Projekt „Cyberbezpieczna Gmina Miastków Kościelny" dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd" z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa.

I.271.5.2025

Załącznik nr 1 – Opis Przedmiotu Zamówienia

DOSTAWA URZĄDZEŃ I OPROGRAMOWANIA ZWIĘKSZAJĄCYCH ODPORNOŚĆ NA CYBERATAKI WRAZ Z WDROŻENIEM W RAMACH REALIZACJI PROJEKTU „CYBERBEZPIECZNA GMINA MIASTKÓW KOŚCIELNY"

PRZEDMIOTEM ZAMÓWIENIA JEST (WYMAGANIA MINIMALNE):

1. Dostosowanie usług katalogowych dla użytkowników wraz z wdrożeniem Centralnego Systemu Bezpieczeństwa (CSB) – 1 usługa w ilości maks. 100 godzin.

W ramach zadania obowiązkiem Wykonawcy będzie dostosowanie usług katalogowych dla użytkowników wraz z wdrożeniem Centralnego Systemu Bezpieczeństwa. Z uwagi na minimalizowanie ingerencji w prace Urzędu, wdrożenie usług katalogowych wraz z wdrożeniem Centralnego Systemu Bezpieczeństwa nie może trwać dłużej niż 100 roboczogodzin, realizowanych w trakcie 120 dni przeznaczonych na realizację. Obowiązkiem Wykonawcy jest omówienie harmonogramu wykonania usługi z Zamawiającym. W harmonogramie powinna znaleźć się informacja o anonsowaniu planowanych prac przez Wykonawcę i forma jej potwierdzenia przez Zamawiającego. Harmonogram musi być zaakceptowany przez strony. Wdrożenie i skonfigurowanie usług katalogowych musi zapewniać efektywne zarządzania dostępem do zasobów informatycznych u Zamawiającego. Obowiązkiem Wykonawcy będzie utworzenie struktury organizacyjnej, grup, kont użytkowników oraz polityk bezpieczeństwa. Szczegółowy zakres prac zawiera:

a) Analiza i Projektowanie:
   - Ocena infrastruktury istniejącej w celu dostosowania projektu do istniejących zasobów.
   - Zaprojektowanie struktury organizacyjnej usług katalogowych z uwzględnieniem potrzeb Zamawiającego. Efektem działań będzie utworzenie dokumentu zawierającego ustalaną strukturę usług katalogowych. Dokument ten zostanie zatwierdzony przez zamawiającego w celu kontynuowania prac.

b) Wdrożenie:
   - Instalacja na infrastrukturze Zamawiającego (serwerach z oprogramowaniem).
   - Konfiguracja globalnych i lokalnych polityk bezpieczeństwa.
   - Utworzenie grup użytkowników i przydzielanie odpowiednich uprawnień.
   - Integracja usługi z istniejącymi systemami.
   - Wpięcie maksymalnie **10 sztuk** urządzeń klienckich, wraz z przeniesieniem profili użytkownika.
   - Wsparcie w rozwiązaniu problemów związanych z wdrażaniem urządzeń klienckich. Efektem działań będzie przekazanie maszyny z zainstalowaną i skonfigurowaną usługą katalogową.

c) Testowanie i akceptacja:
   - Przeprowadzenie testów funkcjonalnych w celu potwierdzenia poprawności działania usługi katalogowej.
   - Protokolarne przekazanie dokumentacji dotyczącej konfiguracji, w tym haseł dostępowych instrukcji i postępowania w razie problemów.

Wdrożenie oferowanego Centralnego Systemu Bezpieczeństwa (dalej CSB), polegające w szczególności na instalacji oraz uruchomieniu rozwiązania. Do obowiązków Wykonawcy należeć będą:

a) Instalacja fizyczna i konfiguracja funkcjonalna komponentów systemu CSB.

b) Konfiguracja systemu CSB w środowisku Zamawiającego. Zdefiniowanie niezbędnych do poprawnego działania systemu parametrów konfiguracyjnych.
c) Integracja z usługą katalogową w zakresie autentykacji użytkowników. Konfiguracja ról Użytkowników.
d) Podłączenie do 3 rodzajów źródeł zdarzeń (np. UTM, switch, serwer) rozpoznawanych przez system CSB. Wykonawca przekaże wytyczne dla Zamawiającego dotyczące koniecznej konfiguracji źródeł zdarzeń Zamawiającego.
e) Budowa minimum 1 parser dla źródeł zdarzeń nieobsługiwanych automatycznie przez system CSB.
f) Możliwość tworzenia niestandardowych reguł korelacyjnych/scenariuszy oraz aktywacja/konfiguracja wbudowanych reguł korelacyjnych.
g) Konfiguracja polityk retencji danych.
h) Przygotowanie dokumentacji powykonawczej, zawierającej co najmniej zbiór haseł dostępowych, instrukcji i postępowania w razie problemów.
i) Przygotowanie i przetestowanie procedur kopii bezpieczeństwa i odtwarzania systemu po awarii.
j) Instalacja najnowszej wersji składników systemu.

Efektem wdrożenia musi być działanie CSB (systemu klasy SIEM) w środowisku IT Zamawiającego. Dodatkowe konfiguracje (aktualizacje) będą wykonywane w ramach Specjalistycznego wsparcia IT opisanego w dalszej części dokumentu.

2. Specjalistyczne wsparcie IT w zakresie cyberbezpieczeństwa w wymiarze 8h stacjonarnie, 30h online miesięcznie - łącznie usługa wsparcia nie będzie trwać dłużej jak do 30.06.2026 r. - 1 szt.

W ramach zadania obowiązkiem Wykonawcy będzie świadczenie specjalistycznego wsparcia IT w zakresie cyberbezpieczeństwa. Wnioskodawca w ramach każdej z zaoferowanych paczek roboczogodzin będzie świadczył specjalistyczne wsparcie IT w wymiarze 8h stacjonarnie, 30h online w następującym zakresie:

a) Wdrożenie reguł zgodności z przepisami prawnymi oraz standardami bezpieczeństwa.
b) Konfiguracja i zarządzanie firewallami, IDS/IPS i innymi mechanizmami obronnymi.
c) Zarządzanie dostępem i autoryzacją użytkowników.
d) Monitoring sieci i alarmowanie w czasie rzeczywistym.
e) Wdrożenie (na zlecenie) reguł dla Backupu i archiwizacji danych.
f) Szyfrowanie danych wrażliwych.
g) Zabezpieczenie przed oprogramowaniem złośliwym – konfiguracja: antywirus, antimalware.
h) Opracowanie i implementacja planu reagowania na incydenty bezpieczeństwa.
i) Analiza po incydentach i rekomendacje.
j) Stałe monitorowanie logów i zdarzeń związanych z bezpieczeństwem.
k) Zlecone raporty dotyczące stanu bezpieczeństwa.
l) Reagowanie na zgłoszone incydenty związane z bezpieczeństwem
m) Wsparcie w obsłudze wdrożonego w ramach projektu Centralnego Systemu Bezpieczeństwa – oprogramowania klasy SIEM.

Wszystkie zapisy rozumiane jako doradztwo i konfiguracja urządzeń oraz systemów zakupionych w ramach projektu będą realizowane zgodnie z założonymi incydentami. Incydenty będą mogły być zakładane przez Zamawiającego poprzez udostępnione przez Wykonawcę kanały komunikacji, takie jak co najmniej:

- Strona www (24h)
- Adres email (24h)
- Telefon w dni robocze (7:30 – 15:30) – infolinia w języku polskim.

Dla wsparcia stacjonarnego, Wykonawca zapewni realizację incydentów zgodnie z SLA (1/5) co oznacza 1 dzień roboczy na reakcję na zgłoszenie i 5 dni roboczych na realizację. Dla wsparcia online, Wykonawca zapewni realizację incydentów zgodnie z SLA (1/3) co oznacza 1 dzień roboczy na reakcję na zgłoszenie i 3 dni robocze na realizację.

WSPARCIE STACJONARNE 8H W RAMACH PACZKI GODZIN

W przypadku usług wykonywanych **stacjonarnie**, po zgłoszeniu przez Zamawiającego incydentu - konieczności wizyty stacjonarnej w Urzędzie, Wykonawca ma 5 dni roboczych na realizację tego zadania. Wykonawca musi zaanonsować dzień swojej wizyty w Jednostce Zamawiającego w ramach czasu wskazanego na reakcję (1 dzień roboczy). Wezwanie Wykonawcy do świadczenia usługi stacjonarnej odbywać będzie się maksymalnie w ramach dwóch wizyt w ramach jednej paczki godzin. Każda wizyta i jej długość zostanie zaraportowana przez Wykonawcę i potwierdzona przez Zamawiającego. Raportowanie wykonanych godzin jest obowiązkiem Wykonawcy, może ono odbywać się z wykorzystaniem systemu informatycznego lub w formie tradycyjnej (raporty), jednak każdorazowo wykonanie usługi musi być potwierdzone przez Zamawiającego.

