu graficznego web, bez konieczności tworzenia/modyfikowania skryptów, makr lub plików systemu operacyjnego.

17. Oferowane rozwiązanie musi być dostarczone w formie urządzenia fizycznego spełniającego następujące wymagania:
    1) Obudowa - rozmiar max 2U, wyposażone w ramię do kabli umożliwiające wysunięcie urządzenia z szafy rack na potrzeby serwisowe bez konieczności wyłączania. Wentylatory urządzenia muszą być wymienialne w trakcie pracy urządzenia i być redundantne skierowane ruchem przepływu powietrza front -> tył.
    2) Interfejsy sieciowe - minimum 4 porty 1Gbit LAN + 1 dedykowany 1Gbit porty do zarządzania sprzętem. Konfiguracja parametrów wszystkich interfejsów sieciowych (w tym LACP) musi odbywać się z interfejsu graficznego web oraz musi być szczegółowo opisana w dokumentacji.
    3) Zasilanie - urządzenie musi być wyposażone w 2 źródła zasilania z redundancją 1+1.
    4) Przestrzeń dyskowa - wspierana przez sprzętowy akcelerator SAS RAID-5. Kontroler macierzy dyskowej musi być wyposażony w zapasową baterię lub pamięć flash. Minimum 4 dyski edycji RAID do wykorzystania w warunkach data center. Redundancja dysków nie może wpływać na wymaganą minimalną przestrzeń dyskową. Wymagana przestrzeń składowania danych o rozmiarze przynamniej 4 TB oraz wspierać kompresję przechowywanych danych.
    5) System operacyjny - zamknięty przez producenta bez możliwości połączeń SSH. Aktualizowany z konsoli administracyjnej poprzez protokół https (wszystkie elementy systemu muszą być ustawialne z interfejsu graficznego web, bez konieczności edytowania żadnych plików systemowych, skrytpów lub makr).
    6) Virtual KVM (keyboard, video, mouse) – urządzenie musi posiadać możliwość zdalnego zarządzania oraz być dostarczone z licencją odpowiedniego typu (iLO, iDRAC etc).
18. Zamawiający wymaga aby oferowane rozwiązanie gwarantowało przechowywanie danych w okresie oczekiwanej retencji aby dane były dostępne do przeszukiwania natychmiastowo, bez wprowadzania opóźnienia w postaci importu z zewnętrznych baz danych.

19. W przypadku przeciążenia systemu logi nie mogą być tracone. Wszystkie nieobsłużone logi muszą być buforowane, a administrator systemu powiadamiany w momencie, w którym bufor zacznie się zapełniać. Bufor nie może być mniejszy nić 50GB.
20. Oferent musi dostarczyć kompletną dokumentację – instrukcję obsługi oferowanego rozwiązania. Wymagane jest dostarczenie broszury szczegółowo przedstawiającej parametry techniczne oferowanego systemu. Wymaga się dostarczenia dokumentacji w formie elektronicznej lub linku do jej wersji online na stronach producenta. Nie dopuszcza się dokumentacji odnoszącej się z/do źródeł zewnętrznych, innych niż producenta. Dokumenty te, tj. instrukcję obsługi oraz broszury należy złożyć wraz z ofertą.
21. Zamawiający wymaga możliwości aktualizacji systemu dystrybuowanej w formie pojedynczego pliku i instalowane za pośrednictwem interfejsu graficznego web. Wszystkie aktualizacje muszą być możliwe do zainstalowania bez wsparcia dostawcy/producenta.
22. Wymagamy dostarczenia przynajmniej 4 ostatnich dokumentów release notes w celu zweryfikowania proponowanych parametrów systemu. System musi umożliwiać cofnięcie do poprzedniej wersji oprogramowania w przypadku wystąpienia problemów z działaniem po aktualizacji. Operacja musi być możliwa do wykonania bez wsparcia dostawcy/producenta.
23. Ilość urządzeń z których zbierane są dane oraz ilość logów liczona w GB/dzień nie może być ograniczona licencyjnie.
24. Wymagane wsparcie na sprzęt i oprogramowanie - minimum 5 lat.
25. Dostarczone rozwiązanie musi zostać dostarczone na koszt wykonawcy oraz uruchomione, a personel zamawiającego musi zostać przeszkolony z jego obsługi.

