Załącznik Nr 2 do SWZ

Nr postępowania: ZP.271.24.2024

Zaktualizowany 19.12.2024r.

OPIS PRZEDMIOTU ZAMÓWIENIA

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. **Podniesienie stopnia bezpieczeństwa IT w urzędzie gminy Golub-Dobrzyń w ramach projektu Cyberbezpieczny Samorząd**

DOSTAWA INFRASTRUKTURY SPRZĘTOWEJ ORAZ OPROGRAMOWANIA

Przedmiotem zamówienia jest dostawa sprzętu i oprogramowania podnoszącego poziom cyberbezpieczeństwa systemów teleinformatycznych w Gminie Golub-Dobrzyń
Poniżej wyspecyfikowano minimalne parametry sprzętu oraz oprogramowania, które należy dostarczyć w ramach realizacji przedmiotu zamówienia. W przypadku, gdy nie określono, że parametr określa maksymalną wartość jest to jego wartość minimalna.
Wymagania ogólne:

- Całość dostarczanego sprzętu i oprogramowania standardowego musi pochodzić z autoryzowanego kanału sprzedaży producenta.
- Całość dostarczanego rozwiązania, tzn. każde z dostarczonych urządzeń, musi być nowe, wcześniej nieużywane, rok produkcji nie starszy niż 2023.
- Całość dostarczanego rozwiązania, tzn. każde z dostarczonych urządzeń, w którym nie wskazano szczegółowych warunków gwarancji, musi być objęte minimum 24 miesięczną gwarancją jeśli w opisie parametrów nie wskazano inaczej
- Urządzenia i ich komponenty muszą być oznakowane przez producentów w taki sposób, aby możliwa była identyfikacja zarówno produktu, producenta, jak i daty produkcji danego elementu.
- Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w formie papierowej lub elektronicznej w języku polskim lub angielskim.
- Do każdego urządzenia musi być dostarczony niezbędny sprzęt eksploatacyjny (przewody zasilające, przewody sygnałowe 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.
- Wszystkie urządzenia muszą posiadać oznakowanie CE.
- Wszystkie dostarczane urządzenia na dzień złożenia oferty nie mogą być w fazie end-of-life (EOL)
- Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V ± 10%, 50 Hz.

- Wymagane jest, aby infrastruktura sprzętowa była gotowym produktem posiadającym nazwę handlową i złożonym z zamkniętej, ściśle zdefiniowanej listy komponentów posiadających odpowiednie numery katalogowe.
- Dostarczane oprogramowanie musi zostać dostarczone w najnowszej stabilnej wersji, która uzyskała certyfikację producenta dostarczanego sprzętu (jeśli podlega certyfikacji).

Zamawiający wymaga aby Wykonawca realizując opisane w przedmiocie zamówienia dostawy i usługi uwzględnił uwarunkowania środowiska aktualnie pracującego u Zamawiającego, w szczególności uwzględniając:

- posiadane środowisko domenowe,
- posiadaną konfigurację sieci wraz z segmentacją VLAN, oraz strefą DMZ,
- posiadaną konfiguracją baz danych i backupów,
- konfigurację stacji roboczych.

Wykonawca w ramach postępowania zobowiązany jest do wykonania co najmniej następujących usług związanych z montażem i konfiguracją dostarczanej infrastruktury sprzętowej:

1. Wykonanie Projektu Technicznego dostarczanej infrastruktury sprzętowej, który będzie składał się co najmniej z następujących elementów:
   - Dokładna specyfikacja techniczna wraz z numerami katalogowymi poszczególnych elementów,
   - Nazwy oraz szczegółowa adresacja poszczególnych elementów,
   - Planowana konfiguracja środowiska wraz z połączeniami, konfiguracją poszczególnych elementów w tym logiczną konfiguracją miejsca, zaprojektowanie kompleksowego systemu ochrony danych opartego na funkcjach macierzy oraz oprogramowania standardowego z uwzględnieniem specyfiki całego projektu,
   - Wymagane działania ze strony Zamawiającego w celu poprawnego montażu i konfiguracji,
   - Harmonogram prac.

   Projekt techniczny musi zostać wykonany po wcześniejszej analizie środowiska wykonanej przez Wykonawcę oraz musi zostać zaakceptowany przez Zamawiającego.
2. Konfiguracja serwerów.
3. Instalacja oraz konfiguracji oprogramowania.
4. Testy rozwiązania.
5. Instruktaż dla administratorów demonstrujący sposób zarządzania środowiskiem.
6. Dostarczenie dokumentacji powykonawczej infrastruktury sprzętowej i oprogramowania standardowego, która będzie składała się co najmniej z następujących elementów:
   - Specyfikacja techniczna wraz z numerami katalogowymi poszczególnych elementów oraz numerami seryjnymi poszczególnych elementów,
   - Końcowe nazwy oraz szczegółowa adresacja poszczególnych elementów,
   - Konfiguracja środowiska wraz z połączeniami, konfiguracją poszczególnych elementów w tym logiczną konfiguracją miejsc
   - Komplety poświadczeń do całej infrastruktury – wymagana zmiana haseł domyślnych – dostarczone jako osobny załącznik w postaci zaszyfrowanego pliku kdbx,

- Dokumentacja techniczna w formie elektronicznej do każdego elementu w języku polskim lub angielskim
- Szczegóły dotyczące instalacji i uruchomienia infrastruktury sprzętowej, w zakresie modernizacji infrastruktury szpitala, zostaną ustalone pomiędzy Stronami w trakcie Analizy Przedwdrożeniowej.
- Zamawiający zapewni odpowiedni zapas mocy oraz odpowiednie warunki środowiskowe w komorach serwerowni.
- Po zakończonym montażu Wykonawca przekaże Zamawiającemu wszystkie hasła dostępowe do kont „super użytkowników".

Wszystkie świadczone w ramach zamówienia usługi nie mogą trwać dłużej niż do 12.03.2026.

Opis parametrów minimalnych dostarczanej infrastruktury oraz oprogramowania:
Wymagania dla Wykonawcy który dostarczy infrastrukturę sprzętową oraz oprogramowanie:
Zamawiający wymaga, aby Wykonawca spełniała wymagania w zakresie:

Zestawienie wymaganego sprzętu i oprogramowania

Lp.	Typ sprzętu	Ilość
1.	Oprogramowanie EDR z usługami cyberbezpieczeństwa SOC	1 kpl.
2.	Oprogramowanie do Inwentaryzacji aktywów i ich konfiguracji	1 kpl.
3.	UPS stanowiskowy	20 szt.
4.	Przełącznik LAN 24 porty	1 szt.
5.	Przełącznik LAN 12 porty	10 szt.
6.	Firewall nextgeneration	1 szt.
7.	Rozbudowa licencji backup	1 kpl.
8.	Szkolenie dla pracowników IT	1 kpl.

1. Oprogramowanie EDR z usługami cyberbezpieczeństwa SOC

1.	Usługa musi składać się komponentu lub komponentów programowych oraz usługi wykonawcy opisanej niżej. a. Komponent softwarerowy musi być dostarczony w formie usługi uruchomionej w infrastrukturze dostawcy lub jako usługa SaaS (Software as a Service) producenta b. Wszystkie komponenty centralne w oparciu o które działa System musi być zlokalizowanie na terenie Unii Europeskiej
	Funkcjonalność EDR/EPP
2.	System musi umożliwiać identyfikację i neutralizację zagrożeń cybernetycznych, takich jak ataki bezplikowe, 0-day malware, ransomware, cryptominers, lateral movement, APT, oraz wykorzystywanie podatności software/hardware
3.	System musi działać w oparciu o sztuczną inteligencję, wykorzystując silniki statyczne i dynamiczne
4.	System musi zapewniać autonomiczną reakcję na zagrożenia, działając zarówno, gdy połączenie do konsoli jest dostępne, jak i w gdy jest ono niemożliwe (np. Komputer jest odłączony od sieci)
5.	System musi umożliwiać wyłączenie każdego silnika detekcji dla poszczególnych grup stacji końcowych

6.	System musi obsługiwać następujące mechanizmy wykrywania złośliwego oprogramowania: a) Przed wykonaniem złośliwego kodu (Pre-Execution): System musi identyfikować złośliwe oprogramowanie na podstawie plików poprzez silniki reputacji. b) Przed wykonaniem złośliwego kodu (Pre-Execution): System musi potrafić identyfikować nieznane szkodliwe oprogramowanie oparte na plikach za pomocą analizy statycznej z wykorzystaniem algorytmów uczenia maszynowego. c) W czasie wykonywania złośliwego kodu (Run-Time): System musi identyfikować i reagować na ataki z wykorzystaniem wyrafinowanych technik hackerskich.
7.	System musi umożliwiać odpowiedź na wykryte zagrożenie w oparciu o kwalifikację zdarzenia, z opcjami aktywnej ochrony lub ostrzeżenia.
8.	System musi obsługiwać zaraportowane incydenty poprzez akcje takie jak: a) Zabij proces – System musi umożliwić zatrzymanie procesu zidentyfikowanego jako zagrożenie w celu zatrzymania działania szkodliwego pliku. b) Kwarantanna pliku – System musi umożliwić kwarantannę pliku poprzez zaszyfrowanie, a następnie przenoszone do bezpiecznej ścieżki, w celu uniemożliwienia ponownego uruchomienia. c) Remediacja zagrożenia – System musi umożliwić usunięcie wszystkich plików oraz konfiguracji systemu jakie zostały wykonane przez proces związany z incydentem. d) Rollback – System musi umożliwić przywrócenie stacji roboczej sprzed uruchomienia zagrożenia, a operacje wykonane poprawnie przez użytkownika mają zostaną nienaruszone. e) Kwarantanna hosta – w ramach incydentu System musi umożliwić kwarantannę stacji końcowej. Oznacza to odcięcie urządzenia od funkcji sieciowych z wyłączeniem podłączenia do konsoli, aby uniknąć dalszej propagacji zagrożenia w przypadku, kiedy istnieje taka możliwość.
9.	System musi przechowywać dane o incydentach bezpieczeństwa na serwerach zarządzania przez okres co najmniej 365 dni.
10.	System musi mapować każdy incydent na macierz MITRE, z uwzględnieniem potencjalnych technik wykorzystywanych w ramach podejrzanego procesu.
11.	W ramach Incydentu musi być unikalny numer odpowiedzialny za zebranie ciągu przyczynowo skutkowego działania powiązanych ze sobą danych, a następnie zaprezentowane za pomocą drzewa procesów
12.	System musi zezwalać na uruchomienie skryptów, których celem jest zebranie dodatkowych informacji z stacji końcowej.
13.	System musi zbierać zdarzenia wykonywane w ramach działania stacji końcowej. Niniejsze zdarzenia muszą być możliwe do ręcznego przeszukiwania zebranych danych z użyciem odpowiednich zapytań, które pomogą operatorowi w poszukiwaniu podejrzanej aktywności czy konkretnego IOC. Niniejsze dane muszą być przechowywane przez okres minimum 14 dni z możliwością ich rozszerzenia do 365 dni.
14.	System musi umożliwiać tworzenie własnych reguł pozwalających na automatyzację zapytań w celu przeszukania zebranych danych z stacji końcowej. Ta funkcjonalność ma umożliwić analitykowi przekształcenia zapytań (EDR / XDR) w automatyczne reguły detekcyjne, które wyzwalają alerty i automatyczne odpowiedzi, gdy reguły wykryją tego typu zachowanie stacji końcowej.
15.	Polityka bezpieczeństwa umożliwia dostosowanie danych zebranych ze stacji