WSPARCIE ONLINE 30H W RAMACH PACZKI GODZIN

W przypadku usług wykonywanych **online**, po zgłoszeniu przez Zamawiającego incydentu - konieczności wsparcia online, Wykonawca ma 3 dni robocze na realizację tego zadania. Wykonawca musi zaanonsować termin wykonywanych prac w ramach czasu wskazanego na reakcję (1 dzień roboczy). Wezwanie Wykonawcy do świadczenia usługi wsparcia online odbywać będzie się maksymalnie w ramach 5 zleceń w ramach jednej paczki. Każda usługa wsparcia online i jej długość zostanie zaraportowana przez Wykonawcę i potwierdzona przez Zamawiającego. Raportowanie wykonanych godzin jest obowiązkiem Wykonawcy, może ono odbywać się z wykorzystaniem systemu informatycznego, lub w formie tradycyjnej (raporty), jednak każdorazowo wykonanie usługi musi być potwierdzone przez Zamawiającego. Dla zgłoszeń obu typów incydentów Zamawiający przekaże wykonawcy imienną listę osób uprawnionych do zgłaszania i raportowania incydentów (maksymalnie 3 osoby).

WYKORZYSTANIE PACZKI GODZIN

W ramach zadania, Wykonawca świadczy na rzecz Zamawiającego usługę specjalistycznego wsparcia IT w wymiarze 8h stacjonarnie, 30h online (dalej **paczka godzin**), a także pozostaje w trybie gotowości do podjęcia ww. zleceń w okresie o mniejszej intensyfikacji zgłoszeń. Specjalistyczne wsparcie IT świadczone będzie od dnia podpisania umowy. Wykonawca przez cały okres świadczenia usługi utrzymuje stan gotowości, do realizacji zleceń – incydentów na rzecz zamawiającego. Paczka godzin, będzie wykorzystana maksymalnie w ciągu 30 dni. Okres 30 dni stanowi okres rozliczeniowy dla każdej kolejnej paczki godzin, rozpoczynając od dnia podpisania umowy. Kolejne okresy rozliczeniowe będą liczone od dnia wykorzystania paczki godzin, lub upływie 30 dni. Zamawiający w okresie 30 dni może wykorzystać maksymalnie 2 paczki godzin. Wykorzystanie większej ilości wsparcia – paczek godzin, może odbyć się tylko za obopólną zgodą Zmawiającego i Wykonawcy. Wykorzystanie paczki godzin, klasyfikowane będzie zawsze dla okresu, w którym Zamawiający przekazał zgłoszenie incydentu, także w przypadkach, kiedy Wykonawca w jego obsłudze wyszedł poza okres trwania paczki godzin (np. zgłoszenie przekazane w 29 dniu okresu rozliczeniowego pierwszej paczki godzin, obsłużone w 32 dniu będzie zaliczane dla pierwszej paczki godzin). W przypadku nie wykorzystania wszystkich godzin (stacjonarnych, lub online) w ciągu 30 dni, w ramach jednej paczki godzin niewykorzystane godziny nie przechodzą na kolejny okres. Nie zmienia to wynagrodzenia Wykonawcy, pod warunkiem pozostania w gotowości do wykonania zleceń incydentów na rzecz Zamawiającego. Jeżeli Zamawiający wykorzysta jeden typ wsparcia (godziny stacjonarne, lub online) może wymienić typ wsparcia według przelicznika: 1 godzina stacjonarna = 6 godzin online. Podmiot realizujący usługę musi posiadać kompetencje z wdrażanego w ramach projektu Centralnego Systemu Bezpieczeństwa – oprogramowania klasy SIEM.

3. **Centralny System Bezpieczeństwa - Oprogramowanie klasy SIEM z elementami XDR Extended Detection and Response, EDR Endpoint Detection and Response oraz monitoringiem infrastruktury IT – 1 szt.**

LICENCJA

W ramach postępowania Wykonawca jest zobowiązany dostarczyć Oprogramowanie wraz z licencją bezterminową. Oprogramowanie musi posiadać wsparcie do dnia **30.06.2026 roku**, w ramach wsparcia, Zamawiający musi posiadać możliwość aktualizacji do najnowszej dostępnej wersji oprogramowania, zgłaszać błędy w Oprogramowaniu do serwisu producenta. Licencje na oprogramowanie dostarczone będą do siedziby Zamawiającego w formie papierowej lub elektronicznej. Dostarczona licencja na Oprogramowanie Systemu nie może limitować wielkości przechowywanych danych oraz możliwości wyszukiwania informacji z zgromadzonych danych.

WYMAGANIA DOT. SYSTEMU BEZPIECZEŃSTWA:

Automatyczne Odkrywanie: Centralny System Bezpieczeństwa (dalej CSB) musi używać różnych metod, takich jak skanowanie sieci, obsługa protokołów SNMP, IPMI, i JMX, aby automatycznie wykrywać i konfigurować urządzenia w sieci. Monitorowanie Wysokiej Wydajności: CSB musi umożliwiać monitorowanie wydajności przy wykorzystaniu rozwiązań agentowych lub bez agentowych metodami monitorowania (np. przez SNMP, ICMP, IPMI), CSB musi efektywnie zbierać dane o wydajności i dostępności urządzeń. System powinien być skalowalny i umożliwiać obsługę co najmniej 100 urządzeń i metryk. Elastyczne Wyzwalacze: Wyzwalacze (akcje) w CSB powinny być wyrażeniami logicznymi, które określają warunki dla powiadomień alarmowych. W systemie musi być możliwość definiowania złożonych warunków dla generowania alertów, na przykład po przekroczeniu pewnych progów lub w przypadku wystąpienia określonych wzorców. Wizualizacja Danych: CSB powinien posiadać intuicyjny i przejrzysty interface, umożliwiający wizualizację danych pod kontem ich analizy. System musi umożliwiać wizualizację przy wykorzystaniu m.in interaktywnych wykresów i grafik ponadto system musi posiadać wbudowaną zaawansowaną wyszukiwarkę umożliwiającą odfiltrowywanie danych i ich wizualizację wg. wybranych kategorii (np. poziom istotności). Alerty i Powiadomienia: CSB powinien umożliwiać konfigurację zaawansowanych scenariuszy powiadomień, które mogą być wysyłane poprzez e-mail, SMS, czy integracje z systemami biletowymi. Użytkownicy powinni mieć możliwość ustawiania różnych poziomów priorytetów dla alertów, a także definiowania eskalacji dla poważniejszych problemów. Raportowanie: CSB powinien umożliwiać użytkownikom generowanie szczegółowych raportów dotyczących wydajności i dostępności monitorowanych systemów. Wsparcie dla Szyfrowania: CSB musi być systemem bezpiecznym, umożliwiającym szyfrowaną komunikację między agentami a serwerem, co zapewnia bezpieczeństwo danych monitorowania. Skalowalność: Architektura CSB powinna być zaprojektowana z myślą o skalowalności, co powinno pozwalać na łatwą adaptację do rosnących wymagań w miarę rozwoju infrastruktury IT. Przetwarzanie i Wyszukiwanie Danych: CSB pod kątem agregacji logów musi być oparty na technologii, która umożliwia indeksowanie, wyszukiwanie i analizowanie dużych ilości danych w czasie rzeczywistym. Użytkownicy powinni móc wykonywać skomplikowane zapytania, aby szybko odnaleźć konkretne informacje. Szybkość i Wydajność: Zaprojektowany do szybkiego przetwarzania dużych ilości danych, co jest kluczowe w środowiskach produkcyjnych z intensywnym ruchem danych. Elastyczne Zbieranie Danych: CSB musi gromadzić dane z różnych źródeł jednocześnie (co najmniej urządzenia sieciowe, serwery, urządzenia klienckie). Przetwarzanie i Wzbogacanie Danych: CSB musi posiadać bogaty zestaw filtrów do przetwarzania danych. Odkrywanie i Analiza Danych: System musi umożliwia użytkownikom przeszukiwanie, przeglądanie i analizowanie zgromadzonych danych ułatwiając identyfikację wzorców i trendów. Wsparcie dla Wielu Platform: CSB musi być kompatybilny z wieloma systemami operacyjnymi, co najmniej Linux, Windows, macOS. Treści pojawiające się w interfejsie użytkowników CSB będą spełniać standardy WCAG 2.1 na poziomie AA. Cały interfejs użytkownika powinien być dostosowany pod aktualne wymagania prawne związane z dostępnością serwisów użyteczności publicznej dla osób z niepełnosprawnościami. Na podstawie uzyskanych efektów serwis będzie mógł być udostępniony publicznie. Treści multimedialne muszą być dostępne z poziomu klawiatury i oprogramowania dla osób niepełnosprawnych. Multimedia, które nie mogą być z przyczyn technicznych tak zbudowane, by uczynić je dostępnymi dla wszystkich użytkowników muszą posiadać alternatywny opis tekstowy, który wyjaśnia ich cel i funkcje zastosowania na stronie. Zgodność ze standardami HTML i CSS całego serwisu www. Kontrast kolorystyczny między tłem, a tekstem

musi być zgodny z zaleceniami WCAG 2.1 AA. System CSB musi rejestrować zdarzenia akcje i reakcje użytkowników w CSB. Historia akcji poszczególnych użytkowników musi być raportowana i możliwa do odtworzenia w logach systemowych – chronologicznie.

