Zamówienie współfinansowane ze środków FUNDUSZY EUROPEJSKICH NA ROZWÓJ CYFROWY 2021-2027 (FERC)
Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa.

Załącznik nr 6 do SWZ

Opis przedmiotu zamówienia (OPZ)

Nazwa zamówienia:

Dostawa urządzeń i oprogramowania zwiększających odporność na cyberataki wraz z wdrożeniem w ramach Projektu „Cyberbezpieczny Samorząd”

Zamawiający:

Miasto i Gmina Czarny Dunajec

ul. Józefa Piłsudskiego 2, 34-470 Czarny Dunajec

Znak sprawy**:** **RB.271.12.2024**

Spis treści

1. Centralny System Bezpieczeństwa

EDR
Narzędzie do badania podatności
Usługa SOC
Urządzenie do analizy ruchu sieciowego

LICENCJA	W ramach postępowania Wykonawca jest zobowiązany dostarczyć Oprogramowanie wraz z licencją. Wykonawca musi dostarczyć **licencję wieczystą** z możliwością bezpłatnych automatycznych aktualizacji w ciągu 24 miesięcy od rejestracji i wdrożenia oraz min. 24 **miesięczną** gwarancję producenta Oprogramowania dla licencji (tj. licencji dostarczonych w ramach niniejszego postępowania). Oprogramowanie musi posiadać możliwość aktualizacji do najnowszej dostępnej wersji w okresie gwarancji. W ramach gwarancji Zamawiający ma prawo 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 interfejs, 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:** 1. **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 mieć 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. 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. 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, 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. 3.6. 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. 3.7. 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. 3.8. 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** 4.1.1 Integracja z systemem EDR/XDR. CSB musi mieć możliwość integracji z systemami EDR/XDR *przy wykorzystaniu API*, tak aby umożliwiał informowanie użytkownika/administratora o pojawiających się incydentach i zdarzeniach dotyczących np. próby ataku czy wykrycia złośliwego oprogramowania na poszczególnych hostach. 4.1.1. Możliwość zarządzania systemem EDR z pojedynczej, centralnej konsoli, znajdującej się na serwerach producenta, do której dostęp zapewniony jest przez przeglądarkę internetową. 4.1.2. Brak konieczności instalacji dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, 4.1.3. Rozwiązanie musi posiadać możliwość instalacji/działania na stacjach roboczych z co najmniej systemami operacyjnymi: Microsoft Windows 10, Microsoft Windows 11, MacOS 11. 4.1.4. Rozwiązanie musi posiadać możliwość instalacji/działania na serwerach z co najmniej następującymi systemami operacyjnymi: Microsoft® Windows Server 2012, 2016, 2019, 2022. 4.1.5. Rozwiązanie musi posiadać polski interfejs użytkownika. 4.1.6. Oprogramowanie instalowane na stacjach końcowych i serwerach, zwane agentem, ma możliwość współpracy z oprogramowaniem antywirusowym posiadanym przez Zamawiającego. 4.1.7. Agent instalowany na stacjach końcowych i serwerach posiada możliwość instalacji z wykorzystaniem mechanizmów dystrybucji oprogramowania Active Directory.

	4.1.8. Agent instalowany na stacjach końcowych i serwerach posiada możliwość ręcznej instalacji, bez wykorzystania zewnętrznych systemów dystrybucji oprogramowania. 4.1.9. Oprogramowanie nie wymaga restartu systemu operacyjnego po dokonaniu aktualizacji oprogramowania agenta monitorującego na stacjach końcowych i serwerach. 4.1.10. Dane zebrane przez agenta instalowanego na stacjach końcowych są przesyłane w trybie ciągłym, szyfrowanym protokołem HTTPS, do centrum przetwarzania danych producenta, w celu wykrywania niebezpiecznych zdarzeń. 4.1.11. Agent instalowany na stacjach końcowych i serwerach monitoruje i zbiera informacje na temat co najmniej następujących zdarzeń: - dostęp do pliku; - tworzenie nowego procesu; - nawiązane połączenia sieciowe; - wpisy dziennika systemu, niezbędne do wykrycia naruszeń bezpieczeństwa; - zawartość skryptów uruchamianych na monitorowanej stacji. 4.1.12. W celu zmniejszenia obciążenia stacji końcowych wszystkie procesy związane z analizą zebranych danych oraz wykrywaniem podejrzanych zdarzeń odbywają się w centrum przetwarzania danych producenta, a nie na monitorowanej stacji końcowej. 4.1.13. Dane zbierane przez agenta instalowanego na stacjach końcowych, przed wysłaniem do centrum przetwarzania danych, są kompresowane w celu optymalizacji wykorzystania łączy sieciowych. 4.1.14. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, z centrum przetwarzania danych producenta, odbywa się jedynie z wykorzystaniem protokołów HTTP oraz HTTPS. 4.1.15. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, wspiera komunikację za pomocą serwera pośredniczącego http (http proxy). 4.1.16. W przypadku braku dostępu do sieci Internet, na monitorowanej stacji, która skutkuje brakiem możliwości przesłania danych zebranych przez agenta do centrum przetwarzania danych producenta, dane zebrane na stacji końcowej są buforowane i przesłane do analizy od razu po uzyskaniu przez agenta dostępu do sieci Internet. 4.1.17. Dane zbierane przez agentów na stacjach końcowych i serwerach są, przechowywane i przetwarzane na obszarze Europejskiej Wspólnoty Gospodarczej. 4.1.18. Rozwiązanie na bazie zebranych danych generuje detekcje, które stanowią powiązane ze sobą podejrzane zdarzenia, zebrane przez agentów ze stacji roboczych i serwerów. 4.1.19. Detekcje są generowane za pomocą statycznych reguł, przygotowanych przez producenta, jak również przy wykorzystaniu mechanizmów uczenia maszynowego uwzględniających specyfikę pracy środowiska informatycznego. 4.1.20. Detekcje są generowane w czasie rzeczywistym na podstawie danych zebranych i przesłanych przez agentów uruchomionych na stacjach końcowych i serwerach w środowisku informatycznym. 4.1.21. Detekcje widoczne są w konsoli zarządzającej w postaci graficznych diagramów, przedstawiających wykryte anomalie i powiązania pomiędzy biorącymi udział w detekcji elementami. 4.1.22. Detale dotyczące detekcji przedstawiane są w postaci drzewa zawierającego szczegółowe informacje dotyczące poszczególnych elementów biorących udział w wykrytej anomalii. 4.1.23. Rozwiązanie posiada możliwość filtrowania zdarzeń biorących udział w detekcji w zależności od poziomu ryzyka – od poziomu informacyjnego do zdarzeń o charakterze krytycznym. 4.1.23. Każda detekcja zawiera co najmniej następujące informacje: - Lista urządzeń na których rozwiązanie zarejestrowało podejrzane zdarzenia. - Data i czas wystąpienia podejrzanych zdarzeń. - Listę podejrzanych zdarzeń zidentyfikowanych przez rozwiązanie. - Opis dla każdego z podejrzanych zdarzeń, wyjaśniający, dlaczego dane zdarzenie zostało uznane za podejrzane.

	- Sumę kontrolną (co najmniej SHA1) plików, które zostały uznane za podejrzane. - Poziom ryzyka, określający istotność danej detekcji. - Typ detekcji, określający techniki ataku, które zostały wykryte podczas tworzenia detekcji (np. nieuprawnione podniesienie uprawnień, połączenia z sieciami C&C, nieuprawnione wykonanie skryptu). 4.1.24. Zdarzenia, występujące w detekcjach, które wskazują na wykorzystanie znanej techniki ataku na systemy informatyczne, zawierają odnośniki do ogólnodostępnych materiałów opisujących zastosowanie tych technik (np. matryca MITRE ATT&CK). 4.1.25. Zdarzenia, występujące w detekcjach, które odnoszą się do plików oraz aplikacji uruchomionych na monitorowanych komputerach, zawierają odnośniki do ogólnodostępnej bazy reputacji, pozwalającej sprawdzić reputację tych plików (np. VirusTotal). 4.1.26. Rozwiązanie umożliwia oznaczanie wygenerowanych detekcji jako błędne. 4.1.27. Oznaczenie detekcji jako błędnej, musi powodować, automatyczne identyfikowanie przyszłych takich samych detekcji i odpowiednie ich oznaczenie w interfejsie centralnego zarządzania. 4.1.28. Rozwiązanie posiada możliwość stworzenia archiwum zawierającego dodatkowe informacje dotyczące hosta, na którym wystąpiła detekcja w celu przeprowadzenia analizy śledczej incydentu. 4.1.29. Rozwiązanie pozwala na dodanie własnego komentarza przy wykrytej detekcji. 4.1.30. Rozwiązanie umożliwia wykupienie usługi pozwalającej na przesłanie detekcji do laboratorium producenta w celu analizy, zwrotnie administrator otrzymuje szczegółowy raport przygotowany przez analityka dotyczący incydentu. 4.1.31. Rozwiązanie pozwala na przesłanie wiadomości e-mail informującej o wygenerowaniu nowej detekcji w systemie. 4.1.32. Rozwiązanie pozwala na izolację sieciową komputerów przez administratora. 4.1.33. Rozwiązanie umożliwia tworzenie reguł automatycznej izolacji stacji roboczych i serwerów, jeśli zostaną one uwzględnione w wygenerowanych detekcjach. 4.1.34. Rozwiązanie umożliwia wykonanie zdalnie reakcji na chronionym hoście w tym co najmniej pozwala na: pobranie plików, pobranie historii PowerShell, pobranie wpisów dziennika zdarzeń, pobranie dziennika ochrony antywirusowej, pobranie informacji o wpisach rejestru systemowego, pobranie informacji o MBR, wylistowanie procesów, wylistowanie informacji z systemowego harmonogramu zadań, wylistowanie usług, umożliwia zatrzymanie procesu lub wątku, umożliwia usuwanie plików, usług, wartości rejestru systemowego oraz zadań systemowego harmonogramu zadań. 4.1.35. Rozwiązanie umożliwia tworzenie raportów zawierających co najmniej listę wygenerowanych detekcji, wraz z ich opisem, za zadany okres. 4.1.36. Rozwiązanie pozwala na eksport raportów, w postaci plików PDF. 4.1.37. Rozwiązanie wspiera dostęp do danych na temat utworzonych detekcji za pomocą interfejsu REST API, na potrzeby integracji z innymi systemami zabezpieczającymi. 4.1.38. Rozwiązanie umożliwia wyszukanie zdarzeń napływających do konsoli co najmniej w oparciu o: PID nowego procesu, SHA-1 nowego procesu, nazwę procesu, ścieżkę, nazwę procesu docelowego, docelową ścieżkę, typ zdarzenia, nazwę systemu, typ systemu, wersję systemu, adres IP źródłowy oraz zdalny, port lokalny oraz port zdalny, wartość klucza rejestru. 4.1.39. Lista urządzeń posiadających zainstalowanego agenta systemu EDR zawiera informacje dotyczące: nazwy hosta, adresu IP, poziomu ważności, przypisanego profilu, systemu operacyjnego, informacji o ostatnim podłączeniu oraz aktualnym statusie. 4.1.40. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji. 4.2. 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. Bezpośrednie przekierowanie do zaawansowanych opcji zintegrowanego systemu EDR/XDR (panelu administracyjnego)

Poza integracją i prezentacją incydentów/zdarzeń występujących na poszczególnych hostach w module musi znajdować się funkcjonalność umożliwiająca użytkownikowi/administratorowi przejście do panelu administracyjnego systemu EDR/XDR udostępniającego zaawansowane opcje.

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.

6.3. 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.