Oprogramowanie zapewniające zabezpieczenie urządzeń, użytkowników i dostępu zdalnego – 40 licencji na urządzenia końcowe

1. Warunki ogólne.
   1) Wsparcie dla systemów
      a) Windows: 7/8/10/11
      b) Windows Server: 2008 R2, 2012 R2, 2016, 2019, 2022
      c) Linux Ubuntu
   2) Wsparcie dla 32- i 64-bitowej wersji systemu Windows tam, gdzie jest to dostępne.
   3) Klient antywirusowy musi wspierać systemy pracujące w środowisku zwirtualizowanym
   4) Wsparcie dla rozwiązań VDI
   5) Plik instalacyjny musi umożliwiać prostą instalację w środowisku rozproszonym wykorzystując skrypty instalacyjne czy pozwalając na instalację z poziomu GPO i SCCM.
   6) Rozwiązanie musi posiadać własny system dystrybucji nowych paczek instalacyjnych w środowisku rozproszonym, który nie wykorzystuje technologii zewnętrznych takich jak np. Microsoft SCCM czy Intune.
2. Funkcje systemu ochrony antywirusowej
   1) Klient antywirusowy musi posiadać następujące moduły bezpieczeństwa:
      a) Antymalware,
      b) URL Filtering,
      c) Moduł analizy behawioralnej,
      d) Moduł blokowania dostępu do urządzeń podłączanych do komputera,
      e) Firewall i kontrola aplikacji,
      f) Moduł weryfikacji zgodności,
      g) Moduł VPN,
      h) Moduł emulacji zagrożeń,
   2) Klient antywirusowy musi posiadać moduł anty-ransomware umożliwiający wykrycie, zablokowanie infekcji i przywrócenie zaszyfrowanych plików.
   3) Moduł anty-ransomware musi wykonywać kopię zapasowa plików z których korzysta użytkownik. Wielkość kopii zapasowej, oraz typy plików nią obejmowane muszą być definiowalne przez administratora po stronie konsoli centralnego zarządzania.
   4) Klient antywirusowy musi posiadać w wparcie technologii Intel TDT.
   5) Klient antywirusowy musi posiadać moduł ochrony przed wirusami bezplikowymi.
   6) Klient antywirusowy musi być zintegrowany z interfejsem Microsoft Anti-Malware Scan Interface (AMSI) w celu odbierania i analizowania zdekodowanych skryptów.

7) Klient antywirusowy musi posiadać moduł wykrywający komunikację do serwerów C&C, oraz umożliwiać jej blokowanie.
8) Rozwiązanie w ramach podstawowej licencji musi umożliwiać aktualizacje baz serwerów C&C i ataków typu zero-day w czasie rzeczywistym, bezpośrednio z chmury producenta.
9) Klient antywirusowy musi mieć możliwość instalacji modułowej tj. pozwolić na instalację każdego z dostępnych modułów z osobna.
10) Klient antywirusowy musi umożliwiać ukrycie ikony programu na tacce systemowej
11) Klient antywirusowy musi umożliwiać na zezwolenie, lub zablokowanie możliwości przeglądania logów programu przez użytkownika komputera
12) Klient antywirusowy musi umożliwiać definiowanie jakie typy komunikatów będą wyświetlane użytkownikowi przynajmniej na 3 poziomach
13) Klient antywirusowy musi umożliwiać na wgranie pliku graficznego z logo firmy, które będzie wykorzystywane w komunikatach programu antywirusowego, wyświetlanych użytkownikowi
14) Klient antywirusowy musi umożliwiać konfiguracje tła logowania w systemie Windows, na zdefiniowane przez administratora.
15) Klient antywirusowy musi umożliwiać zabezpieczenie odinstalowania programu poprzez zdefiniowanie hasła wymagane do odinstalowania programu.
16) Klient antywirusowy musi dawać możliwość wykorzystania jednego z 3 silników antywirusowych, z czego 2 muszą pochodzić od innego producenta, niż oferowane rozwiązanie.
17) Klient antywirusowy musi mieć możliwość wykorzystania sandbox-a lokalnego obsługiwanego przez dedykowany sprzęt
18) Klient antywirusowy musi generować raporty, z każdej wykrytej infekcji. Raport będzie rejestrował, prezentował i usuwał zaciemnienia skryptów PowerShell używanych podczas ataku. Raport z ataku musi być dostępny z poziomu logów, jak i możliwy do pobrania na komputer z konsoli administracyjnej. Będzie zawierał minimum poniższe informacje:
    a) informacje na temat źródła ataku,
    b) pliki jakie zostały zaatakowane przez wirusa,
    c) adresy sieciowe do jakich niebezpieczny proces próbował się połączyć,
    d) informacje na temat wyleczenia lub usunięcia wirusa,
    e) mapowanie wykrytych metod ataku na matrycę MITRE ATT&CK
19) Klient antywirusowy musi posiadać plugin do przeglądarki internetowej umożliwiający skanowanie w czasie rzeczywistym ruchu WWW przynajmniej dla przeglądarek:
    a) Chrome,
    b) Firefox,

