

Załącznik nr 1 do SWZ

Opis Przedmiotu Zamówienia (OPZ)

- dokumentacja SZBI
- infrastruktura sprzętowa
- oprogramowanie z wdrożeniem
- szkolenia



Spis treści

I.	WSTĘP.....	3
II.	WYMAGANIA OGÓLNE.....	4
	RÓWNOWAŻNOŚĆ OFEROWANYCH ROZWIĄZAŃ.....	4
	w zakresie oprogramowania	4
	w zakresie Infrastruktury sprzętowej.....	5
III.	CZĘŚĆ I – DOKUMENTACJA SZBI.....	6
	dokumentacja SZBI (System Zarządzania Bezpieczeństwem Informacji)	6
IV.	CZĘŚĆ II – INFRASTRUKTURA SPRZĘTOWA I OPROGRAMOWANIE WRAZ Z PAKIETEM SZKOLENIOWYM.....	12
1.	UTM (Unified Threat Management) – typ I.....	12
2.	UTM (Unified Threat Management) – typ II.....	20
3.	Zarządzalne urządzenie sieciowe.....	28
4.	Zarządzalne urządzenie sieciowe – typ II.....	30
5.	Zasilacz awaryjny UPS	32
6.	Oprogramowanie typu XDR Extended Detection and Response	34
7.	Oprogramowanie SIEM (Security Information and Event Management).....	56
8.	Usługa backupu w chmurze.....	85
9.	Elementy serwera plików – dyski.....	88
10.	Oprogramowanie menadżer haseł	89
11.	Serwerowy system operacyjny	96
12.	Serwerowy system operacyjny	100
13.	Szkolenia dla działu IT i dla pracowników spoza działu IT	104



I. WSTĘP

Załącznik określa minimalne wymagania dla opracowania i wdrożenia dokumentacji, dostawy/wdrożenia/uruchomienia oprogramowania oraz infrastruktury sprzętowej dla Gminy Kolsko realizowanego w ramach projektu grantowego pn. „Cyberbezpieczny Samorząd” Fundusze Europejskie na Rozwój Cyfrowy 2021-2027, Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa.

Celem projektu jest wsparcie JST w zakresie realizacji usług publicznych na drodze teleinformatycznej, poprzez zwiększenie cyfryzacji jednostek samorządu terytorialnego wraz z jednostkami podległymi (z ograniczeniem do jednostek sektora publicznego, z wyłączeniem placówek ochrony zdrowia) w kontekście zwiększenia poziomu cyberbezpieczeństwa.

II. WYMAGANIA OGÓLNE

RÓWNOWAŻNOŚĆ OFEROWANYCH ROZWIĄZAŃ

w zakresie oprogramowania

W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega znacząco od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym, przy czym nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób, za rozwiązanie równoważne nie można uznać rozwiązania identycznego (tożsamego), a jedynie takie, które w porównywanych cechach wykazuje dokładnie tą samą lub bardzo zbliżoną wartość użytkową. Przez bardzo zbliżoną wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic nie wpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są dedykowane. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów, czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego. Dostarczenie przez Wykonawcę rozwiązania równoważnego musi być zrealizowane w taki sposób, aby wymiana oprogramowania na równoważne nie zakłóciła bieżącej pracy Zamawiającego. W tym celu Wykonawca musi do oprogramowania równoważnego przenieść wszystkie dane niezbędne do prawidłowego działania nowych systemów, przeszkolić użytkowników, skonfigurować oprogramowanie, zapewnić gwarancję i serwis, uwzględnić niezbędną asystę ze strony pracowników Wykonawcy w operacji uruchamiania oprogramowania w środowisku produkcyjnym itp.

Mając na uwadze powyższe, w przypadku jeżeli Wykonawcy nie mają możliwości uzyskania odpowiedniego do realizacji dostępu do oprogramowania firm trzecich, w celu zapewnienia zasady konkurencyjności, przejrzystości, jawności a także równego traktowania wykonawców w trakcie prowadzenia postępowania, Zamawiający dopuszcza każdorazowo wymianę Oprogramowania u Zamawiającego pod warunkiem, że:

- a) Rozwiązania zastępujące dotychczas funkcjonujące u Zamawiającego systemy Wykonawca dostarcza i wdraża na swój koszt z zachowaniem warunków licencjonowania wskazanych w niniejszym dokumencie.
- b) Wykonawca przeprowadzi migrację danych w zakresie wskazanym przez Zamawiającego na swój koszt, w sposób opisany w niniejszym OPZ a migracja musi objąć pełny zakres danych bieżących i archiwalnych.



- c) Wykonawca przeprowadzi instruktaże stanowiskowe, zapewni gwarancje i serwis gwarancyjny a także helpdesk oraz będzie świadczył asystę techniczną w zakresie umożliwiającym pracownikom Zamawiającego płynną obsługę oprogramowania.
- d) Wymiana oprogramowania nie może zakłócić bieżącej pracy Zamawiającego oraz musi zapewnić ciągłość pracy wynikającą z obowiązujących terminów, przepisów prawa i stosowanych procedur.
- e) Wszelkie uzgodnienia i konsultacje w zakresie transmisji danych powinny być dokonane w siedzibie Zamawiającego na podstawie zatwierdzonego harmonogramu.
- f) Proces migracji musi objąć pełne dane zawarte we wcześniej użytkowanym systemie.
- g) Nowe rozwiązania muszą realizować wszystkie wymienione wymagania względem oprogramowania.

w zakresie Infrastruktury sprzętowej

W przypadkach, kiedy w opisie przedmiotu zamówienia wskazane zostały znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę co prowadziłoby do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń i jest to uzasadnione specyfiką przedmiotu zamówienia. W takich sytuacjach ewentualne wskazania na znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, należy odczytywać z wyrazami „lub równoważne”.

W sytuacjach, kiedy Zamawiający opisuje przedmiot zamówienia poprzez odniesienie się do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 i ust. 3 ustawy z dnia 11 września 2019 r Prawo zamówień publicznych (Dz.U.2024.1320 t.j.) dalej Pzp, Zamawiający dopuszcza rozwiązania równoważne opisywanym, a wskazane powyżej odniesienia należy odczytywać z wyrazami „lub równoważne”.

Pod pojęciem rozwiązań równoważnych Zamawiający rozumie taki sprzęt, który posiada parametry techniczne i/lub funkcjonalne co najmniej równe do określonych w OPZ. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy lub usługi spełniają wymagania określone przez Zamawiającego.

O ile inaczej nie zaznaczono, wszelkie zapisy OPZ zawierające parametry techniczne należy odczytywać jako parametry minimalne, np. zapis: “Zainstalowane dwa procesory 8-rdzeniowe klasy x86, min. 3.2GHz, dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 143 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej” należy rozumieć jako:

“Zainstalowane co najmniej dwa procesory, posiadające co najmniej 8 rdzeni, klasy co najmniej x86, posiadające taktowanie co najmniej 3.2GHz, umożliwiające osiągnięcie wyniku co najmniej 143 w teście SPACrate2017_int_base, dla oferowanego serwera, dostępnym na stronie www.spec.org w konfiguracji dwuprocesorowej”.

III. CZĘŚĆ I – DOKUMENTACJA SZBI

dokumentacja SZBI (System Zarządzania Bezpieczeństwem Informacji)

W ramach realizowanego przedmiotu zamówienia Wykonawca jest zobowiązany do:

1. Wykonania analizy dokumentacji związanej z bezpieczeństwem informacji obowiązującej u Zamawiającego, która pozwoli na określenie potrzeb związanych z koniecznością dostosowania dokumentacji do wymagań nowelizowanej ustawy o krajowym systemie cyberbezpieczeństwa oraz norm ISO 27000 w zakresie bezpieczeństwa informacji (w szczególności zgodnego z wymaganiami aktualnych norm PN-EN ISO/IEC 27001 oraz zaleceniami aktualnych norm PN-ISO/IEC 27002, PN-ISO-27005) i ISO 31000 w zakresie zarządzania ryzykiem oraz zapewnienia zarządzania ciągłością działania w nawiązaniu do normy PN-EN ISO 22301 wraz z przedstawieniem zaleceń w zakresie aktualizacji dokumentacji i potrzeby jej uzupełnienia w ramach systemu zarządzania bezpieczeństwem informacji.
2. Opracowania i wdrożenia dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji.
3. Powyższe czynności Wykonawca zobowiązany jest wykonać dla Urzędu Gminy w Niegostawicach.

Szczegółowy opis realizowanych w ramach zamówienia czynności związanych z wykonaniem analizy dokumentacji związanej z bezpieczeństwem informacji obowiązującej u Zamawiającego, która pozwoli na określenie potrzeb związanych z koniecznością dostosowania dokumentacji (punkt numer 1):

1. W ramach wykonywanych prac Wykonawca przeprowadzi kompleksową weryfikację dokumentacji posiadanej przez Zamawiającego w celu stwierdzenia zasadności pozostawienia wybranych elementów dokumentacji i wykonania ich aktualizacji.
2. W ramach wykonanej weryfikacji Wykonawca sporządzi raport dokumentujący rezultaty wykonanej analizy, który będzie zawierał porównanie obecnie posiadanej dokumentacji przez Zamawiającego z oczekiwaniami sformułowanymi w ramach zamówienia.
3. Wykonawca w ramach realizacji procesu przeprowadzi kompleksową analizę aktywów posiadanych przez Zamawiającego, które przedstawi do zatwierdzenia Zamawiającemu w raporcie. Aktywa staną się podstawą opracowywania dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji.
4. Wykonawca opracuje raport podsumowujący rezultaty przeprowadzonej analizy oraz zalecenia w zakresie aktualizacji dokumentacji i potrzeby jej uzupełnienia w ramach systemu zarządzania bezpieczeństwem informacji. zgodnie z wymaganiami określonymi w ramach punktu 1 niniejszego zamówienia, który będzie miał formę pisemną oraz odwoływał się do wybranych punktów norm.

Szczegółowy opis realizowanych w ramach zamówienia czynności związanych z wdrożeniem dokumentacji systemu zarządzania bezpieczeństwem informacji (punkt numer 2):

1. W ramach wykonywanych prac Wykonawca zapewni zgodność dokumentacji z wymaganiami nakładanymi przez poniższe akty prawne:
 - a) rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany

- informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych;
- b) ustawa z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa wraz z nowelizacjami ustawy, które zostaną dokonane w czasie realizacji zamówienia;
 - c) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
 - d) wymagania norm ISO 27001, a w szczególności PN-EN ISO/IEC 27001, PN-ISO/IEC 27002, PN-ISO-27005 i w oparciu o główne założenia norm ISO 31000 w zakresie zarządzania ryzykiem oraz PN-EN ISO 22301 w zakresie ciągłości działania;
 - e) wymagania regulaminu konkursu grantowego oraz umowy o powierzenie grantu zawartej w ramach projektu „Cyberbezpieczny Samorząd”.
2. Wdrażany System Zarządzania Bezpieczeństwem Informacji powinien składać się z następujących procedur szczegółowych:
- a) Procedura zarządzania aktywami,
 - b) Procedura zarządzania ryzykiem,
 - c) Procedura zapewnienia bezpieczeństwa systemów informatycznych oraz ich rozwoju,
 - d) Procedura zapewnienia bezpieczeństwa fizycznego,
 - e) Procedura kontroli dostępu do oprogramowania i infrastruktury sieciowej,
 - f) Procedura klasyfikacji informacji oraz nadzoru nad dokumentacją,
 - g) Procedura bezpieczeństwa zasobów ludzkich,
 - h) Procedura wykonywania kopii zapasowych,
 - i) Procedura stosowania kryptografii,
 - j) Procedura obsługi incydentów i realizacji działań korygujących,,
 - k) Procedura prowadzenia wewnętrznych audytów bezpieczeństwa,
 - l) Procedura prowadzenia przeglądów zarządzania,
 - m) Procedura ciągłości działania i przywracania normalnej działalności po wystąpieniu zakłóceń,
 - n) Procedura zapewnienia bezpieczeństwa łańcucha dostaw,
 - o) Procedura postępowania z podatnościami systemów i sieci,
 - p) Deklaracja stosowania (w oparciu o załącznik A do normy ISO/IEC 27001:2022).
3. W ramach opracowania i wdrożenia dokumentacji SZBI wykonawca zobowiązany jest przygotować komplet polityk, procedur i instrukcji, które odnoszą się do wszystkich zabezpieczeń (controls) określonych w Załączniku A normy ISO/IEC 27001:2022, w tym:
- wskazują odpowiedzialności i role za wdrożenie każdego zabezpieczenia,
 - definiują sposób monitorowania oraz kryteria oceny skuteczności,
 - określają wymagane zapisy/dowody pozwalające potwierdzić zgodność.
- Wdrożenie (techniczne) samych zabezpieczeń pozostaje w gestii Zamawiającego.
- a) Zabezpieczenia organizacyjne
 - i. Polityki bezpieczeństwa informacji
 - ii. Role i obowiązki w zakresie bezpieczeństwa informacji
 - iii. Rozdzielenie obowiązków

- iv. Odpowiedzialność kierownictwa
- v. Kontakty z organami władzy
- vi. Kontakty z grupami zainteresowanych specjalistów
- vii. Informacja o zagrożeniach
- viii. Bezpieczeństwo informacji w zarządzaniu projektami
- ix. Inwentaryzacja informacji i innych powiązanych aktywów
- x. Akceptowalne użycie informacji i innych powiązanych aktywów
- xi. Zwrot aktywów
- xii. Klasyfikacja informacji
- xiii. Oznaczanie informacji
- xiv. Przesyłanie informacji
- xv. Kontrola dostępu
- xvi. Zarządzanie tożsamością (prawami dostępu)
- xvii. Informacje uwierzytelniające
- xviii. Prawa dostępu
- xix. Bezpieczeństwo informacji w relacjach z dostawcami
- xx. Uwzględnienie bezpieczeństwa informacji w umowach z dostawcami
- xxi. Zarządzanie bezpieczeństwem informacji w łańcuchu dostaw technologii informacyjno- komunikacyjnych (ICT)
- xxii. Monitorowanie, przegląd i zarządzanie zmianą usług świadczonych przez dostawców
- xxiii. Bezpieczeństwo informacji w usłudze chmury
- xxiv. Planowanie i przygotowywanie się do zarządzania incydentami bezpieczeństwa informacji
- xxv. Ocena i podejmowanie decyzji w sprawie zdarzeń związanych z bezpieczeństwem informacji
- xxvi. Reagowanie na incydenty bezpieczeństwa informacji
- xxvii. Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji
- xxviii. Gromadzenie materiałów dowodowych
- xxix. Bezpieczeństwo informacji podczas zakłóceń
- xxx. Gotowość teleinformatyczna do zapewnienia ciągłości działania
- xxxi. Wymogi prawne, ustawowe, regulacyjne i umowne
- xxxii. Prawa własności intelektualnej
- xxxiii. Ochrona zapisów
- xxxiv. Prywatność i ochrona danych osobowych (PII)
- xxxv. Niezależny przegląd bezpieczeństwa informacji
- xxxvi. Zgodność z politykami, zasadami i standardami bezpieczeństwa informacji
- xxxvii. Dokumentowanie procedur operacyjnych

b) Zabezpieczenia związane z ludźmi

- i. Postępowanie sprawdzające
- ii. Warunki zatrudnienia

- iii. Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji
- iv. Postępowania dyscyplinarne
- v. Zakończenie zatrudnienia lub zmiana zakresu obowiązków
- vi. Umowy o zachowaniu poufności
- vii. Praca zdalna
- viii. Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji

c) Zabezpieczenia fizyczne

- i. Fizyczna granica obszaru bezpiecznego
- ii. Zabezpieczenie fizycznych wejść
- iii. Zabezpieczenie biur, pomieszczeń i obiektów
- iv. Monitorowanie bezpieczeństwa fizycznego
- v. Ochrona przed zagrożeniami fizycznymi i środowiskowymi
- vi. Praca w obszarach bezpiecznych
- vii. Polityka czystego biurka i czystego ekranu
- viii. Lokalizacja i ochrona sprzętu
- ix. Bezpieczeństwo sprzętu i aktywów poza siedzibą
- x. Zarządzanie nośnikami danych
- xi. Systemy wspomagające
- xii. Bezpieczeństwo okablowania
- xiii. Konserwacja sprzętu
- xiv. Bezpieczne zbywanie lub przekazywanie do ponownego użycia

d) Zabezpieczenia technologiczne

- i. Urządzenia końcowe użytkowników
- ii. Uprzywilejowane prawa dostępu
- iii. Ograniczenie dostępu do informacji
- iv. Dostęp do kodów źródłowych
- v. Bezpieczne uwierzytelnienie
- vi. Zarządzanie pojemnością
- vii. Zabezpieczenie przed szkodliwym oprogramowaniem
- viii. Zarządzanie podatnościami technicznymi
- ix. Zarządzanie konfiguracją
- x. Usuwanie informacji
- xi. Maskowanie danych
- xii. Zapobieganie wyciekom danych
- xiii. Zapasowe kopie bezpieczeństwa
- xiv. Redundancja środków przetwarzania informacji
- xv. Rejestrowanie działań
- xvi. Działania monitorujące
- xvii. Synchronizacja zegarów
- xviii. Użycie uprzywilejowanych programów narzędziowych
- xix. Instalacja oprogramowania w systemach operacyjnych

- xx. Zabezpieczenia sieci
 - xxi. Bezpieczeństwo usług sieciowych
 - xxii. Rozdzielenie sieci
 - xxiii. Filtrowanie stron internetowych
 - xxiv. Użycie kryptografii
 - xxv. Bezpieczeństwo prac rozwojowych
 - xxvi. Wymagania bezpieczeństwa aplikacji
 - xxvii. Zasady projektowania bezpiecznych systemów
 - xxviii. Bezpieczne programowanie
 - xxix. Testowanie bezpieczeństwa w fazie rozwoju i akceptacja
 - xxx. Outsourcing prac rozwojowych
 - xxxi. Rozdzielenie środowisk deweloperskich, testowych i produkcyjnych
 - xxxii. Zarządzanie zmianami
 - xxxiii. Ochrona danych testowych
 - xxxiv. Ochrona systemów informatycznych podczas testów audytowych
4. W ramach wdrażanej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji uregulowane zostaną następujące obszary, które w ramach odrębnych dokumentów zostaną dostosowane do potrzeb osób o szczególnych potrzebach, zgodnie z wymogami ustawy z dnia 19 lipca 2019 r. o zapewnianiu dostępności osobom ze szczególnymi potrzebami:
- a) dokumentacja nadawania uprawnień użytkownikom systemów informatycznych należących do Zamawiającego oraz w systemach informatycznych niepodlegających nadzorowi ze strony Zamawiającego (np. ZUS, systemy bankowe),
 - b) zasady nadawania uprawnień uprzywilejowanych (np. administratora systemów),
 - c) zasady użytkowania zewnętrznych nośników informacji,
 - d) zasady użytkowania komputerów mobilnych,
 - e) zasady wykonywania pracy zdalnej przez pracowników Zamawiającego,
 - f) zasady nawiązywania połączeń zdalnych.
5. W toku wdrażania dokumentacji nie mogą zostać przekazane Zamawiającemu puste druki (wzorce) dokumentów, jednakże ich wdrożenie powinno opierać się na wypełnieniu wdrażanej dokumentacji zgodnie ze stanem przypadającym na okres wdrożenia. Zamawiający deklaruje przekazywanie niezbędnych danych Wykonawcy, jednakże Wykonawca powinien odpowiednio wdrożyć zapisy do dokumentów przekazywanych Zamawiającemu.
6. Zamawiający wymaga, żeby zapisy dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji odnosiły się do wymagań norm ISO 27001, a w szczególności PN-EN ISO/IEC 27001, PN-ISO/IEC 27002, PN-ISO-27005. Dokumentacja powinna być przygotowana w oparciu o wytyczne wynikające z norm ISO 31000 w zakresie zarządzania ryzykiem oraz zarządzania ciągłością działania PN-EN ISO 22301. Zamawiający dokona weryfikacji zgodności na etapie odbioru dokumentacji. W przypadku wykrycia niezgodności Wykonawca będzie zobowiązany do wprowadzenia poprawek zgodnych z wolą Zamawiającego, przy czym wprowadzane poprawki będą realizowane w ramach zawartej umowy, bez dodatkowego wynagrodzenia.