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

	7.1. 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. 7.2. 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. 7.3. 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. 8. **PANEL UŻYTKOWNIKA** 8.1. 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. 8.2. 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. 8.3. 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). 8.4. 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. 8.5. 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.
Skanowanie sieci i zarządzanie podatnościami	1. Rozwiązanie zapewnia wykrywanie oraz zarządzanie podatnościami bezpieczeństwa, w środowisku informatycznym. 2. Architektura rozwiązania składa się z systemu zarządzania oraz osobnego, dedykowanego oprogramowania wykonującego skanowania podatności, które jest zarządzane za pomocą jednej centralnej konsoli zarządzania. 3. Dostęp do konsoli centralnego zarządzania odbywa się z poziomu interfejsu WWW, niezależnie od zastosowanej platformy sprzętowej i programowej. 4. Konsola zarządzania jest dostępna w postaci usługi hostowanej na serwerach producenta 5. Konsola zarządzania oferuje dostęp za pomocą następujących wspieranych przeglądarek internetowych: • Microsoft Edge • Mozilla Firefox • Google Chrome • Safari 6. Rozwiązanie realizuje skanowania podatności za pomocą dedykowanego oprogramowania, instalowanego w środowisku, zarządzanego z poziomu konsoli centralnego zarządzania. 7. Oprogramowanie skanujące podatności, w postaci aplikacji instalowanej lokalnie, wspiera poniższe systemy operacyjne: • Windows Server 2012 R2 i nowsze • Ubuntu server 18.x LTS 8. Rozwiązanie umożliwia przeprowadzenie skanowania, wykrywającego urządzenia pracujące w skanowanej sieci komputerowej. 9. Skanowanie wykrywające urządzenia pracujące w skanowanej sieci umożliwia:

	a) wykrywanie urządzeń pracujących w skanowanej sieci na podstawie protokołów: ARP, ICMP PING, SSH, HTTP, HTTPS, RDP. b) wykrycie pracujących urządzeń w oparciu o analizę wszystkich dostępnych otwartych portów sieciowych. c) Pozwala na konfigurację parametrów skanowania takich jak: a. zakres przeszukiwanych portów, b. wydajność skanowania (ilość jednoczesnych połączeń sieciowych), c. liczbę jednoczesnych wątków skanowania, d. możliwość wykrycia wersji systemu operacyjnego. d) konfigurację harmonogramu uruchamiania skanu (np. dziennie, tygodniowo, w określony dzień miesiąca, kwartalnie oraz wskazanie godziny rozpoczęcia skanowania) e) konfigurację wysyłania powiadomień na wskazany adres e-mail, informujących o rozpoczęciu skanowania oraz jego zakończeniu. 10. Konsola zarządzająca umożliwia podgląd listy skonfigurowanych skanów wykrywających dostępne hosty w sieci, wraz z informacją o zmianach w stosunku do ostatniego przeprowadzonego skanu. 11. Konsola zarządzania umożliwia eksport wyniku skanu wykrywającego dostępne urządzenia w sieci do pliku XLS oraz XML. 12. Rozwiązanie umożliwia uruchomienie skanowania wykrywającego znane podatności bezpieczeństwa na urządzeniach sieciowych. 13. Skan wykrywający znane podatności bezpieczeństwa na urządzeniach sieciowych umożliwia: a) określenie skanowanego celu za pomocą adresu IP, oraz grupy celów za pomocą adresu podsieci IP. b) masowe wprowadzenie listy skanowanych celów (adresów IP), za pomocą ustrukturyzowanego pliku z rozszerzeniem CSV. c) konfigurację parametrów skanowania, takich jak: a. zakres skanowanych portów sieciowych TCP/UDP, b. parametr wydajności skanowania, c. rodzaj uwierzytelniania na skanowanej stacji. d) konfigurację harmonogramu uruchamiania skanu: dziennie, tygodniowo, w określony dzień miesiąca, oraz wskazanie godziny rozpoczęcia. e) konfigurację wysyłania powiadomień na wskazany adres e-mail informujących o momencie rozpoczęcia skanowania oraz jego zakończeniu. 14. Konsola zarządzania umożliwia podgląd listy skonfigurowanych skanów wykrywających znane podatności bezpieczeństwa, wraz z informacją o zmianach w stosunku do ostatniego przeprowadzonego skanu. 15. Konsola zarządzania umożliwia eksport wyniku skanu wykrywającego znane podatności bezpieczeństwa do pliku. 16. Rozwiązanie umożliwia uruchomienie skanu wykrywającego luki bezpieczeństwa w aplikacjach webowych. 17. Skanowanie wykrywające luki bezpieczeństwa w aplikacjach webowych umożliwia: a) określenie skanowanego celu za pomocą adresu URL lub adresu IP. b) konfigurację parametrów skanowania takich jak: a. rodzaje testowanych ataków, b. wyjątki ze skanowania (adresy URL omijane podczas testowania aplikacji web), c. parametr wydajności skanowania (ilość jednoczesnych zapytań przesyłanych do skanowanej aplikacji). c) konfigurację uwierzytelniania w testowanej aplikacji web. d) konfigurację harmonogramu uruchamiania skanowania: dziennie, tygodniowo, w określony dzień miesiąca, oraz wskazanie godziny rozpoczęcia skanowania.

	e) konfigurację wysyłania powiadomień na wskazany adres e-mail informujących o momencie rozpoczęcia skanowania oraz jego zakończeniu. 18. Konsola zarządzania umożliwia podgląd listy skonfigurowanych skanów wykrywających luki w aplikacjach webowych wraz z informacją o zmianach w stosunku do ostatniego przeprowadzonego skanu. 19. Rozwiązanie umożliwia skorzystanie z narzędzia do identyfikacji zasobów informatycznych dostępnych z publicznej sieci Internet. 20. Narzędzie do identyfikacji zasobów informatycznych dostępnych z publicznej sieci Internet umożliwia: a) przeszukiwanie adresów internetowych, skatalogowanych przez automatyczne systemy producenta, spełniających wskazane warunki wyszukiwania. b) zapisywanie wskazanych warunków wyszukiwania jako szablony. c) podgląd listy wyników wyszukiwania z informacją o wykrytym adresie IP, nazwie oraz słowach kluczowych. d) dodanie wybranych wyników wyszukiwania do grupy skanowania podatności bezpieczeństwa. 21. Rozwiązanie umożliwia podgląd listy wszystkich wykrytych podatności bezpieczeństwa z wszystkich przeprowadzonych skanowań. 22. Lista wszystkich wykrytych podatności musi umożliwiać: a) filtrowanie podatności ze względu na ich rodzaj, przypisany znacznik (opis), urządzenie sieciowe na którym została znaleziona podatność, stopień zagrożenia, status jego naprawy. b) wyświetlenie szczegółów poszczególnych podatności bezpieczeństwa wraz z informacjami na jakich urządzeniach sieciowych dana podatność została wykryta. c) eksport listy urządzeń na których została wykryta dana podatność bezpieczeństwa do pliku CSV. 23. Rozwiązanie umożliwia podgląd listy wygenerowanych raportów. 24. Rozwiązanie umożliwia utworzenie nowego raportu podsumowującego. 25. Raport podsumowujący umożliwia: a) konfigurację szablonu jaki będzie wykorzystany do przygotowania raportu, b) wybranie grup urządzeń, które będą znajdowały się w raporcie, c) wybranie poszczególnych statusów oraz poziomu zagrożenia podatności, które będą znajdowały się w raporcie, d) personalizację danych, którymi zostanie podpisany raport. 26. Lista wygenerowanych raportów musi umożliwiać: a) filtrowanie raportów ze względu na ich autora, nazwę, szablon oraz opis, b) eksport wyniku raportu do pliku XML, DOCX, XLSX. 27. Rozwiązanie umożliwia zarządzanie wykrytymi podatności w co najmniej następujący sposób: a) podgląd listy utworzonych zgłoszeń, b) filtrowanie zgłoszeń ze względu na ich status oraz czas zamknięcia, c) podgląd listy szablonów dla poszczególnych rodzajów skanów, d) dodanie szablonu dla poszczególnych rodzajów skanów oraz wprowadzenie ich konfiguracji
Ochrona punktów końcowych urządzeń komputerowych	Ochrona antywirusowa niżej wymienionego systemu monitorowana i zarządzana z pojedynczej, centralnej konsoli, znajdującej się na serwerach producenta, do której dostęp zapewniony jest przez przeglądarkę internetową. Od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, do prawidłowego działania wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli znajdującej się na serwerach producenta.

Rozwiązanie dla ochrony antywirusowej stacji roboczych wspiera następujące systemy operacyjne:

- Microsoft Windows 10
- Microsoft Windows 11
- macOS 11 "Big Sur"
- macOS 10.15 "Catalina"
- macOS 10.14 "Mojave"
- MacOS 10.15 “Catalina”

Rozwiązanie dla ochrony antywirusowej systemów serwerowych wspiera następujące systemy operacyjne:

- Microsoft Windows Server 2012
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- Microsoft Windows Server 2022

Wspierane przeglądarki internetowe do obsługi konsoli zarządzającej:

- Microsoft Internet Explorer
- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Safari

Zarówno konsola jak i oprogramowanie antywirusowe do ochrony stacji roboczych oraz serwerów posiada Polski interfejs użytkownika.
Ten sam agent zainstalowany na systemach Windows umożliwia rozbudowę funkcjonalności o system EDR i mechanizm zarządzania podatnościami – aktywacja dodatkowych funkcji uzależniona jest tylko od posiadanej licencji, automatycznie aktywowana w momencie jej dodania i nie wymaga reinstalacji agenta w środowisku oraz posiadania osobnej konsoli zarządzającej.
Funkcjonalności systemu mogą różnić się w zależności od platformy na jakiej zainstalowany jest agent ze względu na ich ograniczenia, jednak chronione platformy są zarządzane z tej samej konsoli zarządzającej

Opis technologii

1. Ochrona antywirusowa realizowana na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanowania heurystycznego, modułu skanującego nośniki wymienne, monitora ruchu http oraz modułu wykrywającego rootkity.
2. Rozwiązanie posiada wbudowany mechanizm ochrony przed zagrożeniami typu ransonmware.
3. Rozwiązanie wspiera technologię Antimalware Scan Interface (AMSI)
4. Rozwiązanie umożliwia wybór plików do skanowania – wszystkich plików lub tylko plików o określonych rozszerzeniach.
5. W momencie wykrycia infekcji rozwiązanie automatycznie stara się wyleczyć plik, a jeśli nie jest to możliwe przenosi go do bezpiecznego folderu kwarantanny.
6. Rozwiązanie posiada możliwość ręcznej reakcji na wykryte zagrożenie, w takim przypadku pozwala na: wyleczenie pliku, usunięcie, przeniesienie do kwarantanny, zmiany nazwy, zablokowania.
7. Rozwiązanie chroni plik systemowy HOSTS przed nieautoryzowanymi zmianami.
8. Rozwiązanie posiada mechanizmy skanujące dyski sieciowe.
9. Skanowanie dysków sieciowych jest możliwe dla dowolnych operacji na takich zasobach lub tylko przy wykonywaniu znajdujących się tam plików.

	10. Rozwiązanie posiada możliwość tworzenia wykluczeń dla mechanizmów ochrony w czasie rzeczywistym, w tym co najmniej dla: plików, folderów, procesów. 11. Rozwiązanie posiada mechanizm ochrony ruchu http chroniący użytkownika przed malware oraz phishingiem. 12. Istnieje możliwość stworzenia wykluczenia dla wskazanej aplikacji, tak aby nie skanowała ona ruchu http. 13. Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie przez wywołanie funkcji w interfejsie lokalnym oprogramowania. 14. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione. 15. Rozwiązanie posiada możliwość dystrybuowania aktualizacji baz definicji wirusów oraz aktualizacji oprogramowania zainstalowanego na stacji końcowej, za pomocą serwera pośredniczącego. 16. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej do nowej wersji, następuje w sposób automatyczny, niewidoczny dla użytkownika końcowego. 17. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej nie wymaga dodatkowych czynności konfiguracyjnych ze strony administratora systemu i następuje automatycznie w momencie udostępnienia takiej aktualizacji przez producenta. 18. Rozwiązanie posiada możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli zarządzania. 19. Rozwiązanie posiada możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej w określone dni i godziny tygodnia i miesiąca. 20. Rozwiązanie posiada możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli lub lokalnie przez określonego klienta. 21. Rozwiązanie posiada możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera. 22. Rozwiązanie posiada możliwość wywołania procesu skanowania z niskim priorytetem, co pozwala na skanowanie z użyciem mniejszej ilości zasobów systemowych. 23. Rozwiązanie posiada możliwość wywołania skanowania uwzględnionych rozszerzeń a także ich wykluczanie. 24. Rozwiązanie posiada możliwość skanowania urządzeń przenośnych takich jak pendrive, dyski zewnętrzne itp. 25. Skanowanie dysków przenośnych może odbywać się w sposób automatyczny bez wiedzy użytkownika, automatycznie z wyświetleniem podsumowania skanowania użytkownikowi oraz z możliwością zablokowania opcji przerwania skanowania przez użytkownika końcowego. 26. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie. 27. Rozwiązanie posiada funkcję skanowania na żądanie pojedynczych plików, katalogów, napędów przy pomocy skrótu w menu kontekstowym 28. Mikrodefinicje wirusów – przyrostowe (inkrementalne) pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji). 29. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.