	końcowych jakie wysyłane są do systemu, względem poszczególnych grup.
16.	System musi wspierać systemy operacyjne Windows, Linux, MacOS.
17.	System musi umożliwiać instalację agenta z wykorzystaniem operacji automatycznych takich jak SCCM, GPO.
18.	System musi chronić agenta przed nieautoryzowaną deinstalacją lub modyfikacją konfiguracji poprzez funkcję anty-tamper, zabezpieczoną silnym, automatycznie generowanym hasłem unikalnym dla każdej stacji roboczej.
19.	System musi informować o znalezionych podatnościach aplikacji zainstalowanych na chronionym hoście, dostarczając informacje z CVE o jej krytyczności.
20.	System musi udostępniać interfejs API do wykonania każdej operacji.
21.	System musi obsługiwać architekturę Multi-Site oraz Multi-Tenancy.
22.	System musi integrować się z Active Directory, umożliwiając automatyczne przypisywanie agentów do grup zgodnie z zasadami AD, aby możliwe było automatyczne przypisywanie agentów do grup, w celu powiązania ich z zasadami AD. Konsola zarządzania nie może łączyć się z usługą Active Directory bezpośrednio za pośrednictwem programu ADFS ani żadnej innej metody uzyskiwania atrybutów usługi Device i User AD. Serwer zarządzania rozwiązaniem nie mogą mieć żadnych zależności od stanu usługi AD
23.	System musi zapewniać funkcjonalność lokalnego firewalla dla chronionej stacji końcowej. Ochrona firewall ma umożliwić realizację unikalnych polityk dla każdej chronionej grupy hostów. Tworzone reguły muszą uwzględnić: protokół, aplikację, kierunek ruchu, adres IP lokalny/zdalny, port lokalny/zdalny, lokalizację, system operacyjny
24.	System musi kontrolować urządzenia próbujące uzyskać dostęp do chronionej stacji, umożliwiając tworzenie reguł dla interfejsów USB, Bluetooth, Thunderbolt
25.	System musi umożliwiać tworzenie własnych dashboardów przedstawiających aktualny stan infrastruktury oraz filtrowanie komputerów na podstawie różnych atrybutów
26.	System musi posiadać intuicyjny i prosty interfejs, który w sposób graficzny umożliwia prezentacje wykrytego zagrożenia - drzewa procesów, w celu uproszczenia i automatyzacji analizy wykrytego przez System zdarzenia
27.	Rozwiązanie musi zawierać dashboard pokazujący wszystkie komputery oraz możliwość ich filtrowania na podstawie atrybutów takich jak: OS, typ stacji końcowej, wersja agenta, występujące podatności, atrybuty AD, informacyjne telemetryczne, adresacja IP, charakterystyki hardware, ilości CPU, adresy Mac, interfejsy, nazwa hosta, nazwa grupy, domena).
28.	System musi zapewnić opcję wyświetlenia szczegółów stacji, takie jak aspekty telemetrii, stan stacji, aplikacje oraz umożliwia podjęcie na końcówce następujące opcje działania: Odłącz/ Połącz się od sieci (kwarantanna sieciowa, Uruchom ponownie OS, Zamknij system, Wyślij wiadomość do użytkownika, Odinstaluj agenta, Wyświetl zagrożenia
29.	System musi zapewnić funkcjonalność wykonywania przez administratora poleceń na stacji końcowej (sesji zdalnej), nawet gdy jest ona w stanie izolacji sieciowej. Dodatkowo System tworzy transkrypcję zestawionej sesji. Taka transkrypcja musi być chroniona hasłem, a dostęp do powłoki zdalnej wymusza na administratorze uwierzytelnianie dwuskładnikowe (2FA) w celu udzielenia dostępu. Funkcjonalność ta jest możliwa do Włączenia/Wyłączenia w polityce bezpieczeństwa rozwiązania.
30.	System musi zapewnić integrację z rozwiązaniami z użyciem protokołu Syslog
Funkcjonalność systemu SIEM i kolekcji logów	
31.	System musi umożliwiać pobieranie logów, zdarzeń i metryk z dowolnych systemów i

	urządzeń. Przez pozyskiwanie logów rozumie się: a) pobranie danych i zapisanie w bazie systemu, b) klasyfikacja danych wg typów (np. zalogowanie użytkownika, nawiązanie połączenia, itp.), c) normalizację, czyli nadanie kontekstów znaczeniowych dla poszczególnych fragmentów danych np. username, source_ip itp
32.	Rozwiązanie musi pozwalać na modyfikację mechanizmów klasyfikacji zdarzeń i normalizacji logów dostarczonych razem z produktem (otwarty kod dostarczonych mechanizmów normalizacji). Aktualizacje oprogramowania lub jego części nie mogą nadpisywać ww. modyfikacji
33.	System musi umożliwiać pobieranie logów i innych danych co najmniej następującymi protokołami: a) syslog UDP/TCP, b) HTTP i HTTPS POST c) pliki tekstowe d) wynik działania programów i skryptów uruchamianych na urządzeniu/serwerze lub na podłączonym systemie źródłowym e) logi i informacje przechowywane w bazach danych. Nie mniej niż Oracle, MS SQL, MySQL, PostgreSQL. Musi istnieć możliwość instalacji sterowników do innych typów baz danych w standardzie JDBC lub ODBC (alternatywnie), f) NetFlow v5 i v9, sFlow, jFlow, IPFIX g) Ruch sieciowy, h) RESTful API, i) Windows EventLog j) Windows Performance Monitor k) Windows Management Infrastructure (WMI) l) Windows Registry Ww. Metody muszą być wspierane przez producenta.
34.	System musi umożliwiać stosowanie agentów na monitorowanych serwerach i stacjach roboczych. Agent musi również umożliwiać pobieranie informacji zarówno z systemu, na którym został zainstalowany, jak również z zewnętrznych systemów (np. w celu obsłużenia logów w strefach DMZ lub lokalizacjach zdalnych). Konfiguracja agenta, po podłączeniu do serwera zarządzającego musi odbywać się centralnie
35.	Agent musi zapewniać możliwość szyfrowania i uwierzytelnia komunikacji z serwerem centralnym
36.	Musi istnieć możliwość ograniczenia przepustowości wykorzystywanej przez agenta do transmisji danych
37.	Agent musi mieć możliwość równoważenia obciążenia (wysyłanych danych) pomiędzy kilka serwerów centralnych rozwiązania działających w klastrze lub niezależnie
38.	System musi posiadać możliwość potwierdzania poprawnego dostarczenia danych od agenta do elementów odpowiedzialnych za przechowywanie danych.
39.	Rozwiązanie musi umożliwiać, w oparciu o wyrażenia regularne, wydzielanie ze strumienia logów danych, które nie będą indeksowane w systemie i przesyłanie ich tych danych na storage obiektowy zgodny z S3 lub ich ignorowanie. Dane w ten sposób wydzielone nie będą liczone w limitach licencyjnych produktu
40.	System musi umożliwiać zmianę klasyfikacji i sposobu normalizacji danych w trakcie używania systemu (np. dodanie nowych pól, zmianę znaczenia lub nazwy istniejących itp.) bez konieczności przeprowadzania ponownego odbudowywania bazy danych. System musi pozwalać na równoległe używanie różnych sposobów normalizacji logów

41.	System musi umożliwiać obsługę logów w formacie XML bez konieczności tworzenie parserów. Nazwy pól powinny być określone strukturą XML
42.	System musi umożliwiać obsługę logów w formacie CEF bez konieczności tworzenie parserów. Nazwy pól powinny być określone strukturą CEF
43.	System musi umożliwiać obsługę logów w formacje JSON bez konieczności tworzenie parserów. Nazwy pól powinny być określone strukturą JSON
44.	System musi umożliwiać obsługę logów w formacje CSV bez konieczności tworzenie parserów. Nazwy pól powinny być wierszem nagłówkowym CSV. Musi istnieć możliwość obsługi różnych delimiterów (przecinek, kropka, średnik, tabulator itp.) oraz wartości pól w cudzysłowach.
45.	System musi umożliwiać automatyczną normalizację logów zawierających w treści pary zmienna i wartość np. „user=jkowalski” powinno tworzyć pole „user” o wartości „jkowalski”.
46.	Musi istnieć możliwość wzbogacania danych pochodzących o informacje zwarte w zewnętrznych repozytoriach: a) Katalogi LDAP, b) Bazy danych, c) Bazy noSQL. d) Dane geolokalizacyjne. e) Dane zawarte w logach (np. watchlisty budowane w na podstawie zdarzeń z różnych systemów). W celu ograniczenia zajętości przestrzeni dyskowej dane wzbogacające nie mogą być przechowywane razem z logami, a wzbogacanie powinno odbywać w locie w trakcie odczytu danych z źródeł zewnętrznych.
47.	System musi umożliwiać rozwiązywanie adresów IP do nazw hostów i na odwrót.
48.	System musi umożliwiać analizę logów różnych językach, w tym co najmniej w języku angielskim i polskim. Znaki w logach źródłowych kodowane przy użyciu różnych stron kodowych muszą być konwertowane do wspólnego kodowania (preferowane UTF8 lub UTF16).
49.	System musi utrzymywać repozytorium danych z możliwością ich przeglądania w formie rzeczywistej (raw) oraz udostępniać użytkownikowi dane w formie znormalizowanej (z uwzględnieniem znaczenia poszczególnych zmiennych/pól logu). Dostęp do danych w formie rzeczywistej jak i znormalizowanej musi być możliwy w oparciu o te same narzędzia
50.	Wyszukiwanie danych musi być możliwe z wykorzystaniem filtrów opartych o dane znormalizowane np. zapytanie o konkretny adres IP występujący jako adres źródłowy połączeń. System musi również pozwalać na wyszukiwanie danych w oparciu o wyrażenia regularne zastosowane wobec całego logu jak również pojedynczych pól
51.	System musi analizować zdarzenia w oparciu o znaczniki czasu zawarte w oryginalnych logach jeśli tylko są dostępne. System musi uwzględniać przy prezentacji wyniku możliwość pozyskiwania logów z urządzeń skonfigurowanych w innych strefach czasowych
52.	System musi posiadać możliwość tworzenia wielu typów raportów generowanych zgodnie z kryteriami ustalonymi przez administratorów oraz na podstawie predefiniowanych wzorców (raportów). Raporty muszą być tworzone są w wielu formatach – minimum PDF, CSV, JPG
53.	Zestaw funkcjonalności analitycznych musi uwzględniać co najmniej następujące funkcje:

	a) Statystyki typu suma, średnia, mediana, odchylenie standardowe, najstarszy, najnowszy dla zadanego klucza (np. średni godzinny wolumen danych dla adresu źródłowego), b) Funkcje wykrywania anomalii danych liczbowych. Rozwiązania musi pozwalać na wykrywanie anomalii dla dowolnych parametrów zawartych w logach, a nie tylko parametrów ruchu sieciowego. c) Rozwiązanie musi wykrywać rzadkie wystąpienia wartości i zdarzeń w określonym podzbiorze, d) Budowanie korelacji w oparciu o zdarzenia zawierające jednakowe wartości danych pól. e) Badanie zmian wartości danego pola i alarmowanie lub raportowanie w oparciu o zmianę tej wartości (np. wzrost liczby niepoprawnych zalogowań o 50%).
54.	System musi umożliwiać wykorzystanie w regułach, raportach i dashboardach mechanizmów uczenia maszynowego. System musi posiadać gotowe do użycia algorytmy ML co najmniej: a) detekcja anomalii: funkcja gęstości, współczynnik odstępstwa lokalnego (local outlier factor), OneClassSVM, modele Kelmana, b) Klasyfikacji: BernoulliNB, GausianNB, klasyfikator drzewa decyzyjnego, regresja logistyczna, gradient boosting, perceptron wielowarstwowy,las losowy, c) klasteryzacji: BIRCH, DBSCAN, algorytm centroidów (K-means), spectral clustering. d) Regresji: drzewo decyzyjne, regresja liniowa, las losowy, Lasso, RIDGE, e) Analizy linii czasowy: ARIMA, równanie stanu.
55.	System musi zawierać wizualne narzędzia wspomagające parametryzację i testowanie modeli uczących.
56.	System musi umożliwiać alarmowanie i raportowanie o anomaliach statystycznych dla dowolnych parametrów liczbowych zawartych w logach polegając na odchyleniach w stosunku do wartości przewidywanych (zarówno w górę, jak i w dół) z uwzględnieniem sezonowości (np. różnic wynikających z pory dnia, czy dnia tygodnia).
57.	System musi pozwalać na akceleracje zapytań i raportów, które wykonywane są często, tak by automatycznie budował agregaty pozwalające na szybkie wykonania raportu obejmującego dowolnie długie okresy czasu. Akceleracja musi być dostępna zarówno dla raportów wbudowanych jak i własnych definiowanych przez użytkownika. Raporty takie powinny być dostępne w czasie nie przekraczającym kilku sekund od ich uruchomienia dla dowolnego okresu czasu
58.	System musi posiadać możliwości wizualizacji danych na raportach i dashboardach z wykorzystaniem: a) Tabel, b) Lista zdarzeń, c) Wykresy (co najmniej: słupkowy, kołowy, liniowy, punktowy, bąbelkowy), d) Map, e) Map kolorowanych.
59.	Musi istnieć możliwość tworzenie interaktywnych dashboardów zawierających elementy interfejsu użytkownika takie jak np. pola tekstowe, listy wyboru, checkbox itp. pozwalające na parametryzacje wyświetlanych informacji. Musi istnieć możliwość tworzenie ich bez konieczności programowania (z wykorzystaniem narzędzi graficznych).
60.	Musi istnieć możliwość definiowania akcji typu drill down związanych powiązanych z różnymi typami zdarzeń oraz pól. Dostępne akcje powinny obejmować zewnętrzny URL lub raport/dashboard w samym systemie. Dla zewnętrznych URL musi istnieć możliwość przekazania parametru lub parametrów na podstawie wartości pól, których

	dotyczy akcja drilldown. Musi istnieć możliwość przekazania parametrów metodami GET i POST.
61.	Musi istnieć możliwość tworzenie na podstawie tego samego zapytania do bazy systemu zarówno alarmów jak i raportów. Musi istnieć możliwość utworzenia panelu dashboardu na podstawie dowolnego raportu
62.	System musi umożliwiać korelację zdarzeń pochodzących z różnych systemów źródłowych na podstawie dowolnych pól i zmiennych logu lub dowolnych innych danych wzbogacających log (dane o tożsamości, geolokalizacja, dane o zasobach).
63.	Musi istnieć możliwość zastosowania bez modyfikacji reguł korelacyjnych dla danych historycznych, w celu wykrycia podobnych zdarzeń w przeszłości.
64.	System musi umożliwiać tworzenie reguł korelacyjnych o długim okresie działania (czas pomiędzy najstarszym, a najnowszym zdarzeniem w ramach grupy zdarzeń powiązanych ze sobą). Okres ten nie może być ograniczany żadnymi innymi limitami, poza dostępnością danych w systemie.
65.	System musi pozwalać na przypisanie jednej lub większej liczby akcji do reguły. W szczególności wynikiem działania reguły korelacyjnej powinno być utworzenie alarmu (notable event) lub zwiększenie współczynnika ryzyka związanego z obiektem uczestniczącym w zdarzeniu (użytkownik, host, port itp.).
66.	Dostępne akcje muszą obejmować co najmniej: a) Utworzenie alarmu, b) Zwiększenie współczynnika ryzyka związanego z aktorem bądź obiektem zdarzenia, c) Utworzenie lub modyfikacja list kontrolnych wykorzystywanych w innych alarmach, dashboardach lub raportach, d) Powiadomienie email e) Utworzenie zgłoszenia w systemie ticketingowym.
67.	System musi umożliwiać wzbogacanie informacji o incydentach poprzez automatyczne uruchomienie dodatkowych zapytań i raportów, które pozwolą na automatyczną ocenę wpływu lub potwierdzenie istnienie incydentu.
68.	Musi istnieć możliwość filtracji, alarmowania i korelowania w oparciu o dane geolokalizacyjne np. kraj lub miasto.
69.	Musi istnieć możliwość tworzenia list kontrolnych dowolnego typu (użytkownik, adres IP itp.) wykorzystywanych w alarmach i raportach
70.	System musi pozwalać na definiowanie własnych i modyfikację raportów, zapytań i dashboardów dostarczonych przez producenta
71.	Komunikacja użytkownika z systemem musi odbywać się przy użyciu przeglądarki internetowej (wsparcie dla co najmniej: Edge, Firefox, Chrome).
72.	Nie jest dopuszczalne wymaganie instalacji jakiegokolwiek dedykowanego oprogramowania klienckiego na stacjach roboczych użytkowników w tym wtyczek i środowisk uruchomieniowych w rodzaju Adobe Flash, Java lub Microsoft Silverlight.
73.	System musi utrzymywać szczegółowy log audytowy rejestrujący co najmniej następujące operacje administratorów – login/logoff, uruchamiane zapytania i zmiany konfiguracji systemu
74.	System musi być dostarczony w formie usługi o następujących parametrach: a) Musi umożliwiać przetwarzanie logów o wielkości do 10GB surowych danych (logów) dziennie. Ew. przekroczenia nie mogą skutkować utratą danych. Mogą skutkować opóźnieniem w ich przetwarzaniu. b) Dostawca zapewni możliwość przechowywania danych (dane surowe i wszelkie metadane) przez okres 365 dni od ich powstania. c) Dostępność usługi centralnej SIEM na poziomie 99,5% w roku.

	d) Do 15 dnia każdego miesiąca kalendarzowego wykonawca przygotuje archiwum zebranych danych z poprzedniego miesiąca, w formie skompresowanego, zaszyfrowanego pliku udostępnionego do ściągnięcia przez Zamawiającego. Dostęp do archiwum musi być zapewniony przez cały okres funkcjonowania usługi i 90 dni po zakończeniu jej świadczenia. e) Dostawca dostarczy oprogramowanie SIEM umożliwiające odtworzenie danych przygotowanych w takiej formie jak opisana wyżej. Oprogramowanie musi być możliwe do zainstalowania na systemie Linux lub Windows.
Zakres usługi reagowania na incydenty i utrzymania cyberbezpieczeństwa	
75.	Wykonawca zobowiązany jest utworzyć środowisko EDR i SIEM dla Klienta, w pełni skonfigurowane do poprawnego działania oprogramowania. Zamawiający musi uzyskać dostęp do konsoli EDR i SIEM.
76.	Wykonawca zapewni w ramach usługi wszelkie komponenty sprzętowe i programowe niezbędne do uruchomienia ww. usług po stronie Wykonawcy oraz jeśli konieczne do poprawnego funkcjonowania usługi do zainstalowania w sieci Zamawiającego, w szczególności agentów systemów będących składową usługi oraz ew. sprzęt komputerowy służący do zapewnienie transmisji logów i innych danych do elementów centralnych.
77.	Komunikacja pomiędzy agentami i innymi elementami systemu zlokalizowanymi w sieci Zamawiającego a elementami centralnymi musi być szyfrowania. Zamawiający dopuszcza stworzenie tuneli VPN z wykorzystaniem urządzeń dostarczonych w ramach niniejszego zamówienia.
78.	Przedmiot zamówienia musi zostać uruchomiony w terminie do 30 dni roboczych od daty podpisania umowy
79.	Umowa umożliwi instalację agentów systemu EDR na min. 60 stacjach roboczych i min. 10 serwerach
80.	Umowa w żaden sposób nie będzie ograniczała liczby podłączonych źródeł logów do SIEM lub instalowanych agentów SIEM
81.	Obsługa incydentów musi być dostępna w trybie ciągłym 24 godziny na dobę, 7 dni w tygodniu
82.	Źródłem wykrycia incydentów będą: a) System EDR b) System SIEM c) Dedykowane narzędzia bezpieczeństwa posiadane przez Zamawiającego d) Zgłoszenia pracowników Zamawiającego w formie poczty elektronicznej w szczególności wiadomości podejrzanych o phishing
83.	Wykonawca zobowiązany jest do obsługi incydentów raportowanych przez System w następującym zakresie: a) Niezwłoczne telefoniczne powiadomienie wyznaczonego przedstawiciela Zamawiającego o alarmie o poziomie “critical”. b) Weryfikacja każdego alarmu o poziomie “critical”, “high” i “medium” i określenie go jako incydent lub fałszywy alarm. c) W przypadku wystąpienia incydentu podjęcie reakcji na incydent zgodnie z ustalonymi z Zamawiającym procedurami. d) Celem minimalizacji czasu reakcji na zagrożenia musi zostać dostarczony i wykorzystany system klasy SOAR do automatyzacji zadań, w szczególności czynności takich jak:

<table>
<tr><td></td><td>

zablokowanie określonego ruchu (ip, url, użytkownik) na dostarczonych urządzeniach firewall,
izolacja stacji roboczej/serwera w oparciu o system EDR/XDR i/lub firewall,
zablokowanie konta użytkownika
zabicie procesu na stacji roboczej lub serwerze,
usunięcie maila ze skrzynek użytkowników
uzyskanie potwierdzenia dla ww.czynności od administratora ze strony Zamawiającego
zadanie pytania użytkownikowi lub administratorowi przez formularz WWW w celu uzyskania informacji o incydencie i automatyczne przetworzenie odpowiedzi w systemie SOAR.

e) Przedstawienia raportu z obsługi każdego incydentu w ciągu 72h od zakończenia procedur IR.
f) Realizacja czynności określonych powyżej musi spełniać poniższe wymagania SLA:
<table>
<tr><td></td><td>Critical</td><td>High</td><td>Medium</td></tr>
<tr><td>Powiadomienie o incydencie</td><td>30 min</td><td>n/d</td><td>n/d</td></tr>
<tr><td>Weryfikacja (triage) liczone od wystąpienia alarmu</td><td>2h</td><td>8h</td><td>Do końca 2go dnia roboczego od wystąpienia alarmu</td></tr>
<tr><td>Uruchomienie wbudowanej procedury IR na systemie EDR oraz wykonanie automatycznych procedur SOAR</td><td>Poniżej 5 min</td><td>Poniżej 5 min</td><td>Poniżej 5 min</td></tr>
<tr><td>Uruchomienie manualnej procedury IR liczone od wystąpienia incydentu</td><td>30 min</td><td>8h</td><td>Niezwłocznie po weryfikacji incydentu.</td></tr>
</table>
</td></tr>
<tr><td>84.</td><td>Wykonawca przygotuje w uzgodnieniu z Zamawiającym xx procedury obsługi incydentu następujących typów:

a) Ransomware (EDR);
b) Podejrzenie wycieku informacji związanego z malware;
c) Instalacja/ posiadanie nieautoryzowanego oprogramowania (EDR)
d) Informowanie o wykrytych podatnościach, informowanie o nowych podatnościach i ich proponowanych mitygacjach dla posiadanego oprogramowania (EDR);
e) Podejrzenie przejęcia konta (SIEM)
f) Wykrycie podejrzanego ruchu wychodzącego do sieci Internet (SIEM lub firewall) np. ruch TOR, złośliwe strony, nielegalne treści, wykorzystanie prywatnych skrzynek pocztowych.
g) Monitorowanie TOP 10 technik MITRE dla ransomware w oparciu o raport MITRE Engenuity: https://top-attack-techniques.mitre-engenuity.org/#/top-10-lists</td></tr>
<tr><td>85.</td><td>Wykonawca zobowiąże się do dostarczenia paczek instalacyjnych agentów systemu EDR i SIEM w najnowszej wersji, a także późniejszej jej zdalnej aktualizacji</td></tr>
</table>