7. Zamawiający wymaga, aby Wykonawca po przekazaniu dokumentów przeprowadził szkolenie pracowników z zakresu stosowania dokumentacji, przy czym w ramach prowadzonych szkoleń powinna zostać określona rola osób zaangażowanych w proces zarządzania dokumentami oraz szkolenie powinno w sposób przystępny prezentować zadania poszczególnych osób zaangażowanych w realizację zadań w ramach wdrożonej dokumentacji, w szczególności w obszarze analizy ryzyka, ciągłości działania, zarządzania systemami informatycznymi oraz ochroną danych osobowych. Szkolenie musi zostać zrealizowane stacjonarnie w min. 3 grupach w taki sposób aby nie paraliżować bieżącej pracy Zamawiającego. Wykonawca zobowiązany jest do przedstawienia pracownikom w siedzibie Zamawiającego sposobu posługiwania się dokumentacją oraz dbałości o jej aktualizację i bieżące zarządzanie dokumentami.
8. Wykonawca w ramach realizacji umowy zapewni przez cały okres realizacji umowy wsparcie Pełnomocnika ds. SZBI, który będzie dostępny na żądanie pracowników Zamawiającego w zakresie prawidłowego wykorzystywania dokumentacji systemu zarządzania bezpieczeństwem informacji. Możliwość wsparcia Pełnomocnika ds. SZBI powinna zostać zapewniona w ciągu 5 dni roboczych od zgłoszenia potrzeby pracowników Zamawiającego.
9. W związku z koniecznością zapewnienia wysokiej jakości oraz adekwatności opracowywanych dokumentów do specyfiki działalności Urzędu, wszelkie prace związane z opracowaniem systemu zarządzania bezpieczeństwem informacji (SZBI) będą realizowane na miejscu, w siedzibie Zamawiającego oraz jego jednostek podległych. Przeprowadzenie analiz, konsultacji oraz wszelkich niezbędnych prac w celu uzyskania informacji wymaga bezpośredniego kontaktu z pracownikami Urzędu oraz dostępem do środowiska pracy, co umożliwi dokładniejsze zrozumienie procesów i procedur funkcjonujących w Urzędzie. Taki sposób realizacji projektu ma na celu zapewnienie możliwości natychmiastowej reakcji na wszelkie pytania oraz wątpliwości, a także umożliwi efektywniejsze szkolenie pracowników. W związku z powyższym, nie przewiduje się realizacji prac zdalnych poprzez ankiety czy inne narzędzia zdalnego kontaktu.



IV. CZĘŚĆ II – INFRASTRUKTURA SPRZĘTOWA I OPROGRAMOWANIE WRAZ Z PAKIETEM SZKOLENIOWYM

1. UTM (Unified Threat Management) – typ I

Nazwa	Minimalne wymagania sprzętu
Typ	UTM (Unified Threat Management)
Obsługa sieci	<p>Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP</p>
Zapora korporacyjna (Firewall)	<p>Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.</p> <p>Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.</p> <p>Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).</p> <p>Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.</p> <p>Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.</p> <p>Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.</p> <p>Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.</p> <p>Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.</p> <p>Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.</p> <p>Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).</p> <p>System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.</p>
Intrusion Prevntion System (IPS)	<p>System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.</p> <p>Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.</p>

	<p>Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.</p> <p>Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.</p> <p>Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS.</p> <p>Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.</p> <p>Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.</p> <p>Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV).</p> <p>Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.</p>
Kształtowanie Pasma (Traffic Shapping)	<p>Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.</p> <p>Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.</p> <p>Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).</p> <p>Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.</p>
Ochrona antywirusowa	<p>Urządzenie ma być dostarczone wraz z komercyjnym, zaawansowanym skanerem antywirusowym oraz umożliwiać skanowanie plików w oparciu o sandboxing zlokalizowany w Internecie na serwerach producenta i na terenie Unii Europejskiej. Nie dopuszcza się aby analiza sandboxingu była przeprowadzana na urządzeniu lub wymagała instalacji dodatkowego urządzenia lub oprogramowania. Nie dopuszcza się również żeby analiza sandboxingu była przeprowadzana przez firmy trzecie.</p> <p>Skaner antywirusowy ma pochodzić od europejskiego producenta.</p> <p>Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.</p> <p>Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.</p>
Ochrona Antyspam	<p>Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).</p> <p>Ochrona antyspam ma działać w oparciu o:</p> <ol style="list-style-type: none"> białe/czarne listy, DNS RBL,

	<p>c. Skaner heurystyczny.</p> <p>W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.</p> <p>Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.</p>
Wirtualne sieci prywatne (VPN)	<p>Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).</p> <p>Urządzenie ma wspierać co najmniej następujące typy sieci VPN:</p> <ol style="list-style-type: none"> PPTP VPN, IPSec VPN, SSL VPN. <p>SSL VPN ma działać co najmniej w trybach tunelu i portalu.</p> <p>Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.</p> <p>Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal).</p> <p>Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).</p> <p>Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf.</p> <p>Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.</p>
Filtr dostępu do stron www	<p>Urządzenie ma posiadać wbudowany filtr URL.</p> <p>Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.</p> <p>Administrator ma mieć możliwość dodawania własnych kategorii URL.</p> <p>Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii.</p> <p>Do wyboru ma być przynajmniej:</p> <ol style="list-style-type: none"> blokowanie dostępu do adresu URL, zezwolenie na dostęp do adresu URL, blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora. <p>Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.</p> <p>Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.</p> <p>Filtr URL musi uwzględniać komunikację po protokole HTTPS.</p> <p>Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.</p> <p>Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.</p> <p>Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch.</p>
Uwierzytelnianie	<p>Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:</p> <ol style="list-style-type: none"> lokalną bazę użytkowników (wewnętrzny LDAP), zewnętrzną bazę użytkowników (zewnętrzny LDAP),



	<p>c. usługę katalogową Microsoft Active Directory.</p> <p>Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.</p> <p>Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły:</p> <ul style="list-style-type: none"> a. SSL, b. Radius, c. Kerberos. <p>Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.</p> <p>Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.</p> <p>Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.</p> <p>Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS).</p> <p>Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).</p> <p>Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.</p>
Administracja łączami do Internetu (IPS)	<p>Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).</p> <p>Mechanizm równoważenia obciążenia łączy internetowego ma działać w oparciu o następujące dwa mechanizmy:</p> <ul style="list-style-type: none"> a. równoważenie względem adresu źródłowego, b. równoważenie względem połączenia. <p>Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.</p> <p>Urządzenie ma umożliwiać przełączenie na łącznie zapasowe w przypadku awarii łączy podstawowego (tzw. Failover).</p> <p>Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łączy.</p> <p>W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnień, jitter, wskaźnika utraty pakietów).</p> <p>Monitorowanie dostępności łączy musi być możliwe w oparciu o ICMP oraz TCP.</p>
Routing (Trasowanie)	<p>Urządzenie ma umożliwiać statyczne trasowanie pakietów.</p> <p>Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącznie zapasowe w przypadku awarii łączy podstawowego.</p> <p>Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).</p>

**Administracja
urządzeniem**

Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.

Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.

Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.

Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.

Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.

Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.

Urządzenie ma umożliwiać zarządzanie z poziomu konsoli (SSH).

Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.

Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.

Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.

Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.

Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.

Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording).

System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).

Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.

Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).

Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.

Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:

- a. manualnego eksportu do pliku w dowolnym momencie czasu,
 - b. automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu.
-

	<p>Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.</p> <p>Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.</p> <p>Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.</p>
Raportowanie	<p>Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.</p> <p>System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.</p> <p>System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.</p> <p>System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.</p> <p>System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.</p> <p>System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.</p> <p>Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.</p> <p>Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.</p> <p>Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).</p>
Pozostałe usługi i funkcje	<p>Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.</p> <p>Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).</p> <p>Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.</p> <p>Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsiaci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny).</p> <p>Urządzenie ma posiadać usługę DNS Proxy.</p> <p>Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.</p> <p>Urządzenie musi mieć zaimplementowane Open API.</p> <p>Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.</p> <p>Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.</p>

Gwarancja i serwis	<p>Urządzenie musi być objęte gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa do dnia minimum 30.06.2026r.</p> <p>W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.</p>
Parametry sprzętowe	<p>Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.</p> <p>Urządzenie ma być wyposażone w zintegrowany port na kartę microSD.</p> <p>Liczba portów Ethernet 2,5Gbps- minimum 8.</p> <p>Liczba portów światłowodowych 1Gbps- minimum 1.</p> <p>Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.</p> <p>Przepustowość Firewall (1518 bajtów UDP) – minimum 4Gbps.</p> <p>Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 2Gbps.</p> <p>Przepustowość filtrowania Antywirusowego – minimum 500Mbps.</p> <p>Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 1Gbps.</p> <p>Maksymalna liczba tuneli VPN IPSec – minimum 100.</p> <p>Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 50.</p> <p>Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 50.</p> <p>Obsługa interfejsów 802.11q (VLAN) – minimum 128.</p> <p>Liczba równoczesnych sesji – minimum 300 000 i nie mniej niż 20 000 nowych sesji/sekundę.</p> <p>Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.</p> <p>Urządzenie nie ma limitu na liczbę użytkowników.</p> <p>Liczba reguł filtrowania – minimum 8 192.</p> <p>Liczba tras statycznego routingu – minimum 512.</p> <p>Liczba tras dynamicznego routingu – minimum 10 000.</p> <p>Urządzenie ma umożliwiać podłączenie zewnętrznego nadmiarowego zasilacza (zasilanie redundantne). Stan pracy każdego zasilacza musi być sygnalizowany bezpośrednio na obudowie urządzenia.</p> <p>Urządzenie musi być wyposażone w moduł TPM.</p>
Wdrożenie	<p>Zamawiający wymaga przeprowadzenie wdrożenia dostarczonego urządzenia UTM w zakresie minimum:</p> <ul style="list-style-type: none"> • Wstępna konfiguracja urządzenia UTM/NGFW - dostępy administracyjne, synchronizacja czasu • Przeniesienie konfiguracji z obecnie posiadanego rozwiązania (Reguły firewall/NAT, konfiguracja interfejsów, routing statyczny, DHCP, IPSec VPN do 10 tuneli) • Uruchomienie SSL VPN (wewnętrzna baza użytkowników lub Active Directory/LDAP) • Integracja z Active Directory + Agent SSO • Dostosowanie wyjątków dla alarmów lub zaawansowanej konfiguracji systemu IPS. • Uruchomienie funkcji automatycznego backupu konfiguracji. • Uruchomienie funkcji DNS proxy. • Uruchomienie wbudowanego systemu raportowania.

-
- Uruchomienie powiadomień mailowych
 - Konfiguracja zbierania logów
 - Uruchomienie agenta SNMP
 - Przygotowanie Dokumentacji powdrożeniowej

Wymagane jest, aby wdrożenie przeprowadzone było przez Inżyniera Wykonawcy, posiadającego certyfikat producenta dostarczanego rozwiązania, który będzie potwierdzeniem posiadania umiejętności min z zakresu: (Certyfikat należy załączyć do oferty).

- Sieci i routingu w dostarczonym rozwiązaniu
- Przechwytywania i analizy ruchu sieciowego
- Konfiguracji i diagnostyki połączeń IPSec VPN oraz SSL VPN
- Konfiguracji systemu IPS oraz dostosowywania jego konfiguracji
- Konfiguracji i analizy polityk bezpieczeństwa
- Konfiguracji mechanizmu NAT
- Konfiguracji uwierzytelniania użytkowników
- Kontroli dostępu do stron WWW oraz deszyfrowania ruchu sieciowego w celu analizy przez systemy bezpieczeństwa
- Konfiguracji i diagnostyki mechanizmów zapewniania wysokiej dostępności
- Konfiguracji mechanizmów PKI w dostarczonym rozwiązaniu
- Przeszukiwania logów dotyczących ruchu sieciowego oraz pracy urządzenia
- Wsparcia technicznego i rozwiązywania problemów z dostarczonym rozwiązaniem

Ilość	1 szt.
-------	--------

2. UTM (Unified Threat Management) – typ II

Nazwa	Minimalne wymagania sprzętu
Typ	UTM (Unified Threat Management)
Obsługa sieci	<p>Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP</p>
Zapora korporacyjna (Firewall)	<p>Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.</p> <p>Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.</p> <p>Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).</p> <p>Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.</p> <p>Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.</p> <p>Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.</p> <p>Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.</p> <p>Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.</p> <p>Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.</p> <p>Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).</p> <p>System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.</p>
Intrusion Prevntion System (IPS)	<p>System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.</p> <p>Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.</p> <p>Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.</p> <p>Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.</p>

	<p>Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.</p> <p>Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS.</p> <p>Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.</p> <p>Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.</p> <p>Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV).</p> <p>Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.</p>
Kształtowanie Pasma (Traffic Shapping)	<p>Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.</p> <p>Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.</p> <p>Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).</p> <p>Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.</p>
Ochrona antywirusowa	<p>Urządzenie ma umożliwić rozbudowę o zaawansowany skaner antywirusowy dostarczany przez firmy trzecie (inne niż producent rozwiązania).</p> <p>Po rozbudowie administrator ma mieć możliwość określenia akcji w przypadku wykrycia zagrożenia bądź gdy analiza skanerem antywirusowym została zakończona błędem.</p> <p>Skaner antywirusowy ma pochodzić od europejskiego producenta.</p> <p>Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.</p> <p>Po rozbudowie administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.</p>
Ochrona Antyspam	<p>Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).</p> <p>Ochrona antyspam ma działać w oparciu o:</p> <ol style="list-style-type: none"> białe/czarne listy, DNS RBL, Skaner heurystyczny. <p>W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.</p>

	<p>Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.</p>
Wirtualne sieci prywatne (VPN)	<p>Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).</p> <p>Urządzenie ma wspierać co najmniej następujące typy sieci VPN:</p> <ol style="list-style-type: none"> PPTP VPN, b. IPsec VPN, c. SSL VPN. <p>SSL VPN ma działać co najmniej w trybach tunelu i portalu.</p> <p>Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.</p> <p>Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal).</p> <p>Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).</p> <p>Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf.</p> <p>Urządzenie ma umożliwiać tworzenie tuneli IPsec Policy Based oraz Route Based.</p>
Filtr dostępu do stron www	<p>Urządzenie ma posiadać wbudowany filtr URL.</p> <p>Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.</p> <p>Administrator ma mieć możliwość dodawania własnych kategorii URL.</p> <p>Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii.</p> <p>Do wyboru ma być przynajmniej:</p> <ol style="list-style-type: none"> blokowanie dostępu do adresu URL, zezwolenie na dostęp do adresu URL, blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora. <p>Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.</p> <p>Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.</p> <p>Filtr URL musi uwzględniać komunikację po protokole HTTPS.</p> <p>Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.</p> <p>Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.</p> <p>Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch.</p>
Uwierzytelnianie	<p>Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:</p> <ol style="list-style-type: none"> lokalną bazę użytkowników (wewnętrzny LDAP), zewnętrzną bazę użytkowników (zewnętrzny LDAP), usługę katalogową Microsoft Active Directory. <p>Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.</p>



	<p>Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły:</p> <ul style="list-style-type: none"> a. SSL, b. Radius, c. Kerberos. <p>Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.</p> <p>Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.</p> <p>Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.</p> <p>Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS).</p> <p>Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).</p> <p>Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.</p>
Administracja łączami do Internetu (IPS)	<p>Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).</p> <p>Mechanizm równoważenia obciążenia łączy internetowego ma działać w oparciu o następujące dwa mechanizmy:</p> <ul style="list-style-type: none"> a. równoważenie względem adresu źródłowego, b. równoważenie względem połączenia. <p>Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.</p> <p>Urządzenie ma umożliwiać przełączenie na łącznie zapasowe w przypadku awarii łączy podstawowego (tzw. Failover).</p> <p>Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łączy.</p> <p>W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnień, jitter, wskaźnika utraty pakietów).</p> <p>Monitorowanie dostępności łączy musi być możliwe w oparciu o ICMP oraz TCP.</p>
Routing (Trasowanie)	<p>Urządzenie ma umożliwiać statyczne trasowanie pakietów.</p> <p>Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącznie zapasowe w przypadku awarii łączy podstawowego.</p> <p>Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).</p> <p>Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.</p> <p>Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.</p>

**Administracja
urządzeniem**

Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.

Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.

Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.

Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.

Urządzenie ma umożliwiać zarządzania z poziomu konsoli (SSH).

Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.

Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.

Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.

Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.

Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki hasła stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.

Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording).

System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services). Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.

Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).

Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.

Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:

- a. manualnego eksportu do pliku w dowolnym momencie czasu,
- b. automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu.

Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.

Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.



	Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.
Raportowanie	<p>Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.</p> <p>System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.</p> <p>System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.</p> <p>System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.</p> <p>System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.</p> <p>System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.</p> <p>Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.</p> <p>Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.</p> <p>Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).</p>
Pozostałe usługi i funkcje	<p>Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.</p> <p>Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).</p> <p>Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.</p> <p>Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny).</p> <p>Urządzenie ma posiadać usługę DNS Proxy.</p> <p>Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.</p> <p>Urządzenie musi mieć zaimplementowane Open API.</p> <p>Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.</p> <p>Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.</p>
Gwarancja i serwis	<p>Urządzenie musi być objęte gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa do dnia minimum 30.06.2026r.</p> <p>W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.</p>

Parametry sprzętowe

Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.

Urządzenie ma być wyposażone w zintegrowany port na kartę microSD.

Liczba portów Ethernet 2,5Gbps- minimum 4.

Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.

Przepustowość Firewall (1518 bajtów UDP) – minimum 3Gbps.

Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 1Gbps.

Przepustowość filtrowania Antywirusowego – minimum 300Mbps.

Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 1Gbps.

Maksymalna liczba tuneli VPN IPSec – minimum 50.

Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 25.

Obsługa interfejsów 802.11q (VLAN) – minimum 128

Liczba równoczesnych sesji – minimum 150 000 i nie mniej niż 15 000 nowych sesji/sekundę.

Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.

Urządzenie nie ma limitu na liczbę użytkowników.

Liczba reguł filtrowania – minimum 1024.

Liczba tras statycznego routingu – minimum 512.

Liczba tras dynamicznego routingu – minimum 10 000.

Urządzenie musi posiadać pasywny system chłodzenia.

Urządzenie musi być wyposażone w moduł TPM.

Wdrożenie

Zamawiający wymaga przeprowadzenie wdrożenia dostarczonego urządzenia UTM w zakresie minimum:

- Wstępna konfiguracja urządzenia UTM/NGFW - dostępy administracyjne, synchronizacja czasu
- Uruchomienie SSL VPN (wewnętrzna baza użytkowników lub Active Directory/LDAP)
- Integracja z Active Directory + Agent SSO
- Dostosowanie wyjątków dla alarmów lub zaawansowanej konfiguracji systemu IPS.
- Uruchomienie funkcji automatycznego backupu konfiguracji.
- Uruchomienie funkcji DNS proxy.
- Uruchomienie wbudowanego systemu raportowania.
- Uruchomienie powiadomień mailowych
- Konfiguracja zbierania logów
- Uruchomienie agenta SNMP
- Przygotowanie Dokumentacji powdrożeniowej

Wymagane jest, aby wdrożenie przeprowadzone było przez Inżyniera Wykonawcy, posiadającego certyfikat producenta dostarczanego rozwiązania, który będzie potwierdzeniem posiadania umiejętności min z zakresu: (Certyfikat należy załączyć do oferty).

- Sieci i routingu w dostarczonym rozwiązaniu
- Przechwytywania i analizy ruchu sieciowego
- Konfiguracji i diagnostyki połączeń IPSec VPN oraz SSL VPN
- Konfiguracji systemu IPS oraz dostosowywania jego konfiguracji



-
- Konfiguracji i analizy polityk bezpieczeństwa
 - Konfiguracji mechanizmu NAT
 - Konfiguracji uwierzytelniania użytkowników
 - Kontroli dostępu do stron WWW oraz deszyfrowania ruchu sieciowego w celu analizy przez systemy bezpieczeństwa
 - Konfiguracji i diagnostyki mechanizmów zapewniania wysokiej dostępności
 - Konfiguracji mechanizmów PKI w dostarczonym rozwiązaniu
 - Przeszukiwania logów dotyczących ruchu sieciowego oraz pracy urządzenia
 - Wsparcia technicznego i rozwiązywania problemów z dostarczonym rozwiązaniem
-

Ilość

1 szt.

3. Zarządzalne urządzenie sieciowe

Nazwa	Minimalne wymagania dla sprzętu
Typ	Zarządzalne urządzenia sieciowe z obsługą VLAN, standardu 802.1X
Obudowa	Do montażu w szafie Rack 19", o wysokości nie więcej niż 1U, wraz z kompletem uchwytów montażowych, wyposażona w zintegrowany zasilacz, chłodzona aktywnie.
Porty	Minimum 22 portu PoE++ 10/100/1000/2500 Mbps RJ45 802.3 bt, i 2 porty PoE++ 100/1000/2500/10000 Mbps RJ45 802.3 bt minimum: <ul style="list-style-type: none"> 4 porty SFP/SFP+ 1/10GbE,
Wydajność przełącznika	Minimum 32000 adresów MAC Switch fabric capacity minimum 220 Gbps Forwarding rate minimum 170 Mpps
Funkcjonalność warstwy II	DHCP Server (Local Networks) DHCP Relay Inter-VLAN Routing (Local Networks) Static Routing (Local Networks) LACP Port Aggregation STP & RSTP QoS (DSCP) Pro AV Profiles (Play, Dante, Q-SYS, NDI, SDVoE, Shure, AES67, Crestron) Advanced IGMP Configuration (Querier, Fast Leave, Router Port) IGMP Snooping 802.1X Control MAC-Based ACLs & Device Isolation DHCP Snooping & Guarding Egress Rate Limit Flow Control Storm Control Multicast & Broadcast Rate Limiting MAC Address Blocking IP-Based ACLs & Network Isolation MAC-Based Port Restriction Port Isolation Port Mirroring Jumbo Frames LLDP-MED Voice VLAN Loop Protection Virtual Network Override



Funkcjonalność warstwy III	DHCP Server (Local Networks)
	DHCP Relay
	Inter-VLAN Routing (Local Networks)
	Static Routing (Local Networks)
Inne	Wykonawca dostarczy wraz z urządzeniem 4 szt. modułów SFP+ do RJ-45 10GbE
Gwarancja	Co najmniej 60 miesięcy gwarancji producenta, wraz z bezpłatnym dostępem do aktualizacji oprogramowania.
Ilość	1 szt.