	30. Rozwiązanie posiada heurystyczną technologię do wykrywania nowych, nieznanych wirusów. 31. Umożliwia wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger", „dialer", „trojan", „rootkit". 32. Posiada mechanizm wykrywania nowych i nieznanych zagrożeń (0-day), bazujący na technologii chmurowej, analizującej podejrzane pliki wykonywalne. 33. Rozwiązanie posiada technologię wykrywania nowych i nieznanych zagrożeń typu 0-day, technologia ta powinna w głównej mierze bazować na metadanych na temat analizowanego pliku. Pliki sklasyfikowane jako bezpieczne, nie są wysyłane do analizy w infrastrukturze producenta. 34. Rozwiązanie posiada technologię wykrywania nowych i nieznanych zagrożeń, która w przypadku podejrzanych plików umożliwia automatyczne ładowanie ich do systemu sandbox, utrzymywanego w infrastrukturze dostawcy oprogramowania antywirusowego w celu przeprowadzenia dodatkowej strukturalnej i behawioralnej analizy podejrzanego pliku. 35. Rozwiązanie posiada możliwość wyłączenia mechanizmu automatycznego przesyłania podejrzanych plików do dodatkowej analizy przez producenta. 36. Rozwiązanie posiada możliwość umieszczenia oprogramowania typu „spyware", „adware", „keylogger", „dialer", „trojan" w kwarantannie. 37. Rozwiązanie posiada możliwość obsługi plików skompresowanych obejmującego najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2 HQX. 38. Rozwiązanie posiada możliwość logowania historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów jest możliwy z poziomu GUI aplikacji jak i konsoli centralnego zarządzania. 39. Rozwiązanie automatycznie powiadamia użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem czy stacja robocza jest odpowiednio zabezpieczona. 40. Rozwiązanie posiada możliwość wyłączenia powiadomień dla użytkowników stacji końcowej o wykrytych zagrożeniach. 41. Rozwiązanie posiada możliwość wyłączenia interfejsu użytkownika oprogramowania zainstalowanego na stacji końcowej. 42. Rozwiązanie umożliwia blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http. 43. Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez system reputacyjny producenta. 44. Rozwiązanie posiada możliwość instalacji dodatku do przeglądarki internetowej (Google Chrome, Mozilla FireFox, MS Edge) pozwalającego na wyświetleniu graficznej informacji o reputacji witryny, która pojawia się w wynikach wyszukiwania w wyszukiwarkach internetowych. 45. Rozwiązanie jest wyposażone w mechanizm ochrony przeglądarki internetowej, w tym analizujący uruchamiane skrypty ActiveX i pobierane pliki. 46. Rozwiązanie posiada możliwość ochrony podczas przeglądania sieci Internet na podstawie badania reputacji witryn. 47. Rozwiązanie umożliwia blokowanie dostępu do kategorii witryn WWW skatalogowanych przez systemy producenta. 48. Oprogramowanie zapewnia co najmniej 30 kategorii klasyfikacji witryn WWW. 49. Użytkownik podczas próby przejścia na witrynę znajdująca się w zablokowanej przez Administratora kategorii, jest powiadomiony o nałożonej na niego blokadzie komunikatem w przeglądarce internetowej. 50. Rozwiązanie umożliwia blokowanie witryn na podstawie kategorii zarówno dla protokołu HTTP jak i HTTPS.

	51. Rozwiązanie posiada wbudowany mechanizm zabezpieczenia połączenia do witryn skategoryzowanych przez producenta jako „bankowość elektroniczna”. 52. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie blokuje możliwość uruchamiania od strony chronionego hosta poleceń cmd oraz skryptów. 53. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie automatycznie blokuje zdalny dostęp do hosta za pomocą takich narzędzi jak pulpit zdalny, TeamViewer, LogMein, VNC itp. 54. Kontrola połączenia umożliwia zabezpieczenie sesji do dowolnej witryny HTTPS wskazanej przez administratora – administrator ma możliwość tworzenia własnej listy takich witryn. 55. Rozwiązanie posiada wbudowaną funkcję, która po zakończeniu sesji z witrynami sklasyfikowanymi jako „bankowość elektroniczna” czyści zawartość schowka systemowego. 56. Rozwiązanie posiada funkcję zarządzania zaporą ogniową (tzw. personal firewall) wbudowaną w system Windows, z opcją definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup. 57. Profile bezpieczeństwa zapory ogniowej zawierają predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej. 58. Rozwiązanie pozwala na tworzenie własnych reguł w oparciu co najmniej o: kierunek komunikacji sieciowej, protokół sieciowy oraz możliwość wyboru akcji zezwolenia lub zablokowania wskazanej komunikacji. 59. Rozwiązanie posiada możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej). 60. Rozwiązanie umożliwia stworzenie zestawów reguł do natychmiastowego zastosowania, które zablokują komunikację sieciową w celu izolacji hosta na żądanie administratora. 61. Rozwiązanie jest wyposażone w mechanizm aktualizacji aplikacji (patch management), umożliwiający instalację dostępnych poprawek dla systemu operacyjnego oraz aplikacji na nim zainstalowanych. 62. Mechanizm aktualizacji aplikacji (patch management) nie wymaga instalowania dodatkowych agentów oprócz agenta AV. 63. Moduł aktualizacji aplikacji, okresowo skanuje aplikacje zainstalowane na stacji roboczej i umożliwia ich aktualizację do najnowszych wersji. 64. Moduł aktualizacji aplikacji pełni role mechanizmu łatającego podatności i instalującego aktualizacje oprogramowania, a nie jedynie pasywnego skanera luk w bezpieczeństwie aplikacji. 65. Administrator posiada możliwość określenia, kiedy i jakie aktualizacje mają zostać zainstalowane automatycznie. 66. Administrator posiada możliwość uruchomienia aktualizacji dla systemu operacyjnego jak i aplikacji znajdujących się na nim na żądanie dla wybranych lub wszystkich hostów. 67. Mechanizm aktualizacji aplikacji umożliwia automatyczne wyświetlenie komunikatu użytkownikowi od strony hosta o konieczności zamknięcia danej aplikacji, tak aby proces aktualizacji mógł się zakończyć. 68. W przypadku gdy instalacja aktualizacji dla systemu operacyjnego lub innej aplikacji wymaga restartu hosta w celu jej zastosowania, administrator posiada możliwość wymuszenia automatycznego restartu, wymuszenia restartu po określonej liczbie godzin, lub wyświetlenia komunikatu użytkownikowi o konieczności restartu. 69. Administrator konsoli zarządzającej ma możliwości zapoznania się z opisem danej podatności aplikacji uruchamiając aktywny link z konsoli zarządzającej z przekierowaniem na strony producenta aplikacji.

	70. Mechanizm aktualizacji aplikacji (patch management) nie wymaga uprawnień administratora lokalnego do instalacji poprawek i jest realizowany, jako dedykowany proces. 71. Administrator ma możliwość zdefiniowania aplikacji, które nie podlegają aktualizacji, poprzez wpisanie nazwy aplikacji na listę wykluczeń w konsoli zarządzającej. 72. Rozwiązanie umożliwia wyświetlenie w GUI od strony chronionego hosta informacji o brakujących poprawkach dla systemu lub aplikacji i umożliwienie, ich instalacji przez użytkownika końcowego. 73. System centralnego zarządzania prezentuje niezaktualizowane aplikacje występujące na wszystkich chronionych hostach lub listę nieaktualizowanego oprogramowania dla pojedynczej stacji końcowej. 74. Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej. 75. Mechanizm kontroli urządzeń zewnętrznych wspiera m.in. urządzenia takie jak: pamięci masowe, napędy CD/DVD, modemy, porty COM i LTP, drukarki, czytniki kart pamięci, kamery, urządzenia bluetooth. 76. Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączania do stacji końcowej. 77. Lista urządzeń zaufanych jest tworzona co najmniej w oparciu o nazwę urządzenia i identyfikator sprzętowy. 78. Rozwiązanie posiada możliwość blokady zapisywania plików na zewnętrznych dyskach USB urządzenia takie są wówczas dostępne w trybie tylko do odczytu. 79. Mechanizm kontroli urządzeń umożliwia blokadę uruchamiania plików wykonywalnych z nośników pamięci. Blokada ta pozwala na korzystanie z pozostałych danych zapisanych na takich nośnikach. 80. Rozwiązanie posiada opcję zabezpieczenia hasłem możliwości deinstalacji agenta przez użytkownika końcowego. 81. Zmiany w konfiguracji mogą być dokonywane przez użytkownika końcowego tylko dla poszczególnych funkcji aplikacji wskazanych przez administratora w profilu. 82. Rozwiązanie posiada możliwość przekazywania do konsoli administracji zdalnej kluczy odzyskiwania funkcji BitLocker 83. Rozwiązanie pozwala na zdalne wymuszenie procesu szyfrowania dysków systemowych za pomocą funkcji Bitlocker wbudowanej i obsługiwanej przez system Windows. 84. W momencie zdalnego uruchomienia procesu szyfrowania za pomocą funkcji Bitlocker administrator posiada możliwość wymuszenia ustanowienia kodu PIN na stacji roboczej, wymaganego do logowania. 85. Rozwiązanie pozwala na zdalne uruchomienie procesu deszyfrowania wcześniej zaszyfrowanych dysków systemowych. 86. Administrator w konsoli zarządzającej posiada dostępne informacje dotyczące stanu zaszyfrowania dysków systemowych. 87. Rozwiązanie posiada wbudowany mechanizm przywracania plików zaszyfrowanych przez zagrożenia typu ransomware. 88. Mechanizm w swoim działaniu wykorzystuje własną technologię producenta, nie inne technologie takie jak Volume Shadow Copy Service (VSS) 89. W przypadku wykrycia szkodliwego działania ransomware, moduł blokuje aktywność szkodliwego procesu oraz przywraca pliki, które zostały zaszyfrowane do oryginalnej formy i lokalizacji. 90. Moduł przywracania plików zaszyfrowanych może działać w trybie monitorowania, bez podejmowania reakcji. 91. Administrator ma możliwość wskazania własnego folderu, do którego będą kopiowane pliki tworzonej kopii zapasowej plików. 92. Administrator posiada możliwość określenia maksymalnej wielkości pliku, którego kopia zapasowa będzie tworzona przez moduł przywracania.

93. Rozwiązanie jest wyposażone w dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware niezależnie od pozostałych modułów ochrony. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.
94. Moduł posiada możliwość pracy w trybie monitorowania (bez blokowania) przekazując administratorowi informacje dotyczące prób modyfikacji plików w chronionych folderach.
95. Administrator posiada możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.
96. Istnieje możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną antyransomware.
97. Rozwiązanie potrafi automatycznie wykryć zaufane aplikacje, dla których będzie zezwolony dostęp do plików w chronionych folderach, oraz daje możliwość wskazania zaufanych aplikacji przez administratora.
98. Rozwiązanie posiada funkcjonalność kontroli uruchamianych aplikacji.
99. Tryb kontroli aplikacji umożliwia uruchomienie wszystkich aplikacji, uruchomienie i monitorowanie wszystkich aplikacji, blokowanie niezaufanych aplikacji
100. Istnieje możliwości blokowania, zezwolenia lub monitorowania aplikacji w oparciu, co najmniej o docelowy identyfikator SHA1,SHA256, lokalizację pliku, wersję pliku, nazwę aplikacji, wielkość pliku, wydawcę, ważność podpisu cyfrowego aplikacji.
101. Tworzone reguły dotyczyć mogą czynności: uruchomienia aplikacji, ładowania modułu, uruchomienia instalatora, dostępu do pliku.
102. Na wspieranych systemach Windows rozwiązanie pozwala na zdalne wywołanie procesu szyfrowania za pomocą funkcji BitLocker wbudowanej w system operacyjny.
103. Administrator posiada w momencie konfiguracji procesu szyfrowania, możliwość wymuszenia od strony użytkownika ustanowienia dodatkowego zabezpieczenia w postaci kodu PIN
104. Rozwiązanie pozwala na uzyskiwanie informacji pochodzących z dziennika systemu Windows dotyczących między innymi: Czyszczenia dziennika audytu, zablokowania konta użytkownika, utworzenia konta użytkownika, zmiany konta użytkownika, błędnych prób logowania użytkownika, wystąpienia błędu krytycznego (BSOD)
105. Administrator ma możliwość wyboru, które z informacji pochodzących z dziennika systemu Windows mają być przekazywane do konsoli zarządzającej.
106. Rozwiązanie pozwala na wygenerowanie pliku za pocą którego administrator może wywołać zdalne podłączenie za pomocą usług Microsoft RDP (Remote Desktop).
107. Wygenerowany plik może być otwarty i wykorzystany do zdalnego podłączenia za pomocą Microsoft Terminal Services Client (MSTSC), Microsoft Remote Desktop i innych wspierających usług i aplikacji.