86.	Wykonawca zobowiązuje się do proponowania aktualizacji aplikacji, które System uznał za podatne
87.	Wykonawca zobowiązany jest do cyklicznego raportowania o wykonanej pracy oraz stanu infrastruktury klienta pod względem incydentów raportowanych przez System.
88.	Wykonawca zobowiązany jest do cyklicznego, minimum raz na 6 m-cy przeprowadzenia symulacji/testu phishingowego na ustalony temat z Zamawiajacym.
89.	Wykonawca zapewni SLA w zakresie usuwania usterek Systemu na poziomie: a) Wykonawca będzie przyjmował zgłoszenie o awarii systemu poprzez jeden z kanałów komunikacji: email, telefon, system ticketowy Wykonawcy; b) przyjęcie każdego zgłoszenia będzie potwierdzone wiadomością email wysłaną na wskazany w umowie adres Zamawiającego, w dzień roboczy w godzinach 7:00-17:00 w ciągu jednej godziny od wysłania zgłoszenia, w dzień roboczy poza godzinami 7:00-17:00 oraz w dni wolne od pracy do godziny 8:00 następnego dnia roboczego; c) zgłoszenia email oraz ticketowe będą przyjmowane całodobowo, w trybie 24/7/365; d) usunięcie usterki do 16 godzin od chwili przyjęcia zgłoszenia przez Zamawiającego w przypadku całkowitego unieruchomienia Systemu, realizowane w dni robocze; Dostawca nie odpowiada za przekroczenie tego czasu, w przypadkach mających swoje źródło po stronie Zamawiającego (np. brak możliwości kontaktu z osobą wyznaczoną do kontaktów po stronie Zamawiającego.)
90.	Usługa realizowana do 12.03.2026

2. Oprogramowanie do Inwentaryzacji aktywów i ich konfiguracji

Architektura / budowa	
1.	System musi umożliwić bezproblemową i stabilną obsługę co najmniej 70 Klientów jednocześnie.
2.	Klient – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przesyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej.
3.	Konsola administracyjna – przeznaczona do zarządzania całym systemem, w formie w pełni funkcjonalnej aplikacji internetowej (webowej).
4.	Panel pracownika – aplikacja webowa, niewymagająca dodatkowego logowania, dostępna dla pracowników, udostępniająca wybrane dane z konsoli administracyjnej oraz pozwalająca na interakcję z pracownikiem w wybranych obszarach.
5.	Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z Klientami.
6.	Baza danych pracująca na silniku Microsoft SQL Server w wersjach wyspecyfikowanych poniżej
7.	Konfiguracja Architektury: a. Komponenty systemu (Klient, konsola administracyjna, serwer, baza danych) aktualizują się automatycznie poprzez bezpieczne połączenie. b. System zawiera mechanizmy automatycznej konserwacji zgodnie z harmonogramem.
Wymagania systemowe	
8.	Konsola administracyjna musi działać w pełni responsywnie (niezależnie od wielkości i rozdzielczości ekranu urządzenia wyświetlającego) na dowolnej przeglądarce stron

	WWW zgodnej z HTML5 (np. Internet Explorer 11, FireFox, Chrome, Opera).
9.	Klient musi działać na systemach 32 i 64 bitowych: Windows Server 2012/2012R2/2016/2019/2022, Windows 7/8/8.1/10/11, MacOS 10.7/10.8, Linux dla wersji: Ubuntu v.11.04 lub wyższa, Debian v.6.0 lub wyższa, RedHat v.6.0 lub wyższa, CentOS v.6.0 lub wyższa, Fedora v.16 lub wyższa
10.	Serwer musi działać na systemach 64 bitowych: Windows Server 2016/2019/2022, Windows 7/8/8.1/10/11
11.	Serwer www musi być oparty o platformę Microsoft 64 bit (Windows Server 2016/2019/2022, Windows 10 oraz Java 8 (JRE lub JDK), Apache Tomcat 9
12.	Baza danych musi działać na silniku Microsoft SQL Server 2014/2016/2017/2019/2022 w wersji 64 bitowych zarówno komercyjnych jak i bezpłatnych (np. Microsoft SQL Server Express Edition)
13.	System musi mieć możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare.
	Interfejsy
14.	System musi umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory, przy czym import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej zdefiniowanej w systemie
15.	System musi umożliwiać import danych z CSV, Excel, Microsoft SQL Server, MySQL, PostgreSQL
16.	System zapewnia integrację z modelem LLM
	Funkcjonalności systemu zarządzania infrastrukturą IT
17.	System musi umożliwiać pełne zdalne zarządzanie Klientami, obejmujące uruchamianie i wyłączanie, zmianę konfiguracji Klienta, inicjowanie skanowania oraz wykonanie poleceń systemowych. Klient powinien wyświetlać komunikaty w HTML z dokładnymi danymi o czasie wyświetlenia i użytkowniku.
18.	Konsola administracyjna musi być wielojęzyczna (polski i angielski) i oferować intuicyjny interfejs z pełnym zestawem funkcji zarządzania (dodawanie, modyfikowanie, usuwanie). Musi także zawierać co najmniej 140 różnorodnych dashboardów, w tym dashboardy użytkownika, prezentujące parametry infrastruktury, sieci oraz bezpieczeństwa. Użytkownicy powinni mieć możliwość samodzielnego konfigurowania dashboardów użytkownika, a dashboardy sieciowe i bezpieczeństwa muszą zawierać szczegółowe widżety z informacjami o stanie usług i bezpieczeństwie.
19.	W konsoli powinna istnieć funkcja filtrowania danych na dashboardach oraz możliwość personalizacji interfejsu przez użytkownika, w tym definiowanie własnych pól, filtrów i widoków, z zachowaniem tych ustawień pomiędzy sesjami. Konsola musi także umożliwiać definiowanie poziomów uprawnień dla użytkowników i grup, z opcją dziedziczenia oraz integrację z Active Directory dla zarządzania dostępem.
20.	Konsola powinna posiadać zaawansowane funkcje zarządzania rekordami, w tym wykonanie poleceń na wielu rekordach jednocześnie oraz dostęp do szczegółowych informacji o pracy urządzeń
21.	Panel pracownika systemu musi automatycznie uruchamiać się i autoryzować przy logowaniu użytkownika, z możliwością definiowania zakresu dostępnych informacji przez administratora dla poszczególnych grup pracowników. Panel kierownika powinien dodatkowo agregować i analizować dane z paneli pracowników. Informacje w panelu muszą być organizowane w logiczne sekcje, które można indywidualnie lub grupowo włączać i wyłączać przez administratora
22.	System musi umożliwiać kompleksowe zarządzanie licencjami w różnych modelach i

	strukturach organizacyjnych, w tym audyty, zarządzanie oprogramowaniem i oprogramowaniem zabronionym, oraz przypisywanie i rozliczanie różnych typów licencji. Musi także rejestrować historię licencji oraz zapewniać funkcje inwentaryzacji i zdalnej dezinstalacji oprogramowania
23.	System powinien posiadać rozbudowaną bazę wzorców oprogramowania, umożliwiać definiowanie własnych wzorców i automatycznie importować nowe wzorce od producenta. Musi także dostarczać szczegółowe informacje o zainstalowanych pakietach i ich wykorzystaniu, w tym edycje Microsoft Office
24.	System musi oferować rozbudowane funkcje inwentaryzacji sprzętu komputerowego, włączając automatyczną inwentaryzację zarówno w sieci lokalnej jak i zdalnej, szczegółowe skanowanie komponentów (np. RAM, monitory, dyski twarde) oraz zarządzanie informacjami o zainstalowanym sprzęcie. Powinien także umożliwiać ewidencję zmian konfiguracji sprzętu, identyfikować i klasyfikować urządzenia podłączane do komputerów oraz monitorować historię ich podłączeń.
25.	System musi umożliwiać wszechstronną inwentaryzację sprzętu, włączając urządzenia inne niż komputery (np. drukarki, routery). Musi zapewniać zarządzanie dokumentacją związaną z urządzeniami, monitorować ich ruch oraz przypominać o terminach gwarancji i umowach utrzymaniowych
26.	Ochrona danych (DLP) musi obejmować automatyczne tworzenie listy podłączanych do komputerów urządzeń USB i ich klasyfikację. System powinien dostarczać informacje o historii użytkowania urządzeń zewnętrznych oraz umożliwiać zarządzanie dozwolonymi do użytku urządzeniami USB zgodnie z zdefiniowanymi regułami
27.	System musi oferować kompleksową zdalną administrację komputerami, włączając w to automatyczne wykonywanie dowolnych poleceń (np. zarządzanie aplikacjami, plikami, rejestrami systemowymi) oraz zarządzanie cyklicznymi zadaniami z harmonogramem. Powinien obsługiwać technologię Intel vPro dla zdalnej konfiguracji i zarządzania, a także pozwalać na zdalne przejęcie kontroli nad komputerem za pomocą technologii Ultra VNC, umożliwiając operowanie na wielu sesjach jednocześnie. System powinien integrować zaawansowane mechanizmy skryptowe wspierane przez AI dla automatycznego generowania poleceń oraz umożliwiać zarządzanie i tworzenie zadań cyklicznych z różnorodnymi opcjami cykliczności i zakończenia
28.	System musi umożliwić monitorowanie i zarządzanie wydrukami z dowolnej drukarki (lokalnej czy sieciowej), rejestrując szczegółowe informacje o każdym wydruku, w tym koszty, dzięki wbudowanemu cennikowi. System powinien również prognozować przyszłe koszty drukowania oraz pozwalać na zarządzanie drukarkami według różnych parametrów, w tym statusu i materiałów eksploatacyjnych.
29.	System musi oferować monitorowanie aktywności internetowej użytkowników na różnych przeglądarkach, nawet przy szyfrowanych połączeniach (https), rejestrując detale takie jak adresy IP, czas połączenia, a także analizując treści stron za pomocą algorytmów sztucznej inteligencji do klasyfikacji i kontroli treści.
30.	System musi zapewniać monitorowanie wybranych serwerów WWW, prezentując informacje o ich statusie i aktywności, umożliwiając analizę treści stron oraz graficzną prezentację danych związanych z ich działaniem, w tym czasem odpowiedzi i aktywnością w określonym okresie
31.	System musi umożliwiać monitorowanie komunikatów Syslog.
32.	System musi oferować monitorowanie pracy komputerów, w tym dat startu i zakończenia pracy, logowania użytkowników, a także zdalne monitorowanie sesji połączeń, rejestrując szczegóły takie jak adresy IP i dane użytkowników.
33.	System musi integrować monitoring warunków środowiskowych za pomocą sensorów po SNMP, umożliwiając graficzną prezentację danych, wysyłanie alertów

34.	System musi posiadać zintegrowane repozytorium CMDB, umożliwiające zarządzanie zasobami IT, w tym szczegółowe informacje o użytkownikach, urządzeniach, licencjach, a także o oprogramowaniu i jego licencjach, z możliwością importu i eksportu danych.
35.	System musi umożliwiać monitorowanie i analizę czasu pracy użytkowników, z możliwością definiowania grup przypisanych do przełożonych i prezentacji szczegółowych danych o aktywności użytkowników w formie widżetów i danych analitycznych. Informacje o czasie pracy, sesjach, aktywności w aplikacjach oraz produktywności powinny być możliwe do udostepnienia w panelu pracownika
36.	System musi oferować zaawansowane możliwości raportowania i eksportu danych, umożliwiając wyeksportowanie informacji do różnych formatów, w tym xls, csv, html, oraz graficznych. Powinien także wspierać generowanie wieloparametrycznych raportów z możliwością stosowania filtrów, obsługę wieloinstancyjności raportowania oraz integrację z narzędziami do tworzenia raportów takimi jak SAP Crystal Reports i Stimulsoft, obejmując co najmniej 150 zdefiniowanych raportów. Dodatkowo, system musi posiadać możliwość konfiguracji harmonogramu umożliwiającego cykliczne wysyłanie raportów oraz zapisywanie ich w dowolnym miejscu, z automatycznym generowaniem raportu w formacie PDF jako wynikiem wykonania harmonogramu.
37.	System musi oferować rozbudowany interfejs API, umożliwiający komunikację za pomocą REST API. Musi on zapewniać szyfrowaną komunikację z użyciem protokołu TLS 1.3 oraz możliwość tworzenia złożonych requestów JSON. Klucze zabezpieczeń powinny być modyfikowalne i mogą mieć co najmniej 32 znaki
38.	System musi umożliwiać generowanie różnorodnych powiadomień, w tym alertów w konsoli, e-maili oraz wiadomości SMS, z możliwością edycji treści powiadomień i definiowania grup odbiorców. Powinien obsługiwać automatyczne wywoływanie zadań i integrować się z CMD oraz Windows PowerShell, zapewniając co najmniej 30 predefiniowanych powiadomień oraz możliwość ich personalizacji
39.	System musi zapewniać rozbudowane funkcje bezpieczeństwa, w tym definicję i zarządzanie prawami dostępu oraz zaawansowane opcje uwierzytelniania. Wymaga silnych haseł, obsługuje wieloskładnikowe uwierzytelnianie i posiada mechanizmy szyfrowania danych.