4. Zarządzalne urządzenie sieciowe – typ II

Nazwa	Minimalne wymagania dla sprzętu
Typ	Zarządzalne urządzenia sieciowe z obsługą VLAN, standardu 802.1X
Obudowa	Do montażu w szafie Rack 19", o wysokości nie więcej niż 1U, wraz z kompletem uchwytów montażowych, wyposażona w zintegrowany zasilacz, chłodzona aktywnie.
Porty	Minimum 32 porty 10/100/1000 Mbps RJ45, i 16 portów 100/1000/2500 Mbps RJ45 minimum: <ul style="list-style-type: none"> 4 porty SFP/SFP+ 1/10GbE,
Wydajność przełącznika	Minimum 32000 adresów MAC Switch fabric capacity minimum 220 Gbps Forwarding rate minimum 160 Mpps
Funkcjonalność warstwy II	DHCP Server (Local Networks) DHCP Relay Inter-VLAN Routing (Local Networks) Static Routing (Local Networks) LACP Port Aggregation STP & RSTP QoS (DSCP) Pro AV Profiles (Play, Dante, Q-SYS, NDI, SDVoE, Shure, AES67, Crestron) Advanced IGMP Configuration (Querier, Fast Leave, Router Port) IGMP Snooping 802.1X Control MAC-Based ACLs & Device Isolation DHCP Snooping & Guarding Egress Rate Limit Flow Control Storm Control Multicast & Broadcast Rate Limiting MAC Address Blocking IP-Based ACLs & Network Isolation MAC-Based Port Restriction Port Isolation Port Mirroring Jumbo Frames LLDP-MED Voice VLAN Loop Protection Virtual Network Override

Funkcjonalność warstwy III	DHCP Server (Local Networks)
	DHCP Relay
	Inter-VLAN Routing (Local Networks)
	Static Routing (Local Networks)
Inne Funkcjonalności	DHCP Server (Local Networks)
	DHCP Relay
	Inter-VLAN Routing (Local Networks)
	Static Routing (Local Networks)
	LACP Port Aggregation
	STP & RSTP
	QoS (DSCP)
	Pro AV Profiles (Play, Dante, Q-SYS, NDI, SDVoE, Shure, AES67, Crestron)
	Advanced IGMP Configuration (Querier, Fast Leave, Router Port)
	IGMP Snooping
	802.1X Control
	MAC-Based ACLs & Device Isolation
	DHCP Snooping & Guarding
	Egress Rate Limit
	Flow Control
	Storm Control
	Multicast & Broadcast Rate Limiting
	MAC Address Blocking
	IP-Based ACLs & Network Isolation
	MAC-Based Port Restriction
	Port Isolation
	Port Mirroring
	Jumbo Frames
	LLDP-MED
	Voice VLAN
	Loop Protection
	Virtual Network Override
Inne	Wykonawca dostarczy wraz z urządzeniem 4 szt. modułów SFP+ do RJ-45 10GbE
Gwarancja	Co najmniej 60 miesięcy gwarancji producenta, wraz z bezpłatnym dostępem do aktualizacji oprogramowania.
Ilość	1 szt.

5. Zasilacz awaryjny UPS

Nazwa	Minimalne wymagania dla sprzętu
Typ	UPS
Wymagania minimalne	Moc wyjściowa (pozorna / czynna): minimum 3000 VA minimum 3000 W Topologia: VI (line interactive) Typ obudowy: Rack / Tower Chłodzenie: Wymuszone, wewnętrzne wentylatory
Wejścia	Napięcie znamionowe (wartość skuteczna): 230 V AC Zakres napięcia wejściowego (wartości skuteczne) i tolerancja: 178 ÷ 281 V AC ± 2 % Częstotliwość znamionowa napięcia wejściowego: 50 Hz Zakres częstotliwości i tolerancja: 45 ÷ 55 Hz ± 1 Hz Progi przełączania: sieć – UPS: 178 ÷ 281 V AC ± 2 %
Wyjścia	Napięcie znamionowe (wartość skuteczna): 230 V AC Zakres napięcia wyjściowego (wartości skuteczne) i tolerancja – praca sieciowa: 195 ÷ 253 V AC ± 2 % Zakres napięcia wyjściowego (wartości skuteczne) i tolerancja – praca rezerwowa: 230 V AC ± 5 % Automatyczna regulacja napięcia (AVR): ± 10 % Kształt napięcia wyjściowego (przy pracy rezerwowej / sieciowej): Sinusoidalny / Tak jak na wejściu Częstotliwość znamionowa napięcia wyjściowego: 50 Hz Filtracja napięcia wyjściowego: Filtr przeciwzakłóceńowy RFI/EMI, tłumik warystorowy Progi przełączania: UPS – sieć: 183 ÷ 276 V AC ± 2 % Czas przełączenia na pracę rezerwową < 3 ms Czas powrotu na pracę sieciową: 0 ms Przeciążalność > 105% - 15 s (wyłączenie UPS)
Akumulatory i czas podtrzymania	Akumulatory wewnętrzne: minimum 8x 12 V / 7 Ah Czas podtrzymania (100 % / 80 % / 50 % Pmax): minimum 4 / 7 / 12 min Maksymalny czas ładowania baterii UPS - po 80% wyładowaniu baterii: maksymalnie 4 h
Zabezpieczenia	Zabezpieczenie wejściowe <ul style="list-style-type: none"> Przeciwwzwarciowe – Bezpiecznik automatyczny 16 A / 250 V AC Przeciwpzepięciowe Zabezpieczenie wyjściowe: Elektroniczne – przeciwwzwarciowe i przeciążeniowe Zabezpieczenia wejścia DC (akumulatory wewnętrzne): Zabezpieczenie nadprądowe

Przyłącza wyjściowe (liczba i typ gniazd)

- minimum 6 x IEC320 C13 (10 A)
- minimum 2 x PL (z bolcem uziemiającym)

Sygnalizacja minimum: Akustycznie – optyczna; graficzny wyświetlacz LCD

Interfejsy komunikacyjne minimum: USB HID

Wyposażenie i funkcje dodatkowe

Wsporniki do montażu w szafie RACK

- Oprogramowanie tego samego producenta co UPS, bezpłatne bez ograniczeń funkcjonalności oraz ilości podłączonych stanowisk komputerowych - możliwość zamykania systemu na stanowiskach komputerowych w sieci - możliwość pobierania ze strony producenta i dokonywania aktualizacji przez użytkownika bez dodatkowych kosztów. możliwość edycji nazw urządzeń na liście monitorowanych UPSów

Możliwość aktualizacji firmware w UPS przez użytkownika

Certyfikaty	Producent oferowanego sprzętu musi posiadać ISO 9001:2008 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisowania;
Gwarancja	minimum 36 miesięcy na elektronikę i 24 miesiące na akumulatory; Serwis musi być realizowany przez autoryzowany serwis producenta. Zamawiający wymaga, aby serwis realizowany był w systemie door to door

6. Oprogramowanie typu XDR Extended Detection and Response

Nazwa	Minimalne wymagania
LICENCJA	<p>W ramach postępowania Wykonawca jest zobowiązany dostarczyć Oprogramowanie wraz z licencją. Wykonawca musi dostarczyć licencje czasową do 30.06.2026 roku.</p> <p>Oprogramowanie musi posiadać od dnia podpisania protokołu odbioru, do 30.06.2026 roku gwarancję producenta Oprogramowania dla licencji (tj. licencji dostarczonych w ramach niniejszego postępowania).</p> <p>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.</p> <p>Licencje na Oprogramowanie dostarczone będą do siedziby Zamawiającego w formie papierowej lub elektronicznej.</p> <p>Dostarczona licencja na Oprogramowanie Systemu nie może limitować wielkości przechowywanych danych oraz możliwości wyszukiwania informacji z zgromadzonych danych.</p> <p>Ilość licencji dla komputerów: 45 szt.</p> <p>Ilość licencji dla serwerów: 6 szt.</p>
Ochrona punktów końcowych urządzeń komputerowych	<p>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.</p> <p>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.</p> <p>Ten sam agent zainstalowany na systemach Windows umożliwia rozbudowę funkcjonalności o system EPP 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.</p> <p>Rozwiązanie dla ochrony antywirusowej stacji roboczych wspiera następujące systemy operacyjne:</p> <ul style="list-style-type: none"> • Microsoft Windows 10 • Microsoft Windows 11 • MacOS version 14 "Sonoma" • MacOS version 13 "Ventura" • MacOS version 12 "Monterey" <p>Wspierane przeglądarki internetowe do obsługi konsoli zarządzającej:</p>

-
- 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 XDR 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

1. Oprogramowanie instalowane na stacjach końcowych, zwane dalej agentem, ma możliwość współpracy z każdym oprogramowaniem antywirusowym dostępnym na rynku.
 2. Agent instalowany na stacjach końcowych posiada możliwość instalacji z wykorzystaniem mechanizmów dystrybucji oprogramowania Active Directory.
 3. Agent instalowany na stacjach końcowych posiada możliwość ręcznej instalacji, bez wykorzystania zewnętrznych systemów dystrybucji oprogramowania.
 4. Oprogramowanie nie wymaga restartu systemu operacyjnego po dokonaniu aktualizacji oprogramowania agenta monitorującego na stacjach końcowych.
 5. 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.
 6. Agent instalowany na stacjach końcowych 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.
 7. 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.
 8. Dane zbierane przez agenta instalowanego na stacjach końcowych, przed wysłaniem do centrum przetwarzania danych, są
-

kompresowane w celu optymalizacji wykorzystania łączy sieciowych.

9. Komunikacja agentów instalowanych na stacjach roboczych, z centrum przetwarzania danych producenta, odbywa się jedynie z wykorzystaniem protokołów HTTP oraz HTTPS.
 10. Komunikacja agentów instalowanych na stacjach roboczych, wspiera komunikację za pomocą serwera pośredniczącego http (http proxy).
 11. 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.
 12. Dane zbierane przez agentów na stacjach końcowych są, przechowywane i przetwarzane na obszarze Europejskiej Wspólnoty Gospodarczej.
 13. Rozwiązanie na bazie zebranych danych generuje detekcje, które stanowią powiązane ze sobą podejrzane zdarzenia, zebrane przez agentów ze stacji roboczych.
 14. Detekcje są generowane za pomocą statycznych reguł, przygotowanych przez producenta, jak również przy wykorzystaniu mechanizmów uczenia maszynowego uwzględniających specyfikę pracy środowiska informatycznego.
 15. Detekcje są generowane w czasie rzeczywistym na podstawie danych zebranych i przesłanych przez agentów uruchomionych na stacjach końcowych w środowisku informatycznym.
 16. Detekcje widoczne są w konsoli zarządzającej w postaci graficznych diagramów, przedstawiających wykryte anomalie i powiązania pomiędzy biorącymi udział w detekcji elementami.
 17. Detale dotyczące detekcji przedstawiane są w postaci drzewa zawierającego szczegółowe informacje dotyczące poszczególnych elementów biorących udział w wykrytej anomalii.
 18. Rozwiązanie posiada możliwość filtrowania zdarzeń biorących udział w detekcji w zależności od poziomu ryzyka – od poziomu informacyjnego do zdarzeń o charakterze krytycznym.
 19. Każda detekcja zawiera co najmniej następujące informacje:
 - Lista urzędów 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).
20. 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).
 21. 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).
 22. Rozwiązanie umożliwia oznaczanie wygenerowanych detekcji jako błędne.
 23. Oznaczenie detekcji jako błędnej, musi powodować, automatyczne identyfikowanie przyszłych takich samych detekcji i odpowiednie ich oznaczenie w interfejsie centralnego zarządzania.
 24. Rozwiązanie posiada możliwość stworzenia archiwum zawierającego dodatkowe informacje dotyczące hosta, na którym wystąpiła detekcja w celu przeprowadzenia analizy śledczej incydentu.
 25. Rozwiązanie pozwala na dodanie własnego komentarza przy wykrytej detekcji.
 26. Rozwiązanie umożliwia wykupienie usługi pozwalającej na przesłanie detekcji do laboratorium producenta w celu analizy, zwrotnie administrator otrzymuje szczegółowy raport przygotowany przez analityka dotyczący incydentu.
 27. Rozwiązanie pozwala na przesłanie wiadomości e-mail informującej o wygenerowaniu nowej detekcji w systemie.
 28. Rozwiązanie pozwala na izolację sieciową komputerów przez administratora.
 29. Rozwiązanie umożliwia tworzenie reguł automatycznej izolacji stacji roboczych, jeśli zostaną one uwzględnione w wygenerowanych detekcjach.
 30. 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.
 31. Rozwiązanie umożliwia tworzenie raportów zawierających co najmniej listę wygenerowanych detekcji, wraz z ich opisem, za zadany okres.
 32. Rozwiązanie pozwala na eksport raportów, w postaci plików PDF.
-

-
33. Rozwiązanie wspiera dostęp do danych na temat utworzonych detekcji za pomocą interfejsu REST API, na potrzeby integracji z innymi systemami zabezpieczającymi.
 34. Konsola centralnego zarządzania, oferuje interfejs w języku Polskim.
 35. Konsola zarządzająca wyposażona jest w panel kontrolny (dashboard) w którym administrator ma możliwość weryfikacji stanu bezpieczeństwa organizacji.
 36. 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.
 37. Konsola wyposażona w dedykowaną zakładkę zawierającą listę urzędów posiadających zainstalowanego agenta systemu EDR.
 38. Lista urzędów posiadających zainstalowanego agenta systemu EDR zawiera informacje dotyczące: nazwy hosta, adresu IP, poziomu ważności, przypisanego profilu, systemu operacyjnego, informacji o ostatnim połączeniu oraz aktualnym statusie.
 39. 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. Rozwiązanie posiada wbudowany mechanizm ochrony przed zagrożeniami typu ransomware.
 40. Rozwiązanie wspiera technologię Antimalware Scan Interface (AMSI)
 41. Rozwiązanie umożliwia wybór plików do skanowania – wszystkich plików lub tylko plików o określonych rozszerzeniach.
 42. W momencie wykrycia infekcji rozwiązanie automatycznie stara się wyleczyć plik, a jeśli nie jest to możliwe przenosi go do bezpiecznego folderu kwarantanny.
 43. Rozwiązanie posiada możliwość ręcznej reakcji na wykryte zagrożenie, w takim przypadku pozwala na: wyleczenie pliku, usunięcie, przeniesienie do kwarantanny, zmiany nazwy, zablokowania.
 44. Rozwiązanie chroni plik systemowy HOSTS przed nieautoryzowanymi zmianami.
 45. Rozwiązanie posiada mechanizmy skanujące dyski sieciowe.
 46. Skanowanie dysków sieciowych jest możliwe dla dowolnych operacji na takich zasobach lub tylko przy wykonywaniu znajdujących się tam plików.
 47. Rozwiązanie posiada możliwość tworzenia wykluczeń dla mechanizmów ochrony w czasie rzeczywistym, w tym co najmniej dla: plików, folderów, procesów.
 48. Rozwiązanie posiada mechanizm ochrony ruchu http chroniący użytkownika przed malware oraz phishingiem.
-

-
49. Istnieje możliwość stworzenia wykluczenia dla wskazanej aplikacji, tak aby nie skanowała ona ruchu http.
 50. 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.
 51. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
 52. Rozwiązanie posiada możliwość dystrybuowania aktualizacji baz definicji wirusów oraz aktualizacji oprogramowania zainstalowanego na stacji końcowej, za pomocą serwera pośredniczącego.
 53. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej do nowej wersji, następuje w sposób automatyczny, niewidoczny dla użytkownika końcowego.
 54. 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.
 55. 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.
 56. Rozwiązanie posiada możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej w określone dni i godziny tygodnia i miesiąca.
 57. 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.
 58. Rozwiązanie posiada możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.
 59. Rozwiązanie posiada możliwość wywołania procesu skanowania z niskim priorytetem, co pozwala na skanowanie z użyciem mniejszej ilości zasobów systemowych.
 60. Rozwiązanie posiada możliwość wywołania skanowania uwzględnionych rozszerzeń a także ich wykluczanie.
 61. Rozwiązanie posiada możliwość skanowania urządzeń przenośnych takich jak pendrive, dyski zewnętrzne itp.
 62. 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.
 63. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie.
-

-
64. Rozwiązanie posiada funkcję skanowania na żądanie pojedynczych plików, katalogów, napędów przy pomocy skrótu w menu kontekstowym
 65. 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).
 66. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.
 67. Rozwiązanie posiada heurystyczną technologię do wykrywania nowych, nieznanych wirusów.
 68. Umożliwia wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware”, „adware”, „keylogger”, „dialer”, „trojan”, „rootkit”.
 69. Posiada mechanizm wykrywania nowych i nieznanych zagrożeń (0-day), bazujący na technologii chmurowej, analizującej podejrzane pliki wykonywalne.
 70. 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.
 71. 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.
 72. Rozwiązanie posiada możliwość wyłączenia mechanizmu automatycznego przesyłania podejrzanych plików do dodatkowej analizy przez producenta.
 73. Rozwiązanie posiada możliwość umieszczenia oprogramowania typu „spyware”, „adware”, „keylogger”, „dialer”, „trojan” w kwarantannie.
 74. Rozwiązanie posiada możliwość obsługi plików skompresowanych obejmującego najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2 HQX.
 75. 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.
 76. Rozwiązanie automatycznie powiadamia użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem czy stacja robocza jest odpowiednio zabezpieczona.
 77. Rozwiązanie posiada możliwość wyłączenia powiadomień dla użytkowników stacji końcowej o wykrytych zagrożeniach.
 78. Rozwiązanie posiada możliwość wyłączenia interfejsu użytkownika oprogramowania zainstalowanego na stacji końcowej.
-

-
79. Rozwiązanie umożliwia blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http.
 80. Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez system reputacyjny producenta.
 81. 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.
 82. Rozwiązanie jest wyposażone w mechanizm ochrony przeglądarki internetowej, w tym analizujący uruchamiane skrypty ActiveX i pobierane pliki.
 83. Rozwiązanie posiada możliwość ochrony podczas przeglądania sieci Internet na podstawie badania reputacji witryn.
 84. Rozwiązanie umożliwia blokowanie dostępu do kategorii witryn WWW skatalogowanych przez systemy producenta.
 85. Oprogramowanie zapewnia co najmniej 30 kategorii klasyfikacji witryn WWW.
 86. Użytkownik podczas próby przejścia na witrynę znajdującą się w zablokowanej przez Administratora kategorii, jest powiadomiony o nałożonej na niego blokadzie komunikatem w przeglądarce internetowej.
 87. Rozwiązanie umożliwia blokowanie witryn na podstawie kategorii zarówno dla protokołu HTTP jak i HTTPS.
 88. Rozwiązanie posiada wbudowany mechanizm zabezpieczenia połączenia do witryn skategoryzowanych przez producenta jako „bankowość elektroniczna”.
 89. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie blokuje możliwość uruchamiania od strony chronionego hosta poleceń cmd oraz skryptów.
 90. 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.
 91. Kontrola połączenia umożliwia zabezpieczenie sesji do dowolnej witryny HTTPS wskazanej przez administratora – administrator ma możliwość tworzenia własnej listy takich witryn.
 92. Rozwiązanie posiada wbudowaną funkcję, która po zakończeniu sesji z witrynami sklasyfikowanymi jako „bankowość elektroniczna” czyści zawartość schowka systemowego.
 93. 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.
-

-
94. Profile bezpieczeństwa zapory ogniowej zawierają predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej.
 95. 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.
 96. Rozwiązanie posiada możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej).
 97. Rozwiązanie umożliwia stworzenie zestawów reguł do natychmiastowego zastosowania, które zablokują komunikację sieciową w celu izolacji hosta na żądanie administratora.
 98. Rozwiązanie jest wyposażone w mechanizm aktualizacji aplikacji (patch management), umożliwiający instalację dostępnych poprawek dla systemu operacyjnego oraz aplikacji na nim zainstalowanych.
 99. Mechanizm aktualizacji aplikacji (patch management) nie wymaga instalowania dodatkowych agentów oprócz agenta AV.
 100. Moduł aktualizacji aplikacji, okresowo skanuje aplikacje zainstalowane na stacji roboczej i umożliwia ich aktualizację do najnowszych wersji.
 101. Moduł aktualizacji aplikacji pełni rolę mechanizmu łąiącego podatności i instalującego aktualizacje oprogramowania, a nie jedynie pasywnego skanera luk w bezpieczeństwie aplikacji.
 102. Administrator posiada możliwość określenia, kiedy i jakie aktualizacje mają zostać zainstalowane automatycznie.
 103. Administrator posiada możliwość uruchomienia aktualizacji dla systemu operacyjnego jak i aplikacji znajdujących się na nim na żądanie dla wybranych lub wszystkich hostów.
 104. Mechanizm aktualizacji aplikacji umożliwia automatyczne wyświetlenie komunikatu użytkownikowi od strony hosta o konieczności zamknięcia danej aplikacji, tak aby proces aktualizacji mógł się zakończyć.
 105. 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.
 106. Administrator konsoli zarządzającej ma możliwości zapoznania się z opisem danej podatności aplikacji uruchamiając aktywny link z konsoli zarządzającej z przekierowaniem na strony producenta aplikacji.
 107. Mechanizm aktualizacji aplikacji (patch management) nie wymaga uprawnień administratora lokalnego do instalacji poprawek i jest realizowany, jako dedykowany proces.
-