Centralna administracja

1. Portal zarządzający jest dostępny w języku polskim.
2. Komunikacja pomiędzy portalem centralnego zarządzania a stacjami roboczymi odbywa się w formie zaszyfrowanej.
3. W celu korzystania z centralnej administracji, od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli zarządzającej znajdującej się na serwerach producenta.
4. Interfejs zarządzania posiada funkcję wyświetlania monitów o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.
5. Interfejs jest wyposażony w panel kontrolny zawierający podsumowanie stanu bezpieczeństwa organizacji w postaci graficznych wykresów.

	6. Wykresy są interaktywne, tzn., że po wybraniu interesującego elementu, następuje przekierowanie do zawierającego bardziej szczegółowe dane menu. 7. Rozwiązanie posiada dedykowaną zakładkę zawierającą informację o wszystkich hostach posiadających zainstalowane oprogramowanie do ochrony, w tym: ich nazwy, status ochrony, przypisany profil bezpieczeństwa. 8. Istnieje możliwość eksportu listy wszystkich hostów do pliku CSV. 9. Administrator ma możliwość wglądu w szczegóły zgłaszającego się hosta, w których zawarte są informacje dotyczące: ostatniego podłączenia do konsoli zarządzającej, wersji zainstalowanego produktu, systemu operacyjnego, stanu ochrony, akcji związanych z wykrytymi zagrożeniami i skanowaniami. 10. Administrator ma możliwość z poziomu szczegółów klienta, uruchomienia skanowania antywirusowego, instalacji aktualizacji dla aplikacji i systemu operacyjnego, przypisania profilu, usunięcia urządzenia, zmiany klucza subskrypcji, odizolowania hosta od sieci i pobrania pliku diagnostycznego. 11. Komputery nie nawiązujące komunikacji z konsolą zarządzającą mogą być automatycznie usuwane z listy po określonym przez administratora czasie - co najmniej 60 dni. 12. Rozwiązanie posiada dodatkową zakładkę zawierającą informacje dotyczącą brakujących aktualizacji dla zainstalowanych aplikacji i systemu operacyjnego. 13. Istnieje możliwość posortowania i filtrowania brakujących poprawek pod względem ich poziomu krytyczności. 14. Informacje dotyczące brakujących poprawek dla aplikacji i systemu operacyjnego zawierają liczbę i typ hostów, na których został wykryty brak danej poprawki. 15. Po wskazaniu danej poprawki administrator posiada możliwość jej instalacji na wskazanych komputerach lub na wszystkich komputerach i serwerach, dla których dana poprawka została wydana. 16. Administrator ma możliwość wglądu w historię instalowanych poprawek na chronionych hostach. 17. Rozwiązanie posiada moduł raportujący w którym wyświetlane są informacje dotyczące stanu ochrony, infekcji malware, instalowanych aplikacji. 18. Raporty mogą być tworzone zgodnie z harmonogramem i wysyłane na wskazane adresy email. 19. Rozwiązanie posiada wbudowany mechanizm zarządzania subskrypcjami, z możliwością dodawania nowych kluczy licencyjnych. 20. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji. 21. Portal zarządzający umożliwia dodawanie kluczy licencyjnych dla innych produktów w celu aktywacji danej funkcjonalności, co najmniej dla systemu EDR, mechanizmów zarządzania podatnościami, ochrony usług Microsoft 365. 22. Dodanie klucza licencyjnego skutkuje pojawieniem się dedykowanej zakładki obsługującej dany produkt w portalu zarządzającym. 23. Rozwiązanie ma możliwość definiowania różnych profili ustawień dla chronionych urządzeń z poziomu portalu zarządzającego. 24. Profile mogą być przypisane do pojedynczych hostów lub do grup. 25. Profile mogą być automatycznie przypisywane do hostów spełniających określone warunki w tym: adresy IP, DNS, nazwa WINS, przynależność do AD. 26. W przypadku automatycznego przypisywania profili, system pozwala na automatyczne dodawanie tagów dla hostów które otrzymają dany profil konfiguracyjny. 27. Istnieje możliwość porównania 2 profili konfiguracyjnych w celu wyświetlenia różnic pomiędzy nimi. 28. Rozwiązanie pozwala administratorowi podczas tworzenia profili wskazanie funkcjonalności, które mogą być zmieniane przez użytkownika od strony

	chronionego hosta – możliwość wprowadzanych zmian jest do określenia dla poszczególnych funkcji programu oraz całości konfiguracji. 29. Z poziomu portalu zarządzającego istnieje możliwość pobrania plików instalacyjnych, wykorzystywanych do instalacji agenta na objętych licencją hostach. 30. Pliki instalacyjne mają posiadać plików .EXE, .MSI, .MPKG, .DEB, .RPM w zależności od platformy i typu systemu na jakich ma zostać zainstalowany agent. 31. Tworzone profile muszą dają administratorowi możliwość blokowania ustawień konfiguracyjnych aplikacji zainstalowanych od strony stacji roboczych w celu uniemożliwienia ich modyfikacji przez lokalnego użytkownika. 32. Administrator posiada możliwość wyświetlenia dodatkowych szczegółów dotyczących chronionych hostów. 33. Administrator posiada do wyboru ponad 100 różnych dodatkowych informacji, które mogą być widoczne w tym co najmniej: wersji BIOS, identyfikatora CPU, ilości rdzeni procesora, wolnej ilości miejsca na dysku, informacji o fakcie wykorzystania systemu operacyjnego Windows który osiągnął cykl end of life, aktywnego wygaszacza ekranu, zalogowanego konta administracyjnego. 34. Portal zarządzający pozwala na zarządzanie oprogramowaniem instalowanym na urządzeniach mobilnych (smartphony) w przypadku posiadania odpowiedniej licencji. 35. Konsola posiada możliwość definiowania wielu kont administratorów o różnych poziomach dostępu. 36. W ramach posiadanych licencji istnieje możliwość przenoszenia oprogramowania w ramach danego klucza subskrypcji z jednej stacji roboczej na inną.
Certyfikaty i standardy	• Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Products In Endpoint Protection Platforms Market na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/endpoint-protection-platforms minimalne wymaganie: minimalna liczba referencji 65 minimalna ocena z referencji 4,5 (załączyć wydruk do oferty) • Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Endpoint Detection and Response (EDR) Solutions Market https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions minimalne wymaganie: minimalna liczba referencji 17 minimalna ocena z referencji 4,4 (załączyć wydruk do oferty) system musi posiadać certyfikaty: • OPSWAT (dla EDR na poziomie min. Platinium), • AVLAB +++ • AV Comperative Advance + • AV-TEST (ochrona w 2023 na poziomie min.6) • producent systemu lub autoryzowany dystrybutor producenta musi posiadać certyfikat ISO 9001 oraz 27001 oraz usługi związane z cyberbezpieczeństwem

Rozszerzone wsparcie serwisowe - SOC – Security Operation Center	System jest objęty rozszerzonym wsparciem technicznym gwarantującym czas reakcji wsparcia technicznego do 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora. System jest objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie: • Wsparcie telefoniczne zespołu certyfikowanych inżynierów. • Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu. • Doradztwo w zakresie konfiguracji. • Zdalne wsparcie techniczne. • Pomoc w zakładaniu zgłoszeń serwisowych u producenta. • Przygotowanie do zdalnej konfiguracji. • Zdalna konfiguracja (połączenia szyfrowane) zgodnie z wymaganiami użytkownika. • Minimum 5 zdalnych rekonfiguracja urządzenia w związku ze zmianą środowiska lub wymagań użytkownika. • Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich. • Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich. • Monitorowanie krytycznych incydentów EDR 24/7 przez certyfikowanych ekspertów producenta oprogramowania. • Walidacja i dochodzenie czy incydenty są prawdziwe oraz czy wymagają natychmiastowej akcji by zatrzymać incydent, bądź czy są fałszywymi incydentami. • Eskalacja incydentu do adekwatnego reprezentanta klienta mającego możliwość i autorytet, aby odpowiedzieć na incydent. • Porada ekspertów jak zatrzymać i naprawić incydent – na przykład, rekomendując izolację systemów bądź zatrzymanie złośliwych procesów **Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 oraz 27001 w szczególności w zakresie świadczenia usług wsparcia technicznego oraz usług związanych z cyberbezpieczeństwem. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7.** Oferent winien przedłożyć dokumenty: • Oświadczanie Producenta lub Autoryzowanego Dystrybutora producenta świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). • Certyfikat ISO 9001 oraz 27001 autoryzowanego podmiotu serwisującego.

2. Doposażenie infrastruktury zasilania awaryjnego

UPS 10000VA (parametry minimalne)	
Parametr	**Wymagania minimalne**
Moc pozorna	**min. 10000VA**
Moc rzeczywista	min. 10000W
Technologia	on-line (VFI), podwójna konwersja
Sprawność max (dla VFI)	95%

Typ obudowy	rack/tower
praca sieciowa	
Napięcie wejściowe	110 ÷ 275 V AC ± 3%
Częstotliwość napięcia wejściowego	50 / 60 Hz
Zakres napięcia wyjściowego	208 V AC / 220 V AC / 230 V AC / 240 V AC - domyślnie 230 V AC
Wartość napięcia wyjściowego ustawiana z panelu LCD	tak
Kształt napięcia wyjściowego	sinusoidalny
Czas przełączania sieć – UPS	0ms
Współczynnik odkształceń prądu wejściowego THDi	< 3%
praca bateryjna	
Napięcie wyjściowe	~230V
Częstotliwość napięcia wyjściowego	50Hz/60Hz ± 0,1Hz
Kształt napięcia wyjściowego na pracy bateryjnej	sinusoidalny
Zabezpieczenie przeciwzwarciowe gniazd wyjściowych	Bezpiecznik automatyczny 20 A
Zabezpieczenie przeciążeniowe	elektroniczne
Akumulatory wewnętrzne w UPS lub w Modułach Bateryjnych	minimum 20 x 12V 9Ah; szczelne, bezobsługowe
Czas podtrzymania (dla obciążenia 3500W) przy wykorzystaniu baterii w zewnętrznych modułach bateryjnych	minimum 15min
pozostałe	
Przeciążalność	100%＜obciążenie ≤105%: ciągłe 105%＜obciążenie ≤125%: 10 minut 125%＜obciążenie ≤150%: 30s >150% : 500ms
Wejście zasilania	Listwa zaciskowa
Ilość i typ gniazd wyjściowych	W UPS minimum 2x IEC 320 C13 (10 A) + listwa zaciskowa
Sygnalizacja	Wyświetlacz LCD (informacje wskazujące pracę sieciową, bateryjną, przeciążenie i ładowanie akumulatora). Diody LED
Możliwość podłączenia zewnętrznych modułów bateryjnych	Wymagana możliwość podłączenia minimum 5 zewnętrznych modułów bateryjnych
Interfejs komunikacyjny	RS232, USB HID, SNMP/HTTP - opcja
Złącze EPO	wymagane
Styki bezpotencjałowe zamontowane na stałe w obudowie UPS	wymagany minimum 1x wejściowy i 1x wyjściowy
Wsporniki do montażu w szafie RACK	wymagane
Waga UPSa	do 16,5kg
Waga pojedynczego MODUŁU BATERYJNEGO	do 69kg

Wymiary UPS - wersja RACK	nie większe niż: wysokość 86mm; szerokość 438mm; głębokość 576mm
Wymiary MODUŁ BATERYJNY - wersja RACK	nie większe niż: wysokość 130mm; szerokość 438mm; głębokość 596mm
Łączna wysokość w szafie RACK 19" dla oferowanego zestawu	nie więcej niż 5U
Gwarancja	min 24 miesięcy na elektronikę i 24 miesięcy na akumulatory;
Serwis	autoryzowany serwis producenta zlokalizowany w Polsce. naprawa w maksymalnie 5 dni roboczych serwis realizowany w systemie door to door
Oprogramowanie	oprogramowanie tego samego producenta co UPS, w języku polskim do zarządzania i monitorowania pracy UPS dla Windows, Linux oraz systemów wirtualizacji VMware, Hyper-V, Citrix XenServer bez ograniczeń co do ilości moniotorowanych stanowisk (bez dodatkowych opłat za licencje); możliwość edycji nazw urządzeń na liście monitorowanych UPSów; wymagane wsparcie producenta (telefoniczne oraz mailowe) w języku polskim odnośnie konfiguracji i rozwiązywania problemów.
Certyfikaty producenta (załączyć do oferty)	ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisowania; deklaracja CE producenta sprzętu;
Oświadczenia / dokumenty (załączyć do oferty)	oświadczenie producenta o spełnieniu minimalnych wymaganych parametrów specyfikacji; karta katalogowa oferowanego sprzętu