3. UPS stanowiskowy

Lp.	Minimalne parametry	
1.	Pojemność energetyczna	Min. 800VA / 480W
2.	Sprawność w trybie LINE [%] (pełne obciążenie)	Min. 96.2
3.	Czas transferu (tryb AC / linia do trybu bateryjnego) [ms]	Min. 2-6 ms
4.	Zakres napięcia wejściowego	Min. 162-290 VAC
5.	Zakres częstotliwości	Min. 45 Hz – 65 Hz (samoczynna adaptacja do 50/60 Hz)
6.	Nominalne napięcie wyjściowe	230 VAC
7.	Kształt fali wyjściowej	Pełna fala sinusoidalna
8.	Złącze wejściowe	CEE 7/7
9.	Typ wyjścia	Typ E
10.	Typ E (CEE 7/5)	Min. 2
11.	Ochrona linii danych	Min. Port RJ-11, port RJ-45 (100 mbit)
12.	Sygnalizacja pracy	Wyświetlacz LCD

13.	Zabezpieczenia	a. Automatyczna regulacja Napięcia (AVR)
14.	Obudowa	b. Wolnostojąca
15.	Wyposażenie	Kabel zasilający Instrukcja obsługi Oprogramowanie
16.	Gwarancja	co najmniej 24 miesięcy bezpłatnej gwarancji, której termin liczony będzie od dnia podpisania końcowego protokołu odbioru.

4. Przełącznik LAN 24 porty

Lp.	Parametry
1.	Przełącznik musi być dedykowanym urządzeniem sieciowym o wysokości 1U przystosowanym do montowania w szafie rack.
2.	Przełącznik musi posiadać 24 porty dostępowe Ethernet 10/100/1000 Auto-MDI/MDIX.
3.	Przełącznik musi być wyposażony w nie mniej niż 4 wbudowane porty uplink typu SFP/SFP+ obsługujące co najmniej standardy 10GBASE-USR, SR, LR, oraz 1000BASE-T, SX, LX, LH, a także BX-U i BX-D.
4.	Przełącznik musi posiadać wbudowany zasilacz AC oraz wentylację.
5.	Przełącznik musi być wyposażony w port konsoli oraz dedykowany interfejs Ethernet do zarządzania OOB (out-of-band).
6.	Przełącznik musi być wyposażony w nie mniej niż 2 GB pamięci Flash oraz 2 GB pamięci DRAM. Przełącznik musi posiadać slot USB pozwalający na podłączenie zewnętrznego nośnika danych. Przełącznik musi umożliwiać uruchomienie systemu operacyjnego z zewnętrznego nośnika danych umieszczonego w slocie USB.
7.	Zarządzanie urządzeniem musi odbywać się za pośrednictwem interfejsu linii komend (CLI) przez port konsoli, telnet, ssh, a także za pośrednictwem interfejsu WWW.
8.	Przełącznik musi posiadać architekturę non-blocking. Wydajność przełączania w warstwie 2 nie może być niższa niż 120 Gb/s i 90 milionów pakietów na sekundę. Przełącznik nie może obsługiwać mniej niż 16 000 adresów MAC.
9.	Przełącznik musi obsługiwać ramki Jumbo (9216 bajtów).
10.	Przełącznik musi obsługiwać sieci VLAN zgodne z IEEE 802.1Q w ilości nie mniejszej niż 2048. Przełącznik musi obsługiwać sieci VLAN oparte o porty fizyczne (port-based) i adresy MAC (MAC-based).
11.	Urządzenie musi obsługiwać agregowanie połączeń zgodne z IEEE 802.3AD - nie mniej niż 128 grup LAG, maksymalna liczba portów wspieranych w grupie LAG nie może być mniejsza niż 8.
12.	Przełącznik musi obsługiwać protokół Spanning Tree i Rapid Spannig Tree, , a także Multiple Spanning Tree (nie mniej niż 64 instancje MSTP).
13.	Przełącznik musi obsługiwać protokół LLDP i LLDP-MED.
14.	Urządzenie musi obsługiwać ruting między sieciami VLAN – ruting statyczny, oraz protokół rutingu dynamicznego RIP. Ilość tras obsługiwanych sprzętowo nie może być mniejsza niż 512 podsieci (prefixów) i 4096 tras typu „host” (host routes).
15.	Urządzenie musi posiadać mechanizmy priorytetyzowania i zarządzania ruchem sieciowym (QoS) w warstwie 2 i 3 dla ruchu wchodzącego i wychodzącego. Klasyfikacja ruchu musi odbywać się w zależności od co najmniej: interfejsu, typu ramki Ethernet, sieci VLAN, priorytetu w warstwie 2 (802.1P), adresów MAC, adresów IP, wartości pola ToS/DSCP w nagłówkach IP, portów TCP i UDP. Urządzenie musi obsługiwać sprzętowo nie mniej niż 8 kolejek per port fizyczny.

16.	Urządzenie musi obsługiwać filtrowanie ruchu na co najmniej na poziomie portu i sieci VLAN dla kryteriów z warstw 2-4. Urządzenie musi realizować sprzętowo nie mniej niż 1500 reguł filtrowania ruchu. W regułach filtrowania ruchu musi być dostępny mechanizm zliczania dla zaakceptowanych lub zablokowanych pakietów. Musi być dostępna funkcja edycji reguł filtrowania ruchu na samym urządzeniu.
17.	Przełącznik musi obsługiwać takie mechanizmu bezpieczeństwa jak limitowanie adresów MAC, Dynamic ARP Inspection, DHCP snooping.
18.	Przełącznik musi obsługiwać IEEE 802.1X zarówno dla pojedynczego, jak i wielu suplikantów na porcie. Przełącznik musi przypisywać ustawienia dla użytkownika na podstawie atrybutów zwracanych przez serwer RADIUS (co najmniej VLAN oraz reguła filtrowania ruchu). Musi istnieć możliwość pominięcia uwierzytelnienia 802.1x dla zdefiniowanych adresów MAC. Przełącznik musi obsługiwać co najmniej następujące typy EAP: MD5, TLS, TTLS, PEAP.
19.	Urządzenie musi obsługiwać protokół SNMP (wersje 2c i 3), oraz grupy RMON 1, 2, 3, 9. Musi być dostępna funkcja kopiowania (mirroring) ruchu na poziomie portu i sieci VLAN.
20.	Architektura systemu operacyjnego urządzenia musi posiadać budowę modularną (poszczególne moduły muszą działać w odseparowanych obszarach pamięci), m.in. moduł przekazywania pakietów, odpowiedzialny za przełączanie pakietów musi być oddzielony od modułu rutingu IP, odpowiedzialnego za ustalanie tras rutingu i zarządzanie urządzeniem.
21.	Urządzenie musi posiadać mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż 40 poprzednich, kompletnych konfiguracji.
22.	Urządzenie powinno umożliwiać stackowanie z innymi urządzeniami takiego samego typu w ilości nie mniejszej niż 4 sztuki. Stackowanie powinno być możliwe przy wykorzystaniu standardowych portów typu uplink. Dopuszczalne są rozwiązania gdzie stackownie jest wbudowaną funkcjonalnością, oraz takie gdzie stackowanie wymaga zakupu dodatkowej licencji.
23.	Wraz z urządzeniem wymagane jest dostarczenie gwarancji ważnej przez okres 2 lat.

5. Przełącznik LAN 12 porty

Lp.	Parametr
1.	Przełącznik musi być dedykowanym urządzeniem sieciowym o wysokości 1U.
2.	Przełącznik musi posiadać 12 portów dostępowych Ethernet 10/100/1000 Auto-MDI/MDIX.
3.	Przełącznik musi być wyposażony w nie mniej niż 2 wbudowane porty uplink typu SFP/SFP+ obsługujące co najmniej standardy 10GBASE-USR, SR, LR, oraz 1000BASE-T, SX, LX, LH, a także BX-U i BX-D.
4.	Przełącznik musi posiadać wbudowany zasilacz AC.
5.	Przełącznik musi być wyposażony w port konsoli oraz dedykowany interfejs Ethernet do zarządzania OOB (out-of-band).
6.	Przełącznik musi być wyposażony w nie mniej niż 2 GB pamięci Flash oraz 2 GB pamięci DRAM. Przełącznik musi posiadać slot USB pozwalający na podłączenie zewnętrznego nośnika danych. Przełącznik musi umożliwiać uruchomienie systemu operacyjnego z zewnętrznego nośnika danych umieszczonego w slocie USB.
7.	Zarządzanie urządzeniem musi odbywać się za pośrednictwem interfejsu linii komend (CLI) przez port konsoli, telnet, ssh, a także za pośrednictwem interfejsu WWW.