System musi posiadać budowę modułową, która będzie umożliwiać dodawanie nowych modułów oraz wyłączanie już uruchomionych. Dostarczony i uruchomiony system będzie posiadał co najmniej moduły:

MODUŁ ANALIZY PODATNOŚCI

1.1 Integracja ze stale aktualizowaną bazą danych CVE (Common Vulnerabilities and Exposures), gromadzącą informację na temat podatności urządzeń i oprogramowania.

System musi być zintegrowany z publicznym i stale aktualizowanym rejestrem gromadzącym i udostępniającym informację na temat znanych podatności w urządzeniach obsługiwanych przez system oraz oprogramowaniu zainstalowanym na urządzeniach Zamawiającego (np. UTM). Połączenie z bazą danych CVE odbywać się ma przy wykorzystaniu udostępnionego API i nie powinno wymagać od użytkowników końcowych konfiguracji.
Synchronizacja z bazą CVE oraz sprawdzenie dodania do niej nowych podatności dotyczących sprzętu i oprogramowania zainstalowanego w infrastrukturze sieciowej jednostki musi odbywać się przynajmniej raz dziennie. Po zalogowaniu do CSB i wybraniu modułu analizy podatności powinny być wyświetlane wszystkie zsynchronizowane informacje wraz z danymi historycznymi. Podatności "nowe", których użytkownik wcześniej nie widział powinny być w systemie oznaczone np. poprzez pogrubioną czcionkę lub inny kolor.

1.2. Automatyczne sprawdzenie możliwości występowania podatności w infrastrukturze sieciowej na podstawie zinwentaryzowanych urządzeń i oprogramowania.

System musi automatycznie sprawdzać możliwość wystąpienia nowej podatności tylko na urządzeniach i oprogramowaniu znajdującym się w infrastrukturze sieciowej jednostki, a dokładniej wyszczególnionych (dodanych) w module inwentaryzacji.

1.3. Powiadamianie użytkownika o nowych podatnościach występujących w jego środowisku IT.

System musi informować użytkownika/administratora o nowych podatnościach występujących w infrastrukturze sieciowej jednostki. System powinien posiadać możliwość włączenia powiadomień na przeglądarkę internetową oraz wskazany przez użytkownika/administratora adres e-mail. Ponadto użytkownik po zalogowaniu się do systemu i wybraniu modułu analizy podatności musi być powiadomiony przez system o występujących nowych podatnościach na poszczególnych hostach infrastruktury sieciowej poprzez np. graficzne wyróżnienie hosta i oprogramowania na nim zainstalowanego. System musi informować użytkownika o treści podatności oraz jej sklasyfikowania (np. podatność krytyczna).

2. **MODUŁ MONITORINGU ZASOBÓW**

2.1. Monitorowanie zasobów hostów na podstawie zinwentaryzowanych w systemie urządzeń (monitoring obciążenia dysków, procesorów, ruchu sieciowego itp.)

System musi posiadać możliwość monitorowania zasobów wszystkich hostów dodanych w module inwentaryzacji. Monitorowanie, zbieranie informacji na temat obciążenia wybranego hosta musi odbywać się w sposób ciągły w ustalonych krótkich (co najmniej minutowych) odstępach czasowych. Użytkownik po zalogowaniu się do systemu i wybraniu modułu inwentaryzacji musi mieć możliwość wyświetlenia w formie graficznej (wykresów), przebiegów

czasowych istotnych parametrów hosta, co najmniej takich jak: obciążenie procesora, obciążenie pamięci, obciążenie dysków, obciążenie ruchu sieciowego, skoki na procesorze, czas oczekiwania na dysk i odczyt i zapis na dysku. Ponadto system musi na bieżąco informować o aktualnym statusie hosta (dostępny, niedostępny).

2.2. Grupowanie hostów i korelacja obciążeń zasobów pomiędzy hostami

System musi mieć możliwość wyświetlania zgrupowanych wykresów hostów należących do tej samej grupy. Hosty muszą być pogrupowane w zasugerowany przez administratora sieci sposób w celu skorelowania ze sobą istotnych parametrów zasobów, co umożliwi porównanie zachowań poszczególnych hostów na tle grupy. Hosty powinny być podzielone co najmniej, na urządzenia sieciowe (np. serwery) oraz urządzenia końcowe (np. komputery pracowników). Użytkownik musi mieć możliwość filtrowania wykresów na poziomie poszczególnych hostów, oraz tworzenia w systemie nowych grup i wykresów parametrów dostępnych z wybieralnej listy.

2.3. Wysyłanie alertów i powiadomień dotyczących problemów i zdarzeń występujących na hostach

System musi posiadać funkcjonalność umożliwiającą użytkownikowi/administratorowi skonfigurowanie wysyłania alertów i powiadomień dotyczących problemów i zdarzeń. W systemie musi być możliwość ustawienia wysyłania wiadomości i powiadomień, poprzez wysyłanie komunikatów na przeglądarkę internetową, wysyłanie wiadomości e-mali lub wiadomości sms (w systemie powinna być możliwość dodania bramki sms - Zamawiający dopuszcza wykorzystanie autorskiej bramki sms lub wskażę zew. bramkę/serwis sms). Wysyłane przez system wiadomości muszą zawierać co najmniej informacje na temat występującego zdarzenia/problemu tj. opis, sklasyfikowanie (np. błąd, ostrzeżenie, informacja), data i godzina. Użytkownik/Administrator powinien mieć możliwość ustawienia odbiorcy wiadomości poprzez podanie adresu e-mail, czy w przypadku wiadomości SMS numeru telefonu. Użytkownik musi mieć możliwość wyboru w systemie, przy jakiego typu zdarzeniach i problemach będzie wysyłana wiadomość.

2.4. Funkcja korelacji występujących problemów na hostach z modułem analizy logów

Moduł monitoringu zasobów oprócz przebiegów czasowych parametrów hostów powinien również zawierać informację na temat występujących problemów i zdarzeń na poszczególnych hostach. Użytkownik/Administrator po zalogowaniu się do systemu, wybraniu Modułu Monitoringu zasobów i wyborze konkretnego hosta musi posiadać możliwość prześledzenia zdarzeń i problemów naniesionych na osi czasu. Na osi czasu powinny być wyświetlane tylko "nowe" problemy i zdarzenia oraz te, których status nie został zmieniony na "rozwiązany" bądź "anulowany". Użytkownik/Administrator musi mieć możliwość zmiany statusu wybranego zdarzenia czy problemu wraz z dodaniem krótkiego opisu w jaki sposób problem został rozwiązany. Użytkownik/Administrator musi mieć możliwość stłumienia często powielającego się problemu, którego jest świadomy i musi poczekać na jego rozwiązanie (po włączeniu opcji tłumienia problemu, suystem przez pewien czas nie będzie o nim informował/alertował). Wszystkie problemy i zdarzenia raportowane w systemie muszą być skorelowane z logami pochodzącymi z konkretnych hostów. Użytkownik/Administrator po wybraniu w systemie konkretnego problemu występującego na konkretnym hoście po wybraniu zakładki logi musi zostać przekierowany do modułu analizy logów, w którym automatycznie wyświetlone będą tylko logi dotyczące hosta na którym wystąpił problem. Ponadto użytkownik/administrator w ramach tego modułu powinien mieć możliwość zgłoszenia wystąpienia konkretnego problemu do np. zewnętrznego wsparcia IT. W systemie powinna być możliwość integracji systemu z zewnętrznym systemem typu: "help-desk", przynajmniej poprzez podanie adresu e-mail, na który zostanie wysłane zgłoszenie.

2.5. Kategoryzacja istotności zdarzeń występujących w infrastrukturze sieciowej

Wszystkie zdarzenia i problemy raportowane w systemie muszą być skategoryzowane według ich poziomu istotności (priorytetów). W systemie powinny być identyfikowane problemy z priorytetami w co najmniej 4 stopniowej skali, np: Krytyczny, Wysoki, Średni, Niski. Ponadto, system powinien zapewniać dodatkowe dwa priorytety - zdarzenia nie istotne powinny być również sklasyfikowane w systemie jako informacja, a zdarzenia trudne do sklasyfikowania powinny posiadać priorytet o wartości (niesklasyfikowany).