-
108. Administrator ma możliwość zdefiniowania aplikacji, które nie podlegają aktualizacji, poprzez wpisanie nazwy aplikacji na listę wykluczeń w konsoli zarządzającej.
 109. Rozwiązanie umożliwia wyświetlenie w GUI od strony chronionego hosta informacji o brakujących poprawkach dla systemu lub aplikacji i umożliwienie, ich instalacji przez użytkownika końcowego.
 110. System centralnego zarządzania prezentuje niezaktualizowane aplikacje występujące na wszystkich chronionych hostach lub listę nieaktualizowanego oprogramowania dla pojedynczej stacji końcowej.
 111. Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.
 112. 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.
 113. Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączania do stacji końcowej.
 114. Lista urządzeń zaufanych jest tworzona co najmniej w oparciu o nazwę urządzenia i identyfikator sprzętowy.
 115. Rozwiązanie posiada możliwość blokady zapisywania plików na zewnętrznych dyskach USB urządzenia takie są wówczas dostępne w trybie tylko do odczytu.
 116. Mechanizm kontroli urządzeń umożliwia blokadę uruchamiania plików wykonywalnych z nośników pamięci. Blokada ta pozwala na korzystanie z pozostałych danych zapisanych na takich nośnikach.
 117. Rozwiązanie posiada opcję zabezpieczenia hasłem możliwości deinstalacji agenta przez użytkownika końcowego.
 118. Zmiany w konfiguracji mogą być dokonywane przez użytkownika końcowego tylko dla poszczególnych funkcji aplikacji wskazanych przez administratora w profilu.
 119. Rozwiązanie posiada możliwość przekazywania do konsoli administracji zdalnej kluczy odzyskiwania funkcji BitLocker
 120. Rozwiązanie pozwala na zdalne wymuszenie procesu szyfrowania dysków systemowych za pomocą funkcji Bitlocker wbudowanej i obsługiwanej przez system Windows.
 121. W momencie zdalnego uruchomienia procesu szyfrowania za pomocą funkcji Bitlocker administrator posiada możliwość wymuszenia ustanowienia kodu PIN na stacji roboczej, wymaganego do logowania.
 122. Rozwiązanie pozwala na zdalne uruchomienie procesu deszyfrowania wcześniej zaszyfrowanych dysków systemowych.
 123. Administrator w konsoli zarządzającej posiada dostępne informacje dotyczące stanu zaszyfrowania dysków systemowych.
 124. Rozwiązanie posiada wbudowany mechanizm przywracania plików zaszyfrowanych przez zagrożenia typu ransomware.
-

-
125. Mechanizm w swoim działaniu wykorzystuje własną technologię producenta, nie inne technologie takie jak Volume Shadow Copy Service (VSS)
 126. W przypadku wykrycia szkodliwego działania ransomware, moduł blokuje aktywność szkodliwego procesu oraz przywraca pliki, które zostały zaszyfrowane do oryginalnej formy i lokalizacji.
 127. Moduł przywracania plików zaszyfrowanych może działać w trybie monitorowania, bez podejmowania reakcji.
 128. Administrator ma możliwość wskazania własnego folderu, do którego będą kopiowane pliki tworzonej kopii zapasowej plików.
 129. Administrator posiada możliwość określenia maksymalnej wielkości pliku, którego kopia zapasowa będzie tworzona przez moduł przywracania.
 130. 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.
 131. Moduł posiada możliwość pracy w trybie monitorowania (bez blokowania) przekazując administratorowi informacje dotyczące prób modyfikacji plików w chronionych folderach.
 132. Administrator posiada możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.
 133. Istnieje możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną antyransomware.
 134. Rozwiązanie potrafi automatycznie wykryć zaufane aplikacje, dla których będzie zezwolony dostęp do plików w chronionych folderach, oraz daje możliwość wskazania zaufanych aplikacji przez administratora.
 135. Rozwiązanie potrafi automatycznie wykryć zaufane aplikacje, dla których będzie zezwolony dostęp do plików w chronionych folderach, oraz daje możliwość wskazania zaufanych aplikacji przez administratora.
 136. Rozwiązanie posiada funkcjonalność kontroli uruchamianych aplikacji.
 137. Tryb kontroli aplikacji umożliwia uruchomienie wszystkich aplikacji, uruchomienie i monitorowanie wszystkich aplikacji, blokowanie niezauważanych aplikacji.
 138. 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.
 139. Tworzone reguły dotyczyć mogą czynności: uruchomienia aplikacji, ładowania modułu, uruchomienia instalatora, dostępu do pliku.
-

-
140. Na wspieranych systemach Windows rozwiązanie pozwala na zdalne wywołanie procesu szyfrowania za pomocą funkcji BitLocker wbudowanej w system operacyjny.
 141. Administrator posiada w momencie konfiguracji procesu szyfrowania, możliwość wymuszenia od strony użytkownika ustanowienia dodatkowego zabezpieczenia w postaci kodu PIN
 142. 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)
 143. Administrator ma możliwość wyboru, które z informacji pochodzących z dziennika systemu Windows mają być przekazywane do konsoli zarządzającej.
 144. Rozwiązanie pozwala na wygenerowanie pliku za pomocą którego administrator może wywołać zdalne podłączenie za pomocą usług Microsoft RDP (Remote Desktop).
 145. 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.
 1. Komunikacja pomiędzy portalem centralnego zarządzania a stacjami roboczymi odbywa się w formie zaszyfrowanej.
 2. 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.
 3. Interfejs zarządzania posiada funkcję wyświetlania monitów o zbliżającym się zakończeniu licencji, a także powiadomienia o zakończeniu licencji.
 4. Interfejs jest wyposażony w panel kontrolny zawierający podsumowanie stanu bezpieczeństwa organizacji w postaci graficznych wykresów.
 5. Wykresy są interaktywne, tzn., że po wybraniu interesującego elementu, następuje przekierowanie do zawierającego bardziej szczegółowe dane menu.
 6. Rozwiązanie posiada dedykowaną zakładkę zawierającą informację o wszystkich hostach posiadających zainstalowane oprogramowanie do ochrony, w tym: ich nazwy, status ochrony, przypisany profil bezpieczeństwa.
 7. Istnieje możliwość eksportu listy wszystkich hostów do pliku CSV.
-

-
8. 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.
 9. 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.
 10. Komputery nie nawiązujące komunikacji z konsolą zarządzającą mogą być automatycznie usuwane z listy po określonym przez administratora czasie - co najmniej 60 dni.
 11. Rozwiązanie posiada dodatkową zakładkę zawierającą informacje dotyczącą brakujących aktualizacji dla zainstalowanych aplikacji i systemu operacyjnego.
 12. Istnieje możliwość posortowania i filtrowania brakujących poprawek pod względem ich poziomu krytyczności.
 13. Informacje dotyczące brakujących poprawek dla aplikacji i systemu operacyjnego zawierają liczbę i typ hostów, na których został wykryty brak danej poprawki.
 14. Po wskazaniu danej poprawki administrator posiada możliwość jej instalacji na wskazanych komputerach dla których dana poprawka została wydana.
 15. Administrator ma możliwość wglądu w historię instalowanych poprawek na chronionych hostach.
 16. Rozwiązanie posiada moduł raportujący w którym wyświetlane są informacje dotyczące stanu ochrony, infekcji malware, instalowanych aplikacji.
 17. Raporty mogą być tworzone zgodnie z harmonogramem i wysyłane na wskazane adresy email.
 18. Rozwiązanie posiada wbudowany mechanizm zarządzania subskrypcjami, z możliwością dodawania nowych kluczy licencyjnych.
 19. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji.
 20. 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.
 21. Dodanie klucza licencyjnego skutkuje pojawieniem się dedykowanej zakładki obsługującej dany produkt w portalu zarządzającym.
 22. Rozwiązanie ma możliwość definiowania różnych profili ustawień dla chronionych urządzeń z poziomu portalu zarządzającego.
 23. Profile mogą być przypisane do pojedynczych hostów lub do grup.
-

**Moduł wykrywania i
reagowania na
podejrzanych aktywności
na urządzeniach
końcowych**

24. Profile mogą być automatycznie przypisywane do hostów spełniających określone warunki w tym: adresy IP, DNS, nazwa WINS, przynależność do AD.

25. W przypadku automatycznego przypisywania profili, system pozwala na automatyczne dodawanie tagów dla hostów które otrzymają dany profil konfiguracyjny.

26. Istnieje możliwość porównania 2 profili konfiguracyjnych w celu wyświetlenia różnic pomiędzy nimi.

27. 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.

28. Z poziomu portalu zarządzającego istnieje możliwość pobrania plików instalacyjnych, wykorzystywanych do instalacji agenta na objętych licencją hostach.

29. Pliki instalacyjne mają posiadać plików .EXE, .MSI, .MPKG, .DEB, .RPM w zależności od platformy i typu systemu na jakich ma zostać zainstalowany agent.

30. Tworzone profile muszą dawać administratorowi możliwość blokowania ustawień konfiguracyjnych aplikacji zainstalowanych od strony stacji roboczych w celu uniemożliwienia ich modyfikacji przez lokalnego użytkownika.

31. Administrator posiada możliwość wyświetlenia dodatkowych szczegółów dotyczących chronionych hostów.

32. 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.

33. Portal zarządzający pozwala na zarządzanie oprogramowaniem instalowanym na urządzeniach mobilnych (smartphony) w przypadku posiadania odpowiedniej licencji.

34. Konsola posiada możliwość definiowania wielu kont administratorów o różnych poziomach dostępu.

35. W ramach posiadanych licencji istnieje możliwość przenoszenia oprogramowania w ramach danego klucza subskrypcji

System klasy EDR/XDR zarządzany 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.

Ten sam agent zainstalowany na systemach Windows umożliwia rozbudowę funkcjonalności o 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.

Rozwiązanie posiada możliwość instalacji agenta monitorowania na stacjach roboczych z co najmniej następującymi systemami operacyjnymi:

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

Rozwiązanie posiada możliwość instalacji agenta monitorowania na serwerach z co najmniej następującymi systemami operacyjnymi:

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

Wspierane przeglądarki internetowe:

- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Safari

Rozwiązanie posiada polski interfejs użytkownika centralnej konsoli zarządzania oraz agenta instalowanego na stacji końcowej oraz serwerze.

1. Oprogramowanie instalowane na stacjach końcowych i serwerach, zwane dalej agentem, ma możliwość współpracy z każdym oprogramowaniem antywirusowym dostępnym na rynku.
 2. Agent instalowany na stacjach końcowych i serwerach posiada możliwość instalacji z wykorzystaniem mechanizmów dystrybucji oprogramowania Active Directory.
 3. Agent instalowany na stacjach końcowych i serwerach posiada możliwość ręcznej instalacji, bez wykorzystania zewnętrznych systemów dystrybucji oprogramowania.
 4. Oprogramowanie nie wymaga restartu systemu operacyjnego po dokonaniu aktualizacji oprogramowania agenta monitorującego na stacjach końcowych i serwerach.
 5. 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.
-

6. 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.

7. 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.

8. Dane zbierane przez agenta instalowanego na stacjach końcowych, przed wysłaniem do centrum przetwarzania danych, są kompresowane w celu optymalizacji wykorzystania łączy sieciowych.

9. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, z centrum przetwarzania danych producenta, odbywa się jedynie z wykorzystaniem protokołów HTTP oraz HTTPS.

10. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, wspiera komunikację za pomocą serwera pośredniczącego http (http proxy).

11. 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.

12. Dane zbierane przez agentów na stacjach końcowych i serwerach są, przechowywane i przetwarzane na obszarze Europejskiej Wspólnoty Gospodarczej.

13. Rozwiązanie na bazie zebranych danych generuje detekcje, które stanowią powiązane ze sobą podejrzane zdarzenia, zebrane przez agentów ze stacji roboczych i serwerów.

14. Detekcje są generowane za pomocą statycznych reguł, przygotowanych przez producenta, jak również przy wykorzystaniu mechanizmów uczenia maszynowego uwzględniających specyfikę pracy środowiska informatycznego.

15. Detekcje są generowane w czasie rzeczywistym na podstawie danych zebranych i przesłanych przez agentów uruchomionych na stacjach końcowych i serwerach w środowisku informatycznym.

16. Detekcje widoczne są w konsoli zarządzającej w postaci graficznych diagramów, przedstawiających wykryte anomalie i powiązania pomiędzy biorącymi udział w detekcji elementami.

17. Detale dotyczące detekcji przedstawiane są w postaci drzewa zawierającego szczegółowe informacje dotyczące poszczególnych elementów biorących udział w wykrytej anomalii.

18. Rozwiązanie posiada możliwość filtrowania zdarzeń biorących udział w detekcji w zależności od poziomu ryzyka – od poziomu informacyjnego do zdarzeń o charakterze krytycznym.

19. Każda detekcja zawiera co najmniej następujące informacje:

- Lista urzędów 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).

20. 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).

21. 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).

22. Rozwiązanie umożliwia oznaczanie wygenerowanych detekcji jako błędne.

23. Oznaczenie detekcji jako błędnej, musi powodować, automatyczne identyfikowanie przyszłych takich samych detekcji i odpowiednie ich oznaczenie w interfejsie centralnego zarządzania.

24. Rozwiązanie posiada możliwość stworzenia archiwum zawierającego dodatkowe informacje dotyczące hosta, na którym wystąpiła detekcja w celu przeprowadzenia analizy śledczej incydentu.

25. Rozwiązanie pozwala na dodanie własnego komentarza przy wykrytej detekcji.

26. Rozwiązanie umożliwia wykupienie usługi pozwalającej na przesłanie detekcji do laboratorium producenta w celu analizy, zwrótnie administrator otrzymuje szczegółowy raport przygotowany przez analityka dotyczący incydentu.

27. Rozwiązanie pozwala na przesłanie wiadomości e-mail informującej o wygenerowaniu nowej detekcji w systemie.

28. Rozwiązanie pozwala na izolację sieciową komputerów przez administratora.

29. Rozwiązanie umożliwia tworzenie reguł automatycznej izolacji stacji roboczych i serwerów, jeśli zostaną one uwzględnione w wygenerowanych detekcjach.

30. 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.

31. Rozwiązanie umożliwia tworzenie raportów zawierających co najmniej listę wygenerowanych detekcji, wraz z ich opisem, za zadany okres.

32. Rozwiązanie pozwala na eksport raportów, w postaci plików PDF.

33. Rozwiązanie wspiera dostęp do danych na temat utworzonych detekcji za pomocą interfejsu REST API, na potrzeby integracji z innymi systemami zabezpieczającymi.

34. Konsola centralnego zarządzania, oferuje interfejs w języku Polskim.

35. Konsola zarządzająca wyposażona jest w panel kontrolny (dashboard) w którym administrator ma możliwość weryfikacji stanu bezpieczeństwa organizacji.

36. 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.

37. Konsola wyposażona w dedykowaną zakładkę zawierającą listę urządzeń posiadających zainstalowanego agenta systemu EDR.

38. 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.

39. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji.

40. Portal zarządzający umożliwia dodawanie kluczy licencyjnych dla innych produktów w celu aktywacji danej funkcjonalności, co najmniej dla systemu antywirusowego oraz mechanizmów zarządzania podatnościami.

41. Dodanie klucza licencyjnego skutkuje aktywowaniem dedykowanej zakładki obsługującej dany produkt w portalu zarządzającym.

Opis technologii monitorowania podejrzanej aktywności na poziomie kont MS Entra ID

1. Rozwiązanie pozwala na synchronizację z usługami Entra ID

-
2. Rozwiązanie w przypadku wykrycia podejrzenia aktywności kont monitorowanych na poziomie Entra ID generuje detekcję widoczną w konsoli.
 3. Wygenerowana detekcja posiada: ID Detekcji, określony poziom krytyczności, datę detekcji, datę ostatniej modyfikacji, status, informacje o dodanym komentarzu.
 4. Administrator posiada możliwość wglądu w szczegóły danej detekcji.
 5. W ramach szczegółów detekcji administrator ma możliwość manualnego określenia statusu detekcji, w zależności od etapu jej analizy.
 6. Administrator posiada informacje dotyczące źródła detekcji, organizacji, dla której detekcja została wygenerowana, zasobu oraz lokacji dotkniętej wykrytą podejrzaną aktywnością.
- W ramach szczegółów detekcji administrator otrzymuje jej podsumowanie, opis, informacje o ryzyku z jakim związana jest dana aktywność oraz sugerowane rekomendacje.

Oprogramowanie do ochrony antymalware dla pakietu Microsoft 365, zapewniające zabezpieczenie usług poczty elektronicznej, przestrzeni współdzielonej oraz komunikacji zespołowej, integrujące się bezpośrednio z chmurowymi usługami producenta systemu bez konieczności instalacji dodatkowych serwerów w infrastrukturze użytkownika.

1. Rozwiązanie zapewnia ochronę antymalware dla pakietu Microsoft 365, obejmując ochronę poczty email MS Exchange, usługi MS SharePoint, usługi MS OneDrive oraz MS Teams.
 2. Integruje się bezpośrednio z usługami Microsoft bez konieczności instalacji dodatkowych serwerów pośredniczących w środowisku klienta.
 3. Zarządzanie odbywa się przez chmurową konsolę dostępną przez przeglądarkę internetową.
 4. Konsola administracyjna umożliwia zarządzanie innymi produktami producenta, takimi jak endpoint protection, systemy EDR, mechanizmy zarządzania podatnościami – dostęp do funkcji zależny od typu licencji.
 5. Wyposażone w dashboard podsumowujący stan ochrony i objętych ochroną usług.
 6. Konfiguracja połączenia z usługami Microsoft odbywa się za pomocą kreatora.
 7. Umożliwia określenie, czy ochroną objęte są wszystkie konta pocztowe czy tylko wybrane przez administratora.
 8. Pozwala na tworzenie polityk konfiguracyjnych przypisywanych do poszczególnych usług.
 9. Ochrona poczty Microsoft Exchange obejmuje mechanizmy ochrony antymalware w czasie rzeczywistym dla wiadomości przychodzących.
 10. Obsługuje białe listy adresów email oraz domen.
-

11. Administrator może określić czas przechowywania obiektów w kwarantannie (1 miesiąc, 3 miesiące, 6 miesięcy, 1 rok).
12. Możliwość wyboru typów skanowanych plików oraz filtrowania po rozszerzeniach.
13. Obsługa skanowania wewnątrz plików archiwów.
14. Podejrzane pliki mogą być automatycznie detonowane w sandboxingu producenta.
15. W przypadku wykrycia zagrożenia możliwe działania: przeniesienie do kwarantanny, usunięcie wiadomości, usunięcie załącznika lub pozostawienie obiektu.
16. Obsługa powiadomień email o wykrytych zagrożeniach i personalizacja treści tych wiadomości.
17. Możliwość skanowania adresów URL pod kątem szkodliwej zawartości.
18. Wykrycie szkodliwego adresu URL pozwala na podjęcie działań: kwarantanna, usunięcie, zmiana tematu wiadomości, odlinkowanie.
19. Możliwość informowania administratora o wykrytych szkodliwych adresach URL.
20. Obsługa listy zaufanych i zablokowanych adresów URL.
21. Monitorowanie reguł poczty przychodzącej pod kątem podejrzanych działań (przenoszenie, usuwanie, przekazywanie emaili).
22. Monitorowanie chronionych kont email pod kątem wycieków danych oraz powiadamianie administratora.
23. W przypadku wycieku administrator uzyskuje szczegółowe informacje: adres email, źródło wycieku, forma wycieku hasła, data ostatniej zmiany hasła.
24. Mechanizm zarządzania kwarantanną umożliwiający administratorowi wgląd w szczegóły detekcji oraz możliwość usuwania i uwalniania obiektów z kwarantanny.
25. Możliwość generowania raportów dziennych, tygodniowych, miesięcznych w formacie PDF.
26. Skanowanie plików przesyłanych do objętej ochroną instancji MS SharePoint i MS OneDrive w ramach Microsoft 365.
27. Skanowanie wszystkich typów plików, plików o określonych rozszerzeniach oraz wykluczonych przez administratora.
28. Skanowanie plików archiwów i automatyczna detonacja podejrzanych obiektów w sandboxingu producenta.
29. W przypadku wykrycia zagrożenia na MS SharePoint i MS OneDrive możliwe podjęcie działań: kwarantanna, usunięcie lub brak akcji.
30. Możliwość skanowania obiektów dostępnych na platformie MS Teams w ramach organizacji.
31. Możliwość włączenia i wyłączenia automatycznego restartu w przypadku wymaganym przez instalację sterowników czy aplikacji.
32. Rozwiązanie monitoruje zmiany w konfiguracji ochrony i rejestruje je w logach audytowych.
33. Możliwość ręcznego przeskanowania obiektów na żądanie administratora.