c) Edge (Chromium),

20) Plugin do przeglądarki musi posiadać możliwość weryfikacji ponownego użycia hasła firmowego na innych stronach niż strony firmowe zdefiniowane przez administratora.
21) Rozwiązanie antywirusowe musi mapować wykryte ataki wirusów na matrycę MITRE ATT&CK z wykorzystaniem minimum 44 technik
22) Klient antywirusowy musi posiadać możliwość kontroli dostępu do portów USB.
23) Klient antywirusowy musi posiadać możliwość blokowania zainstalowanych aplikacji na komputerze
24) Klient antywirusowy musi posiadać funkcjonalność weryfikowania zgodności z polityką firmy gdzie sprawdzane i raportowane do konsoli może być m.in.
    a) aktualizacje systemu Windows Update i ostatnia zainstalowana aktualizacja systemu operacyjnego,
    b) status wygaszacza ekranu wraz z włączoną opcją wymagania hasła po jego wyłączeniu,
    c) weryfikacja dowolnych wartości kluczy rejestru,
25) Klient antywirusowy musi być zdolny do zmiany ustawień wbudowanego firewall-a, zależni od statusu zgodności komputera, weryfikowanego przez moduł zgodności.
26) Możliwość blokowania urządzeń podłączanych przez port USB do komputera.
27) Automatyczne logowanie wszystkich urządzeń USB podpiętych do komputera chronionego przez rozwiązanie.
28) Ochrona developerska zapobiegająca wyciekowi kluczy RSA, haseł, tokenów, przy wykorzystaniu Git'a
29) Współpraca z chmurą producenta wspomagającą wykrywanie zagrożeń, oraz wymianę metadanymi na temat wykrytych zagrożeń. Producent musi dostarczać zamkniętą listę zasobów, do których agent będzie uzyskiwał dostęp aby funkcja działała poprawnie.
30) Chmura producenta wspomagająca wykrywanie zagrożeń musi być zasilana przynajmniej przez trzy niezależne od siebie typy rozwiązań np. rozwiązania typu NGFW, rozwiązania typu Endpoint Security, oraz rozwiązania typu Cloud Native Security CI/CD.
31) Klient antywirusowy musi posiadać technologię usuwania niebezpiecznej zawartości (makra, składniki aktywne, adresy URL) plików ściąganych z Internetu i dostarczania ich przed detonacją oryginalnego pliku w sandbox-ie.

3. System centralnego zarządzania.
    1) W przypadku zarządzania opartego o chmurę producenta, środowisko musi być zlokalizowane w ramach Europejskiego Obszaru Gospodarczego.