2.6 Lista predefiniowanych zdarzeń najczęściej występujących w środowiskach IT

System musi być wyposażony w listę wcześniej zdefiniowanych zdarzeń/scenariuszy, które najczęściej występują w środowiskach IT. Użytkownik/Administrator powinien mieć możliwość wybrania konkretnego hosta lub grupy hostów i przypisania im predefiniowanych zdarzeń (np. brak miejsca na dyskach, czy zbyt wysoki ruch sieciowy). W predefiniowanych zdarzeniach/scenariuszach użytkownik/administrator powinien mieć możliwość ustawienia/edycji reguł oraz zmiany wykonywanych operacji, gdy warunki reguł zostaną spełnione. Użytkownik powinien mieć możliwość używania w regułach operatorów logicznych takich jak AND i OR oraz operatorów relacyjnych takich jak: "==", "<=", ">=", "!=". Użytkownik/Administrator systemu musi mieć możliwość ustawienia operacji różnego typu takich jak.: wysłanie wiadomości e-mail, wysłanie wiadomości SMS (Zamawiający dopuszcza wykorzystanie autorskiej bramki sms lub wskażę zew. bramkę/serwis sms), wysłanie zapytania (Request), czy uruchomienie predefiniowanego skryptu.

2.7 Dobór oraz dodawanie zdarzeń do konkretnego środowiska IT

System musi umożliwiać użytkownikowi/administratorowi dodawanie własnych zdarzeń/scenariuszy dostosowanych do jego konkretnych potrzeb. Tworzenie nowego zdarzenia w systemie powinno się odbywać poprzez podanie jego unikalnej nazwy, wybranie hosta lub grupy hostów, których dotyczy tworzone zdarzenie, zdefiniowanie warunków opisujących zdarzenie, oraz podanie operacji jakie mają być wykonane, gdy warunki zostaną spełnione. Warunki powinny korzystać z operatorów logicznych takich jak AND i OR oraz operatorów relacyjnych takich jak: "==", "<=", ">=", "!=". Użytkownik/Administrator systemu musi mieć możliwość ustawienia operacji różnego typu takich jak.: wysłanie wiadomości e-mail, wysłanie wiadomości SMS (Zamawiający dopuszcza wykorzystanie autorskiej bramki sms lub wskażę zew. bramkę/serwis sms), wysłanie zapytania (Request), czy uruchomienie predefiniowanego skryptu.

2.8 Zdalny dostęp do urządzeń końcowych

System musi umożliwiać zdalne połączenie się do wybranego hosta/urządzenia, które zostało wcześniej odpowiednio skonfigurowane. Zdalny dostęp musi odbywać się poprzez przeglądarkę internetową bez konieczności instalowania dodatkowego oprogramowania. Połączenie zdalne musi być możliwe przy wykorzystaniu co najmniej dwóch protokołów, konkretnie RDP i SSH.

2.9 Wywoływanie predefiniowanych skryptów na urządzeniach końcowych

System musi dawać możliwość wywołania podstawowych skryptów na hostach końcowych, na których został zainstalowany jego agent. Predefiniowane w systemie skrypty muszą obejmować co najmniej: wyłączenie i restart hosta, wysłanie wiadomości tekstowej do hosta, włączenie i wyłączenie blokady ruchu sieciowego, włączenie i wyłączenie trybu izolacji z infrastruktury sieciowej hosta z możliwością zdalnego połączenia się z nim.

2.10 Analiza ruchu sieciowego

System musi posiadać możliwość śledzenia logów pochodzących z urządzeń sieciowych typu UTM zwłaszcza tych najczęściej używanych i polecanych w środowiskach informatycznych. Użytkownik systemu/administrator musi mieć możliwość filtrowania wyświetlanych informacji, co najmniej poprzez podanie przedziału czasowego i wyboru nazwy zinwentaryzowanego urządzenia typu UTM.

2.11 Monitorowanie problemów i zdarzeń występujących na drukarkach

System musi umożliwiać monitorowanie problemów występujących na drukarkach sieciowych wykorzystujących protokół SNMP. System powinien zbierać informacje na temat występujących problemów w osi czasu, umożliwiać tłumienie problemów, wskazywać ich istotność. Ponadto w systemie powinny znajdować się możliwe do pobrania wartości parametrów drukarki oraz informacji na temat dostępności urządzenia.

3. MODUŁ ANALIZY LOGÓW

3.1 Przegląd i analiza logów pochodzących z inwentaryzowanych urządzeń/maszyn.

Moduł Analizy Logów i Moduł Monitoringu Zasobów musi być powiązany z Modułem Inwentaryzacji i wykorzystywać informację przez niego posiadane. Użytkownik/Administrator systemu musi posiadać możliwość przeglądania i analizowania logów pochodzących z wszystkich hostów dodanych w Module inwentaryzacji. W ramach modułu system musi agregować logi pochodzące z systemów operacyjnych, aplikacji i systemów dziedzinowych. Agregacja logów powinna odbywać się w sposób ciągły i po osiągnięciu limitu związanego z zasobami dyskowymi serwera nadpisywać historyczne logi, począwszy od najstarszych.

3.2 Możliwość analizy tzw. „customowych" logów pochodzących z dowolnego oprogramowania, w tym systemów dziedzinowych.

System musi posiadać możliwość analizy logów pochodzących z dowolnego oprogramowania, a przede wszystkim z oprogramowania dziedzinowego stosowanego przez Zamawiającego. Użytkownik/Administrator musi mieć możliwość dodawania w module nazwy, lokalizacji i typu tzw. "customowych" logów, które będą agregowane w systemie, w celu późniejszej ich analizy. Zdefiniowane przez Użytkownika/Administratora logi powinny być skorelowane z problemami występującymi na hostach w module monitoringu zasobów. Jeśli wystąpi jakiś problem związany z działaniem np. systemu dziedzinowego, to użytkownik/administrator analizując problemy musi mieć opcję automatycznego przekierowania do logów związanych z tym system.

3.3 Zawansowane filtrowanie, zarówno po hostach jak i zainstalowanym na nich oprogramowaniu.

Moduł analizy logów musi być wyposażony w zaawanasowaną wyszukiwarkę umożliwiającą użytkownikowi/administratorowi wyszukiwanie i filtrowanie konkretnych logów. System powinien umożliwiać odfiltrowanie logów dla konkretnego hosta, grupy hostów, oprogramowania (w szczególności oprogramowania dziedzinowego - "customlogów"), kategorii, dowolnie wpisanej frazy oraz zakresu czasu (data – godzina, od -do). W Systemie muszą być zastosowane mechanizmy stronicowania, umożliwiające płynne przeglądanie dużej ilości informacji.

3.4 Przegląd i analiza logów dotyczących działań użytkowników.

W module analizy logów muszą być agregowane logi dotyczące działań użytkowników. W zależności od rodzaju systemu czy oprogramowania zainstalowanego na hoście w logach znajdują się informacje dotyczące różnej aktywności użytkowników (m.in. data zalogowania się użytkownika do systemu, data wylogowania, czy wybór konkretnej funkcjonalności). Użytkownik/Administrator CSB musi mieć możliwość sprawdzenia tych aktywności poprze wyszukanie i odfiltrowanie logów po nazwie użytkownika, typie aktywności, czy dowolnie wpisanej frazie.

3.5 Dostęp do logów historycznych.

System oprócz dostępu do aktualnych logów musi uwzględniać również logi historyczne. Użytkownik/Administrator musi mieć możliwość przeglądania wszystkich logów agregowanych na zasobach dyskowych. Ilość oraz zakres czasowy agregowanych logów limitowany ma być tylko zarezerwowaną przestrzenią dyskową na serwerze. Po osiągnięciu założonego limitu, system powinien nadpisywać logi począwszy od najstarszych. Użytkownik/Administrator podobnie jak w przypadku logów aktualnych musi mieć możliwość przeszukiwania oraz filtrowania logów historycznych po hostach, oprogramowaniu, czasie i dowolnie wpisanej frazie.

3.6 Informowanie i powiadomienia dotyczące pojawienia się nowych istotnych logów w obrębie całej infrastruktury sieciowej.

System musi być wyposażony w mechanizmy powiadamiające użytkownika/administratora o pojawieniu się istotnych logów pochodzących z urządzeń infrastruktury sieciowej. System musi posiadać możliwość konfiguracji tych powiadomień pod katem istotności pojawiającego się wpisu w lagach oraz wyboru typu logu (m.in. log systemowy, log "customowy"). Ponadto CSB musi informować użytkownika/administratora o "nowych" zagregowanych logach z poszczególnego hosta. Informacja ta powinna być wyświetlana w systemie po zalogowaniu użytkownika/administratora, a "nowe" logi to logi dodane do systemu od czasu ostatniego logowania użytkownika/administratora.