3. Rozwiązanie typu NAC

Opis funkcjonalności rozwiązania	Wymagane jest dostarczenie rozwiązania typu NAC (Network Access Control), służącego do monitorowania sieci lokalnych w celu uwidocznienia pracujących w nich urządzeń oraz wykrywania nowych urządzeń pojawiających się w sieci, w czasie rzeczywistym. Rozwiązanie musi raportować aktualny stan każdego urządzenia, z uwzględnieniem takich atrybutów, jak adres MAC, adres IP, nazwa hosta, system operacyjny, itp., pozyskując te informacje bezagentowo bezpośrednio od samych urządzeń oraz od usług zarządzania infrastrukturą sieciową (np. Active Directory, serwery DNS/DHCP, serwery AV, WMI, itp.). Rozwiązanie ma za zadanie zapewnić, aby tylko urządzenia, których aktualny stan spełnia zdefiniowaną przez administratora politykę bezpieczeństwa, mogły bez ograniczeń ze strony NAC pracować w sieci lokalnej. Rozwiązanie musi być wyposażone w mechanizm kwarantanny, nakładanej przez NAC automatycznie na urządzenia, których aktualny stan nie spełnia danych warunków polityki bezpieczeństwa (np. nowe, po raz pierwszy pojawiające się urządzenie lub stacja robocza z wyłączonym oprogramowaniem antywirusowym). Mechanizm kwarantanny powinien umożliwiać całkowite blokowanie komunikacji urządzenia z otoczeniem sieciowym, jak również blokowanie częściowe, w zakresie definiowanym przez administratora (przez wskazanie adresów IP, z którymi urządzenie może się komunikować). Mechanizm kwarantanny musi działać bezagentowo, wykorzystując protokół ARP, bez konieczności dokonywania jakichkolwiek zmian w konfiguracji infrastruktury sieciowej.

	Rozwiązanie musi posiadać funkcjonalność typu Captive Portal, służącą do rejestrowania i kontrolowania dostępu do sieci dla niezarządzanych urządzeń zewnętrznych, podłączanych przez pracowników (BYOD), gości i zewnętrznych konsultantów.
Wymagania ogólne rozwiązania NAC	1. Ma zapewnić widoczność i monitorowanie wszystkich urządzeń pracujących w sieci lokalnej oraz powiadamiać o nowych urządzeniach pojawiających się w sieci. 2. Musi zapewniać automatyczne blokowanie komunikacji sieciowej między nowym, niezaufanym urządzeniem a zaufanymi, zarządzanymi urządzeniami pracującymi w sieci. 3. Musi umożliwiać sprawdzanie statusu aktualizacji oprogramowania antywirusowego i poprawek systemowych na zarządzanych stacjach roboczych Windows i w przypadku nie spełniania określonych wymagań, automatycznie ograniczać tym stacjom roboczym możliwość pracy w sieci. 4. Musi umożliwiać odbieranie komunikatów bezpieczeństwa z innych systemów bezpieczeństwa (np. firewalla) i automatyczne blokowanie na tej podstawie wskazanych urządzeń w sieci. 5. Musi mieć funkcję wykrywania faktu skanowania urządzeń i portów wykonywanego przez urządzenie w sieci lokalnej i automatycznie blokować takie urządzenie, aby zapobiegać potencjalnemu szerzeniu się malware. 6. Stosowany mechanizm blokowania musi wykorzystywać protokół ARP i działać całkowicie niezależnie od innych elementów infrastruktury sieciowej. 7. Rozwiązanie musi działać bezagentowo, bez konieczności instalowania jakichkolwiek agentów na urządzeniach w sieci oraz bez konieczności dokonywania zmian w infrastrukturze sieciowej. 8. Rozwiązanie musi umożliwiać wysyłanie alertów do administratora za pomocą e-maila oraz SMS 9. Rozwiązanie musi być zarządzane przez interfejs webowy, obsługiwany przeglądarką internetową 10. Wymaga się, aby rozwiązanie było dostarczone w postaci maszyny wirtualnej na platformę VMware oraz Hyper-V. System musi pozwalać na monitorowanie co najmniej 10 sieci VLAN i monitorowanie łącznie co najmniej 300 urządzeń. 11. Wymaga się, aby rozwiązanie było licencjonowane w modelu licencji wieczystej i dostarczone z licencją pozwalającą na monitorowanie 125 urządzeń wraz ze wsparciem technicznym.
Wymagania szczegółowe – monitorowanie podsieci	1. Rozwiązanie musi w czasie rzeczywistym raportować widoczność wszystkich urządzeń pracujących w monitorowanych podsieciach. 2. Rozwiązanie musi wykrywać nowe nieznane urządzenie, dołączające się do sieci LAN lub WLAN, w czasie nie dłuższym, niż 5 sekund oraz wysyłać powiadomienie mailowe do administratora 3. Rozwiązanie musi wykrywać przypadki skanowania urządzeń i portów w monitorowanych podsieciach i blokować urządzenie inicjujące takie skanowanie 4. Rozwiązanie musi określać aktualny stan każdego urządzenia, pozyskując informacje bezagentowo bezpośrednio od samych urządzeń oraz od usług zarządzania infrastrukturą sieciową (np. Active Directory, serwery DNS/DHCP, serwery AV, WMI, itp.) oraz odświeżać te informacje cyklicznie. Musi być możliwość wykorzystania pozyskanych informacji do definiowania polityk bezpieczeństwa. 5. Rozwiązanie musi chronić przed podszywaniem się pod adres MAC (MAC spoofing), umożliwiając zdefiniowanie „odcisku palca” (fingerprint) dla każdego zaufanego urządzenia. Odcisk palca musi być kombinacją co najmniej: adresu MAC, adresu IP, nazwy hosta, nazwy systemu operacyjnego, otwartych portów TCP. Jeśli przeprowadzana cyklicznie weryfikacja odcisku palca wykaże jego zmianę, urządzenie powinno zostać zablokowane. 6. Rozwiązanie musi obsługiwać VLANy, tj. umożliwiać monitorowanie przez jeden fizyczny interfejs sieciowy wielu podsieci, zdefiniowanych jako VLANy

Wymagania szczegółowe – polityka bezpieczeństwa	1. Rozwiązanie musi umożliwiać definiowanie polityki bezpieczeństwa, czyli określenie przez administratora, jakie warunki musi spełniać aktualny stan urządzenia, aby uzyskało ono określony dostęp do sieci. 2. W definiowaniu polityki bezpieczeństwa musi być możliwość wykorzystania informacji o aktualnym stanie urządzenia, pozyskanych bezagentowo bezpośrednio od samych urządzeń oraz od usług zarządzania infrastrukturą sieciową (np. Active Directory, serwery DNS/DHCP, serwery AV, WMI, itp.), poprzez integrację z tymi systemami. 3. Polityka bezpieczeństwa musi umożliwiać przypisanie do urządzenia jednego z trzech trybów dostępu do sieci: a. pełny dostęp b. blokowanie (całkowity brak dostępu) c. ograniczony dostęp 4. Zakres ograniczonego dostępu powinien być definiowany przez administratora, np. w postaci list ACL, określających, do których adresów IP i portów urządzenie ma dostęp. Musi być możliwość zdefiniowania wielu różnych zakresów ograniczonego dostępu. 5. Rozwiązanie powinno automatycznie sprawdzać, które warunki polityki bezpieczeństwa spełnia urządzenie i na tej podstawie przypisywać do urządzenia właściwy zakres dostępu. 6. Zakres dostępu, wynikający ze spełnienia przez urządzenie danych warunków polityki bezpieczeństwa powinien być egzekwowany przez mechanizm kwarantanny. 7. Musi być możliwość łatwego, manualnego tworzenie białej listy adresów MAC, czyli listy urządzeń mogących bez żadnych ograniczeń ze strony NAC pracować w sieci.
Wymagania szczegółowe – mechanizm kwarantanny	1. Rozwiązanie musi być wyposażone w mechanizm kwarantanny, nakładanej przez NAC automatycznie na urządzenie, aby wyegzekwować ograniczenia dostępu do sieci, wynikające z polityki bezpieczeństwa 2. Mechanizm kwarantanny powinien umożliwiać: a. całkowite blokowanie komunikacji urządzenia z otoczeniem sieciowym, b. częściowe blokowanie komunikacji urządzenia z otoczeniem sieciowym, w zakresie definiowanym przez administratora przez wskazanie adresów IP i portów, z którymi urządzenie może się komunikować 3. Mechanizm kwarantanny powinien blokować komunikację urządzenia w czasie nie dłuższym niż 5 sekund od zaistnienia warunku, powodującego nałożenie kwarantanny 4. Dla urządzeń zaufanych, czyli w polityce bezpieczeństwa spełniających kryteria pełnego dostępu do sieci, rozwiązanie nie powinno w żaden sposób przekierowywać ani blokować komunikacji wychodzącej z tych urządzeń 5. Kwarantanna powinna być zdejmowana z urządzenia automatycznie, gdy spełni ono kryteria polityki bezpieczeństwa, pozwalające na pełny dostęp 6. Mechanizm kwarantanny musi działać bezagentowo, wykorzystując protokół ARP, bez konieczności dokonywania jakichkolwiek zmian w konfiguracji infrastruktury sieciowej, musi być niezależny od stosowanych w sieci przełączników, zarządzalnych bądź niezarządzalnych 7. Awaria rozwiązania nie może powodować blokady komunikacji w sieci, tj. w przypadku awarii rozwiązania wszystkie urządzenia mają mieć pełny dostęp do sieci 8. Rozwiązanie musi umożliwiać włączenie i wyłączenie mechanizmu kwarantanny (blokowania komunikacji) w każdej monitorowanej podsieci osobno
Wymagania szczegółowe – integracja z systemami zewnętrznymi	1. Rozwiązanie musi umieć sprawdzić, czy urządzenia z systemem Windows są dołączone do domeny AD 2. Rozwiązanie powinno umożliwiać sprawdzanie statusu oprogramowania antywirusowego, poprawek systemowych i firewalla bezpośrednio na zarządzanych stacjach roboczych Windows w domenie AD, w sposób bezagentowy, przy użyciu WMI. 3. Rozwiązanie musi umożliwiać bezagentową integrację z serwerem zarządzającym poprawkami Windows i sprawdzanie statusu zainstalowanych poprawek na zarządzanych urządzeniach z systemem Windows. Wymagana jest możliwość integracji co najmniej z systemami: Microsoft WSUS.