34. Rozwiązanie może współpracować z dodatkowymi systemami klasy SIEM w celu lepszej analizy incydentów bezpieczeństwa.
35. Obsługa różnych poziomów uprawnień użytkowników w konsoli administracyjnej.
36. Możliwość definiowania harmonogramu skanowania dla różnych obszarów ochrony.
37. Automatyczne aktualizacje mechanizmów ochrony, baz sygnatur oraz silnika skanującego.
38. Obsługa powiadomień push dla administratorów w przypadku krytycznych zagrożeń.
39. Możliwość wdrożenia dodatkowych mechanizmów ochrony w zależności od poziomu licencji.
40. Możliwość integracji z narzędziami analityki zagrożeń producenta.
41. Pełne wsparcie dla środowisk hybrydowych Microsoft 365.
42. Możliwość eksportowania logów detekcji i działań administracyjnych do formatu XML.
43. Mechanizm wykrywania anomalii w ruchu sieciowym w kontekście przesyłania plików do chronionych zasobów.
44. Automatyczna synchronizacja polityk ochrony między różnymi usługami Microsoft 365.
45. Możliwość korzystania z zabezpieczeń wielopoziomowych, w tym dodatkowej autoryzacji administratora przy podejmowaniu krytycznych działań.

- Oferowany produkt musi znajdować się w kwadracie 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 4,6
(załączyć wydruk)

Certyfikaty i standardy –
dokumenty załączyć wraz
z ofertą lub na wezwanie
Zamawiającego

- Oferowany produkt musi znajdować się w kwadracie 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)

system musi posiadać normy i certyfikaty:

- OPSWAT (dla EDR/XDR na poziomie min. Platinum),
- AV-TEST (ochrona w 2023 na poziomie min.6)
- Rozwiązanie wyróżnione przez AV-Test jako "najlepszy wykonawca" w testach Advanced EDR Test 2024 na podstawie scenariuszy cyberataków - APT18, TA577, Turla i FIN6

-
- › producent systemu lub autoryzowany dystrybutor producenta musi posiadać certyfikat ISO 9001 oraz 27001 oraz usługi związane z cyberbezpieczeństwem.
 - › Producent systemu lub autoryzowany dystrybutor producenta musi posiadać certyfikację ISAE 3000 assurance-based SOC 2 Type 2, potwierdzającymi zaawansowane zarządzanie bezpieczeństwem informacji
 - › Producent systemu lub autoryzowany dystrybutor producenta musi być aktywnym członkiem Cloud Security Alliance, co podkreśla zaangażowanie w rozwój najlepszych praktyk dla cybernetycznych środowisk chmurowych.
 - › Zespół reagowania na incydenty od producenta systemu lub autoryzowany dystrybutor producenta musi posiadać certyfikację CREST i NCSC, które potwierdzają zdolność do skutecznego reagowania na zagrożenia cybernetyczne.
 - › Producent lub oferowany produkt/rozwiązanie musi być uznane za lidera (np. "Champion" w raportach Software Reviews Emotional Footprint) w co najmniej jednej kategorii, takich jak zarządzanie punktami końcowymi (Endpoint Management) lub zarządzanie podatnościami (Vulnerability Management).
-

**Rozszerzone wsparcie
serwisowe**

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 przez okres do 30.06.2026 r.

- Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich.
- Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 oraz 27001 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:

- Oświadczenie 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.
-

7. Oprogramowanie SIEM (Security Information and Event Management)

Nazwa	Minimalne wymagania dla oprogramowania
Typ	Oprogramowanie SIEM (Security Information and Event Management)
Wymagania ogólne	<p>Platforma przeciwdziałania cyberzagrożeniom, oferująca możliwość wykrywania i obsługi zdarzeń, incydentów oraz podatności, spełniająca wymagania minimalne:</p> <ol style="list-style-type: none"> 1. Przedmiotem zamówienia jest zakup, dostarczenie i wdrożenie w środowisku informatycznym Zamawiającego systemu przeciwdziałającemu cyberzagrożeniom, umożliwiającego ich wykrywanie przy wsparciu mechanizmów uczenia maszynowego oraz zapewniającego automatyzację i orkiestrację ich obsługi. 2. System musi umożliwić odbieranie logów wygenerowanych przez systemy zabezpieczeń, systemy sieciowe, systemy operacyjne i aplikacje następującymi protokołami: Syslog, TLS syslog, NetFlow, Windows Event Forwarding. 3. Logi pozyskiwane z systemów Microsoft Windows nie mogą wymagać instalowania dedykowanego oprogramowania bezpośrednio na tych systemach. 4. System musi posiadać wbudowane mechanizmy zapewniające możliwość pobierania zdarzeń poprzez wykorzystanie RestFull-API, sterownika ODBC, agenta do czytania plików płaskich, protokołów IMAPS, POP3S, MAPI do pobierania wiadomości ze skrzynek poczty elektronicznej oraz obsługi zapytań WQL w ramach protokołu WMI; 5. System powinien pozwalać na pracę z logami zdarzeń jednoliniowych oraz wieloliniowych. 6. System musi być wyposażony w mechanizmy normalizacji (parsowania) pozyskanych zdarzeń umożliwiające ich podział na poszczególne pola, na podstawie których może odbywać się dalsze przetwarzanie oraz wyszukiwanie ich w systemie. 7. System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, obejmującą zmianę wartości tych pól lub dodanie nowych w oparciu o ich wartości lub wzorzec wyszukiwania. Cały proces musi odbywać się na bieżąco na etapie rejestrowania danych w systemie. 8. Proces normalizacji musi wspierać następujące typy składni: CEF, LEEF, URI, SYSLOG (zgodny z RFC 3164) i automatycznie tworzyć na ich podstawie pola i ich wartości zgodne z zasadami określonymi przez te składnie. Parsowanie powyższych składni nie może być realizowane za pomocą wyrażeń regularnych. 9. Normalizacja musi umożliwiać automatyczne nadawanie kategorii zdarzeń w formie nowych pól, np.: logowanie, wylogowanie, zmiana uprawnień, błąd konfiguracji, wykryte skanowanie systemu czy

zablokowany malware.

10. Normalizacja logów musi posiadać mechanizm geolokalizacyjny, pozwalający na wzbogacenie pól o nazwę lub kod kraju korzystając z wbudowanej w produkt bazy.

11. System musi posiadać predefiniowany zestaw parserów oraz umożliwiać ich wersjonowanie, aby po wgraniu nowej wersji parsera, w razie przypadku, gdy będzie to konieczne przywrócić jedną z poprzednich wersji.

12. System musi być wyposażony w graficzny interfejs do tworzenia dodatkowych reguł normalizacji (parserów) dla zdarzeń z niestandardowych źródeł danych, w oparciu o następujące składnie: CEF, LEEF, URI, XML, JSON, SYSLOG, REGEX. System musi umożliwiać zastosowanie wszystkich typów składni dla pojedynczego zdarzenia, przykładowo pole „msg” znormalizowane automatycznie według standardu CEF powinno mieć możliwość dalszej normalizacji np.: zgodnej z URI lub REGEX.

13. Proces normalizacji musi posiadać możliwość optymalizacji, poprzez automatyczny dobór odpowiedniego parsera dla źródła logów w zależności od składni, w której te logi są przesyłane. Przykładowo, jeżeli logi są przesyłane w standardzie CEF system dobierze odpowiedni parser, w przypadku, gdy źródło zmieni format generowania zdarzeń na LEEF system musi automatycznie zmienić parser bez ingerencji operatora.

14. System musi rejestrować i przechowywać pozyskane logi w postaci surowej (RAW) oraz znormalizowanej.

15. System musi być wyposażony w graficzny interfejs umożliwiający określenie miejsca składowania logów (wskazania właściwego repozytorium logów) w zależności od zawartości tych logów, gdzie reguły przekierowania muszą umożliwiać definiowanie warunków po wszystkich sparsowanych polach. Przykładowo jeżeli w zdarzeniu znajduje się informacja o danych poufnych to zdarzenie to zostanie przekierowane do repozytorium A, natomiast w przypadku gdy tej informacji nie będzie to zdarzenie zostanie przekierowane do repozytorium B.

16. Każde z repozytorium logów musi mieć możliwość definiowania własnych zasad retencji uwzględniających zdefiniowanie okresu przechowywania lub ilości miejsca przeznaczonego na dane repozytorium. Dla każdego z repozytorium w przypadku jego zapełnienia musi być możliwa konfiguracja, która zapewni automatyczne przeniesienie logów do archiwum lub umożliwi ich nadpisanie.

17. System musi umożliwiać fizyczne rozdzielenie repozytoriów logów pobieranych z systemów informatycznych od repozytoriów zdarzeń generowanych w ramach systemu, w tym m.in. odseparowanie zdarzeń korelacyjnych na oddzielne repozytoria danych składowane na osobnych serwerach i dedykowanych do tego celu zasobów dyskowych od wszelkich

repozytoriów logów.

18. Ze względu na możliwość wygenerowania dużej ilości danych przez algorytmy uczenia maszynowego system musi mieć możliwość rozdzielania ich składowania na osobny serwer i dedykowane zasoby dyskowe.

19. System musi umożliwiać automatyczną archiwizację danych na zewnętrzne repozytoria danych w postaci skompresowanej.

20. System musi zapewnić mechanizmy bezpieczeństwa dla danych przechowywanych w repozytoriach uniemożliwiające ich nieautoryzowaną modyfikację oraz zapewnić operatorom mechanizmy weryfikacyjne integralność danych.

21. System musi udostępniać możliwość konfiguracji automatycznego odrzucenia logów niezawierających istotnych dla zamawiającego informacji. Definiowanie, które logi mają zostać odrzucone i niezapisane w repozytorium logów musi być realizowane za pomocą reguł, które pozwolą zdefiniować warunki po wszystkich sparsowanych polach.

22. System musi być wyposażony w graficzny interfejs umożliwiający przeglądanie i przeszukiwanie zarejestrowanych zdarzeń w formie znormalizowanej i pierwotnej. Interfejs musi prezentować wyniki wyszukiwania z zastosowaniem filtrów opartych na wartościach pól, złożonych wyrażeniach logicznych, wskazaniach zakresu czasowego i źródła danych. Interfejs wyszukiwania musi umożliwiać zapisywanie zapytań z możliwością ich ponownego wykorzystania w przyszłości. Tworzenie zapytań musi być możliwe poprzez bezpośrednie wskazanie pola zdarzenia za pomocą wskaźnika myszy i dodanie tego pola do filtra wyszukiwania, wraz z określeniem warunków wyszukiwania przez wyrażenie logiczne.

23. System musi zapewniać możliwość utrzymywania dokumentacji sieci, systemów oraz usług, umożliwiającej na gromadzenie i edycję danych istotnych w kontekście oceny generowanych przez system zdarzeń bezpieczeństwa.

24. Elektroniczna dokumentacja musi posiadać możliwość wizualizacji w formie interaktywnej mapy sieci, gdzie na pierwszym planie będą widoczne urządzenia zabezpieczeń, strefy bezpieczeństwa oraz połączenia sieciowe wskazujące jakie mechanizmy zabezpieczeń chronią poszczególne strefy bezpieczeństwa. „Kliknięcie” na dowolny z obiektów na pierwszym planie musi pozwolić na podgląd oraz edycję parametrów tego obiektu. Przykładowo po kliknięciu na strefę bezpieczeństwa musi istnieć możliwość definiowania komputerów należących do tej strefy, ich adresacji oraz innych z nimi związanych parametrów.

25. System musi umożliwiać prezentację danych zgromadzonych w elektronicznej dokumentacji również w formie tabelarycznej.

26. System musi pozwalać na definiowanie własnych parametrów dla wszystkich typów obiektów zgromadzonych w elektronicznej dokumentacji sieci, np.: poziom krytyczności systemów oraz usług.

27. System musi umożliwiać generowanie elektronicznej dokumentacji sieci i systemów w sposób automatyczny na podstawie dostarczonych przez producenta reguł wykrywania oraz edytora graficznego pozwalającego utworzyć dodatkowe reguły.

28. System musi zawierać narzędzia służące do ustalania wrażliwych zbiorów informacji, jakie są narażone w razie incydentu bezpieczeństwa. Ma umożliwiać definiowanie własnego schematu klasyfikacji danych w organizacji (np. własność intelektualna, dane osobowe, dane finansowe) oraz zapewnić wyszukiwanie lokalizacji zasobów teleinformatycznych, gdzie znajdują się dane określonej kategorii ze wskazaniem ich na graficznej mapie systemu teleinformatycznego.

29. Definiowanie reguł wykrywania musi bazować na sparsowanych polach oraz wyszukanych zależnościach między różnymi zdarzeniami z wielu źródeł oraz po aktywacji automatycznie uzupełnić elektroniczną dokumentację o następujące informacje:

- a) nowe zasoby wykryte w sieci,
- b) typy wykrytych zasobów (np.: serwer lub stacja robocza),
- c) zastosowane na nich zabezpieczenia,
- d) usługi z którymi się komunikują,
- e) nowe usługi wykryte na zasobie
- f) komunikację do usług wykrytych na zasobie.

30. System musi umożliwiać uwiarygodnianie uzyskiwanych informacji na bazie wartości progowych osiągniętych w zadanej jednostce czasu i dopiero po ich uwiarygodnieniu uzupełniać automatycznie elektroniczną dokumentację.

31. System powinien posiadać zestaw predefiniowanych reguł do automatycznego uzupełniania elektronicznej dokumentacji, których uruchomienie będzie automatycznie aktualizować elektroniczną dokumentację bez ingerencji operatora.

32. Interfejs interaktywnej mapy sieci musi posiadać mechanizm definiowania dozwolonej komunikacji sieciowej dla każdego zasobu IT który został zdefiniowany w elektronicznej dokumentacji oraz nazwę usługi, której ta komunikacja dotyczy.

33. System musi posiadać wbudowaną bazę wskaźników kompromitacji, która umożliwi zbieranie, przechowywanie oraz przypisywanie wskaźników kompromitacji (IoC) do incydentów. Baza powinna obsługiwać protokół TLP w wersji 2.0 oraz obsługiwać następujące typy wskaźników:

- a) fqdn,
- b) e-mail,
- c) nazwa pliku,
- d) ścieżka do pliku,
- e) hash,
- f) adres IP,

- g) klucz rejestru,
- h) cmd.

34. System musi umożliwiać synchronizację wskaźników kompromitacji (IOC) z platformami dostępnymi publicznie. Wymagane jest aby produkt posiadał gotowy mechanizm pobierania wskaźników z platformy MISP (<https://www.misp-project.org/>).

35. System musi umożliwiać definiowanie list referencyjnych zarówno z jedną wartością jak i łączących unikalne wartości w pojedynczym wierszu (np: obraz pliku, hash, nazwa procesu).

36. Listy referencyjne muszą mieć możliwość synchronizacji z listami publikowanymi publicznie (np.: „Malicious IPs”, „Malicious domain” czy „Tor Exit Nodes”).

37. System musi być zintegrowany z usługą katalogową Microsoft Active Directory celem pobrania informacji o poświadczeniach oraz atrybutach użytkowników i komputerów zarejestrowanych w domenie. Minimum to: nazwa komputera wraz z systemem operacyjnym, nazwa użytkownika, login, e-mail, przynależność do grup, przełożonego, jednostkę organizacyjną oraz listę kont uprzywilejowanych.

38. System powinien umożliwiać zdefiniowanie struktury organizacyjnej oraz zapewniać możliwość jej synchronizacji z usługą katalogową Microsoft Active Directory.

39. System musi umożliwiać analizę konfiguracji systemów IT poprzez ich skanowanie bezpośrednio w ramach mechanizmów dostępnych w samym rozwiązaniu oraz poprzez integrację ze skanerami podatności. Oczekiwanym wynikiem analizy jest lista niezgodności, (np: czy na zasobie jest ustawione wymuszanie zmiany haseł w zadanym okresie czasu).

40. System powinien posiadać zestaw predefiniowanych reguł weryfikacji konfiguracji zasobów IT.

41. System musi zawierać mechanizm integracji ze skanerami podatności co najmniej trzech producentów. W ramach integracji system musi mieć możliwość uruchamiania skanowania podatności, importowania jego wyników zawierających listę podatności i ich atrybuty oraz możliwość kasowania ze skanera zaimportowanych wcześniej skanów. Wszystkie powyższe operacje muszą być konfigurowalne z poziomu graficznego interfejsu systemu.

42. Rozwiązanie musi zawierać mechanizm pasywnej analizy podatności, obejmującej systemy IT uzupełnione o informację zgodne z słownikiem CPE (ang. Common Platform Enumeration), umożliwiającą import wykrytych podatności zasobu do systemu z publicznie dostępnej bazy CVE (ang. Common Vulnerabilities and Exposures) i dalszą obsługę tych podatności w systemie.

43. System musi umożliwiać mapowanie zdarzeń bezpieczeństwa na poszczególne techniki z bazy wiedzy MITRE ATT&CK® oraz zapewniać

mechanizmy filtrowania zdarzeń po tych technikach oraz wyświetlania szczegółów związanych z daną techniką, w szczególności:

- a) id techniki,
- b) taktykę,
- c) platformy których dotyczy,
- d) potencjalne źródła,
- e) opis zagrożenia,
- f) mityzację,
- g) sposób detekcji,
- h) referencje.

44. System w swoim działaniu musi korzystać z wbudowanych algorytmów uczenia maszynowego dla celów zbudowania i utrzymywania modelu danych użytkowników i komputerów.

45. Modele zachowania użytkowników (UBA) i komputerów (EBA) muszą być tworzone automatycznie na bazie zdarzeń historycznych ze skonfigurowanego (wskazanego) okresu lub zdefiniowanej ilości zdarzeń wymaganych do ukończenia procesu nauczania. Algorytm nauczania musi mieć możliwość konfiguracji sposobu odrzucania wartości skrajnych mogących wpłynąć negatywnie na wyniki procesu nauczania oraz umożliwić odrębne uczenie w ramach zdefiniowanych zakresów czasowych (np.: rozdzielenie zdarzeń do nauczania w godzinach pracy od zdarzeń po godzinach pracy).

46. System musi posiadać zestaw predefiniowanych i konfigurowalnych reguł do automatycznego przyporządkowania użytkowników i zasobów do właściwych profili nauczania, reguły te muszą zapewnić minimum:

- a) rozdzielenie procesu nauczania zachowania użytkowników uprzywilejowanych od użytkowników nieuprzywilejowanych,
- b) rozdzielenie procesu nauczania zachowania stacji roboczych od serwerów,
- c) rozdzielenie serwerów świadczących usługi w sieci Internet od serwerów świadczących usługi lokalnie w organizacji,
- d) rozdzielenie procesu nauczania serwerów należących do domeny od pozostałych serwerów.

47. System uczenia maszynowego musi posiadać wbudowane mechanizmy nie wymagające żadnej dodatkowej konfiguracji, które po zakończeniu procesu nauki umożliwią detekcję anomalii zachowania użytkowników oraz zasobów (UEBA).

48. Wykryte przez mechanizmy uczenia maszynowego anomalie muszą generować zdarzenia, zawierające minimum informację o użytkowniku lub adresie IP na którym została wykryta anomalia oraz wykorzystany algorytm. System musi umożliwiać wykorzystanie tych zdarzeń w celu dalszej korelacji.

49. System musi pozwalać na zautomatyzowaną ocenę wpływu incydentu

bezpieczeństwa IT na działalność organizacji względem zagrożeń natury informatycznej (np: utrata wizerunku, związana z zagrożeniem przełamania zabezpieczeń serwera webowego organizacji dostępnego z sieci Internet).

50. System musi zapewniać kontrolę dostępu do systemu i oferowanych przez niego funkcjonalności w oparciu o zdefiniowane role.

51. Dostarczone rozwiązanie musi umożliwiać gromadzenie i korelacje zdarzeń przesyłanych lub pobieranych z innych systemów. Przez korelację zdarzeń rozumie się automatyczne, realizowane na bieżąco wyszukiwanie zależności między różnymi zdarzeniami z wielu źródeł oraz ich agregację.

52. System musi posiadać interfejs graficzny do tworzenie własnych reguł korelacyjnych odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie. Korelacja musi odbywać się na bieżąco na etapie rejestrowania danych w systemie a mechanizm tworzenie reguł musi uwzględniać:

- a) sparsowane pola oraz ich wartości,
- b) listy referencyjne,
- c) atrybuty użytkowników z Active Directory,
- d) atrybuty komputerów z Active Directory,
- e) bazę wskaźników kompromitacji (IOC),
- f) informacje z elektronicznej dokumentacji,
- g) anomalie w zachowaniu użytkowników (UBA),
- h) anomalie w zachowaniu zasobów (EBA),
- i) podatności na zasobach,
- j) wyniki analizy konfiguracji,
- k) techniki MITRE ATT&CK®,

53. Reguły korelacyjne bazujące na sparsowanych polach i ich wartościach muszą umożliwić:

- a) wykrycie dowolnej treści w logach,
- b) wykrycie zmiany jednego z kilku pól,
- c) wykrycie zaniku wiadomości,
- d) wykrycie nowej wartości pola w zadanym okresie czasu,
- e) wykrycie incydentu będącego pochodną zdarzeń występujących w określonej kolejności,
- f) wykrycie zdefiniowanej ilości przesłanych danych w zadanym okresie czasu,
- g) wykrycie chwilowego wzrostu ilości przesłanych danych (tzw. peek) w stosunku do całkowitej ilości przesłanych danych w zadanym okresie czasu,
- h) wykrycie sumarycznego wzrostu przesłanych danych w zdefiniowanej strefie bezpieczeństwa,
- i) wykrycie zdefiniowanej ilości przesyłanych pakietów w zadanym okresie czasu,
- j) wykrycie chwilowego wzrostu (tzw. peek) w stosunku do ilości przesyłanych pakietów w zadanym okresie czasu,

k) wykrycie sumarycznego wzrostu ilości pakietów przesyłanych w zdefiniowanej strefie bezpieczeństwa,

l) wykrycie ilości uruchomionych procesów w zadanym okresie czasu,

m) wykrycie skanowania portów.