3.7 Kategoryzacja istotności logów (np.: informacja, ostrzeżenie, błąd).
System musi być wyposażony w mechanizmy kategoryzujące logi pod kontem ich istotności. System w szczególności powinien informować użytkownika/administratora o pojawieniu się logów dotyczących nieprawidłowości działania poszczególnych hostów, czy oprogramowania na nich zainstalowanych. Następnie w zależności od potrzeb użytkownika/administratora system powinien informować o pojawieniu się ostrzeżeń w oprogramowaniu kluczowym dla użytkownika. Jeśli log dotyczy tylko informacji takiej jak zalogowanie się, czy wyłączenie hosta, to użytkownik/administrator nie powinien otrzymywać powiadomienia (alertu), z wyjątkiem logów które użytkownik/administrator uzna za istotne (pomimo tego, że są skategoryzowane jako informacja).

4. MODUŁ EDR/XDR

4.1 System musi posiadać moduł EDR/XDR, stanowiący zintegrowane rozwiązanie bezpieczeństwa, którego główne funkcje to: monitorowanie i gromadzenie danych o aktywnościach użytkowników i oprogramowania na urządzeniach końcowych, analiza tych danych w celu identyfikacji wzorców zagrożeń.

4.2 Moduł musi posiadać podgląd informacji, alertów i zdarzeń występujących w środowisku IT. W CSB powinna być możliwość podglądnięcia statystyk incydentów/zdarzeń oraz ich kategorie. Użytkownik/Administrator z poziomu CSB powinien mieć możliwość uzyskania takich informacji jak rodzaj, nazwa lub źródło incydentu, opis, data wykrycia oraz kategoria/priorytet.

4.3 Oprócz posiadanego modułu EDR/XDR, system musi być otwarty tj. posiadać możliwość integracji z rozwiązaniami EDR/XDR innych producentów (co najmniej ESET, WithSecure, Bitdefender). System musi umożliwiać bezpośrednie przekierowanie do zaawansowanych opcji zintegrowanego systemu EDR/XDR (panelu administracyjnego). Dzięki integracji w module musi znajdować się funkcjonalność umożliwiająca użytkownikowi/administratorowi przejście do panelu administracyjnego systemu EDR/XDR udostępniającego zaawansowane opcje takie jak automatyczne reagowanie na zidentyfikowane zagrożenia w celu ich usunięcia lub powstrzymania, powiadamianie personelu bezpieczeństwa o zidentyfikowanych anomaliach.

5. MODUŁ INWENTARYZACJI

5.1 Automatyczny (przy wykorzystaniu agentów), półautomatyczny (przy wykorzystaniu pliku CSV) lub ręczny sposób dodawania hostów oraz oprogramowania zainstalowanego w infrastrukturze sieciowej.

System musi dawać użytkownikowi/administratorowi możliwość dodawania hostów/urządzeń/oprogramowania należących do infrastruktury sieciowej na trzy różne sposoby. Pierwszy dotyczy automatycznego wykrywania i dodawania przy wykorzystaniu usług katalogowych. Wszystkie hosty i urządzenia należące do wybranej domeny powinny być automatycznie dodane do CSB wraz z zainstalowanym na nich oprogramowaniem. Drugi i trzeci sposób natomiast ma umożliwiać użytkownikowi/administratorowi dodanie urządzeń/hostów/oprogramowania nie należących do domeny poprzez "ręczne" wpisanie informacji (wypełnienie formularza) lub wczytanie pliku w formacie CSV posiadającego usystematyzowaną strukturę. Moduł inwentaryzacji musi być ściśle skorelowany (powiązany) z pozostałymi modułami systemu CSB.

5.2 Gromadzenie pełnych informacji na temat urządzeń (tj. nazwa hosta, adres IP, główny użytkownik) jak i oprogramowania (nazwa, wersja).

Informacje o urządzeniach/hostach/oprogramowaniu, które muszą znaleźć się zarówno w formularzu jak i pliku CSV to m.in. dla hosta/urządzenia: nazwa, adres IP, przypisany użytkownik, typ urządzenia/hosta oraz lista zainstalowanego na nim oprogramowania wraz z wersjami. Przy wprowadzaniu "ręcznym" system musi umożliwiać użytkownikowi/administratorowi wybór nazwy i wersji oprogramowania z listy znajdującej się bazie CVE, bądź wpisanie własnych wartości.

5.3. Generowanie raportu w formacie PDF, CSV zawierającego aktualne informację na temat urządzeń oraz oprogramowania zainstalowanego w infrastrukturze sieciowej.

Moduł musi być wyposażony w funkcjonalności umożliwiającą użytkownikowi/administratorowi wygenerowania raportów z całej dodanej w systemie CSB infrastruktury sieciowej. Raporty powinny być generowane w co najmniej dwóch formatach tj. PDF i CSV oraz powinny zawierać wszystkie istotne informację na temat urządzenia/hosta/oprogramowania m. in takie jak: nazwa, adres, główny użytkownik, lista oprogramowania wraz z wersjami. Ponadto raport musi zawierać m.in. datę i godzinę wygenerowania, nazwę jednostki organizacyjnej oraz imię i nazwisko osoby generującej raport. Dokładny wzór (wizualny) generowanego raportu zostanie ustalony przez zamawiającego w trakcie realizacji zamówienia. Moduł musi umożliwiać generowanie raportów zarówno z całości jak i z odfiltrowanych urządzeń/hostów/oprogramowania. Użytkownik/Administrator musi mieć możliwość odfiltrowania informacji według co najmniej takich kategorii jak: nazwa użytkownika, grupa urządzeń, dowolnie wpisana fraza.

6. **MODUŁ ZGŁASZANIA INCYDENTÓW (e-mail, system help-deskowy)**

6.1. Integracja z systemem tiketowym.

System CSB musi w prosty i intuicyjny sposób umożliwiać użytkownikowi/administratorowi integrację z systemem typu: help-desk. Integracja powinna odbywać się poprzez ustawienie w konfiguracji CSB odpowiedniego adresu e-mail systemu help-deskowego, na który będą wysyłane zgłoszenia dotyczące problemów. Wysyłanie wiadomości ma się odbywać automatycznie po wybraniu przez użytkownika/administratora konkretnego zdarzenia w systemie CSB. Wiadomość e-mail powinna zwierać minimum nazwę jednostki organizacyjnej wysyłającej zgłoszenie, treść zgłoszenia oraz dane zgłaszającego: Imię Nazwisko, adres e-mail, numer telefonu.

6.2. Zgłaszanie incydentu/problemu, który został namierzony przez system.

Moduł zgłaszania incydentu powinien być ściśle powiązany z modułem monitoringu zasobów, a dokładniej z funkcjonalnością wyświetlającą zidentyfikowane na urządzeniach/hostach problemy. Użytkownik/Administrator systemu powinien posiadać możliwość wyboru problemu namierzonego przez CSB i automatycznego zgłoszenia go do help-desk, poprzez wybranie np. przycisku "Zgłoś Problem". Po wybraniu opcji zgłoszenia system powinien automatycznie wysyłać do systemu tiketowego zgłoszenie zawierające pełne informacje dotyczące wybranego problemu.

6.3. Bezpośrednie zgłaszane zagrożeń/cyberataków do CSIRT NASK.

System powinien umożliwiać generowanie co najmniej pliku w formacie pdf ze zgłoszeniem zagrożenia/incydentu/ cyberataku zgodnego z formularzem udostępnianym przez NASK.

7. MODUŁ WYKRYWANIA ZAGROŻEŃ

7.1. Wykrywanie zagrożeń na podstawie powszechnie znanych taktyk i technik wykorzystywanych przez cyberprzestępców udostępnione w ogólnodostępnej bazie danych MITRE ATT&CK.

System musi umożliwiać użytkownikowi/administratorowi włączenie reguł sprawdzających, czy w jego infrastrukturze sieciowej nie zostały zastosowane taktyki i techniki różnego rodzaju cyberataków. System musi być zintegrowany z powszechnie dostępną bazą danych MITRE ATT&CK zawierającą zbiór taktyk i technik zaobserwowanych przez specjalistów na całym świecie. System powinien posiadać wbudowane reguły umożliwiające wykrycie wielu zagrożeń opisanych w matrycy MITRE ATT&CK, system powinien wskazywać użytkownikowi, przed jakiego rodzaju taktykami i technikami jest chronione jego środowisko IT. System musi pokazywać ilość wbudowanych w nim reguł wraz z ilością włączonych reguł. Użytkownik/Administrator systemu musi mieć możliwość sprawdzenia w systemie ile reguł dotyczących konkretnej techniki jest włączonych, a ile jeszcze pozostało do wyłączenia. System musi pokazywać pokrycie matrycy MITRE ATT&CK ilościom włączonych/wyłączonych reguł wykrywających cyberzagrożenia.