	4. Rozwiązanie musi umożliwiać bezagentową integrację z serwerem zarządzającym agentami antywirusowymi i sprawdzanie statusu agentów AV zainstalowanych na zarządzanych urządzeniach (co najmniej, czy agent jest zainstalowany, aktywny i ma aktualne sygnatury wirusów). Wymagana jest możliwość integracji co najmniej z systemami: Bitdefender, Carbon Black, CrowdStrike, Cybereason, Eset, FireEye, McAfee, SentinelOne, Sophos, Symantec, TrendMicro, Webroot. 5. Rozwiązanie musi umożliwiać wykorzystanie pozyskanych informacji, wymienionych w poprzedzających punktach 1-4, do definiowania polityki bezpieczeństwa. 6. Rozwiązanie musi umieć odbierać alerty przysyłane za pomocą e-mail lub syslog z innych urządzeń bezpieczeństwa (np. firewalla) i na podstawie zawartych w nich informacji blokować wskazane podejrzane urządzenie
Wymagania szczegółowe – rejestracja urządzeń zewnętrznych: pracowników, gości i konsultantów (Captive Portal)	1. Rozwiązanie musi posiadać wbudowaną funkcję Captive Portal, służącą do rejestrowania i kontrolowania dostępu do sieci dla niezarządzanych urządzeń zewnętrznych, podłączanych przez pracowników (BYOD), gości i zewnętrznych konsultantów. NAC musi przekierowywać ruch HTTP/S od nieznanych urządzeń do tego portalu. 2. Captive Portal musi umożliwiać pracownikom rejestrowanie urządzeń prywatnych (BYOD) i wnioskowanie o dostęp do sieci w ograniczonym zakresie, zdefiniowanym przez administratora. 3. Przy rejestracji przez pracowników ich prywatnych urządzeń, Captive Portal powinien umożliwiać użycie ich kont Active Directory 4. Powinna istnieć możliwość ograniczenia ilości i rodzaju rejestrowanych przez pracownika prywatnych urządzeń 5. Powinna być możliwość przypisania ograniczonego dostępu dla zarejestrowanych urządzeń prywatnych 6. Captive Portal musi umożliwiać osobom niebędącym pracownikami (gościom lub konsultantom) wnioskowanie o ograniczony dostęp do sieci 7. W przypadku rejestracji urządzeń gości powinna być możliwość rejestracji samodzielnie przez gościa oraz przez uprawnionego pracownika firmy 8. Zarejestrowane urządzenia gości powinny automatycznie tracić przydzielony dostęp po upływie zdefiniowanego czasu 9. Powinna istnieć możliwość ograniczenia ilości urządzeń rejestrowanych przez gościa 10. Dla zarejestrowanych urządzeń gości powinna być możliwość ograniczenia, w jakich przedziałach czasu i z jakich podsieci będą one miały dostęp do sieci 11. Dla urządzeń gości powinna być możliwość przypisania dostępu ograniczonego tylko do dostępu do internetu 12. Dla urządzeń konsultantów powinna być możliwość przypisania dostępu ograniczonego do wybranych zasobów lokalnych 13. Rozwiązanie musi umożliwiać zatwierdzenie dostępu dla zarejestrowanego urządzenia gościa i konsultanta drogą mailową. Osoba zatwierdzająca powinna otrzymać z systemu e-mail z wnioskiem o dostęp i udzielić go, odpowiadając na maila lub klikając przygotowany link w treści maila. 14. Rozwiązanie musi przechowywać historyczne raporty dostępu do sieci użytkowników typu gość i konsultant 15. Wygląd Captive Portal musi być edytowalny w zakresie co najmniej zmiany firmowego logo i kolorów oraz informacji, jakie we wniosku rejestracyjnym musi podać gość lub konsultant
Pozostałe wymagania	1. Rozwiązanie powinno oferować możliwość zainstalowania opcjonalnego agenta na zarządzanych stacjach roboczych (wymagane wsparcie dla Windows, Linux i MacOS), który przesyła do serwera zarządzającego NAC szczegółowe informacje na temat stacji roboczej, umożliwiając definiowanie na bazie tych informacji precyzyjnych polityk bezpieczeństwa. 2. Rozwiązanie nie powinno pogarszać wydajności pracy przełączników i routerów, nie może wymagać współpracy z przełącznikami przez port mirroring czy port spanning. 3. Rozwiązanie nie powinno pogarszać wydajność łącz WAN 4. Rozwiązanie nie powinno pogarszać wydajności pracy monitorowanych urządzeń w sieci

Usługi	Wymaga się, aby dostawca zaoferował usługę wdrożenia rozwiązania w infrastrukturze Zamawiającego, przeprowadzoną przez inżyniera certyfikowanego przez producenta rozwiązania, w zakresie: - instalacja i konfiguracja rozwiązania w maszynie wirtualnej na platformie Zamawiającego - szkolenie dla administratora rozwiązania - wsparcie w języku polskim w trybie 8x5 w dni robocze - kwartalny przegląd konfiguracji rozwiązania

4. System DLP – kontrola przed wyciekiem danych

System zabezpieczenia danych przed wyciekiem informacji	Wymaga się dostawy kompletnego rozwiązania do ochrony stacji roboczych Windows przed wyciekiem danych, pochodzącego od jednego producenta, o minimalnej funkcjonalności opisanej poniżej. Wymagane jest, aby cała funkcjonalność była dostępna w ramach jednej, jednolitej instalacji oferowanego systemu ochrony danych przed wyciekiem ze zintegrowanym systemem kontroli portów i szyfrowaniem – całość realizowana w ramach jednego agenta na stacjach roboczych.
Wymagania ogólne	Rozwiązanie ma chronić dane na stacjach roboczych Windows przed wyciekiem, poprzez kontrolę portów fizycznych i podłączanych do nich nośników zewnętrznych oraz przez szyfrowanie danych na dyskach lokalnych i nośnikach zewnętrznych. Rozwiązanie powinno działać w oparciu o definiowanie polityk bezpieczeństwa i integrować się z Active Directory przez wiązanie polityk bezpieczeństwa z obiektami Active Directory. Wymaga się, aby polityka mogła być powiązania z różnymi rodzajami obiektów AD: • Domena • Jednostka Organizacyjna (OU) • Grupa • Użytkownik • Komputer Rozwiązanie nie może w żaden sposób modyfikować, usuwać ani tworzyć obiektów w drzewie AD. Rozwiązanie powinno składać się z pojedynczego serwera zarządzającego, oferującego konsolę administracyjną do zarządzania politykami bezpieczeństwa, konfigurowania i monitorowania pracy systemu oraz z agenta, instalowanego na stacjach roboczych, który egzekwuje polityki bezpieczeństwa przypisane do komputera bądź użytkownika. Dystrybucja polityk bezpieczeństwa i ich odświeżanie na stacjach roboczych muszą zachodzić automatycznie i cyklicznie z częstotliwością definiowaną przez administratora, ale również z możliwością wymuszonego odświeżenia na żądanie z poziomu konsoli administracyjnej oraz ze stacji roboczej. Wymaga się, aby polityki bezpieczeństwa były egzekwowane również w trybie „offline", czyli gdy stacja robocza nie ma kontaktu z serwerem zarządzającym (np. laptop poza firmą). Wymagane jest dostarczenie pliku instalacyjnego agenta w postaci pakietu MSI, z możliwością dystrybucji tego pakietu co najmniej przez Active Directory GPO lub inne systemy dystrybucji centralnej oprogramowania. Agent musi być wspierany dla stacji roboczych z biznesową wersją Windows 10/11.
Kontrola portów fizycznych i nośników zewnętrznych	Produkt musi umożliwiać całkowite blokowanie użycia portów fizycznych: • USB • Firewire • PCMCIA • Secure Digital

	• Serial • Paralel • Porty wewnętrzne • WiFi • Bluetooth Wymagane jest, aby produkt identyfikował i raportował urządzenia podłączane do portów USB stacji roboczych, według typu, producenta, modelu i numeru seryjnego. Funkcja ta jest konieczna, by usprawnić proces definiowania polityk bezpieczeństwa, dotyczących kontroli nośników zewnętrznych. Niezbędna jest możliwość zdalnego przeskanowania stacji roboczych z poziomu konsoli zarządzającej w celu zidentyfikowania podłączanych do nich urządzeń zewnętrznych. Produkt musi umożliwiać blokowanie wybranych typów urządzeń podłączanych do portu USB, rozróżniając: • Telefony komórkowe • Urządzenia oparte o system Android • Urządzenia oparte o system iOS • Urządzenia PDA • Smart Card • Urządzenia drukujące • Adaptery sieciowe • Urządzenia audio/video • Urządzenia interfejsu HID • Urządzenia do przetwarzania obrazów • Sprzętowe KeyLoggery Produkt musi posiadać funkcję definiowania “białych list”, czyli urządzeń wyjątkowo dopuszczonych do podłączenia, identyfikowanych przez określenie producenta, modelu i numeru seryjnego urządzenia. Dla zewnętrznych urządzeń pamięci masowej typu: pendrive, napędy CD/DVD, zewnętrzne dyski twarde – musi być możliwość zdefiniowania w polityce bezpieczeństwa mechanizmów: • Blokowanie urządzeń danego typu • Korzystanie w trybie „tylko do odczytu” • Wymuszenie szyfrowania danych na nośniku • Blokowanie możliwości odczytu z nośnika plików określonego typu (np. plików wykonywalnych) • Blokowanie możliwości zapisywania na nośniku plików określonego typu • Rejestrowanie w logach wszystkich zapisów i odczytów z nośnika, również wtedy, gdy stacja pracuje „offline” Szyfrowanie danych na nośnikach zewnętrznych musi być przezroczyste dla użytkownika i nie wymagać żadnego zarządzania kluczami szyfrującymi. Musi być możliwość zapisania i odczytania danych z zaszyfrowanego nośnika na dowolnej stacji roboczej wyposażonej w agenta oferowanego rozwiązania.
Szyfrowanie dysku lokalnego	Wymaga się funkcjonalności szyfrowania danych na dysku lokalnym, inicjowanej tym samym jednolitym mechanizmem, co inne funkcjonalności, tj. przez przypisanie odpowiedniej polityki bezpieczeństwa do stacji roboczej. Wymagane jest, aby szyfrowaniem objęte były tylko dane użytkowników, bez szyfrowania sektora rozruchowego i plików systemowych Windows. Przypisanie polityki szyfrowania do stacji roboczej powinno spowodować zaszyfrowanie danych na dysku.

	Szyfrowanie danych na dyskach lokalnych musi być przezroczyste dla użytkownika i nie wymagać żadnego zarządzania kluczami szyfrującymi. Proces deszyfrowania/szyfrowania musi być realizowany w czasie rzeczywistym przy modyfikacji plików przez użytkownika. Obsługa szyfrowania musi być realizowana w całości przez agenta oferowanego rozwiązania, bez konieczności korzystania z rozwiązań zewnętrznych. Wymaga się, aby zaszyfrowane dane były dostępne dla każdego użytkownika, który na stacji roboczej poprawnie zaloguje się na swoje konto domenowe (w zakresie jego uprawnień na poziomie systemu plików). Wymaga się, aby żadne zaszyfrowane dane nie były dostępne, gdy na stacji roboczej zaloguje się pracownik Helpdesku. Umożliwi to udzielanie wsparcia użytkownikom w zakresie utrzymania systemu operacyjnego, bez ryzyka ujawnienia treści ich danych przechowywanych na stacji roboczej. Musi być dostępne narzędzie, pozwalające na odszyfrowanie danych z dysku w przypadku, gdy nie da się uruchomić stacji roboczej w normalnym trybie, np. na skutek uszkodzenia systemu operacyjnego. Skorzystanie z narzędzia musi wymagać akceptacji administratora systemu, np. poprzez wygenerowanie jednorazowego kodu/hasła.
Pozostałe wymagania	Wymaga się, by produkt zaopatrzony był w funkcje zabezpieczające przed próbami ingerencji użytkowników w działanie agenta: • Odinstalowanie oprogramowania możliwe dzięki hasłu, które zna wyłącznie administrator IT • Ochrona przed użytkownikami posiadającymi uprawnienia administratora, chcącymi usunąć bądź wyłączyć oprogramowanie • Rejestrowanie wszelkich prób manipulacji przez użytkowników (łącznie z usuwaniem logów) • Wszystkie pliki logów muszą być zaszyfrowane przed nieautoryzowanym dostępem i próbą skasowania • Wszystkie połączenia między aplikacją agencką na stacji roboczej a serwerem zarządzającym muszą być zaszyfrowane przy użyciu protokołu SSL Musi istnieć możliwość czasowego wstrzymania (zawieszenia) ochrony na stacji roboczej, bez konieczności modyfikacji lub usuwania i ponownego przypisywania polityk bezpieczeństwa. Wstrzymanie ochrony musi wymagać akceptacji administratora systemu, np. przez wygenerowanie jednorazowego hasła. W czasie swojego działania agent na stacji roboczej nie może obciążać zasobów (CPU, RAM, dysk) w stopniu odczuwalnym przez użytkownika i utrudniającym normalną pracę. Dopuszczalne jest większe obciążenie stacji jedynie przy pierwszym szyfrowaniu dysku lokalnego. Powinna być możliwość zdefiniowania własnej treści komunikatów w języku polskim, wyświetlanych przez agenta na stacji roboczej. Wymagana jest możliwość instalacji agenta w trybie ukrytym, tj. bez widoczności żadnych ikonek i bez wyświetlania jakichkolwiek komunikatów na stacji roboczej. Rozwiązanie musi posiadać wbudowany mechanizm automatycznego wykonywania backupu swojej konfiguracji i zgromadzonych logów wg harmonogramu zdefiniowanego przez administratora. System musi umożliwiać całkowite odtworzenie serwera zarządzającego z takiego backupu na wypadek awarii, bez konieczności reinstalowania agentów. Proponowane rozwiązanie musi wspierać instalację na wirtualnej platformie VMware lub Hyper-V i być z nią kompatybilne. Rozwiązanie musi być uruchomione na wskazanych zasobach Zamawiającego i nie może wymagać żadnych dodatkowych zewnętrznych komponentów, np. zewnętrznych baz danych lub zewnętrznych programów szyfrujących. Rozwiązanie musi obsłużyć minimum 60 stacji roboczych. Wymaga się, aby rozwiązanie było licencjonowane w modelu licencji wieczystej z odnawianym corocznie supportem, zawierającym wsparcie techniczne producenta oraz dostęp do poprawek i nowych wersji.