54. Reguły korelacyjne bazujące na listach referencyjnych muszą umożliwić:

a) wykrycie wystąpienia wartości pola na wybranej liście,

b) wykrycie niewystępowania wartości pola na wybranej liście,

c) wykrycie wystąpienia pary wartości na wybranej liście^[11]_{SEP} (np.: proces i obraz pliku z którego został uruchomiony),

d) wykrycie niewystąpienia pary wartości na wybranej liście

e) np.: nazwa użytkownika wraz aplikacją z którą się wcześniej nie łączył).

55. Reguły korelacyjne wykorzystujące atrybuty użytkowników z Active Directory muszą umożliwić:

a) wykrycie czy zdarzenie pochodzi od użytkownika posiadającego konto w Active Directory,

b) wykrycie czy zdarzenie pochodzi od użytkownika posiadającego uprzywilejowane konto w Active Directory,

c) wykrycie czy zdarzenie pochodzi od użytkownika podszywającego się pod konto użytkownika Active Directory (np.: którego e-mail zdefiniowany w Active Directory różni się od e-maila ze zdarzenia mimo, zgodności pozostałych atrybutów konta).

d) wykrycie czy zdarzenie pochodzi od użytkownika należącego do wybranej grupy w Active Directory (np.: Domain Admins),

e) wykrycie czy zdarzenie pochodzi od użytkownika nie należącego do wybranej jednostki organizacyjnej.

56. Reguły korelacyjne wykorzystujące atrybuty komputerów z Active Directory muszą umożliwić:

a) wykrycia czy zdarzenie pochodzi z komputera należącego do domeny Active Directory,

b) wykrycia czy zdarzenie pochodzi z komputera z systemem operacyjnym zdefiniowanym w Active Directory,

c) wykrycia czy zdarzenie pochodzi z komputera z wybranej jednostki organizacyjnej.

57. Reguły korelacyjne wykorzystujące bazę wskaźników kompromitacji (IOC) muszą umożliwić:

a) wykrycie czy źródłowy adres IP nie jest oznaczony w systemie jako wskaźnik kompromitacji;

b) wykrycie czy HASH występujący w zdarzeniu nie jest oznaczony w systemie jako wskaźnik kompromitacji;

c) wykrycie czy docelowa nazwa hosta (FQDN) nie jest oznaczona w systemie jako wskaźnik kompromitacji;

58. Reguły korelacyjne wykorzystujące informacje z elektronicznej

dokumentacji muszą umożliwić:

- a) wykrycie połączenia z serwera do stacji roboczej w przypadku braku informacji o rodzajach zasobu w korelowanym zdarzeniu,
- b) wykrycie połączenia do usługi przez nieautoryzowanego użytkownika,
- c) wykrycie nieautoryzowanej usługi na serwerze,
- d) wykrycie nieautoryzowanego połączenia do usługi na serwerze,
- e) wykrycie nieautoryzowanego połączenia z serwera usług,
- f) wykrycie nieautoryzowanego połączenia do sieci Internet.

59. Reguły korelacyjne wykorzystujące anomalie w zachowaniu użytkowników (UBA) muszą umożliwić:

- a) wykrycie anomalii ilościowej związanej z kontem użytkownika wskazującej na potencjalny atak (D)DoS lub próbę propagacji złośliwego oprogramowania,
- b) wykrycie anomalii związanej ze zmianą zachowania na koncie użytkownika, wskazującej na potencjalny atak APT/Ransomware,
- c) wykrycie różnych typów anomalii na koncie użytkownika wskazujących na możliwe przejęcie konta użytkownika przez cyberprzestępcę lub złośliwe oprogramowanie,
- d) wykrycie anomalii związanych z logowaniami użytkowników w ramach sesji VPN.

60. Reguły korelacyjne wykorzystujące anomalie w zachowaniu zasobów (EBA) muszą umożliwić:

- a) wykrycie anomalii ilościowej związanej z komputerem wskazującej na potencjalny atak (D)DoS lub próbę propagacji złośliwego oprogramowania,
- b) wykrycie anomalii związanej ze zmianą zachowania komputera, wskazującej na potencjalny atak APT/Ransomware,
- c) wykrycie różnych typów anomalii na komputerze, wskazujących na możliwe przejęcie komputera przez cyberprzestępcę lub złośliwe oprogramowanie,
- d) wykrycie anomalii związanych z procesami uruchamianymi na serwerach.

61. Reguły korelacyjne wykorzystujące podatności na zasobach muszą umożliwić:

- a) wykrycie skanowania portów z zasobu posiadającego krytyczne podatności,
- b) wykrycie wielokrotnych prób połączeń do zasobu posiadającego krytyczne podatności,
- c) wykrycie zdarzeń o wysokim „severity” na zasobach posiadających krytyczne podatności,
- d) wykrycie zdarzeń o wysokim „severity” do zasobów posiadających krytyczne podatności.

62. Reguły korelacyjne wykorzystujące wyniki analizy konfiguracji muszą

pozwalać na:

- a) wykrycie wielokrotnych prób nieudanego logowania do komputera, umożliwiające ustawienie hasła zawierającego mniej niż 14 znaków,
- b) wykrycie wielokrotnych prób nieudanego logowania do komputera, który umożliwia tworzenie haseł niespełniających następujących kryteriów złożoności: duża litera, mała litera, liczba, znak specjalny.

63. Reguły korelacyjne wykorzystujące technikach MITRE ATT&CK® muszą umożliwić:

- a) wykrycie zdefiniowanej ilości technik w zdarzeniach dotyczących wybranego hosta identyfikowanego po nazwie lub adresie IP,
- b) wykrycie zdefiniowanej ilości zdarzeń w ramach jednej techniki dotyczących wybranego hosta identyfikowanego po nazwie lub adresie IP,
- c) wykrycie incydentu będącego pochodną zdarzeń z technik występujących w określonej kolejności na wybranym adresie IP lub zasobie identyfikowanym po nazwie.

64. Pojedyncza reguła korelacyjna musi mieć możliwość wzajemnej korelacji wszystkich powyższych mechanizmów umożliwiając, m.in.:

- a) wykrycie anomalii na koncie uprzywilejowanym użytkownika,
- b) wykrycie ruchu z serwera domenowego do skompromitowanej domeny wykazanej w liście referencyjnej,
- c) wykrycie wielu typów anomalii na komputerze z krytyczną podatnością,
- d) wykrycie złośliwego oprogramowania na bazie wskaźnika kompromitacji stanowiącego HASH procesu, z którego następuje nieautoryzowana próba dostępu do usługi,
- e) wykrycie wielokrotnych prób nieudanego logowania na konto uprzywilejowane, którego hasło nie spełnia następujących kryteriów złożoności: duża litera, mała litera, liczba, znak specjalny.

65. System przy wykorzystaniu reguł kwalifikacyjnych musi automatycznie selekcjonować zdarzenia wygenerowane przez reguły korelacyjne, wybierając do obsługi tylko zdarzenia spełniające zdefiniowane warunki (tzw. zdarzenia w obsłudze). Pozostałe zdarzenia powinny być wykluczone z obsługi, ale równocześnie pozostać w systemie, zachowując możliwość ich obsługi na żądanie operatora. Zastosowane reguły selekcji zdarzeń do obsługi muszą równocześnie umożliwiać wyliczenie właściwego dla nich priorytetu. Reguły selekcji i priorytetyzacji zdarzeń w obsłudze muszą uwzględniać:

- a) sparsowane pola oraz ich wartości,
- b) atrybuty użytkowników z Active Directory,
- c) atrybuty komputerów z Active Directory,
- d) informacje z elektronicznej dokumentacji.

66. Zdarzenia w obsłudze, muszą obsługiwać opcje grupowania polegającą na tym, iż każde kolejne zdarzenie wynikające z reguł korelacyjnych,

spełniających tą samą regułę w zdefiniowanym okresie czasu będzie automatycznie dodawane do tego samego zdarzenia w obsłudze. Grupowanie musi odbywać się po:

- a) adresie IP,
- b) koncie domenowym użytkownika,
- c) strefie bezpieczeństwa,
- d) zakresie adresów IP.

67. Obsługiwane zdarzenia muszą posiadać zestaw predefiniowanych scenariuszy obsługi (ang. Playbook) oraz pozwalać na tworzenie własnych scenariuszy obsługi oraz ich edycję z poziomu interfejsu graficznego. System musi wspierać funkcję „Drag and Drop” umożliwiającą m.in. na zamianę kolejności realizacji poszczególnych kroków poprzez ich przenoszenie za pomocą myszki komputerowej.

68. System musi potrafić wczytywać informacje z innych systemów bezpieczeństwa i traktować je, jako elementy/dowody dla zdarzeń w obsłudze.

69. Zdarzenia w obsłudze muszą umożliwiać gromadzenie dodatkowych informacji wygenerowanych podczas ich obsługi oraz umożliwiać do nich dostęp bezpośrednio z poziomu tych zdarzeń, obejmujących m.in.

- a) wszystkie skorelowane zdarzenia,
- b) korespondencja pocztowa,
- c) załączniki z próbkami lub dowodami,
- d) wskaźniki kompromitacji (IoC),
- e) informacje pozyskane z innych systemów.

70. System powinien posiadać możliwość rejestracji zgłoszeń przez stronę webową udostępnianą przez system dla użytkowników z innych jednostek organizacyjnych oraz umożliwić ich przekształcenie w zdarzenia w obsłudze z możliwością rozdzielania uprawnień dla obu tych czynności. System musi umożliwiać scenariusz, gdzie użytkownik zgłasza incydent, który zanim zostanie zakwalifikowany do dalszej obsługi musi zostać autoryzowany przez uprawnionego do tego celu operatora.

71. Dla obsługiwanych zdarzeń system powinien umożliwiać automatyczne pozyskanie informacji z innych systemów oraz bazując na uzyskanej od nich odpowiedzi automatycznie zmieniać ich status, np.: na podstawie pozyskanego wskaźnika kompromitacji (IoC) zmienić status zdarzenia na incydent bezpieczeństwa.

72. Dla zdarzeń w obsłudze dotyczących ruchu sieciowego pomiędzy źródłem a celem transmisji, system musi automatycznie wyznaczyć wektor zagrożenia i zaprezentować go w formie graficznej, na której będą zwizualizowane następujące dane:

- a) identyfikację celu i źródła zagrożenia,
- b) nazwę oraz adres IP źródła zagrożenia,
- c) rodzaj zasobu będący źródłem zagrożenia np.: urządzenie mobilne,

stacja robocza,

- d) lokalizację z której pochodzi zagrożenie np.: Internet,
- e) strefę bezpieczeństwa z której pochodzi zagrożenie,
- f) prawdopodobieństwo zagrożenia ze strefy stanowiącej jego źródło,
- g) wszystkie urządzenia sieciowe chroniące cel zagrożenia i zastosowane na nich mechanizmy zabezpieczeń (np.: Application Control, Network Firewall, User Identification),
- h) nazwę oraz adres IP celu zagrożenia,
- i) zabezpieczenia lokalne chroniące cel zagrożenia,
- j) strefę bezpieczeństwa w której znajduje się cel zagrożenia.

73. Dla każdego wektora zagrożenia system musi automatycznie wyliczać efektywność zastosowanych mechanizmów zabezpieczeń, pozwalającą w ramach wbudowanych w system edytowalnych reguł ocenić prawdopodobieństwo materializacji się cyberzagrożeń. Na przykład: dla serwera webowego dostępnego ze strefy Internet zagrożenie przełamania zabezpieczeń ma niskie prawdopodobieństwo w przypadku gdy jest on zabezpieczony przez rozwiązanie klasy WAF (Web Application Firewall).

74. Dla wyznaczonych w czasie obsługi wektorów zagrożeń przedstawiane wyniki szacowania prawdopodobieństwa muszą być zwizualizowane operatorowi w formie listy zagrożeń z oszacowanymi dla nich poziomami. Przykładowe wartości z listy to: wysoki poziom prawdopodobieństwa włamania na serwer oraz średni poziom prawdopodobieństwa infekcji złośliwym oprogramowaniem.

75. Dla zdarzeń w obsłudze zarówno w odniesieniu do adresów źródłowych jak i docelowych system musi umożliwiać operatorowi uzupełnianie pozyskanych informacji, dotyczących zarówno źródła jak i celu zagrożenia w następującym zakresie:

- a) nazwy zasobu,
- b) rodzaju zasobu,
- c) ważności zasobu dla organizacji,
- d) rodzaj przetwarzanych informacji,
- e) usług, które ten zasób świadczy,
- f) lokalizację użytkowników, którzy z niego korzystają,
- g) usługi z których zasób korzysta.

76. System powinien mieć logikę automatycznego przypisywania zdarzeń zakwalifikowanych do obsługi wraz z powiadomieniem operatora, któremu zostało ono przydzielone (min. e-mail, SMS). Kwalifikacja musi uwzględniać m.in. dostępność operatora, jego obciążenia oraz parametry zasobu którego dotyczy zdarzenie, typ zasobu (np.: serwer lub stacja robocza), jego krytyczność oraz realizowane z jego udziałem usługi z katalogu usług. Na przykład: zdarzenie przypisane do krytycznego serwera realizującego usługę DNS powinny trafić do innego operatora niż zdarzenia dotyczące pozostałych serwerów usług sieciowych.

77. Zdarzenia w obsłudze muszą obejmować statusy właściwe dla procesu obsługi zdarzeń, minimum to:

- a) nowe zdarzenie – jako zdarzenie zarejestrowane w systemie,
 - b) segregacja – segregacja i kwalifikacja zdarzeń,
 - c) incydent bezpieczeństwa – zdarzenie zakwalifikowane jako incydent bezpieczeństwa,
 - d) fałszywy alarm – zdarzenie zakwalifikowane jako fałszywy alarm,
 - e) zdarzenie obsłużone – zdarzenie, które zostało obsłużone w systemie.
- System musi także zapewniać możliwość ich edycji w zakresie dodawania (np.: wydzielenie z segregacji statusu kwalifikacji) lub usuwania statusów oraz konfiguracji przejść pomiędzy nimi. Przykładowo: umożliwiać przejście ze statusu „incydent bezpieczeństwa” do statusu „zdarzenie zamknięte”, ale zablokować zmianę ze statusu „incydent bezpieczeństwa” na status „fałszywy alarm”.

78. System powinien umożliwiać definiowanie parametrów SLA dla wszystkich statusów obsługi zdarzeń oraz dokonywać automatycznego pomiaru tych czasów i ich weryfikacji względem zdefiniowanych wartości. Wyniki pomiarów czasów SLA powinny być stale aktualizowane i prezentowane na liście zdarzeń zakwalifikowanych do obsługi.

79. System musi umożliwiać grupowanie manualne dla zdarzeń w obsłudze, których powiązanie zostanie wykryte przez operatorów w trakcie obsługi i umożliwiać zgrupowanie ich do jednego zdarzenia. Zgrupowane zdarzenia muszą być podrzędne w stosunku do zdarzenia z którym są grupowane oraz synchronizować z nim statusy. Dla zdarzeń przetwarzanych przez operatora, zmiana statusu głównego zdarzenia musi wymusić zmianę statusu pozostałych. Na przykład: zamknięcie nadrzędnego zdarzenia musi zamykać też wszystkie podrzędne. Na liście zdarzeń oraz w podglądzie każdego zdarzenia powinna się pojawić informacja o zdarzeniach z nim powiązanych.

80. Obsługiwane zdarzenia muszą zapewniać historyczność, obejmującą wszystkie aktywności realizowane w ramach poszczególnych statusów. Aktywności muszą uwzględniać zarówno akcje realizowane w ramach samego systemu (m.in. zmiana priorytetu czy przekazanie zdarzenia innemu operatorowi). Dodatkowo historia musi też zawierać wszelkie komentarze wpisywane przez operatorów.

81. Dla każdego obsługiwanego zdarzenia system powinien udostępniać automatyczny raport obejmujący wszystkie podjęte działania wraz z komentarzami operatorów.

82. W ramach obsługi zdarzeń system musi automatycznie porównywać wskaźniki kompromitacji zidentyfikowane w bieżącym zdarzeniu względem wszystkich wskaźników pozyskanych do tej pory w ramach dotychczasowej obsługi. Na przykład: jeżeli w obsługiwanym zdarzeniu znajduje się FQDN oraz HASH to system musi automatycznie porównać je ze wszystkimi

wskaźnikami typu FQDN oraz HASH, zebranymi do tej pory w obsługiwanych zdarzeniach bez względu na to czy wskaźniki te zostały wpisane ręcznie czy zostały pozyskane automatycznie z innych systemów.

83. System powinien pozwalać, przy użyciu języków skryptowych ogólnie dostępnych (np. Python lub PowerShell), na skonfigurowanie nowych integracji z zewnętrznymi systemami oraz zapewnić dla tych systemów mechanizmy bezpiecznego zarządzania i przechowywania danych związanych z tymi integracjami, m.in. loginy, hasła oraz klucze API.

84. W ramach obsługi zdarzenia dla operatora powinien być dostępny dedykowany panel analityczny pozwalający mu na:

- a) podgląd aktywności zagrożonego zasobu na linii czasu,
- b) w przypadku zagrożenia sieciowego podgląd aktywności zarówno ofiary jak i celu ataku,
- c) w przypadku identyfikacji użytkownika podgląd jego aktywności na linii czasu,
- d) podgląd reguły korelacyjnej, która wygenerowała zdarzenie,
- e) w przypadku wykrytej techniki MITRE ATT&CK® jej szczegółowy opis,
- f) listowanie podpiętych zdarzeń wraz z mechanizmami filtrowania po nich,
- g) gotowe i proste w użyciu filtry rozszerzające analizę zdarzeń o:
 - listę wszystkich zdarzeń pomiędzy celem a źródłem ataku w zadanym okresie czasowym, np.: godzinę przed oraz 2 godziny po,
 - listę wszystkich zdarzeń dotyczących źródła lub celu ataku w zadanym okresie czasowym,
- f) gotowe i proste w użyciu filtry rozszerzające analizę logów o:
 - listę wszystkich logów pomiędzy celem a źródłem ataku w zadanym okresie czasowym,
 - listę wszystkich logów dotyczących źródła lub celu ataku w zadanym okresie czasowym.

85. Dla zdarzeń w obsłudze system musi być wyposażony w graficzny interfejs umożliwiający definiowanie własnych powiadomień obejmujących:

- a) warunki powiadomień,
 - zdarzeń o przekroczonych czasach SLA definiowalnych dla wszystkich statusów obsługi,
 - zdarzeń o przekroczonych czasach SLA o definiowalny okres,
 - zdarzeń ze zbliżającym się i definiowalnym terminem przekroczenia SLA,
 - zdarzeń, których priorytet osiągnął określoną wartość,
 - zdarzeń zakwalifikowanych jako incydent bezpieczeństwa,
 - zdarzeń na których doszło do naruszenia bezpieczeństwa,
 - zdarzeń powstałych poprzez zdefiniowaną regułę korelacyjną,

- zdarzeń realizujących zdefiniowaną usługę,
- zdarzeń przetwarzających sklasyfikowaną informację,
- zdarzeń przetwarzanych na krytycznych zasobach,
- b) odbiorców powiadomień, w tym:
 - operatora, któremu zostało przydzielone zdarzenie,
 - właściciela zasobu na którym wystąpiło zdarzenie,
 - zespół obsługi, który odpowiada za obsługę zdarzeń,
 - właściciela usługi która jest realizowana na zasobie na którym wystąpiło zdarzenie,
- podmiot zewnętrzny, jeżeli zdarzenie dotyczy zasobu obsługiwanego przez firmę zewnętrzną.
- c) kanały powiadomień, m.in. e-mail, sms, komunikator,
- d) zastosowanie mechanizmów grupowania:
 - grupowanie wielu powiadomień w jednej wiadomości,
 - ograniczenie liczby wierszy powiadomienia do określonej wartości.

86. System powinien posiadać gotowe szablony powiadomień pozwalające na wysyłanie powiadomień jego operatorom w przypadku gdy system przydzieli im zdarzenia do obsługi. Szablony powinny uwzględniać powiadomienie operatorów w następujących sytuacjach:

- a) utworzenia nowego zdarzenia z określonym priorytetem,
- b) utworzenia nowego zdarzenia na zasobie krytycznym,
- c) utworzenia nowego zdarzenia na zasobie realizującym zdefiniowaną usługę,
- d) utworzenie nowego zdarzenia na zasobie przetwarzającym dane osobowe,
- e) utworzenie nowego zdarzenia na podstawie zdefiniowanej reguły korelacyjnej,
- f) modyfikacji przydzielonego operatorowi zdarzenia przez innego operatora,
- g) zamknięcia przydzielonego operatorowi zdarzenia przez innego operatora,
- h) przejęcia przydzielonego operatorowi zdarzenia przez innego operatora.

87. Dla kadry zarządzającej system musi umożliwiać automatyczną dystrybucję raportów poprzez pocztę elektroniczną. System musi umożliwiać dostęp do kreatora umożliwiającego:

- a) wybór raportu, który ma zostać wysłany,
- b) zdefiniowanie jego tytułu,
- c) zdefiniowanie cyklu w jakim ma zostać wysyłany, np.: tygodniowy lub miesięczny,
- d) możliwość ograniczenia cyklu do dni powszednich,

- e) określenie daty przesłania pierwszego raportu,
- f) możliwości ograniczenia okresu przez jaki raport będzie przesyłany, do:

- zdefiniowanej daty końcowej,
- określonej liczby raportów,

- g) określenie odbiorców raportu.