7.2. Kategoryzacja oraz prezentacja wykrytych zagrożeń

System musi umożliwiać użytkownikowi/administratorowi sprawdzenie zagrożeń wykrytych na poszczególnych hostach/urządzeniach zinwentaryzowanych w module inwentaryzacji. Wykryte w systemie zagrożenia musza zawierać informację na temat: daty i czasu ich wystąpienia, rodzaju/treści oraz poziomu istotności. System powinien kategoryzować zagrożenia w co najmniej czterostopniowej skali: poziom zagrożenia niski, średni, wysoki, krytyczny.

7.3. Historia wykrytych zagrożeń

System musi posiadać możliwość sprawdzenia historii występowania zagrożeń na hostach/urządzeniach. System musi być wyposażony w rozbudowaną wyszukiwarkę hostów i zagrożeń umożliwiającą między innymi: wyszukanie hosta po nazwie, adresie IP, kategorii/priorytetów, daty wykrycia (przedziału czasowego).

7.4. Wsparcie/automatyczna ochrona po wykryciu zagrożenia

System musi posiadać możliwość włączenia "automatycznej ochrony" w wybrane dni tygodnia i w wybranych godzinach. Użytkownik/administrator musi mieć możliwość ustawienia automatycznej ochrony przed wybranymi taktykami i technikami działań cyberprzestępców poza godzinami jego pracy. System musi mieć możliwość ustawienia reakcji na

wykrycie zagrożenia w zależności od wybranego poziomu istotności/priorytetu. Ponadto użytkownik/administrator musi mieć możliwość wybrania operacji/akcji z listy predefiniowanych operacji/akcji, która zostanie wykona w razie wykrycia zagrożenia o wybranym priorytecie. Lista operacji/akcji musi umożliwiać co najmniej wyłączenie/restart hosta/urządzenia na którym wykryto zagrożenie, przesłanie informacji o wystąpieniu zagrożenia do użytkownika/administratora przy wykorzystaniu poczty e-mail bądź bramki sms, blokowanie hosta na którym występuje zagrożenie.

8. MODUŁ RAPORTÓW

8.1. Tworzenie zestawień i raportów z danych pochodzących z pozostałych modułów

System musi posiadać możliwość tworzenie różnego rodzaju zestawień prowadzących do sporządzenia i wyeksportowania raportu w co najmniej dwóch formatach: csv, pdf. Podczas tworzenia zestawienia użytkownik/administrator musi mieć możliwość wyboru konkretnych hostów bądź grupy hostów, dla których tworzony jest raport. Użytkownik musi posiadać możliwość wyboru modułów oraz priorytetów zdarzeń w nich występujących. Ponadto użytkownik przez administrator musie mieć możliwość wyboru przedziału czasowego, dla którego zostanie wykonany raport.

9. PANEL UŻYTKOWNIKA

9.1. Intuicyjny i przejrzysty panel użytkownika dostępny z dowolnej lokalizacji poprzez stronę www.

Panel użytkownika CSB powinien być przejrzysty i intuicyjny oraz wykonany przy wykorzystaniu najnowszych standardów i technologii stosowanych we współczesnych systemach informatycznych. Panel użytkownika/administratora sytemu musi być dostępny poprzez podanie odpowiedniego adresu w przeglądarce internetowej. Dostęp do panelu użytkownika musi być bezpieczny poprzez szyfrowanie (zabezpieczenie certyfikatem SSL) oraz tzw. białą listę adresów IP - która pozwala użytkownikowi/administratorowi systemu blokować dostęp z nie znajdujących się na niej adresów. Panel użytkownika powinien również spełniać wymagania związane z dostępnością serwisów użyteczności publicznej dla osób z niepełnosprawnościami - WCAG 2.1 AA.

9.2. Wizualizacja statystyk zdarzeń i logów

Panel użytkownika CSB, powinien posiadać elementy umożliwiające prezentację statystyk zdarzeń i logów w sposób zrozumiały, ułatwiający analizę działania środowiska IT pod kątem cyberbezpieczeństwa. Wizualizacja statystyk zdarzeń i logów powinna dotyczyć przede wszystkim ilości "nowych" zdarzeń zarejestrowanych w systemie z podziałem na ich kategorię. Natomiast sposób prezentacji samych logów i zdarzeń musi być przejrzysty jasno podkreślający sklasyfikowanie zdarzenia czy wpisu do logów. Zdarzenia i logi powinny w systemie być wyświetlane w kolejności od najnowszych do najstarszych z możliwości odfiltrowania zakresu czasowego ich prezentowania.

9.3. Wykresy zdefiniowanych parametrów zasobowych aktualizowane na „żywo".

Wykresy prezentujące parametry zasobów urządzeń/hostów powinny być aktualizowane w systemie na "żywo", a dokładnie w zależności od ustaleń z zleceniodawcą system musi aktualizować wykresy w określonych odstępach czasowych (co najmniej, co minutę).

9.4. Filtrowanie wyświetlanych danych wg. hostów, oprogramowania, kategorii zdarzeń itd.

Panel użytkownika powinien być tak zaprojektowany, aby użytkownik/administrator w sposób intuicyjny mógł filtrować istotne dla niego informacje dotyczące zarówno obciążeń zasobów, zdarzeń (problemów, ostrzeżeń), czy logów. Panel użytkownika musi być wyposażony w wyszukiwarkę umożliwiająca filtrowanie informacji wg. m.in. nazwy hosta/urządzenia, nazwy oprogramowania czy kategorii zdarzeń i logów. Wyszukiwarka w panelu użytkownika powinna znajdować się w widocznym miejscu i posiadać precyzyjnie oznaczone możliwości filtrowania. Użytkownik/Administrator powinien mieć możliwość nakładania na siebie różnych filtrów.

9.5. Intuicyjny panel zarządzania regułami i definiowania "customowych" logów.

Panel użytkownika powinien być wyposażony w przejrzysty i intuicyjny panel zarządzania regułami (akcjami), na podstawie których użytkownik/administrator informowany jest o zaistniałym w środowisku IT problemie. W panelu tym musi znaleźć się między innymi lista już zdefiniowanych reguł z możliwością ich usunięcia i edycji oraz opcja umożliwiająca dodanie nowej reguły. Reguły w panelu użytkownika powinny być dodawane przy wykorzystaniu przejrzystego i intuicyjnego formularza, w którym użytkownik/administrator musi podać nazwę reguły, dodać warunku oraz wybrać rodzaj operacji, która zostanie wykonana, gdy warunki będą spełnione. Użytkownik/administrator CSB musi mieć możliwość wyboru zarówno warunków, reguł jak i operacji z udostępnionych w systemie opcji. Ponad to panel użytkownika musi być wyposażony w panel zarządzania "customowymi" logami, w którym podobnie jak w przypadku reguł, użytkownik/administrator może wyświetlić listę zdefiniowanych "customlogów" wraz z możliwością ich usunięcia, edycji oraz zdefiniowania nowych. Dodanie do systemu "customlogów" musi być intuicyjne i ma polegać na podaniu unikalnej nazwy definiowanych logów, jego ścieżki (lub ścieżek) dostępu oraz nazwy hosta lub grupy hostów, których ma on dotyczyć.

4. Serwer – 1 szt.

Parametr lub warunek	Minimalne wymagania
Obudowa	• Typu RACK, wysokość nie więcej niż 1U; • Możliwość zamontowania szyn umożliwiające wysunięcie serwera z szafy stelażowej • Szyny umożliwiające wysunięcie serwera z szafy stelażowej • Możliwość zainstalowania 8 dysków twardych hot plug 2,5"; • Zainstalowane fizyczne zabezpieczenie (np. na klucz lub elektrozamek) uniemożliwiającego fizyczny dostęp do dysków twardych; • Możliwość zainstalowania dedykowanego wewnętrznego napędu blu-ray.