	Wymaga się, aby funkcjonalność szyfrowania dysków lokalnych była licencjonowana osobno od funkcjonalności kontroli portów fizycznych i nośników zewnętrznych, pozwalając na elastyczność w doborze licencji do potrzeb. Wymaga się dostarczenia 60 licencji wieczystych ze wsparciem technicznym dla funkcjonalności kontroli portów fizycznych i nośników zewnętrznych oraz 60 licencji wieczystych ze wsparciem technicznym dla funkcjonalności szyfrowania dysków lokalnych.
Usługi	Wymaga się, aby dostawca zaoferował usługę zdalnego wdrożenia rozwiązania w infrastrukturze Zamawiającego, przeprowadzoną przez inżyniera certyfikowanego przez producenta rozwiązania, w zakresie: - instalacja i konfiguracja rozwiązania w maszynie wirtualnej na platformie Zamawiającego - szkolenie dla administratora rozwiązania - wsparcie w języku polskim w trybie 8x5 w dni robocze - kwartalny przegląd konfiguracji rozwiązania

5. Upgrade licencji UTM

Wymagania Ogólne

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. Dla wszystkich funkcji systemu musi być dostarczony dokument potwierdzony przez producenta lub autoryzwanego dytrybutora o gotowości świadczenia usług wsparcia w języku polskim oraz bezpłatnej obsługi procesu wymiany uszkodzonego urządzenia.

System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
   - 16 portami Gigabit Ethernet RJ-45.
   - 8 gniazdami SFP 1 Gbps.
   - 2 gniazdami SFP+ 10 Gbps.
2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System realizujący funkcję Firewall jest wyposażony w lokalną przestrzeń dyskową o pojemności minimum 480 GB.
5. System jest wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 11 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 2.5 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.

Funkcje Systemu Bezpieczeństwa:

W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   - Translację jeden do jeden oraz jeden do wielu.
   - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
   - Amazon Web Services (AWS).
   - Microsoft Azure.
   - Cisco ACI.
   - Google Cloud Platform (GCP).
   - OpenStack.
   - VMware NSX.
   - Kubernetes.

Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19, 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
   - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
   - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
   - Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
   - Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
   - Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
   - Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
   - Mechanizm „Split tunneling" dla połączeń Client-to-Site.
2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
   - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.

- Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Funkcje SD-WAN

1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

Zarządzanie pasmem

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
4. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
5. System dysponuje sygnaturami do ochrony przed atakami na systemy przemysłowe SCADA.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

Logowanie

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W przypadku kiedy usługa logowania i raportowania realizowana jest w chmurze, wymagane są stosowne licencje upoważniające do składowania logów przez okres co najmniej jednego roku.
3. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania, raportowania, korelacji zdarzeń, powiadamiania o incydentach) udostępnianej w chmurze lub musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
4. W przypadku kiedy usługa logowania, raportowania, korelacji zdarzeń realizowana jest w chmurze, wykonawca musi dostarczyć stosowne licencje upoważniające do składowania logów przez okres co najmniej jednego roku.
5. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
6. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
7. Możliwość włączenia logowania per reguła w polityce firewall.
8. System zapewnia możliwość logowania do serwera SYSLOG.
9. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Testy wydajnościowe oraz funkcjonalne

1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.

Serwisy i licencje

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen, Sygnatury ochrony systemów przemysłowych SCADA.

Logowanie i raportowanie w oparciu o usługę realizowaną w chmurze, z czasem retencji logów minimum na okres 24 miesięcy.

Rozszerzone wsparcie serwisowe AHB/SOS

System jest objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora.

System jest objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie:

- Wsparcie telefoniczne zespołu certyfikowanych inżynierów.
- Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu.
- Doradztwo w zakresie konfiguracji.
- Zdalne wsparcie techniczne.
- Pomoc w zakładaniu zgłoszeń serwisowych u producenta.
- Pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą).
- Przygotowanie urządzenia do zdalnej konfiguracji.
- Zdalna konfiguracja urządzenia (połączenia szyfrowane) zgodnie z wymaganiami użytkownika.
- Minimum 5 zdalnych rekonfiguracja urządzenia w związku ze zmianą środowiska lub wymagań użytkownika.
- Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich.
- Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich.

Dla zapewnienia wysokiego poziomu usług, podmiot serwisujący posiada certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Czas reakcji jest nie dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.

Wymagania powinny być potwierdzone dokumentami:

- Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
- Certyfikat ISO 9001 podmiotu serwisującego.

6. Rozbudowa Systemu Backup

OBUDOWA	Tower o wymiarach nie większych niż 170 mm x 350 mm x 250 mm (wysokość x szerokość x głębokość)
PAMIĘĆ RAM	32 GB pamięci SO-DIMM DDR4 ECC tego samego producenta co serwer.
ILOŚĆ OBSŁUGIWANYCH DYSKÓW	- Minimum 8 dysków o maksymalnej pojemności 18TB każdy, po podłączeniu modułów rozszerzających minimum 18 dysków. - Minimum 2 dyski M.2 NVMe SSD 2280
ZAINSTALOWANE DYSKI	1) 8 dysków o pojemności 8TB każdy zgodnych z listą kompatybilności oferowanego serwera oraz charakteryzujących się następującymi parametrami: - prędkość obrotowa: minimum 7200 RPM, - pamięć cache: minimum 256MB,s - gwarancja: minimum 36 miesięcy, - MTBF: minimum 2 miliony. 2) 2 dyski M.2 NVMe o pojemności 800GB każdy zgodne z listą kompatybilności oferowanego serwera oraz charakteryzujące się następującymi parametrami: - interfejs: NVMe PCIe 3.0 x4, - gwarancja: minimum 36 miesięcy, - wytrzymałość: minimum 1000TB.
INTERFEJSY SIECIOWE	Minimum 2 porty 1GbE RJ-45 Minimum 1 porty 10GbE RJ-45 Minimum 2 porty 10Gb SFP+ Wsparcie dla Link Agregation.
PORTY	Minimum 2 porty USB 3.2
WSKAŹNIKI LED	Status, HDD 1-8, zasilanie, LAN 1-3
OBSŁUGA RAID	Basic, JBOD, RAID 0, 1, 5, 6, 10, SHR wraz z obsługa dysków typu hot spare.
FUNKCJE RAID	Możliwość zwiększania pojemności i migracja między poziomami RAID online.
SZYFROWANIE	Możliwość szyfrowania wybranych udziałów sieciowych.
PROTOKOŁY	SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP, VPN (PPTP, OpenVPN™, L2TP)
USŁUGI	1. Stacja monitoringu, Windows ACL, Integracja z Windows ADS, Firewall, Serwer wydruku, Serwer WWW, Serwer plików, Manager plików przez WWW, Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie, Antywirus, Klient VPN, Usługa DDNS, Zarządzanie przez komórkę, Serwer i klient LDAP, Możliwość utworzenia kilku wolumenów w obrębie jednej macierzy RAID, migawki (min. 65 tys. w cały systemie), możliwość tworzenia i uruchamiania maszyn wirtualnych bezpośrednio w systemie bez wykorzystywania zewnętrznych wirtualizatorów. 2. Możliwość utworzenia klastra wysokiej dostępności (HA) z dwóch identycznych urządzeń pracującego minimum w trybie aktywny-pasywny. Wymagane jest, aby klaster obsługiwał w pełni automatyczne przełączanie awaryjne bez ingerencji administratora.
OBSŁUGA MIGAWEK	Liczba migawek folderu współdzielonego: minimum 1000
ZARZĄDZANIE DYSKAMI	SMART, sprawdzanie złych sektorów.
JĘZYK GUI	Polski
GWARANCJA I SERWIS	Minimum 5 lat gwarancji NBD producenta na cały zestaw złożony z serwera, dysków HDD, SSD, pamięci RAM i kart sieciowych. Dostawa sprzętu zastępczego na następny dzień roboczy w przypadku potwierdzonej awarii sprzętowej z opcją pozostawienia uszkodzonego dysku u Zgłaszającego.
WAGA	Maksymalnie 8 kg
POBÓR MOCY	Maksymalnie 100W w trybie pracy.
CERTYFIKATY	CE

SYSTEM PLIKÓW	Dyski wewnętrzne: Btrfs.
SZYFROWANIE	Mechanizm szyfrowania sprzętowego (AES-NI)
LICZBA WOLUMENÓW	Minimum 250
LICZBA ISCSI TARGETÓW	Minimum 250
LICZBA ISCSI LUN	Minimum 500
LICZBA KONT UŻYTKOWNIKÓW	Minimum 2000
LICZBA GRUP	Minimum 255
LICZBA FOLDERÓW UDOSTĘPNIONYCH	Minimum 500
ILOŚĆ JEDNOCZESNYCH POŁĄCZEŃ	Minimum 1500
ZASILACZ	Wewnętrzny zasilacz o mocy minimum 200W.

Wdrożenie w siedzibie Zamawiającego oferowanego rozwiązania wraz z pełną konfiguracją przestrzeni dyskowej i systemu operacyjnego, a także przeprowadzenie szkolenia z zakresu obsługi serwera NAS złożonego z 11 modułów. Szkolenie musi zostać przeprowadzone przez certyfikowanego inżyniera posiadającego fachową wiedzę zdobytą na autoryzowanych szkoleniach przeprowadzanych przez producenta oferowanego rozwiązania w wymiarze czasu nie mniejszym niż 30 godzin.

1. Zarządzanie przechowywaniem.

   a) Omówienie dostępnych typów RAID, ich specyfikacji, algorytmu działania, a także dobór najlepszego wariantu adekwatnie do przedstawionych wymagań. Szczegółowe omówienie tradycyjnych typów RAID takich jak RAID 1, 5, 6, 10 oraz niestandardowych SHR, SHR-2 i F1.
   b) Omówienie dostępnych systemów plików, ich specyfikacji, funkcjonalności oraz architektury, a także dobór najlepszego wariantu do przedstawionych wymagań.
   c) Omówienie specyfikacji dysków HDD i SSD kompatybilnych z posiadanym serwerem NAS pod kątem zastosowania w długoterminowym przechowywaniu danych. Objaśnienie różnic w mechanizmie zapisu na dyskach talerzowych oraz flash'owych.
   d) Wpływ kluczowych parametrów SMART na działanie dysków w macierzy.
   e) Procedura wymiany uszkodzonego dysku w grupie RAID. Rozbicie tematu na różne przypadki wraz z symulacją awarii. Wady i zalety stosowania dysków zapasowych.
   f) Dostępne opcje rozbudowy istniejącej puli pamięci oraz ograniczenia z nimi związane z podziałem na zastosowane typy RAID.
   g) Możliwości skalowalności urządzenia pod kątem zastosowania większej ilości dysków, a co za tym idzie zwiększenia pojemności istniejącej puli pamięci lub utworzenia nowej.
   h) Wybór odpowiedniego priorytetu synchronizacji grupy RAID zależenie od zastosowanych dysków i przeznaczenia serwera NAS. Analiza obciążenia systemu i wykorzystania dysków przy jednoczesnym wykorzystywaniu zasobów serwera przez stacje klienckie.
   i) Omówienie rodzajów testów SMART, ich cech charakterystycznych, przeznaczenia oraz przypadków zastosowania. Implementacja sensownego i bezpiecznego harmonogramu wykonywania testów, pełna automatyzacja poprzez dedykowane skrypty.
   j) Dostępne mechanizmy wpływające na zwiększenie szybkości odczytu i zapisu danych, wymagania związane z implementacją takiego rozwiązania, wady i zalety zależenie od rodzaju środowiska serwerowego i wykorzystywanych aplikacji. Analiza żywotności wybranych nośników, symulacja czasu pracy oraz retencji w celu utrzymania najwyższego poziomu wydajności pamięci podręcznej w danej jednostce czasu z uwzględnieniem szacunkowych ilości zapisu i odczytu danych.

k) Algorytm szyfrowania danych – praktyczne zastosowanie, wpływ na obciążenie serwera i wydajność systemu, możliwości wykorzystania szyfrowania na różnego typu zasobach. Ograniczenia związana z włączeniem szyfrowania, zagrożenia wynikające z niezastosowania takiego algorytmu.
l) Kopiowanie przy zapisie (ang. copy on write) – zasada działania na przykładzie systemu plików btrfs. Zastosowanie praktyczne, wady i zalety, ograniczenia i wymagania.