88. System musi umożliwiać obsługę podatności w ramach scenariuszy obsługi (Playbook).

89. Importowane do systemu podatności muszą być przeanalizowane pod względem ryzyka jakie mogą wygenerować dla organizacji. W tym celu musi być dostępny mechanizm ich automatycznej priorytetyzacji bazujący na regułach, które wyznaczają dla podatności wymagających obsługi priorytet w oparciu o następujące parametry:

- a) strefę bezpieczeństwa w której została wykryta podatność,
- b) prawdopodobieństwo obecności intruza lub złośliwego oprogramowania w tej strefie,
- c) rodzaj zasobu którego dotyczy ta podatność,
- d) ważność tego zasobu dla organizacji,
- e) przetwarzane na tym zasobie informacje, np.: dane osobowe,
- f) usługi realizowane przez ten zasób, np.: DNS,
- g) wartość parametrów CVSS dla podatności, np.: „Confidentiality Impact” = High,
- h) poprawność konfiguracji zasobu na którym została wykryta podatność, np.: brak reguł wymuszenia złożoności haseł,
- i) szacowane prawdopodobieństwo przełamania zabezpieczeń ze zdefiniowanej strefy, która jest autoryzowana do dostępu do tego zasobu, np.: wysokie prawdopodobieństwa zagrożenia ze strefy Internet dla zasobu z wykrytą podatnością, który świadczy usługę w strefie Internet.

90. W systemie musi być dostępny predefiniowany zestaw reguł automatycznej priorytetyzacji wszystkich importowanych podatności oraz interfejs umożliwiający definiowanie własnych reguł umożliwiających zarówno zakwalifikowanie podatności do obsługi jak i możliwość ich wyłączenia z obsługi w przypadku znikomego zagrożenia dla organizacji.

91. Obsługiwane w systemie podatności muszą być dostępne w formie listy umożliwiającej ich filtrowanie po następujących wartościach:

- a) wyliczonym priorytecie podatności,
- b) aktualnym statusie obsługi,
- c) ważności zasobu na którym została wykryta,
- d) adresie IP tego systemu,
- e) parametrów SLA związanych z tym statusem,
- f) przetwarzanych na zasobach informacji, np.: lista podatności dotycząca tylko systemów przetwarzających dane osobowe,
- g) parametrach CVSS, np.: lista podatności których „Access Complexity

(AC)” = „low” oraz „Access Vector (AV) = „Network”.

92. System powinien posiadać gotowe szablony powiadomień, pozwalające na wysyłanie powiadomień dla kadry zarządzającej, obejmujących eskalacje oraz monitorowanie SLA. Szablony powinny uwzględniać powiadomienia kierowników jednostek organizacyjnych w następujących sytuacjach:

- a) przekroczenia czasu reakcji o określony czas np.: o godzinę,
- b) możliwości przekroczenia czasu reakcji, np.: została godzina aby rozpocząć obsługę zdarzenia i uchronić się przed przekroczeniem czasu reakcji,
- c) przekroczenia czasu reakcji dla zdarzenia na zasobie przetwarzającym dane osobowe,
- d) przekroczenia czasu reakcji dla zdarzenia na zasobie krytycznym,
- e) przekroczenia czasu reakcji dla zdarzenia na zasobie realizującym krytyczną usługę,
- f) przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów przetwarzających dane osobowe,
- g) przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów krytycznych,
- h) przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów realizujących krytyczną usługę,
- i) przekroczenia czasu reakcji dla podatności na zasobie przetwarzającym dane osobowe,
- j) przekroczenia czasu reakcji dla podatności na zasobie krytycznym,
- k) przekroczenia czasu reakcji dla podatności na zasobie realizującym krytyczną usługę,

93. Dla obsługiwanych podatności system musi być wyposażony w graficzny interfejs umożliwiający definiowanie własnych powiadomień obejmujących:

- a) warunki powiadomień
 - podatności o przekroczonych czasach SLA definiowalnych dla wszystkich statusów obsługi,
 - podatności o przekroczonych czasach SLA o definiowalny okres,
 - podatności ze zbliżającym się i definiowalnym terminem przekroczenia SLA,
 - podatności, których priorytet osiągnął określoną wartość,
 - zdarzeń realizujących zdefiniowaną usługę,
 - zdarzeń przetwarzających sklasyfikowane informacje,
 - zdarzeń przetwarzanych na krytycznych zasobach,
- b) odbiorców powiadomień, w tym:
 - operatora, któremu została przydzielona podatność,
 - właściciela zasobu na którym wystąpiła podatność,
 - zespół obsługi, który odpowiada za obsługę podatności,

- właściciela usługi na która jest realizowana na zasobie na którym wystąpiła podatność,
- podmiot zewnętrzny, jeżeli zdarzenie dotyczy podatności na zasobie obsługiwanym przez firmę zewnętrzną.

c) kanały powiadomień, m.in. e-mail, sms, komunikator,

d) zastosowanie mechanizmów grupowania:

- grupowanie wielu powiadomień w jednej wiadomości,
- ograniczenie liczby wierszy powiadomienia do określonej wartości.

94. System powinien posiadać gotowe szablony powiadomień, pozwalające na wysyłanie powiadomień jego operatorom w przypadku gdy system przydzieli im podatności do obsługi. Szablony powinny uwzględniać powiadomienie operatorów w następujących sytuacjach:

- a) przydzielenia nowej podatności do obsługi z określonym priorytetem,
- b) przydzielenia nowej podatności do obsługi na zasobie krytycznym,
- c) przydzielenia nowej podatności do obsługi na zasobie realizującym zdefiniowaną usługę,
- d) przydzielenia nowej podatności do obsługi na zasobie przetwarzającym dane osobowe,
- e) modyfikacji przydzielonej operatorowi podatności przez innego operatora,
- f) zamknięcia przydzielonej operatorowi podatności przez innego operatora,
- g) przejęcia przydzielonej operatorowi podatności przez innego operatora.

95. Dla kadry zarządzającej system musi umożliwiać automatyczną dystrybucję raportów poprzez pocztę elektroniczną. System musi umożliwiać dostęp do kreatora pozwalającego na:

- a) wybór raportu który ma zostać wysłany,
- b) zdefiniowanie jego tytułu,
- c) zdefiniowanie cyklu w jakim ma zostać wysyłany, np.: tygodniowy lub miesięczny,
- d) możliwość ograniczenia cyklu do dni powszednich,
- e) określenie daty przesłania pierwszego raportu,
- f) określenie okresu przez jaki będą one przesyłane, poprzez:
 - zdefiniowanie daty końcowej,
 - bez daty końcowej,
 - określenie liczby raportów,
- g) określenie odbiorców raportu.

96. System powinien w formie graficznej prezentować podsumowanie aktualnego stanu bezpieczeństwa organizacji w postaci tzw. „Dashboard’u”, tj. dostosowywać zakres i prezentacje danych do potrzeb zalogowanego użytkownika.

97. System musi pozwalać na tworzenie dedykowanych dashboard'ów obejmujących:

- a) zestaw wykresów dla bieżącego użytkownika,
- b) zestaw wykresów dla wybranego użytkownika,
- c) zestaw wykresów dla roli zdefiniowanej w systemie, np.: administratorzy systemu,
- d) zestaw wykresów dla wybranego zespołu obsługi, np.: operatorzy SOC (Security Operations Center).

98. System musi zapewniać zestaw predefiniowanych dashboard'ów obejmujących następujące wykresy:

- a) wykres przedstawiający status klasyfikacji zdarzeń, który uwzględnia:
 - ilość zdarzeń nowych i niesklasyfikowanych,
 - ilość zdarzeń sklasyfikowanych jako incydenty bezpieczeństwa,
 - ilość zdarzeń sklasyfikowanych jako fałszywe alarmy,
- b) wykres przedstawiający skalę zagrożeń, który uwzględnia:
 - ilość zasobów krytycznych na których są obsługiwane zdarzenia,
 - ilość zasobów niekrytycznych na których są obsługiwane zdarzenia,
- c) wykres przedstawiający źródła zagrożeń, który uwzględnia:
 - ilość nowych zdarzeń dotyczących użytkowników,
 - ilość podjętych zdarzeń dotyczących użytkowników,
 - ilość nowych zdarzeń dotyczących zasobów,
 - ilość podjętych zdarzeń dotyczących zasobów,
- d) wykres przedstawiający poziom zagrożeń, który uwzględnia:
 - ilość nowych zdarzeń w podziale na priorytety,
 - ilość podjętych zdarzeń w podziale na priorytety,
- e) wykres przedstawiający czas obsługi zagrożeń, który uwzględnia:
 - ilość zdarzeń zarejestrowanych w bieżącym dniu,
 - ilość zdarzeń zarejestrowanych w ostatnim tygodniu,
 - ilość zdarzeń zarejestrowanych w ostatnim miesiącu,
 - ilość zdarzeń zarejestrowanych wcześniej niż w ostatnim miesiącu,
- f) wykres przedstawiający zagrożone usługi, który uwzględnia:
 - ilość usług krytycznych zagrożonych przez obsługiwane zdarzenia,
 - ilość pozostałych usług zagrożonych przez obsługiwane zdarzenia,
- g) wykres przedstawiający zagrożone dane, który uwzględnia:
 - ilość nowych zdarzeń dotyczących zasobów krytycznych, przetwarzających sklasyfikowane informacje,
 - ilość podjętych zdarzeń dotyczących zasobów krytycznych, przetwarzających sklasyfikowane informacje,
 - ilość nowych zdarzeń dotyczących pozostałych zasobów, przetwarzających sklasyfikowane informacje,
 - ilość podjętych zdarzeń dotyczących pozostałych zasobów, przetwarzających sklasyfikowane informacje,

- h) wykres przedstawiający skalę podatności, który uwzględnia:
- ilość zasobów krytycznych na których są obsługiwane podatności,
 - ilość zasobów niekrytycznych na których są obsługiwane podatności,
- i) wykres przedstawiający czas obsługi podatności, który uwzględnia:
- ilość podatności zarejestrowanych w bieżącym dniu,
 - ilość podatności zarejestrowanych w ostatnim tygodniu,
 - ilość podatności zarejestrowanych w ostatnim miesiącu,
 - ilość podatności zarejestrowanych wcześniej niż w ostatnim miesiącu,
- j) wykres przedstawiający wagę podatności, który uwzględnia:
- ilość nowych podatności w podziale na priorytety,
 - ilość podjętych podatności w podziale na priorytety,

99. Nawigacja w ramach „Dashboard’u” musi wspierać opcję typu „Drill down” w następującym zakresie:

- a) „kliknięcie” wartości prezentowanej na wykresie, dotyczącej zdarzeń w obsłudze musi przenieść operatora systemu do listy tych zdarzeń z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres,
- b) „kliknięcie” wartości prezentowanej na wykresie, dotyczącej podatności musi przenieść operatora systemu do listy tych podatności z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres,
- c) „kliknięcie” wartości prezentowanej na wykresie, dotyczącej użytkowników (UBA) musi przenieść operatora systemu do listy tych użytkowników z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres,
- d) „kliknięcie” wartości prezentowanej na wykresie, dotyczącej zasobów (EBA) musi przenieść operatora systemu do listy tych zasobów z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres,
- e) „kliknięcie” wartości prezentowanej na wykresie, dotyczącej wybranych zdarzeń korelacyjnych musi przenieść operatora systemu do listy prezentującej te zdarzenia z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres,
- f) „kliknięcie” wartości prezentowanej na wykresie, dotyczącej wybranych logów musi przenieść operatora systemu do listy prezentującej te logi z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres.

100. Rozwiązanie może być dostarczone w ramach odrębnych rozwiązań, jednakże muszą być one zintegrowane w sposób umożliwiający spełnienie wszystkich wymagań z poziomu jednej konsoli.

101. Rozwiązanie musi zapewniać elastyczną i skalowalną architekturę, której rozbudowa nie będzie wymagała zakupu dodatkowych licencji,

zapewniając tym samym możliwość wydzielania następujących warstw funkcjonalnych zwanych dalej kolektorami, do instalacji na osobnych serwerach bądź maszynach wirtualnych:

- a) kolektor parsujący;
- b) kolektor logów;
- c) kolektor korelacyjny;
- d) kolektor zdarzeń;
- e) kolektor sztucznej inteligencji;
- f) kolektor reakcyjny;
- g) kolektor kontrolujący.

102. Kolektor parsujący powinien być odpowiedzialny za odbieranie i parsowanie logów a następnie ich przesyłanie zarówno postaci surowej jak i sparsowanej do odpowiednich kolektorów logów, zgodnie z regułami ich przekierowania zdefiniowanymi w jednym miejscu dla wszystkich kolektorów w interfejsie graficznym. Pojedynczy kolektor parsujący musi zapewniać wydajność co najmniej 20 tysięcy zdarzeń na sekundę w trybie ciągłym oraz posiadać bufor do obsługi natłoku w rozmiarze miliona zdarzeń.

103. Kolektor logów powinien być odpowiedzialny za przechowywanie logów zarówno w postaci surowej jak i sparsowanej oraz przechowywać pliki indeksów. Logi muszą być przechowywane w postaci skompresowanej oraz kolektor musi zapewnić mechanizmy zabezpieczające je przed nieautoryzowaną modyfikacją (np.: Certyfikat cyfrowy czy funkcja skrótu). Pojedynczy kolektor logów powinien mieć wydajność co najmniej 10 tys zdarzeń na sekundę w trybie ciągłym oraz posiadać bufor do obsługi natłoku w rozmiarze miliona zdarzeń.

104. Kolektor korelujący powinien umożliwiać korelację logów oraz ich agregację zgodnie z regułami korelacyjnymi zdefiniowanymi w jednym miejscu dla wszystkich kolektorów w interfejsie graficznym.

105. Kolektor zdarzeń powinien umożliwiać składowanie zdarzeń stanowiących wyniki korelacji oraz umożliwiać ponowne wykorzystanie tych zdarzeń w kolejnych regułach umożliwiając tym korelację zależności pomiędzy nimi. Zdarzenia muszą być przechowywane w postaci skompresowanej oraz kolektor musi zapewnić mechanizmy zabezpieczające je przed nieautoryzowaną modyfikacją (np.: Certyfikat cyfrowy czy funkcja skrótu).

106. Kolektor sztucznej inteligencji powinien zawierać wiedzę pozyskaną ze środowiska obejmującą zarówno linię trendu zachowania użytkowników oraz zasobów obejmujące mechanizmy uczenia maszynowego jak i algorytmy sztucznej inteligencji pozwalające na wypracowanie nowej wiedzy wynikającej z korelacji wyników wiedzy wypracowanej poprzez inne metody.

107. Kolektor reakcyjny musi umożliwiać automatyczną reakcję na wykryte

zagrożenia, która nie będzie wymagała żadnej interakcji ze strony użytkownika, chyba że taka będzie dodatkowo zdefiniowana. W celu automatyzacji reakcji musi posiadać funkcjonalność systemu PAM lub być z nim dostarczony w celu przechowywania danych uwierzytelniających oraz kluczy API potrzebnych do automatyzacji reakcji.

108. Architektura rozwiązania musi w pełni wspierać konfigurację niezawodnościową, zapewniającą zarówno pełną redundancję w zakresie, odbierania logów i ich przechowywania, korelacji oraz reakcji na zagrożenia jak i możliwość zastosowania konfiguracji o ograniczonej redundancji do najważniejszych dla zamawiającego źródeł danych.

109. Konfiguracja niezawodnościowa musi wspierać możliwość zastosowania stosu kolektorów zastępczych które zostaną uruchomione w przypadku awarii stosu podstawowego, przy czym wszystkie one muszą być zarządzane centralnie z poziomu tej samej konsoli co kolektory podstawowe.

110. Kolektory muszą mieć zapewnione mechanizmy automatycznej aktualizacji zarówno w zakresie parserów czy reguł korelacyjnych jak i wersji oprogramowania, przy czym aktualizacja musi odbywać się z poziomu centralnego systemu zarządzania.

111. Rozwiązanie musi zapewnić konsole do aktualizacji pozwalającą na wybór dodatkowych pakietów reguł czy parserów udostępnianych w ramach aktywnego wsparcia producenta w formie usługi, każda aktualizacja musi wspierać mechanizm wersjonowania pozwalający zarówno aktualizację jak i przywracanie poprzednich wersji reguł i parserów.

112. Rozwiązanie musi mieć możliwość skalowania się poprzez dodawanie kolejnych maszyn wirtualnych lub maszyn fizycznych z nowymi typami kolektorów, przy czym dodawanie nowych komponentów nie może wiązać się z koniecznością zakupu nowej licencji, ani posiadać ograniczeń licencyjnych związanych z ilością lub rozmiarem przechowywanych zdarzeń i/lub danych. Jedynym ograniczeniem w tym zakresie (dotyczącym przechowywanych danych) może być rozmiar przestrzeni dyskowej.

113. Skalowanie przez dodawanie nowych kolektorów musi zwiększać wydajność rozwiązania zgodnie z wartościami zadeklarowanymi przez producenta, przykładowo dwa kolektory logów muszą zapewnić dwukrotną wydajność rozwiązania czyli minimum 20 tys zdarzeń na sekundę. Przy czym całe rozwiązanie nie może ograniczać ilość zastosowanych kolektorów.

114. Rozwiązanie nie może posiadać ograniczeń licencyjnych związanych z rozmiarem gromadzonych danych w jednostce czasu. Przykładowo nie może być limitowana licencyjnie ilość bajtów danych w jednostce czasu (KB, GB, etc.)

115. Poszczególne kolektory zdarzeń oraz logów muszą zapewniać przechowywanie danych zarówno na maszynach wirtualnych jak i na dyskach sieciowych.

116. Kolektor logów musi mieć możliwość składowania zbieranych danych zarówno w formie surowej (raw event log) jak i w formie sparsowanych danych (parsed event log)/danych znormalizowanych.

117. Rozwiązanie nie może Przechowywanie logów oraz zdarzeń nie może wykorzystywać klasycznej relacyjnej bazy danych (w tym, choć nie tylko: MS SQL, PostgreSQL, MySQL, Oracle, itp.) celem gromadzenia i przechowywania danych związanych ze zbieranymi zdarzeniami. Rozwiązanie musi wykorzystywać w tym celu nowoczesną bazę taką jak na przykład noSQL lub OLAP lub autorskie rozwiązanie producenta.

118. Rozwiązanie musi zapewniać możliwość zbudowania większej ilości replik danych, aby zapewnić niezawodność przechowywania oraz możliwość zbudowania struktury rozproszonej, zapewniającej większą wydajność zapisu i wyszukiwania.

119. Klasyczne relacyjne bazy danych mogą być wykorzystywane jedynie do przechowywania szablonów, raportów, konfiguracji, bazy CMDB oraz innych ustrukturyzowanych informacji.

120. Rozwiązanie musi zapewniać możliwość automatycznego budowania kontekstu poprzez wykrywanie urządzeń oraz komputerów mających swoją reprezentację w bazie urządzeń (Configuration Management Database - CMDB).

121. Wymagane jest, aby kolektor odpowiedzialny za parsowanie pozwalał na odrzucanie danych, które uznane są za nieistotne lub niepotrzebne. Mechanizm ten nie może mieć żadnego wpływu na model licencjonowania.

122. Musi istnieć możliwość samodzielnej modyfikacji i poprawiania wszystkich parserów

123. Tworzenie własnych parserów musi być w całości możliwe z wykorzystaniem interfejsu graficznego (GUI) bez użycia linii komend (CLI)

124. Tworzenie nowych atrybutów (sparsowanych zmiennych), urządzeń oraz rodzajów zdarzeń (events) musi być w całości możliwe z wykorzystaniem interfejsu graficznego (GUI) bez użycia linii komend (CLI).

125. Parsery mają być tworzone z wykorzystaniem narzędzi wspierających dla XML (XML framework) i jednocześnie zapewniać następujące właściwości:

- a) zdolność do definiowania wzorców które powtarzają się jako zmienne;
- b) zdolność do definiowania funkcji pozwalających na identyfikację par wartości kluczowych;
- c) zdolność do testowania poszczególnych funkcji;
- d) zdolność do przekształcania danych w trakcie ich parsowania.

126. Rozwiązanie SIEM musi wspierać obsługę aplikacji typu agent na systemy Windows (Windows Agent), które posiadają nie mniej niż następujące możliwości:

- a) centralne zarządzanie i możliwość aktualizacji z głównej konsoli

zarządzającej;

- b) możliwość zbierania logów z plików tekstowych na urządzeniach z zainstalowanym systemem z rodziny Windows;
- c) możliwość zbierania logów dotyczących zdarzeń rodzajów innych niż: Security, System, Application;
- d) zdolność do monitorowania integralności plików;
- e) zdolność do monitorowania rejestru systemowego;
- f) zdolność do monitorowania urządzeń zewnętrznych (removable devices);
- g) agent instalowany na systemach z rodziny Windows musi komunikować się z poszczególnymi komponentami rozwiązania SIEM w sposób zaszyfrowany z wykorzystaniem protokołu HTTPS;
- h) musi istnieć możliwość monitorowania stanu agentów w konsoli zarządzającej systemu;
- i) musi istnieć możliwość przygotowania różnych zestawów konfiguracji agenta, a następnie przypisywania ich niezależnie do dowolnej ilości (jeden lub więcej) systemów źródłowych. Np. inne konfiguracje dla kontrolerów domeny, a inne dla serwerów DNS;
- j) musi umożliwiać automatyzację reakcji na zagrożenie, jak blokowanie zdefiniowanego ruchu sieciowego czy blokada procesu.