Płyta główna	• Dwuprocesorowa;
	• Wyprodukowana i zaprojektowana przez producenta serwera;
	• Możliwość instalacji procesorów 64-rdzeniowych;
	• Zainstalowany moduł TPM 2.0 min;
	• 4 złącza PCI Express x16 w tym minimum 3 złącza generacji 5;
	  ◦ Opcjonalnie możliwość uzyskania złącza typu pełnej wysokości tzw. FH;
	• 32 gniazda pamięci RAM;
	• Obsługa 8 TB pamięci operacyjnej RAM DDR5;
	• Wsparcie dla technologii:
	  ◦ Memory Scrubbing;
	  ◦ SDDC;
	  ◦ ECC;
	  ◦ Memory Mirroring;
	  ◦ ADDDC;

	• Możliwość instalacji 2 dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) dyski nie mogą zajmować klatek dla dysków hot-plug.
Procesory	• Zainstalowany jeden procesor 16-rdzeniowy, taktowanie bazowe 2.0 GHz, osiągający w teście SPEC CPU2017 Integer Rate Result wynik SPECrate2017_int_base min. 280 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie http://spec.org/cpu2017/results/cpu2017.html [spec.org].
Pamięć RAM	• min. 128 GB pamięci RAM w kościach 32 GB ; • DDR5 Registered 4800MT/s
Kontrolery dyskowe, I/O	• Kontroler dla dysków wewnętrznych posiadający 2GB pamięci cache, obsługujący poziomy RAID: 0,1,10,5,50,6,60 • Kontroler wyposażony w bateryjne podtrzymanie pamięci cache w przypadku utraty zasilania;
Dyski twarde	• Zainstalowane min. 2 szt. dysków 2,5' SSD SATA 6G 240 GB typu Read Intensive, hot-plug • Zainstalowane 3 szt. dysków 2,5. HDD SAS 10000 obr./min 1,2TB hot-plug
Kontrolery LAN	• Min. 4 x 1Gbit Base-T; wbudowane bądź niezajmujące żadnego z dostępnych slotów PCIe • Zainstalowana karta 2x10G BASE-T
Porty	• Zintegrowana karta graficzna ze złączem VGA z tyłu • 2 porty USB 3.0 dostępne z tyłu serwera; • 2 porty USB 3.0 na panelu przednim; • Opcjonalny port serial, możliwość wykorzystania portu serial do zarządzania serwerem; • Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera.
Zasilanie, chłodzenie	• Redundantne zasilacze hot-plug o sprawności 96% (tzw. klasa Titanium) o mocy 500W; • Redundantne wentylatory hot-plug. • Kable zasilające typu C14-C13 o dł. min. 1,5 m

Zarządzanie	• Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera – system przewidywania, rozpoznawania awarii;
	  • informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:
	  • karty rozszerzeń zainstalowane w dowolnym slocie PCI Express;
	  • procesory CPU;
	  • pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM;
	  • status karty zarządzającej serwera;
	  • wentylatory;
	  • bateria podtrzymująca ustawienia BIOS płyty głównej;
	  • zasilacze;
	  • system przewidywania/rozpoznawania awarii musi być niezależny i działać w przypadku odłączenia kabli zasilających serwera

	(podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym);
	• Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:
	  • Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;
	  • Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;
	  • Dostęp poprzez przeglądarkę Web, SSH;
	  • Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;
	  • Zarządzanie alarmami (zdarzenia poprzez SNMP);
	  • Możliwość przejęcia konsoli tekstowej;
	  • Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM);
	  • Obsługa serwerów proxy (autentykacja);
	  • Obsługa VLAN;
	  • Możliwość konfiguracji parametru Max. Transmission Unit (MTU);
	  • Wsparcie dla protokołu SSDP;
	  • Obsługa protokołów TLS 1.2, SSL v3;
	  • Obsługa protokołu LDAP;
	  • Synchronizacja czasu poprzez protokół NTP;
	  • Możliwość backupu i odtwarzania ustawień bios serwera oraz ustawień karty zarządzającej;
	• Możliwość pograniа oprogramowania zarządzającego i diagnostycznego wyprodukowanego przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna);
	• Dedykowana, do wbudowania w kartę zarządzającą (lub zainstalowana) pamięć flash o pojemności minimum 16 GB;
	• Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN;
	• Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej.

Wspierane OS	• Microsoft Windows Server 2022, 2019; • VMWare vSphere 8.0; • Suse Linux Enterprise Server 15; • Red Hat Enterprise Linux 9, 8;
Gwarancja	• 3 lata gwarancji producenta serwera w trybie on-site z gwarantowaną wizytą technika w ciągu następnego dnia roboczego. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis.

	• W razie awarii dyski twarde pozostają u zamawiającego, opcja ta musi być odstępna przez cały okres trwania gwarancji • Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu; • Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych; • Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie; • Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki.
Dokumentacja, inne	• Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymagane oświadczenie wykonawcy lub producenta; • Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta; • W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji; • Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; • Zgodność z normami: CB, RoHS, WEEE oraz CE.

5. System operacyjny do serwera – 1 szt.

Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana, aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze. Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy:

1) Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
2) Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
3) Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
4) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
5) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.

8) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
9) Wbudowane wsparcie instalacji i pracy na wolumenach, które:
a) pozwalają na zmianę rozmiaru w czasie pracy systemu,
b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
d) umożliwiają zdefiniowanie list kontroli dostępu (ACL).
10) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
11) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
12) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
13) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15) Dostępne dwa rodzaje graficznego interfejsu użytkownika:
a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
b) Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
16) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
17) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
18) Mechanizmy logowania w oparciu o:
a) Login i hasło,
b) Karty z certyfikatami (smartcard),
c) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
19) Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych..
20) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
21) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
22) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
23) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
24) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
25) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:

i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
c) Zdalna dystrybucja oprogramowania na stacje robocze.
d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
i. Dystrybucję certyfikatów poprzez http
ii. Konsolidację CA dla wielu lasów domeny,
iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
f) Szyfrowanie plików i folderów.
g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
i) Serwis udostępniania stron WWW.
j) Wsparcie dla protokołu IP w wersji 6 (IPv6),
k) Wsparcie dla algorytmów Suite B (RFC 4869),
l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
m) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
iii. Obsługi 4-KB sektorów dysków
iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)
26) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
27) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
28) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
29) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
30) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
31) Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

6. <u>Oprogramowanie antywirusowe – 30 szt.</u>

Zakup licencji oprogramowania antywirusowego do dnia **30.06.2026 roku**.

Administracja zdalna w chmurze

1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.
2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.
4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.
9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.
10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
11. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.

Ochrona stacji roboczych

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
2. Rozwiązanie musi wspierać architekturę ARM64.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
10. Rozwiązanie musi integrować się z Intel Threat Detection Technology.

11. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
13. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
14. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
15. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
16. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
    - tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
    - tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
    - tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
    - tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
    - tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
17. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
18. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
19. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
22. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.
23. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:
    - tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,

- tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
- tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
- tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.

24. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
25. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
26. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
27. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
28. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
29. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
30. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

Ochrona serwera

1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7,8 i 9, CentOS 7, Ubuntu Server 18.04 LTS i nowsze, Debian 10, Debian 11 i Debian 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux 8 oraz Amazon Linux.
2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

Dodatkowe wymagania dla ochrony serwerów Windows

9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

13. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
14. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

Dodatkowe wymagania dla ochrony serwerów Linux

18. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
20. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
21. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.

Szyfrowanie

1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit.
2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.

Ochrona urządzeń mobilnych opartych o system Android

1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.
5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
    a. usunięcie zawartości urządzenia,
    b. przywrócenie urządzenie do ustawień fabrycznych,
    c. zablokowania urządzenia,
    d. uruchomienie sygnału dźwiękowego,

e. lokalizację GPS.

6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:
   a. nazwę aplikacji,
   b. nazwę pakietu,
   c. kategorię sklepu Google Play,
   d. uprawnienia aplikacji,
   e. pochodzenie aplikacji z nieznanego źródła.

Sandbox w chmurze

1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
2. Rozwiązanie musi wykorzystywać do działania chmurę producenta.
3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
7. Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów.
8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.
9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.
11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo.
12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:

a) Czysty,
b) Podejrzany,
c) Bardzo podejrzany,
d) Szkodliwy.

13. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
14. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.
15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.

Moduł XDR

1. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
2. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.
3. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.

4. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
5. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica".
6. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.
7. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.
8. Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.
9. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.
10. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.
11. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.
12. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
13. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
14. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej:
    modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.
15. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich.
16. Konsola administracyjna musi mieć możliwość tagowania obiektów.
17. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.

7. Macierz – 1 szt.

Parametr	**Wymagania minimalne**
Procesor	4-rdzeniowy/8-wątkowy procesor 2,2 GHz
Architektura procesora	64-bitowy x86
Mechanizm szyfrowania	AES-NI
Pamięć systemowa	4 GB DDR4

Maksymalna pojemność pamięci	64 GB
Gniazdo pamięci	2 x SODIMM DDR4
Pamięć flash	5 GB
Kieszenie na dyski	8 x 3,5" SATA 6 Gb/s, kompatybilne z SATA 2,5" SSD, kompatybilne dyski, które wypełnią wszystkie dostępne zatoki dyskowe
Obsługa dysków SSD M.2	2 x M.2 2280 PCIe Gen3 (kompatybilne z NVMe SSD PCIe)
Porty Ethernet	2 x 2,5 GbE
Wake on LAN	Tak (tylko dla portów 2,5 GbE)
Ramka Jumbo	Obsługiwane
Gniazda PCIe	1 x PCIe Gen 3 x8
Porty USB	4 (2 x USB 3.2 Gen 2 typu A, 2 x USB 3.2 Gen 2 typu C)
Kształt obudowy	Rackmount 2U (krótkie)
Zasilanie	Dwa zasilacze o mocy 300W, 100–240 V
Wentylatory	3 x 60 mm
Temperatura pracy	0–40°C
Wilgotność robocza	5–95% bez kondensacji