2) Serwer centralnego zarządzania musi obsługiwać do 400000 tysięcy punktów końcowych
3) Serwer centralnego zarządzania musi posiadać działający i bardzo dobrze udokumentowany interfejs API
4) Serwer centralnego zarządzania musi umożliwiać tworzenie reguł dla klientów końcowych, oparty na politykach zarządzających
5) Serwer centralnego zarządzania musi pozwalać na tworzenie odrębnego zestawu polityk dla komputerów podłączonych do serwera centralnego zarządzania, oraz tych będących offline i niepodłączonych do serwera centralnego zarządzania
6) Serwer centralnego zarządzania oparty o chmurę, musi posiadać mechanizm EDR pozwalający na wyszukiwanie i "polowanie" na zagrożenia sieciowe posiadający co najmniej 130 różnych znaczników, z których można budować wyszukiwania
7) Serwer centralne zarządzania musi pozwalać na tworzenie dostępów administracyjnych opartych o role
8) Serwer centralnego zarządzania musi mieć możliwość definiowania wykluczeń m.in. w zakresie:
   a) kontroli filtrowania stron WWW
   b) ochrony antywirusowej w czasie rzeczywistym
   c) skanowania na żądanie
   d) konkretnych nazw ataków
   e) modułów emulacyjnych zagrożenia
   f) ochrony behawioralnej
9) Lista wykluczeń musi być dostępna dla każdej z wyżej wymienionych kategorii z osobna
10) Serwer centralnego zarządzania musi umożliwiać wysyłanie minimum następujących zadań do klienta antywirusowego:
   a) skanowanie komputera,
   b) aktualizacja sygnatur antywirusowych,
   c) przywracania plików z kwarantanny,
   d) analizy konkretnego procesu działającego na systemie operacyjnym,
   e) przeniesienia, lub usunięcia pliku do/z kwarantanny,
   f) izolacji komputera, usunięcia komputera z izolacji,
   g) wypchnięcia nowego klienta antywirusowego,
   h) zebrania logów z klienta,
   i) naprawy instalacji klienta antywirusowego,
   j) wyłączenia komputera,
   k) odinstalowania klienta antywirusowego,
   l) skanowania konkretnej aplikacji,

m) zabicia konkretnego procesu pracującego w systemie operacyjnym,
n) wywołania skryptu PowerShell,
o) wypychania konfiguracji VPN,
p) diagnostyki systemu pozwalającej na weryfikację m.in. jakie procesy obciążają system operacyjny

11) Serwer centralnego zarządzania musi posiadać funkcjonalność logowania zdarzeń z stacji końcowych
12) Serwer centralnego zarządzania musi posiadać funkcjonalność raportowania zdarzeń w formie graficznej
13) Serwer centralnego zarządzani musi umożliwiać zarządzanie wieloma organizacjami z poziomu jednej konsoli centralnego zarządzania
14) Producent oprogramowania musi dostarczać ściśle zdefiniowaną listę URL i/lub zakres adresów IP serwerów producenta oprogramowania udostępniających informacje o zagrożeniach, definicje wirusów oraz aktualizacje.
15) Producent oprogramowania dostarczy zamkniętą listę adresów, z których oprogramowanie zainstalowane na komputerach będzie pobierać aktualizacje.
16) System centralnego zarządzania musi mieć możliwość definiowania wielu poziomów uprawnień dla operatorów i administratorów systemu.
17) System centralnego zarządzania musi mieć możliwość docelowej integracji z modułem XDR tego samego producenta, przy założeniu, że system XDR nie posiada osobnej konsoli centralnego zarządzania, a całość jest obsługiwana z jednej konsoli centralnego zarządzania.

4. Licencja, wsparcie.
   1) 5-letnia licencja producenta.
   2) 5-letnie wsparcie realizowane przez serwis producenta.

Wdrożenie i wsparcie techniczne

1. Dojazd, dostawa, montaż i uruchomienie urządzeń i oprogramowania.
2. Przygotowanie sprzętu (sprawdzenie, aktualizacja, wstępna adresacja).
3. Konfiguracja biblioteki taśmowej, integracja z serwerem backupu, wykonanie testów backupu.
4. Wdrożenie przełączników sieciowych (projekt sieci, VLAN-y, agregacje, wykonanie połączeń ze sprzętem, sprawdzenie poprawności połączeń).
5. Wdrożenie oprogramowania zapewniającego zabezpieczenie urządzeń, użytkowników i dostępu zdalnego (aktywacja licencji, uruchomienie konsoli, konfiguracja konsoli, instalacja na stacji roboczej).
6. Wdrożenie NGFW (instalacja i wstępna konfiguracja zgodna z zaleceniami zamawiającego).
7. Konfiguracja urządzenia do zbierania i analizowania logów z uwzględnieniem obecnej infrastruktury (uruchomienie 5 źródeł Microsoft Windows, uruchomienie 10 źródeł urządzeń przekazujących logi poprzez syslog UDP 514).
8. Usługa wsparcia technicznego online: minimum 8 godzin rocznie, w okresie 5 lat.