8.	Przełącznik musi posiadać architekturę non-blocking. Wydajność przełączania w warstwie 2 nie może być niższa niż 64 Gb/s i 45 milionów pakietów na sekundę. Przełącznik nie może obsługiwać mniej niż 16 000 adresów MACPrzełącznik musi obsługiwać ramki Jumbo (9216 bajtów).
9.	Przełącznik musi obsługiwać sieci VLAN zgodne z IEEE 802.1Q w ilości nie mniejszej niż 2048. Przełącznik musi obsługiwać sieci VLAN oparte o porty fizyczne (port-based) i adresy MAC (MAC-based).
10.	Urządzenie musi obsługiwać agregowanie połączeń zgodne z IEEE 802.3AD - nie mniej niż 128 grup LAG, maksymalna liczba portów wspieranych w grupie LAG nie może być mniejsza niż 8.
11.	Przełącznik musi obsługiwać protokół Spanning Tree i Rapid Spannig Tree, , a także Multiple Spanning Tree (nie mniej niż 64 instancje MSTP).
12.	Przełącznik musi obsługiwać protokół LLDP i LLDP-MED.
13.	Urządzenie musi obsługiwać ruting między sieciami VLAN – ruting statyczny, oraz protokół rutingu dynamicznego RIP. Ilość tras obsługiwanych sprzętowo nie może być mniejsza niż 512 podsieci (prefixów) i 4096 tras typu „host” (host routes).
14.	Urządzenie musi posiadać mechanizmy priorytetyzowania i zarządzania ruchem sieciowym (QoS) w warstwie 2 i 3 dla ruchu wchodzącego i wychodzącego. Klasyfikacja ruchu musi odbywać się w zależności od co najmniej: interfejsu, typu ramki Ethernet, sieci VLAN, priorytetu w warstwie 2 (802.1P), adresów MAC, adresów IP, wartości pola ToS/DSCP w nagłówkach IP, portów TCP i UDP. Urządzenie musi obsługiwać sprzętowo nie mniej niż 8 kolejek per port fizyczny.
15.	Urządzenie musi obsługiwać filtrowanie ruchu na co najmniej na poziomie portu i sieci VLAN dla kryteriów z warstw 2-4. Urządzenie musi realizować sprzętowo nie mniej niż 1500 reguł filtrowania ruchu. W regułach filtrowania ruchu musi być dostępny mechanizm zliczania dla zaakceptowanych lub zablokowanych pakietów. Musi być dostępna funkcja edycji reguł filtrowania ruchu na samym urządzeniu.
16.	Przełącznik musi obsługiwać takie mechanizmu bezpieczeństwa jak limitowanie adresów MAC, Dynamic ARP Inspection, DHCP snooping.
17.	Przełącznik musi obsługiwać IEEE 802.1X zarówno dla pojedynczego, jak i wielu suplikantów na porcie. Przełącznik musi przypisywać ustawienia dla użytkownika na podstawie atrybutów zwracanych przez serwer RADIUS (co najmniej VLAN oraz reguła filtrowania ruchu). Musi istnieć możliwość pominięcia uwierzytelnienia 802.1x dla zdefiniowanych adresów MAC. Przełącznik musi obsługiwać co najmniej następujące typy EAP: MD5, TLS, TTLS, PEAP.
18.	Urządzenie musi obsługiwać protokół SNMP (wersje 2c i 3), oraz grupy RMON 1, 2, 3, 9. Musi być dostępna funkcja kopiowania (mirroring) ruchu na poziomie portu i sieci VLAN.
19.	Architektura systemu operacyjnego urządzenia musi posiadać budowę modularną (poszczególne moduły muszą działać w odseparowanych obszarach pamięci), m.in. moduł przekazywania pakietów, odpowiedzialny za przełączanie pakietów musi być oddzielony od modułu rutingu IP, odpowiedzialnego za ustalanie tras rutingu i zarządzanie urządzeniem.
20.	Urządzenie musi posiadać mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż 40 poprzednich, kompletnych konfiguracji.
21.	Urządzenie powinno umożliwiać stackowanie z innymi urządzeniami takiego samego typu w ilości nie mniejszej niż 4 sztuki. Stackowanie powinno być możliwe przy wykorzystaniu standardowych portów typu uplink. Dopuszczalne są rozwiązania gdzie

	stackownie jest wbudowaną funkcjonalnością, oraz takie gdzie stackowanie wymaga zakupu dodatkowej licencji.
22.	Wraz z urządzeniem wymagane jest dostarczenie gwarancji ważnej przez okres 2 lat.

6. Firewall next-generation

1.	System zabezpieczeń firewall musi być dostarczony jako specjalizowane urządzenie zabezpieczeń sieciowych (appliance). W architekturze systemu musi występować separacja modułu zarządzania i modułu przetwarzania danych. Akceptowana jest również separacja logiczna zasobów zrealizowana za pomocą przypisania dedykowanej ilości rdzeni zasobów procesorów (tzw. CPU cores) do obu z funkcji lub alternatywnie za pomocą oddzielnych dedykowanych procesorów (tzw. CPU) dla każdej z funkcji. Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta
2.	Całość sprzętu i oprogramowania musi być dostarczona i wspierana przez jednego producenta. Producent oferowanego rozwiązania w postępowaniu był wskazywany w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w części („ćwiartce) Leaders w co najmniej jednym raporcie opublikowanym w ciągu ostatnich 18 miesięcy liczonym od terminu składania ofert.
3.	System zabezpieczeń firewall musi posiadać przepływność nie mniej niż 2,6 Gbit/s dla kontroli firewall z włączoną funkcją kontroli aplikacji, nie mniej niż 1,2 Gbit/s dla kontroli zawartości (w tym kontrola anty-wirus, anty-spyware, IPS) i obsługiwać nie mniej niż 195 000 jednoczesnych połączeń oraz 34000 nowych sesji na sekundę.
4.	System zabezpieczeń firewall musi posiadać konstrukcję bez wentylatorową oraz być wyposażony w co najmniej 8 portów tzw. "miedzianych" 1G, dedykowany port do zarządzania 1G oraz port konsolowy RJ45 lub micro USB**.**
5.	Interfejsy sieciowe systemu zabezpieczeń firewall muszą działać w trybie rutera (tzn. w warstwie 3 modelu OSI), w trybie przełącznika (tzn. w warstwie 2 modelu OSI), w trybie transparentnym oraz w trybie pasywnego nasłuchu (sniffer). Funkcjonując w trybie transparentnym urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych jak również nie może wprowadzać segmentacji sieci na odrębne domeny kolizyjne w sensie Ethernet/CSMA
6.	Tryb pracy musi być ustalany w konfiguracji interfejsu sieciowego, a system zabezpieczeń firewall musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny system, wirtualna domena, itp.).
7.	System zabezpieczeń firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Interfejsy sieciowe pracujące w trybie transparentnym, L2 i L3 muszą pozwalać na tworzenie subinterfejsów VLAN. Urządzenie musi obsługiwać 4000 znaczników VLAN
8.	System zabezpieczeń firewall zgodnie z ustaloną polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7).
9.	Polityka zabezpieczeń firewall musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, kategorie URL, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie
10.	System zabezpieczeń firewall musi działać zgodnie z zasadą bezpieczeństwa „The

	Principle of Least Privilege", tzn. system zabezpieczeń blokuje wszystkie aplikacje, poza tymi które w regułach polityki bezpieczeństwa firewall są wskazane jako dozwolone.
11.	System zabezpieczeń firewall musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury i analizę heurystyczną.
12.	Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach.
13.	Zezwolenie dostępu do aplikacji musi odbywać się w regułach polityki firewall (tzn. reguła firewall musi posiadać oddzielne pole gdzie definiowane są aplikacje i oddzielne pole gdzie definiowane są protokoły sieciowe, nie jest dopuszczalne definiowane aplikacji przez dodatkowe profile). Nie jest dopuszczalna kontrola aplikacji w modułach innych jak firewall (np. w IPS lub innym module UTM).
14.	Nie jest dopuszczalne, aby blokownie aplikacji (P2P, IM, itp.) odbywało się poprzez inne mechanizmy ochrony niż firewall.
15.	Nie jest dopuszczalne rozwiązanie, gdzie kontrola aplikacji wykorzystuje moduł IPS, sygnatury IPS ani dekodery protokołu IPS.
16.	System zabezpieczeń firewall musi wykrywać co najmniej 3500 różnych aplikacji (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS. oraz z aplikacjami przemysłowymi (tzw. ICS/OT) np. DNP3, Modbus.
17.	System zabezpieczeń firewall musi pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
18.	System zabezpieczeń firewall musi zapewniać możliwość segmentacji aplikacji na standardowych dla nich portach usług w obrębie pojedynczej reguły polityki firewall, tj. musi istnieć możliwość takiej konfiguracji pojedynczej reguły firewall, która zezwoli na działanie kilku aplikacji, wyłącznie jeśli nawiązanie połączenia następuje na port właściwy dla danej aplikacji, np. jeśli pojedyncza reguła zezwala na ruch SMTP i DNS, to SMTP nie może być dozwolone na porcie 53 (właściwym dla DNS), a DNS na porcie 25 (właściwym dla SMTP).
19.	System zabezpieczeń firewall musi automatycznie weryfikować spójność konfiguracji polityk bezpieczeństwa z punktu widzenia kompletności użytych przez administratora sygnatur aplikacyjnych potrzebnych do prawidłowego działania polityki. Np. jeśli do prawidłowej obsługi dostępu do aplikacji „Facebook" potrzebne jest dodatkowo użycie aplikacji „SSL", a administrator nie uwzględni tej aplikacji w polityce, to system powinien ostrzec o tym fakcie administratora w momencie zatwierdzania nowej polityki.
20.	System zabezpieczeń firewall musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (AV, IPS, AS, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AV, IPS, AS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.
21.	System zabezpieczeń firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: cab, dll, doc, szyfrowany doc, docx, ppt, szyfrowany ppt, pptx, xls, szyfrowany xls, xlsx, rar, szyfrowany rar, zip, szyfrowany zip, exe, gzip, hta, mdb, mdi, ocx, pdf, pgp, pif, pl, tar, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.
22.	System zabezpieczeń firewall musi pozwalać na analizę i blokowanie plików przesyłanych w zidentyfikowanych aplikacjach. W przypadku gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP (np. tcp/80) musi istnieć możliwość

	przydzielania innych, osobnych profili analizujących i blokujących dla każdej aplikacji.
23.	System zabezpieczeń firewall musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołami SSL,TLS 1.3 oraz HTTP/2) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. System musi mieć możliwość deszyfracji niezaufanego ruchu HTTPS i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i anyspyware), filtracja plików, danych i URL.
24.	System zabezpieczeń firewall musi zapewniać inspekcję komunikacji szyfrowanej protokołem SSL dla ruchu innego niż HTTP. System musi mieć możliwość deszyfracji niezaufanego ruchu SSL i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i kontrola aplikacji, wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL.
25.	System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący ruch SSL który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa.
26.	System zabezpieczeń musi posiadać wbudowaną i automatycznie aktualizowaną przez producenta listę aplikacji dla których niemożliwa jest deszyfracja ruchu (np. z powodu wymuszania przez nie uwierzytelnienia użytkownika z zastosowaniem certyfikatu lub stosowania mechanizmu „certificate pinning"). Lista ta stanowi automatyczne wyjątki od ogólnych reguł deszyfracji.
27.	System zabezpieczeń firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.
28.	System zabezpieczeń firewall musi zapewniać możliwość transparentnego ustalenia tożsamości użytkowników sieci (integracja z Active Directory, Ms Exchange, serwerami Terminal Services). Polityka kontroli dostępu (firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.
29.	System zabezpieczeń firewall musi odczytywać oryginalne adresy IP stacji końcowych z pola X-Forwarded-For w nagłówku http i wykrywać na tej podstawie użytkowników z domeny Windows Active Directory generujących daną sesje w przypadku gdy analizowany ruch przechodzi wcześniej przez serwer Proxy ukrywający oryginalne adresy IP zanim dojdzie on do urządzenia.
30.	Po odczytaniu zawartości pola XFF z nagłówka http system zabezpieczeń musi usunąć odczytany źródłowy adres IP przed wysłaniem pakietu do sieci docelowej.
31.	System zabezpieczeń firewall musi posiadać moduł analizujący, w czasie rzeczywistym, zapytania DNS przechodzące przez urządzenie w celu wykrywania domen złośliwych, domen generowanych przez algorytmy DGA oraz tunelowania złośliwej komunikacji (lub wycieku danych) w protokole DNS. Baza domen DNS-owych musi być regularnie aktualizowana w sposób automatyczny. Dodatkowo ochrona DNS powinna działać dla ruchu przechodzącego przez system zabezpieczeń firewall bez potrzeby wskazywania go jako serwer DNS.
32.	System zabezpieczeń firewall musi posiadać możliwość kategoryzowania ruchu DNS i budowania reguł filtrujących wybrane kategorie w zależności od ryzyka z nimi związanego. System powinien rozróżniać co najmniej następujące kategorie domen:

	C&C, złośliwe, DDNS, nowo zarejestrowane, phishing.
33.	System zabezpieczeń firewall musi posiadać funkcję podmiany adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole).
34.	System zabezpieczeń firewall musi posiadać moduł filtrowania stron WWW w zależności od kategorii treści stron HTTP bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza web filtering musi być regularnie aktualizowana w sposób automatyczny.
35.	System zabezpieczeń firewall musi umożliwiać kategoryzacje strony WWW za pomocą mechanizmu przypisującego do konkretnej strony kilka kategorii (np. portal finansowy i portal informacyjny). Dodatkowo, powinna istnieć możliwość budowania własnych kategorii bazujących na kombinacji kategorii standardowych (np. własna kategoria wiadomości finansowe zawierające wszystkie strony skategoryzowane jako portale finansowe i informacyjne) jak również budowanie kategorii na bazie ryzyka bezpieczeństwa danej strony (niskie, średnie, wysokie) i określenia czy dana strona jest stroną nowopowstałą.
36.	System zabezpieczeń firewall musi posiadać mechanizm analizy w czasie rzeczywistym stron WWW i na podstawie algorytmów uczenia maszynowego rozpoznawać i blokować złośliwą zawartość JavaScript, złośliwe pliki wykonywalne (tzw. PE i DLL), złośliwe skrypty PowerShell, ataki Phishing jak również próby wykradania poświadczeń.
37.	System zabezpieczeń firewall musi posiadać moduł filtrowania stron WWW który można uruchomić per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
38.	System zabezpieczeń firewall musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (nie tylko filtrującego) ruch w politykach bezpieczeństwa.
39.	System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.
40.	System zabezpieczeń firewall musi posiadać moduł inspekcji antywirusowej uruchamiany per aplikacja oraz wybrany dekoder taki jak http, http2 smtp, imap, pop3, ftp, smb kontrolującego ruch bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-wirus musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
41.	Rozwiązanie musi posiadać możliwość analizy, identyfikacji oraz blokowania wcześniej nieznanej komunikacji C2 (command-and-control) oraz spyware w oparciu o mechanizmy uczenia maszynowego realizowane w chmurze producenta. Wymagana analiza i detekcja musi umożliwiać blokowanie wykrytej komunikacji C2 w czasie rzeczywistym). Analiza i wykrywanie nieopisanych wcześniej w sygnaturach połączeń C2 musi być możliwa minimum dla ruchu typu: http, http2, ssl, niezidentyfikowanych przez firewall aplikacji działających na protokołach TCP i UDP. Aktualizacja zasad i sposobu pracy silników detekcji, powinna być realizowana w chmurze producenta bez potrzeby aktualizacji oprogramowania i instalacji nowych wersji reguł i sygnatur na firewallu zaimplementowanym w chronionym środowisku.
42.	System zabezpieczeń firewall musi posiadać modułu inspekcji antywirusowej uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per urządzenie lub jego część (np.

	interfejs sieciowy, strefa bezpieczeństwa).
43.	System zabezpieczeń firewall musi posiadać modułu wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI IPS/IDS bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
44.	System zabezpieczeń firewall musi posiadać moduł IPS/IDS uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja IPS/IDS uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
45.	System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
46.	System zabezpieczeń firewall musi posiadać moduł anty-spyware bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
47.	System zabezpieczeń firewall musi posiadać moduł anty-spyware uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja anty-spyware uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
48.	System zabezpieczeń firewall musi posiadać możliwość ręcznego tworzenia sygnatur anty-spyware bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
49.	System zabezpieczeń firewall musi posiadać funkcję automatycznego pobierania, z zewnętrznych systemów, adresów, grup adresów, nazw dns oraz stron www (url) oraz tworzenia z nich obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty.
50.	System zabezpieczeń firewall musi posiadać funkcję automatycznego przeglądania logowanych informacji oraz pobierania z nich źródłowych i docelowych adresów IP hostów biorących udział w konkretnych zdarzeniach zdefiniowanych według wybranych atrybutów. Na podstawie zebranych informacji musi istnieć możliwość tworzenia obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty.
51.	System zabezpieczeń firewall musi umożliwiać zdefiniowanie stron WWW oraz kategorii URL, serwisów do których użytkownicy mogą wysyłać swoje poświadczenia. W przypadku próby wysłania poświadczeń do niezaufanej strony lub serwisu ruch musi zostać zablokowany.
52.	System zabezpieczeń firewall musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.
53.	System zabezpieczeń firewall musi posiadać funkcję wykrywania na podstawie algorytmów uczenia maszynowego złośliwych plików wykonywalnych, skryptów PowerShelll oraz plików MS Office przechodzących przez urządzenie i blokowania ich w czasie rzeczywistym.
54.	System bezpieczeństwa musi zapewniać możliwość przechwytywania i przesyłania do zewnętrznego systemu typu „Sand-Box” (np. dostarczanego przez producenta zaoferowanego Systemu) plików wykonywalnych (minimum pliki typu PE) i dokumentów (minimum MS Office i PDF) przechodzących przez firewall w celu

	ochrony przed zagrożeniami typu zero-day. System zewnętrzny, na podstawie przeprowadzonej analizy, musi aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze końcowym.
55.	Administrator musi mieć możliwość konfiguracji mechanizmu wysyłania plików wykonywalnych (minimum pliki typu PE) i dokumentów (minimum MS Office i PDF) do środowiska chmurowego producenta typu „Sand-Box", zaoferowanego systemu w celu wykrywania potencjalnych nierozpoznanych sygnaturowo zagrożeń.
56.	Administrator musi posiadać możliwość zdefiniowania jaki rodzaj plików będzie wysyłany do „Sand- Box-a" i w jakiej relacji ruchowej (download, upload).
57.	Administrator musi mieć możliwość dostępu do systemu analizy plików wykonywalnych w celu sprawdzenia, które pliki i z jakiego powodu zostały uznane za złośliwe, jak również sprawdzić którzy użytkownicy te pliki pobierali.
58.	System „Sand-Box" działający po stornie producenta, musi zwrotnie przesyłać aktualizacje sygnatur wykrytych zagrożeń, z częstotliwością jaką zapewnia producenta dla działania tego mechanizmu
59.	Urządzenia firewall muszą obsługiwać możliwość deszyfrowania ruchu użytkowników w celu inspekcji dla protokołów HTTP/2, SSL, TLS 1.2, TLS 1.3.
60.	Urządzenia firewall muszą posiadać możliwość zdefiniowania ruchu SSL/TLS, który należy poddać lub wykluczyć z operacji deszyfrowania i inspekcji rozdzielny od polityk bezpieczeństwa.
61.	Wykonywanie operacji deszyfrowanie ruchu musi być odnotowywane w logach urządzeń w dedykowanej do tego celu sekcji. Musi zawierać informacje ułatwiające diagnostykę m.in. informacje o błędach, typ i rozmiar klucza, wersja TLS. Musi istnieć mechanizm automatycznego wykluczania z szyfrowania problematycznych stron na bazie tego logu.
62.	Dla deszyfrowania ruchu TLS 1.3 wymagane jest wsparcie dla X25519, X448 oraz minimum dla zestawów protokołów: TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384 oraz TLS_CHACHA20_POLY1305_SHA256.
63.	System zabezpieczeń firewall musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.
64.	System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.
65.	System zabezpieczeń firewall musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
66.	System zabezpieczeń firewall musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia routingu (tzw. routing-based VPN).
67.	System zabezpieczeń firewall musi pozwalać na budowanie polityk uwierzytelniania definiujący rodzaj i ilość mechanizmów uwierzytelniających (MFA - multi factor authentication) do wybranych zasobów. Polityki definiujące powinny umożliwiać wykorzystanie adresów źródłowych, docelowych, użytkowników, numerów portów usług oraz kategorie URL. Minimalne wymagane mechanizmy uwierzytelnienia to: RADIUS, TACACS+, LDAP, SAML 2.0.
68.	System zabezpieczeń firewall musi wykonywać zarządzanie pasmem sieci (QoS) w

	zakresie oznaczania pakietów znacznikami DiffServ
69.	Dla IKE wymagane jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.
70.	Dla IPsec wymagane jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.
71.	System zabezpieczeń firewall musi posiadać wbudowany dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 128GB. Wszystkie narzędzia monitorowania, analizy logów i raportowania muszą być dostępne lokalnie na urządzeniu zabezpieczeń. Nie jest wymagany do tego celu zakup zewnętrznych urządzeń, oprogramowania ani licencji.
72.	Zarządzanie systemu zabezpieczeń musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW przez dedykowany interfejs do zarządzania lub inny interfejs wypromowany jako interfejs zarządzający. Nie jest dopuszczalne, aby istniała konieczność instalacji lub pobierania dodatkowego oprogramowania na stacji administratora w celu zarządzania systemem.
73.	Urządzenia firewall muszą posiadać koncept konfiguracji kandydackiej (na poziomie API, GUI, oraz CLI), którą można dowolnie edytować na urządzeniu bez automatycznego zatwierdzania wprowadzonych zmian w konfiguracji urządzenia do momentu, gdy zmiany zostaną zaakceptowane i sprawdzone przez administratora systemu.
74.	Konfiguracja kandydacka musi być wspierana przez minimum 7 dni. W tym: a. Możliwość edytowania konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian, których są autorami. b. Możliwość blokowania wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji
75.	System zabezpieczeń firewall musi być wyposażony w interfejs XML API będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI).
76.	Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.
77.	System zabezpieczeń firewall musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS, TACACS+
78.	System zabezpieczeń firewall musi umożliwiać stworzenie sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS).
79.	System zabezpieczeń firewall musi posiadać mechanizm umożliwiający wysyłanie logów do zewnętrznego kolektora danych
80.	System zabezpieczeń firewall musi posiadać mechanizm umożliwiający monitorowanie stanu urządzenia z wykorzystaniem SNMP v2 i v3
81.	System zabezpieczeń firewall musi pozwalać na usuwanie logów i raportów przetrzymywanych na urządzeniu po upływie określonego czasu.
82.	System zabezpieczeń firewall musi zapewniać mechanizm pozwalający na sprawdzenie podczas procesu instalacji nowej bazy sygnatur aplikacyjnych, które reguły bieżącej polityki bezpieczeństwa wykorzystują sygnatury aplikacyjne modyfikowane w ramach bieżącej aktualizacji baz sygnatur.
83.	System zabezpieczeń firewall musi pozwalać na konfigurowanie i wysyłanie logów do różnych serwerów Syslog per polityka bezpieczeństwa.