8. Dyski twarde do macierzy dyskowej – 3 szt.

Dyski	Minimalne parametry dysku: • Format 3.5" • Interfejs SATA III (6 Gb/s) • Pojemność dysku 8TB • Prędkość obrotowa 7200 obr./min. • Rodzaj dysku HDD

9. UPS – 1 szt.

Nazwa elementu, parametru lub cechy	**Opis minimalnych wymagań**
Moc pozorna	3000 VA
Moc rzeczywista	3000 W
Topologia (klasyfikacja IEC 62040-3)	Line-interactive z AVR
Współczynnik mocy	1
Czas przełączenia na baterię	<4 ms
Liczba, typ gniazd wyjściowych	8 x IEC C13 (2 grupy gniazd sterowalnych za pomocą oprogramowania oraz z poziomu wyświetlacza 2x2 IEC C13 10A), 1 x IEC C19 16A
Typ gniazda wejściowego	IEC C20 16A

Czas podtrzymania dla 2500W obciążenia	4 min
Czas podtrzymania przy 1200W obciążenia	13 min
Dodatkowe bateriie	Możliwość dodania do 4 dodatkowych modułow baterii w celu wydłużenia czasu podtrzymania do 84 minut dla 2500W obciążenia przy pf=1,0
Napięcie znamionowe	200/208/220/230/240/250 V
Tolerancja napięci prostownika	160 V – 294 V (regulacja programowa 150-294 V)
Częstotliwość znamionowa	50/60 Hz autodetekcja
Tolerancja częstotliwości	47– 70 Hz
Kształt napięcia	Sinusoidalny
Napięcie znamionowe wyjściowe	200/208/220/230/240 V do wyboru przez użytkownika
Zakres zmian napięcia	+6/-10% napięcia nominalnego
Częstotliwość wyjściowa	50/60 Hz
Współczynnik szczytu	3:1
Baterie wymieniane przez użytkownika "na gorąco"	Tak
Ochrona przed przeładowaniem	Tak (ograniczenie prądu ładowarki, wyłączenie ładowarki / alarm)
Ochrona przed głębokim rozładowaniem	Tak
Okresowy automatyczny test baterii	Tak
Możliwość uruchomienia bez napięcia w sieci "zimny start"	Tak
Baterie wewnętrzne o pojemności nie mniejszej niż	9Ah 12V, minimum 6 szt.
Czas ładowania baterii do poziomu 90%	< 3 godz. do 90% pojemności użytkowej
Interfejs komunikacyjny	• USB
	• RS232 DB-9 żeński (HID)
	• styki przekaźnikowe
	• miniport wyłącznik ON/OFF
	• SNMP/Ethernet

Panel sterowania z wyświetlaczem LCD	• Panel LCD obrotowy (do ułatwienia odczytów przy obu wariantach montażu UPSa). Dostarcza informacji o : stanie pracy urządzenia, stanie obciążenia, pomiarach i ustawieniach. Funkcje ustawień i odczytów: lokalne, wyjścia (napięcie wyjściowe , częstotliwość wyjściowa), baterii (test baterii), pomiary i dane (numer seryjny,napięcie i częstotliwość wejściowa i wyjściowa, poziom obciążenia, pozostały czas podtrzymania, wydajność, zużycie energii w kWh).
	• Poziomy rząd przycisków sterowania
	• Poziomy rząd wskaźników stanu : zasialanie z siec(zielony), trybu bateryjnego (żółty), usterki (czerwony)
	• Sygnalizator akustyczny
Sygnały akustyczne	• Awaria
	• Niski stan naładowania baterii
	• Przeciążenie
	• Serwis
Przyciski sterujące i wskaźniki diodowe LED	• Przycisk Escape (anulowanie)
	• Przyciski funkcyjne (przewijanie w górę i w dół)
	• Przycisk Enter (potwierdzający)
	• Przycisk ON/OFF załączenia i wyłączenia
	• LED trybu zasilania z siec i(kolor zielony)
	• LED trybu baterii (kolor żółty)
	• LED usterki (kolor czerwony)
Typ obudowy	Uniwersalna Tower/Rack 2U
Dane techniczne karty SNMP	Network Support: Ethernet /10Mbps - Half duplex - 10Mbps - Full duplex - 100Mbps - Half duplex - 100Mbps - Full duplex - 1.0 Gbps - Full duplex / HTTP 1.1, SNMP V1, SNMP V3/ NTP, SMTP, DHCP/
	Tymczasowe hasła: Nadawanie użytkownikowi dostępu za pomocą konta. Konto może wygasać po odpowiedniej, wprowadzonej liczbie dni (hasło przestaje być aktywne). Blokowanie konta: Po określonej liczbie nieudanych prób wpisania hasła lub określonej liczbie dni.
	Protokoły: MQTT/RNDIS/LDAP/NVD/SSH/PKI
	Kompatybilność: SNMP v1/v3 i IP v4/v6
	Interfejs: HTML5
	Adresowanie IP: DHCP/BootP/Manualne
	Szyfrowanie: pakiet szyfrów TLS 1.2 z minimum SHA256
	Dostępny port USB (microUSB - port serwisowy)
	Certyfikaty: UL 2900-1, 2900-2-2, IEC 62443-4-2,
Dołączone oprogramowanie	Tak, monitorujące i zarządzające UPS, umożliwiające automatyczne zamykanie systemów operacyjnych.
Zgodność ze standardem Energy Star	Tak

Maksymalna szerokość	438 mm
Maksymalna głębokość	603 mm
Poziom hałasu w odl. 1m	do 40 dBA dla pracy normalnej
Znaki bezpieczeństwa	CE, Energy Star, IEC/EN 62040-1-1, IEC/EN 62040-2 class B, IEC/EN 62040-3
Gwarancja producenta	36 miesięcy dla elektroniki, 24 miesiące dla baterii.
Możliwość montażu ręcznego bypassu serwisowego	Tak

10. <u>UPS per stanowisko – 32 szt.</u>

Parametr	Minimalne wymaganie
Cechy specjalne	System automatycznej regulacji napięcia (AVR) Kompaktowa obudowa typu tower ze standardem HID port USB do automatycznej integracji z popularnymi systemami operacyjnymi Dwa gniazda wyjściowe typu FR
Topologia	Technologia line-interactive
Współczynnik kształtu	Wieża
Rodzaj budowy	Model wolnostojący
Wartość znamionowa VA	850 VA
Moc	480 W
Zawartość pakietu	Szybki start Instrukcje bezpieczeństwa
Ochrona przeciwprzepięciowa	Tak
Wewnętrzne obejście	Nie
Moc wymiany w trakcie pracy	Nie
Automatyczne wyłączanie	Tak
Częstotliwość podstawowa - maks.	63 Hz
Częstotliwość podstawowa - min.	45 Hz
Złącze wejściowe	SCHUKO
Długość przewodu wejściowego	1,5 m
Napięcie znamionowe wejściowe	Domyślnie 230 V (220/230/240 V)
Częstotliwość znamionowa	50/60 Hz
Zakres częstotliwości wejściowych	45-63 Hz
Gniazdo	(2) francuskie

Liczba połączeń wyjściowych, norma francuska (typ E)	2
Zakres napięcia	230 V
Napięcie znamionowe wyjściowe	230 V
Typ zasilania	1
Rodzaj napięcia	AC
Wykres czasu podtrzymywania działania	Pokaż wykres czasu podtrzymania
Zarządzanie akumulatorem	Automatyczny test baterii, ochrona przed głębokim rozładowaniem, zimny start
Parametry znamionowe akumulatora	12 V / 9 Ah
Rodzaj akumulatora	Szczelne, kwasowo-ołowiowe
Zwiększone możliwości akumulatora	Nie
Łączność	Port USB (kompatybilny z HID)
Interfejs użytkownika	Wskaźnik LED
Rodzaj interfejsu	Port USB
Bezpotencjałowy zestyk przełączający	Nie
Wilgotność względna	0-90%, bez kondensacji
Zakres temperatury	od 0°C do 40°C (od 32°F do 104°F)
Temperatura pracy - maks.	40 °C
Temperatura pracy - min.	0 °C
Wyjściowa moc pozorna	900 VA
Napięcie wejściowe — maks.	300 V
Napięcie wejściowe — min.	140 V
Napięcie wyjściowe — maks.	257 V
Napięcie wyjściowe — min.	195 V
Częstotl. wtórna – maks.	60 Hz
Częstotl. wtórna – min.	50 Hz
Liczba akumulatorów	1
Sprawność	95
Zakres napięcia wejściowego	140-300 V
Częstotliwość napięcia wyjściowego	50/60 Hz
Zakres napięcia wyjściowego	195-257 V
Faza (wejście)	1
Faza (wyjście)	1
Pobór mocy	25.3 W