2. Użytkownicy i grupy.

a) Zarządzanie użytkownikami i grupami lokalnymi, konfiguracja strategii bezpiecznego logowania, automatyzacja procesu tworzenia nowych użytkowników i wdrażania ich do korzystania z systemu.
b) Zarządzanie użytkownikami i grupami domenowymi, podłączanie serwera NAS jako klienta domeny, a także tworzenie niezależnego kontrolera domeny opartego o natywne rozwiązanie dostępne w systemie operacyjnym serwera NAS. Pełne wdrożenie testowe z uwzględnieniem zarządzania kontrolerem domeny w sposób rozszerzony poprzez dodatek RSAT, konfigurację profili mobilnych dla użytkowników domenowych z wykorzystaniem zasobów magazynowych serwera NAS. Konfiguracja polis związanych z automatyczną instalacją wskazanych programów na systemach klienckich.
c) Omówienie zasad nadawania uprawnień użytkownikom i grupom z wyszczególnieniem podziału na uprawnienia Unix i ACL. Implementacja obu wariantów w celu wyboru najbardziej odpowiedniego do postawionych wymagań.

3. Foldery współdzielone.

a) Zasada funkcjonowania folderów współdzielonych w systemie operacyjnym. Powiązanie z systemem plików działającym na podstawie wolumenów.
b) Omówienie działania systemu plików btrfs pod kątem utrzymania integralności danych z wykorzystaniem dodatkowych sum kontrolnych.
c) Wskazanie i wyjaśnienie algorytmu wykorzystywanego do kompresji danych. Wykorzystanie praktyczne wraz z testami oszczędności zajmowanej przez pliki przestrzeni po włączeniu kompresji.
d) Szczegółowe wytłumaczenie funkcjonalności WORM (ang. Write Once Read Many) działającej na poziomie folderów współdzielonych. Przykłady wykorzystania praktycznego oraz korzyści z tego płynące.
e) Foldery domowe – zasada funkcjonowania dla użytkowników lokalnych i domenowych.
f) Metody udostępniania plików osobom z zewnątrz z zachowaniem zasad bezpieczeństwa tj. szyfrowania transferu oraz zabezpieczenia dostępu przed osobami nieuprawnionymi.

4. Ustawienia sieciowe.

a) Zasada działania więcej niż dwóch interfejsów LAN w serwerze. Wyjaśnienie domyślnej adresacji LAN oraz przykładowa konfiguracja w sieci LAN bez serwera DHCP.
b) Agregacja łączy ze szczegółowym omówieniem specyfikacji każdego dostępnego trybu dedykowanego dla przełączników bez interfejsu zarządzania oraz dla tych z interfejsem zarządzania i wsparciem dla protokołu LACP (ang. Link Aggregation Control Protocol), standard 802.3ad.
c) Statyczny routing po stronie serwera NAS, ustawienia zasad filtrowania ruchu i sterowania ruchem z podziałem na konkretne usługi i porty.
d) Konfiguracja podstawowych parametrów połączeniowych serwera NAS z siecią Internet. Wyjaśnienie zasady działania takiego połączenia w momencie korzystania z kilku interfejsów LAN. Wady i zalety zamiennego stosowania nazwy serwera do połączeń CIFS/SMB zamiast adresu IP.
e) Zasada działania serwera proxy i przykład wykorzystania w realnym środowisku.

f) Konfiguracja niestandardowych portów zarządzania. Wyszczególnienie dostępnych metod lokalnego i zdalnego zarządzania serwerem poprzez interfejs Web UI oraz linię komend.

5. Kopie zapasowe i ochrona danych.

a) Zasady bezpiecznego przechowywania danych z przykładem implementacji w omawianym środowisku.
b) Metody wykonywania kopii zapasowej z uwzględnieniem różnego typu nośników tj. dysków USB, obudów RAID, bibliotek LTO, innych serwerów fizycznych oraz serwerów NAS.
c) Szczegółowe omówienie metod replikacji danych na inny serwer NAS tego samego producent oraz porównanie procesu do replikacji na inne rozwiązanie firmy trzeciej. Wskazanie najlepszej dostępnej metody do wykorzystania w sieci LAN oraz poprzez WAN.
d) Wyjaśnienie zasady działania mechanizmy migawek z wykorzystaniem kopiowania przy zapisie. Przedstawienie możliwości implementacji harmonogramu wykonywania migawek w systemie oraz związanych z tym najlepszych praktyk. Analiza potencjalnego wykorzystania przestrzeni przez migawki w długoterminowym procesie ich przechowywania oraz omówienie dostępnych strategii retencji wersji.
e) Metody odzyskiwania danych z migawek z opcją przywracania lokalnego oraz zdalnego. Wyjaśnienie różnic i cech szczególnych obu metod.
f) Utworzenie i przedstawienie w praktyce zasady działania replikacji migawek z uwzględnieniem przełączania awaryjnego między serwerami. Szczególnie w przypadku podłączenia do kontrolera domeny i odtwarzania danych wraz z uprawnieniami na serwerze docelowym.
g) Przedstawienie sposobów wykonywania kopii zapasowych do środowisk chmurowych.

6. Klaster wysokiej dostępności.

a) Omówienie wymagań dotyczących utworzenia klastra wysokiej dostępności z dwóch takich samych serwerów NAS.
b) Omówienie wymagań i ograniczeń dotyczących utworzenia klastra wysokiej dostępności z dwóch różnych serwerów NAS.
c) Zasada działania klastra SHA (ang. Synology High Availability). Wady I zalety oraz korzyści płynące z zastosowania rozwiązania klastrowego jako główne miejsce składowania danych i różnego typu usług.
d) Algorytm przełączania awaryjnego serwerów w klastrze. Jakie wymagania musi spełniać połączenie między serwerami, jakie ograniczenia występują, jakie problemy mogą wystąpić oraz jak w praktyce odczuwalna będzie praca na zasobach klastra SHA.

7. Kopie zapasowe komputerów, serwerów i maszyn wirtualnych.

a) Omówienie dostępnych metod wykonywania kopii zapasowych komputerów PC z zaprezentowaniem działania w praktyce z podziałem na kopie plikowe oraz bare-metal.
b) Opracowanie systemu wdrażania odpowiedniego rozwiązania do kopii zapasowej na dużą skalę.
c) Metody przywracania danych dostępne dla zwykłych użytkowników oraz administratorów. Praktyczne zastosowanie oraz instruktarz dotyczący każdej z dostępnych metod na przykładzie komputera z systemem Windows oraz Linux.
d) Możliwości masowego konfigurowania zasad tworzenia kopii zapasowych.
e) Wyjaśnienie i zaprezentowanie realnego wpływy szyfrowania i kompresji transferu danych na komputery lokalne.

f) Strategie przechowywania danych kopii zapasowych w planie długoterminowym z możliwością przywrócenia kopii zapasowej sprzed 6, 12, i 18 miesięcy.
g) Kontrola integralności danych kopii zapasowych i testowe odtwarzanie.
h) Możliwości automatyzacji procesu odtwarzania danych w przypadku awarii komputera.
i) Testowe przywracanie obrazu kopii w formie maszyny wirtualnej w natywnym wirtualizatorze dostępnym na serwerze NAS oraz na zewnętrznych wirtualizatorach.
j) Omówienie różnic w działaniu środowisk wirtualizacji opartych o KVM oraz QEMU.
k) Wyjaśnienie mechanizmów wpływających na redukcję zajmowanej przez kopie zapasowe przestrzeni takich jak deduplikacja i kompresja. Wykazanie algorytmu działania oraz wpływu na żywotność dysków.
l) Przedstawienie metody replikacji centralnego repozytorium kopii zapasowych na zapasowy serwer NAS z opcją przełączenia klientów na tę jednostkę i wznowienia harmonogramów kopii zapasowych.
m) Metody wykonywania kopii zapasowych systemów bazodanowych działających na serwerach fizycznych z systemami operacyjnymi z rodziny Windows oraz Linux oraz adekwatne metody przywracania.
n) Wykonywanie kopii zapasowych maszyn wirtualnych z różnych środowisk wirtualizacji obsługiwanych przez zintegrowane narzędzie dostępne w systemie serwera NAS. Wyjaśnienie zasady działania mechanizmu kopii, opcji przywracania natychmiastowego oraz pełnego.

8. Serwer poczty.

a) Omówienie dostępnych pakietów pozwalających na uruchomienie serwera pocztowego. Jakie są kluczowe różnice, plan licencjonowania, wady i zalety.
b) Wytypowanie odpowiedniego pakietu pozwalającego na utworzenie serwera pocztowego i na jego przykładzie zaprezentowanie praktycznego działania.
c) Wymagania dotyczące utworzenia serwera.
d) Wyjaśnienie zarządzania domeną oraz rekordami DNS.
e) Przekierowywanie portów wymaganych do działania usług na serwerze NAS. Niebezpieczeństwo płynące z tego typu praktyk.
f) Pełnoprawne uruchomienie serwera pocztowego po przeprowadzonej konfiguracji. Testy działania usług SMTP, IMAP i POP3.
g) Obsługa kont pocztowych za pomocą natywnego klienta oraz oprogramowania firm trzecich.
h) Monitorowanie stanu serwera pocztowego, potencjalnych zagrożeń, filtrowanie poczty oraz włączanie silników antyspamowych.
i) Praktyczne zaprezentowanie procedury migracji danych z istniejącego serwera pocztowego na nowe rozwiązanie zaimplementowane na serwerze NAS.

9. System monitoringu.

a) Omówienie wymagań związanych z wdrożeniem systemu monitoringu opartego o serwer NAS z centralnym zarządzaniem podległymi serwerami nagrywającymi.
b) Prezentacja funkcjonalności i zarządzania takim systemem w praktyce z wykorzystaniem co najmniej dwóch różnego typu kamer IP. Minimum jedna standardowa i jedna sterowana (ang. PTZ).
c) Konfiguracja przestrzeni przechowywania nagrań. Najlepsza dopuszczalna strategia retencji.
d) Analiza wydajności zapisu z wykorzystaniem systemów plików ext4 i btrfs. Wybór odpowiedniego rozwiązania pod kątem najlepszych osiągów.

e) Dodawanie różnego typu kamer do systemu monitoringu – kompatybilnych oraz z wykorzystaniem protokołu ogólnego ONVIF.
f) Przetestowanie działania wykrywania ruchu i innych podobnych funkcjonalności na poziomie zarządzania kamery oraz systemu monitoringu.
g) Automatyzacja dotycząca powiadamiania o zaistniałych zdarzeniach wykrytych przez system monitoringu.
h) Sposoby na redukcję przestrzeni zajmowanej przez nagrania, archiwizacja oraz tworzenie tzw. timelapse'ów.

10. Zarządzanie systemem.

a) Zarządzanie serwerem NAS i systemem operacyjnym pracującym na nim poprzez centralny system zarządzania, a także aplikacje mobilne. Wyszczególnienie ograniczeń i wymagań dotyczących każdej metody.
b) Zabezpieczenie serwera poprzez wdrożenie zasada automatycznego blokowania adresów IP, białej oraz czarnej listy, filtrowania ruchu przychodzącego.
c) Wdrożenie uwierzytelniania dwuskładnikowego dla użytkowników posiadających zdalny dostęp do zarządzania serwerem.
d) Konfiguracja systemu powiadomień wykorzystującego dedykowany serwer SMTP lub pośredniczące konto e-mail.
e) Przedstawienie dostępnych narzędzi monitorowania stanu różnego typu urządzeń, które udostępniają stan poszczególnych parametrów i ustawień poprzez protokół SNMP.
f) Omówienie zasad oraz metod wykonywania aktualizacji oprogramowania serwera NAS w przypadku pojedynczego serwera oraz klastra wysokiej dostępności.
g) Automatyzacja procesu wykonywania kopii zapasowej podstawowej konfiguracji systemu. Objaśnienie co dokładnie zawiera ta kopia, w jaki sposób można ją przywrócić i jakie są ograniczenia z tym związane.

11. Sprzęt i konserwacja.

a) Szczegółowe omówienie specyfikacji sprzętowej oferowanego serwera NAS oraz możliwości jego rozbudowy.
b) Przedstawienie instrukcji wymiany pamięci RAM oraz montowania dodatkowych kart rozszerzeń.
c) Omówienie procesu wymiany podzespołów podczas pracy takich jak dyski HDD.
d) Przedstawienie schematu działania w przypadku wystąpienia problemów z połączeniem do systemu zarządzania serwerem NAS lub w przypadku zatrzymania działania niektórych usług.
e) Symulacja różnych typów awarii, które mogą wystąpić podczas użytkowania serwera i sposobów szybkiego rozwiązywania powstałych problemów.
f) Instruktarz dotyczący bezpiecznego czyszczenia serwera NAS z wymontowaniem niektórych podzespołów.