84.	System zabezpieczeń firewall musi pozwalać na selektywne wysyłanie logów bazując na ich atrybutach.
85.	System zabezpieczeń firewall musi pozwalać na generowanie zapytań do zewnętrznych systemów z wykorzystaniem protokołu HTTP/HTTPS w odpowiedzi na zdarzenie zapisane w logach urządzenia.
86.	System zabezpieczeń firewall musi pozwalać na korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach i filtrowaniu stron www.
87.	System zabezpieczeń firewall musi pozwalać na tworzenie wielu raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML.
88.	System zabezpieczeń firewall musi pozwalać na stworzenie raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni.
89.	System zabezpieczeń firewall musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive lub Active-Active. Moduł ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych.
90.	Wykonawca zapewni usługi wdrożeniowe w następującym zakresie: a. Przedmiot zamówienia obejmuje modernizację (wymianę) aktualnie posiadanych przez Zamawiającego urządzeń. b. W ramach wdrożenia Wykonawca dokona instalacji fizycznej w miejscu wskazanym przez zamawiającego, aktualizacji oprogramowania dostarczonych urządzeń do wersji oprogramowania rekomendowanej przez producenta a następnie konfiguracji nowych urządzeń na podstawie konfiguracji urządzeń aktualnie wykorzystywanych przez Zamawiająego wraz z przeniesieniem reguł bezpieczeństwa i konfiguracji uruchomionych funkcjonalności urządzeń (jeśli dotyczy). Odbiór migracji zostanie poprzedzony testami opracowanymi wraz z Zamawiającym w zakresie spełnienia oczekiwanych funkcji. c. Po zakończonym procesie migracji Zamawiający dokona weryfikacji konfiguracji pod kątem bezpieczeństwa oraz elementów nadmiarowych. Zamawiający oczekuje wprowadzenia rekomendacji producenta w zakresie najlepszych praktyk w zakresie polityk i wykorzystywanych mechanizmów bezpieczeństwa.
91.	Wykonawca będzie świadczył Zamawiającemu Usługę Zarządzania przez okres 18 miesięcy jednak nie dłużej niż do 12.03.2026 w zakresie obejmującym: a. Monitoring, co najmniej w zakresie dostępności i obciążenia, dostarczonego urządzenia typu firewall Zamawiającego za pomocą posiadanych przez Wykonawcę narzędzi, b. Opracowywanie i implementowanie korzystnych zmian mogących rozwiązać problemy zaobserwowane w systemie monitoringu, c. Obsługę zgłoszeń serwisowych związaną z niepoprawnym działaniem dostarczonego urządzenia, d. Udzielanie administratorom Zamawiającego wsparcia w postaci porad i wyjaśnień dotyczących Sprzętu, e. Instruowanie administratorów Zamawiającego w zakresie działania i zmian konfiguracji Sprzętu, f. Wykonywania czynności administratorskich zleconych przez Zamawiającego w zakresie działania i zmian w konfiguracji Sprzętu. g. Wykonywania aktualizacji oprogramowania zleconych przez Zamawiającego zgodnie z rekomendacjami producenta dostarczonego rozwiązania,

	h. Usługa Zarządzania będzie każdorazowo zgłaszana Wykonawcy poprzez pocztę elektroniczną lub telefonicznie, z co najmniej 1 dniowym wyprzedzeniem, wskazując jednocześnie zakres asysty, szacunkową liczbę roboczogodzin, termin i sposób jej realizacji. Liczba roboczogodzin nie przekroczy w miesiącu 8. i. Usługa Zarządzania będzie realizowana w Dniach roboczych w godzinach od 7:30 do 15:30 w formie zdalnej lub w uzasadnionych przypadkach w siedzibie Zamawiającego, odpowiednio do zgłoszonego problemu/potrzeby j. Zamawiający wymaga, aby usługa realizowana była przez certyfikowanego (tj. posiadającego certyfikaty producenta oferowanego sprzętu) inżyniera, posługującego się językiem polskim.

7. Rozbudowa licencji backup

Zamawiający wymaga w ramach rozbudowy systemu backup upgradu posiadanej licencji Acronis Cyber Protect do wersji Acronis Cyber Protect Advanced wraz z dostawą serwera oraz biblioteki taśmowej.

1) Biblioteka taśmowa

Komponent	Minimalne wymagania
Obudowa i pojemność	Wysokość maksymalnie 1U do instalacji w szafie Rack. Co najmniej 9 slotów przeznaczonych na zestaw taśm.
Połączenie	Co najmniej 1 port SAS o przepustowości co najmniej 6Gb/s w standardzie umożliwiającym podłączenie serwerów.
Napęd	Wyposażony w co najmniej 1 sztukę napędu SAS LTO 8. W komplecie: • kabel SAS umożliwiający podłączenie biblioteki do serwera o dł. min. 2m • 8x taśma LTO8 • 1x taśma czyszcząca
Gwarancja	• Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lat. • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. • Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych) • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. • Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. • Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.

	• Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. • Możliwość rozszerzenia gwarancji Producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: o Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. o Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy. o Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. o Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. o Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. • Firma serwisująca musi posiadać ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.

2) Serwer

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	• Obudowa Rack o wysokości max 1U z możliwością instalacji do 8 dysków 2.5" Hot-Plug • Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze. • Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych

	komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	• Płyta główna z możliwością zainstalowania do dwóch procesorów. • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci • Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Chipset	• Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	• Zainstalowany jeden procesor 8-rdzeniowy, min. 2.8 GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 127 w teście SPECrate2017_int_base dostępnym na stronie www.spec.org dla dwóch procesorów.
RAM	• Min. 128GB DDR4 RDIMM 3200MT/s,
Funkcjonalność pamięci RAM	• Advanced ECC, • Memory Page Retire, • Fault Resilient Memory, • Memory Self-Healing lub PPR, • Partial Cache Line Sparing

Kontroler RAID	• Sprzętowy kontroler dyskowy, posiadający
	  ○ Min. 8GB nieulotnej pamięci cache,
	  ○ Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.
	  ○ Wsparcie dla dysków samoszyfrujących

Dyski twarde	• Zainstalowane: ○ Min. 2x dysk SSD SATA o pojemności min. 480GB, 6Gb, 2,5“ Hot-Plug. • Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1. • Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde
Gniazda PCI	• Jeden slot PCIe LP
Interfejsy sieciowe/SAS	• Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) • Czteroportowa karta 12Gb SAS HBA
Wbudowane porty	• Przednie: min. 1x VGA, min. 1x USB 2.0, min. 1x micro-USB dedykowane dla karty zarządzającej, • Tylne: min. 1x VGA, min. 2x USB w tym 1x USB 3.0,
Video	• Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900
Wentylatory	• Redundantne
Zasilacze	• Redundantne, Hot-Plug maksymalnie 1100W klasy Titanium
Elementy montażowe	• Komplet szyn umożliwiających montaż w szafie rack
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.

	• Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem • Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
Karta Zarządzania	• Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: o dostęp do graficznego interfejsu Web karty zarządzającej; o wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; o możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera o wsparcie dla Public Key Authentication (PKA) over SSH oraz z możliwością rozszerzenia funkcjonalności o: o zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); o szyfrowane SSL o wsparcie dla IPv6; o możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; o integracja z Active Directory; o wsparcie dla dynamic DNS; o wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. o możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera o możliwość obsługi przez sześciu użytkowników jednocześnie; o możliwość podmontowania zdalnych wirtualnych napędów; o wirtualną konsolę z dostępem do myszy, klawiatury; o możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; o Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej o Przesyłanie danych telemetrycznych w czasie rzeczywistym o Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze o Automatyczna rejestracja certyfikatów (ACE)
Oprogramowanie do zarządzania	• Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:

	○ Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych ○ integracja z Active Directory ○ Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta ○ Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish ○ Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram ○ Szczegółowy opis wykrytych systemów oraz ich komponentów ○ Możliwość eksportu raportu do CSV, HTML, XLS, PDF ○ Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. ○ Grupowanie urządzeń w oparciu o kryteria użytkownika ○ Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji ○ Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach ○ Szybki podgląd stanu środowiska ○ Podsumowanie stanu dla każdego urządzenia ○ Szczegółowy status urządzenia/elementu/komponentu ○ Generowanie alertów przy zmianie stanu urządzenia. ○ Filtry raportów umożliwiające podgląd najważniejszych zdarzeń ○ Integracja z service desk producenta dostarczonej platformy sprzętowej ○ Możliwość przejęcia zdalnego pulpitu ○ Możliwość podmontowania wirtualnego napędu ○ Kreator umożliwiający dostosowanie akcji dla wybranych alertów ○ Możliwość importu plików MIB ○ Przesyłanie alertów „as-is” do innych konsol firm trzecich ○ Możliwość definiowania ról administratorów ○ Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów ○ Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) ○ Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta ○ Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów ○ Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. ○ Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. ○ Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile

	○ Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. ○ Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. ○ Zdalne uruchamianie diagnostyki serwera. ○ Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. ○ Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Oprogramowanie do monitorowania	Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności: • Monitoring: ○ ilość podłączonych oraz rozłączonych systemów ○ stan podłączonych urządzeń ○ informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów ○ Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia ○ informacje o statusie gwarancji dla poszczególnych urządzeń ○ informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń ○ informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. ○ Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych ○ Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych. ○ Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych. ○ Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. ○ Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. ○ Monitoring parametrów serwerów z informacją o minimum: ▪ Obciążeniu procesora ▪ Zużyciu pamięci RAM ▪ Temperaturze procesorów ▪ Temperaturze powietrza wlotowego ▪ Zużyciu prądu ▪ Zmianach w fizycznej konfiguracji serwera ▪ Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.

	○ Monitoring parametrów pamięci masowych z informacją o minimum: ▪ Opóźnieniach ▪ IOPS ▪ Przepustowości ▪ Utylizacji kontrolerów ▪ Pojemność całkowita i dostępna ▪ Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów. ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ▪ Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata ▪ Informacje o poziomie redukcji danych ▪ Informacje o statusie replikacji oraz snapshotów ○ Monitoring parametrów przełączników sieciowych z informacją o minimum: ▪ Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny ▪ Stanie komponentów: zasilacze, wentylatory ▪ Podłączonych hostach ▪ Ilości i statusu portów ▪ Utylizacji procesora ▪ Utylizacji poszczególnych portów ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. • Aktualizacja firmware ○ możliwość aktualizcji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizcji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizcji firmware, oprogramowania zarządzającego dla rozwiazań HCI, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizcji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizcji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania • Raporty ○ Możliwość generowania raportów dla serwerów zawierających informację o: ▪ Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej ▪ Średnim obciążeniu: procesorów, pamięci RAM, IO,

	○ Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o: ▪ Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji ○ Generowanie raportów do plików CSV i PDF • Cyberbezpieczeństwo ○ Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia. ○ Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. ○ Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. ○ Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. • Wspierane urządzenia ○ Urządzenie Producenta dostarczane w ramach postępowania ○ Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) • Wirtualny asystent ○ Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; • Możliwość rozszerzenia funkcjonalności ○ Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. • Inne ○ Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android • Certyfikaty ○ Oferowana platforma musi być zaprojektowana zgodnie ze standardami: ▪ ISO 27001 ▪ NIST Security and Privacy Controls for Federal Information Systems and Organization ▪ CSA Cloud Control Matrix
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklaracja CE. • Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami. • Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych

	plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Bronze według normy wprowadzonej w 2019 roku - Wykonawca złoży dokument potwierdzający spełnianie wymogu. • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.
Dokumentacja użytkownika	• Zamawiający wymaga dokumentacji w języku polskim lub angielskim. • Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Warunki gwarancji	• Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 2 lat. • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. • Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych) • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. • Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. • Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. • Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. • Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa

	produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. • Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: o Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. o Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy. o Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. o Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. o Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. • Firma serwisująca musi posiadać ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.

8. Szkolenie dla pracowników IT

W ramach zamówienia Zamawiający oczekuje przeprowadzenia dedykowanego szkolenia dla pracowników IT z dostarczonego zakresu rozwiązań IT cybersecurity.
Minimalny zakres szkolenia:

Zakres	Program szkolenia musi obejmować min. :
NGF	Szkolenie stacjonarne w wymiarze min. 4 godziny. • Wprowadzenie i wstępna konfiguracja • Polityki zapory sieciowej • Translacja adresów sieciowych (NAT) • Uwierzytelnianie użytkowników • Logowanie i monitoring • Operacje oparte na certyfikatach • Filtr stron www • Kontrola aplikacji • System ochrony przed włamaniami i atakami DoS
System EDR	Szkolenie stacjonarne w wymiarze min. 4 godziny.

	• tworzenie reguł • tworzenie blokad urządzeń usb - oraz dopuszczanie wybranych • update środowiska oraz hostów • analiza logów systemu EDR • w ramach szkolenia należy przekazać wiedze niezbędną do samodzielnego zarządzania przez administratora zamawiającego
Narzędzie do inwentaryzacji zasobów	Szkolenie stacjonarne w wymiarze min. 4 godziny. • zdalne wdrażanie klienta programu • tworzenie reguł • tworzenie blokad urządzeń usb - oraz dopuszczanie wybranych • update środowiska oraz hostów • przechwytywanie sesji , działania związane w wymianą plików , oraz komunikatów , • w ramach szkolenia należy przekazać wiedze niezbędną do samodzielnego zarządzania przez administratora zamawiającego