127. System musi mieć możliwość realizacji funkcjonalności UEBA (User Entity Behaviour Analysis) zarówno w oparciu o dedykowanego Agenta na systemy Windows oraz w oparciu o logi z systemu Windows. Metadane lub logi dotyczące funkcji UEBA nie mogą podlegać licencjonowaniu ze względu na EPS lub rozmiar.

128. Rozwiązanie musi zapewniać wsparcie dla zarządzania w oparciu o role (Role Based Administration) celem ograniczania dostępu do danych oraz do GUI

129. System musi być zintegrowany z zewnętrznymi bazami o zagrożeniach (Threat Intelligence Feeds - TI) oraz zawierać już zintegrowany zestaw niekomercyjnych (open source) lub komercyjnych baz zagrożeń.

130. Rozwiązanie musi mieć możliwość korelacji informacji z baz zagrożeń z danymi otrzymywanymi w czasie rzeczywistym. Korelacja ta ma odbywać się w pamięci systemu względem otrzymywanych danych o zdarzeniach (event data).

131. System musi mieć możliwość korelacji informacji z baz zagrożeń z danymi historycznymi

132. System musi mieć możliwość odpytywania (ręcznego lub automatycznego) zewnętrznych źródeł reputacji takich jak np. VirusTotal.

133. System musi mieć możliwość wizualizacji informacji w oparciu o kategorie MITRE ATT&CK dla standardowego zbioru wbudowanych reguł.

134. Pulpity administracyjne (dashboards) muszą mieć możliwość wspólnej prezentacji.

135. Rozwiązanie musi mieć możliwość integracji z innymi systemami do obsługi zgłoszeń poprzez API (ticketing system) oraz mieć wbudowany mechanizm obsługi zgłoszeń (ticketing system) niezależny od obsługi alarmów/incydentów.

136. System musi wpierać mechanizmy typu Machine Learning w oparciu o zgromadzone zdarzenia. Musi być możliwe użycie przynajmniej 4 różnych rodzajów mechanizmów Machine Learning wraz z możliwością ich ręcznego wybrania oraz działania w trybie automatycznym. W wyniku działania opisanych mechanizmów Machine Learning system SIEM ma tworzyć model bazowy zachowania oraz umożliwiać wykrycie odchyleń i anomalii od niego. Zadania Machine Learning mają mieć możliwość dystrybuowania ich pomiędzy elementy warstwy korelującej i/lub zarządzającej. Mechanizmy Machine Learning mają również umożliwiać wsparcie dla podejmowania decyzji przy rozwiązywaniu incydentów w systemie SIEM.

137. Dostarczone rozwiązanie nie może działać w oparciu o oprogramowanie otwarte (ang: open source) w następującym zakresie funkcjonalnym: składowanie, parsowanie, korelacja logów, algorytmy uczenia maszynowego, analiza zachowania użytkowników i zasobów (UEBA), mechanizmy reakcji/ scenariusze reakcji (SOAR). Zamawiający nie zaakceptuje systemu, który wykorzystuje mechanizmy typu open source np.: Elastic Search, OSSIM, Snort, The Hive, AlienVault itd. lub został stworzony przez modyfikację oprogramowania otwartego.

138. W celach weryfikacji zgodności produktu z wymaganiami, musi być on dodatkowo oferowany przez autoryzowanego dystrybutora, dostarczającego produkty z obszaru cyberbezpieczeństwa na rynku polskim, który w przypadku jakichkolwiek wątpliwości Zamawiającego, związanych z wymaganymi funkcjonalnościami będzie mógł je potwierdzić lub im zaprzeczyć.

139. W związku z tym, że obsługa systemu ma objąć także użytkowników nieposługujących się biegle językiem angielskim, interfejs użytkownika musi umożliwiać obsługę w języku polskim lub posiadać możliwość wgrania plików językowych tłumaczących interfejs na język polski. Pliki tłumaczące interfejs na język polski muszą zostać wgrane w trakcie wdrożenia systemu, przed jego zakończeniem.

140. Zamawiający na obecnym etapie nie jest w stanie zmierzyć ilości danych przekazywanych do systemu, tj. EPS (Events Per Second) oraz nie zna wymagań związanych z architekturą proponowanego rozwiązania, dlatego oferowana licencja nie może nakładać limitów w tym zakresie.

141. Produkt musi umożliwiać równoczesną pracę co najmniej 2 operatorów oraz obsługiwać min 100 źródeł logów dotyczących wszystkich zdarzeń związanych z komputerami oraz serwerami wykorzystywanymi w organizacji oraz zapewnić dla tych źródeł detekcję i obsługę cyberzagrożeń w ramach wszystkich oferowanych w tym postępowaniu funkcjonalności.

142. System ma gwarantować możliwość elastycznej rozbudowy o kolejne źródła logów.

143. Funkcjonowanie rozwiązania musi umożliwiać konfigurację „on-premise”, w której wszystkie funkcjonalności oraz przetwarzanie danych będzie się odbywać całkowicie w infrastrukturze zamawiającego, zapewniając tym samym możliwość konfiguracji systemu w strefie odseparowanej od sieci Internet.

144. System musi umożliwiać instalację na jednej z platform systemowych: Microsoft Windows (minimum Server 2016), Redhat/Oracle Linux (minimum 7.x).

Wymagania dotyczące licencji i wsparcia

Dostarczone rozwiązanie musi być w formie licencji wieczystej oraz być objęte wsparciem producenta lub producentów do 30.06.2026 roku. Wsparcie musi obejmować bezpłatne dostarczanie aktualizacji oprogramowania, reagowanie na zgłaszane błędy systemowe oraz usługę konsultacji powdrożeniowej w formie spotkań z dedykowanym inżynierem, certyfikowanym z procesu konfiguracji i obsługi oferowanego systemu. Przez błąd systemowy Zamawiający rozumie błędy krytyczne (zakłócenie uniemożliwiające działanie rozwiązania), błędy poważne (zakłócenie uniemożliwiające działanie części rozwiązania), błędy zwykłe (inne zakłócenia nie stanowiące błędów krytycznych lub poważnych). Wykonawca musi zapewnić usługę obejmującą proces aktualizacji oprogramowania oraz kontekstu systemu (dotyczy to zwłaszcza bazy reguł korelacyjnych, bazy parserów, bazy dostępnych aktualizacji). Dostęp do centralnej usługi aktualizacyjnej ma pozwalać na automatycznie wyświetlanie i pobieranie z poziomu interfejsu systemu dostępnych aktualizacji. Dla pobranych w procesie aktualizacji reguł oraz parserów musi być dostępne wersjonowanie, pozwalające uruchomić nową wersję reguły korelacyjnej oraz parsera z poziomu interfejsu systemu. Automatyczne wersjonowanie ma umożliwiać wczytanie starszej wersji reguły lub parsera, a zmiana reguł i parserów musi być możliwa z poziomu graficznego systemu.

Wymagania dotyczące wdrożenia

Przedmiot zamówienia musi być dostarczony, wdrożony i zainstalowany w całości w siedzibie Zamawiającego we wskazanym miejscu. Przedmiot Zamówienia będzie realizowany w oparciu o przygotowany uprzednio przez Wykonawcę Harmonogram Ramowy (rzeczowo-finansowy), który musi być uzgodniony i zaakceptowany przez Zamawiającego oraz odpowiednio utrzymywany w toku realizacji Przedmiotu Zamówienia. Wykonawca musi przedstawić Harmonogram Ramowy w terminie 7 dni od daty podpisania umowy. Wykonawca w Harmonogramie Ramowym musi w szczególności uwzględnić podział na zadania takie jak: projektowanie, dostawy, usługi instalacji/konfiguracji, testowanie, wdrożenie i odbiory. Wykonawca zobowiązany jest do udziału w cyklicznych naradach

przeglądu prac w siedzibie Zamawiającego. Dopuszcza się narady prowadzone w trybie zdalnym z wykorzystaniem narzędzi komunikacji elektronicznej, które zapewni Wykonawca. Zamawiający przewiduje częstotliwość narad nie częściej niż jeden raz w miesiącu, narad zdalnych maksymalnie 3 razy w miesiącu, chyba że nadzwyczajna sytuacja w realizacji przedmiotu umowy wymagała będzie częstszych spotkań w siedzibie lub odbywanych zdalnie.

W ramach wdrożenia Wykonawca musi przygotować informacje na temat struktury organizacyjnej Zespołu Wykonawcy zajmującej się realizacją przedmiotu zamówienia, w ramach której muszą zostać powołane minimum następujące role:

- Kierownik Projektu ze strony Wykonawcy,
- Zespół Wdrożeniowy ze strony Wykonawcy.

W ramach wdrożenia rozwiązania SIEM Zamawiający wymaga aby Wykonawca wdrożył rozwiązanie SIEM na minimum 2 maszynach wirtualnych przygotowanych przez Zamawiającego.

Zamawiający wymaga wdrożenia kompletnego systemu w ramach którego zostanie podłączonych do 15 źródeł logów zgodnie z poniższą tabelą:

Rodzaj usługi lub urządzenia	Liczba urządzeń / nodów będących źródłami logów
Serwer	6 szt. (2 serw. fizyczne i 4 wirtualne)
Urządzenie klasy NAS	1 szt.
Urządzenia klasy UTM	1 szt.
Oprogramowanie EDR/XDR	1 szt.
Usługa katalogowa	2 szt.
Przełączniki sieciowe	2 szt.
Punkty dostępowe	2 szt.

Wymaga się, aby Wykonawca przygotował harmonogram wdrożenia uwzględniający 6 etapów wdrożenia:

1. Analiza przedwdrożeniowa,
2. Instalacja systemu,
3. Konfiguracja systemu,
4. Dostrojenie systemu,
5. Szkolenia
6. Dokumentacja powdrożeniowa.

Wykonawca w ramach etapu 1 dokona analizy przedwdrożeniowej

obejmującej wszystkie czynności do wykonania przez Wykonawcę mające na celu analizę oraz wdrożenie rozwiązania SIEM w środowisku informatycznym Zamawiającego. Analiza musi zawierać w szczególności:

1. Dane wstępne:
 - a) plan i sposób komunikacji Stron
 - b) harmonogram wdrożenia
2. Informacje o systemach bezpieczeństwa:
 - a) Analiza stanu bezpieczeństwa użytkowanych systemów przed rozpoczęciem realizacji projektu
 - b) Opis koniecznych działań dla osiągnięcia wymaganego stanu cyberbezpieczeństwa
3. Wymagane dane dotyczące systemów cyberbezpieczeństwa:
 - a) Wykonawca określi w Analizie przedwdrożeniowej optymalną konfigurację środowiska dla Systemu SIEM, m.in. pamięć, liczbę procesorów, wymagana powierzchnia dyskowa.
 - b) Dla każdego systemu cyberbezpieczeństwa Wykonawca opracuje:
 - Wersję oprogramowania wchodzące w skład Systemu
 - Konfigurację Systemu
 - Zastosowane licencje/subskrypcje.
4. Procedura testowania – scenariusze testowe dla wdrażanych systemów
5. Harmonogram wdrożenia
6. Opis instalacji i wdrożenia oprogramowania

Wykonawca w ramach etapu 2 zainstaluje zaoferowane oprogramowanie według wcześniej przedstawionej architektury działania rozwiązania, oraz wcześniej przygotowanego schematu komunikacji sieciowej w sieci lokalnej Zamawiającego.

Wykonawca w ramach etapu 3 zaimplementuje/skonfiguruje opracowane przez producenta reguły bezpieczeństwa wraz z weryfikacją ich działania dla konkretnych procesów określonych na etapie analizy przedwdrożeniowej.

Wykonawca w ramach etapu 4 dostroi system tak, aby nie powodował nadmiernej ilości fałszywych alarmów zaciemniających realne możliwe zagrożenia. Nie dopuszcza się sytuacji w której jedno źródło logów spowoduje destabilizację działania całego systemu SIEM w krótkim okresie czasu np. 10minut.

Wykonawca w ramach etapu 5 przeprowadzi szkolenia w zakresie użytkowania i administrowania wdrożonego systemu lub systemów.

Szkolenie ma zostać przeprowadzone dla maksymalnie 2 osób i muszą być zakończone przyznaniem certyfikatu, potwierdzającego wspomniane umiejętności wydany przez Certyfikowanego Inżyniera systemu/systemów. Szkolenia mogą odbyć się w formie zdalnej.

Wykonawca w ramach etapu 6 sporządzi i przekaże dokumentację powdrożeniową wskazującą wszystkie istotne elementy z punktu widzenia wdrożenia, wraz ze wszystkimi danymi dostępowymi do ewentualnych kont technicznych stworzonych na etapie wdrożenia.

Wykonawca po wdrożonym rozwiązaniu dokona następujących testów opisanych w Dokumentacji. Celem testów jest weryfikacja przez Zamawiającego czy wszystkie prace wykonane w trakcie realizacji przedmiotu zamówienia zostały wykonane prawidłowo i zgodnie z założeniami funkcjonalnymi i jakościowymi. Testy będą przeprowadzane przez Wykonawcę przy współudziale Zamawiającego.

Zamawiający ma prawo do weryfikacji należytego wykonania Umowy dowolną metodą, w tym także z wykorzystaniem opinii zewnętrznego audytora. W szczególności uzgodnienie określonych scenariuszy testowych nie wyklucza prawa do weryfikacji prac innymi testami i scenariuszami.

W przypadku zidentyfikowania Błędów lub Wad Wykonawca jest zobowiązany do ich poprawy przed Odbiorem Końcowym przedmiotu zamówienia.

Zamawiający wymaga, aby Wykonawca przeprowadził testy odbiorcze z zakresu:

- Uruchamianie i zatrzymywanie wdrożonego systemu.
- Weryfikacja wdrożonego systemu zgodnie ze scenariuszami opisanymi w analizie przedwdrożeniowej.
- Weryfikacja poprawności działania procedur.
- Symulację awarii wdrożonego systemu.

Ilość

1 szt.

8. Usługa backupu w chmurze

Nazwa	Minimalne wymagania
Wymagania funkcjonalne	<ol style="list-style-type: none"> Administrator backupu będzie miał możliwość dowolnej konfiguracji mechanizmów backupów danych, w szczególności system umożliwi następującą konfigurację: <ul style="list-style-type: none"> codzienny backup przyrostowy wskazanych wolumenów danych z maszyn fizycznych tygodniowy backup całkowity wskazanych wolumenów danych z maszyn fizycznych raz w tygodniu wykonanie kopii zapasowej backupu lokalnego danych do repozytorium danych w chmurze (replikacja backupu lokalnego) Administrator backupu, korzystając z dedykowanego panelu webowego systemu backupu będzie miał możliwość odtworzenie z backupu wskazanego pliku/folderu z dowolnego okresu w przeszłości z uwzględnieniem zdefiniowanej retencji danych. Administrator backupu będzie miał możliwość przeglądania zawartości backupów (lista plików, folderów wraz z podaniem dat backupu danego wolumenu danych) bez konieczności ich odtwarzania Dedykowany panel służący do zarządzania, konfiguracji backupów, publikowany będzie z serwera lokalnego backupu Zamawiającego. Panel administracyjny działać będzie poprawnie, co najmniej w przeglądarkach EDGE, Chrome, Firefox. Rozwiązanie musi zapewniać: <ul style="list-style-type: none"> archiwizacji otwartych i zablokowanych plików i całych systemów operacyjnych (tylko Windows) szyfrowanie archiwów i transferu zapewniających bezpieczeństwo sieci i informacji wymaganych przez RODO kompresje danych wysyłanie Alertów administracyjnych na e-mail możliwość uruchamiania zewnętrznych programów, skryptów i plików wsadowych na serwerze backupu i na komputerach zdalnych raporty podsumowujące przebieg archiwizacji oraz statystyki
Wymagania dotyczące bezpieczeństwa danych	<ol style="list-style-type: none"> Usługodawca zapewni przechowywanie danych w chmurze na terenie gospodarczym Unii Europejskiej. Usługodawca zapewni dostępność chmury danych na poziomie nie mniejszym niż 99,60% w ciągu miesiąca.



3. Data Center usługodawcy, którym zlokalizowane będzie repozytorium danych w chmurze na potrzeby backupów, musi spełniać wymogi nie mniejsze niż Tier I.
4. Maksymalny czas jednorazowej niedostępności repozytoriów danych w chmurze nie może przekroczyć 50 minut.
5. Przesyłanie danych do repozytorium danych w chmurze realizowane będzie za pośrednictwem bezpiecznego połączenia SSL.
6. wszystkie dane podlegające procesowi backupu przed wysłaniem do chmury będą szyfrowane u źródła przed opuszczeniem firmowej sieci) oraz podczas transferu i przechowywania w repozytorium w chmurze.
6. oferowane rozwiązanie umożliwi automatyczne trwałe kasowanie danych z wybranych lokalizacji po określonym czasie w oparciu o konfigurację, która będzie definiowana przez Administratora danych ze strony Zamawiającego.
7. Usługodawca musi prowadzić dokumentację bezpieczeństwa, w której znajdują się opisy środków bezpieczeństwa, stosownych procedur oraz obowiązków personelu mającego dostęp do danych klienta.
8. Usługodawca realizuje lub umożliwia realizację klientowi - bieżącego tworzenia kopii danych, z których można odzyskać dane klienta.
9. Usługodawca przechowuje kopie danych klienta i procedury odzyskiwania danych w innej lokalizacji niż lokalizacja głównego sprzętu komputerowego służącego do przetwarzania danych klienta.
10. Usługodawca weryfikuje procedury odzyskiwania danych co najmniej raz na sześć miesięcy.
11. Usługodawca rejestruje działania związane z odzyskiwaniem danych, w tym dane osoby odpowiedzialnej, opis przywracanych danych oraz jeśli to niezbędne dane, jakie musiały zostać wprowadzone ręcznie podczas odzyskiwania i dane osoby odpowiedzialnej za ten proces.
12. Usługodawca ma plany awaryjne i plany ciągłości działania dla placówek, w których są zlokalizowane systemy informatyczne Usługodawcy przetwarzające Dane Klienta.
13. Redundantna pamięć masowa Usługodawcy i procedury Usługodawcy dotyczące odzyskiwania danych umożliwiają podjęcie próby rekonstrukcji Danych Klienta w ich oryginalnym lub ostatnio zreplikowanym stanie, w jakim znajdowały się przed ich utratą lub zniszczeniem.

Wymagania techniczne

- początkowa ilość danych podlegająca procesowi backupy – 4TB;
- częstotliwość backupu: codzienny;
- średnie miesięczne wykorzystanie przestrzeni danych w chmurze – 5TB;
- maksymalne miesięczne wykorzystanie przestrzeni danych w chmurze – 10TB;



	<ul style="list-style-type: none"> • możliwość bieżącego śledzenie wykorzystania repozytoriów i konfiguracji powiadomień związanych z osiągnięciem definiowalnych progów zajętości repozytorium; • Usługodawca zapewni transfer danych podczas wysyłania i odtwarzania backupu w cenie rozwiązania; • Usługobiorca dysponuje łączem internetowym o przepustowości nie mniejszej niż 1Gb/s z dedykowanym stałym publicznym adresem IP;
Wdrożenie	<p>Zamawiający wymaga przeprowadzenie wdrożenia dostarczonego rozwiązania (wraz ze szkoleniem):</p> <ul style="list-style-type: none"> • konfiguracja i instalacja agentów fizycznych • stworzenie harmonogramów backupów wskazanych wolumenów danych
Warunki wsparcia technicznego	<ol style="list-style-type: none"> 1. Usługodawca zapewnia możliwość zgłaszania awarii w trybie 24x7. 2. Czas reakcji na zgłoszenie: <ul style="list-style-type: none"> • maksymalnie w ciągu 4h. 2. Serwis świadczony będzie zdalnie 3. W okresie wsparcia technicznego Usługodawca zapewni pomoc techniczną obejmującą minimum: <ul style="list-style-type: none"> • pracę serwisanta aż do rozwiązania problemu; • zdalną pomoc techniczną w zakresie oprogramowania; • licencję na używanie i kopiowanie uaktualnień oprogramowania (w wariantcie bezterminowym lub subskrypcji); • zdalną diagnostykę i pomoc techniczną;
Licencja	<p>Jeżeli oferowane rozwiązanie wymaga: Usługodawca udostępnienia minimum 35 agentów do realizacji usługi backupu w chmurze stanowisk komputerowych i minimum 6 agentów serwerowych. Usługa wraz ze wsparciem technicznym realizowana będzie w okresie do 30.06.2026 r.</p>
Ilość	1 szt.



9. Elementy serwera plików – dyski

Nazwa		Minimalne wymagania sprzętu
Typ	Dysk HDD 3,5"	
Parametry	Pojemność: 16 TB Interfejs: SATA III Prędkość obrotowa: min. 7.200 RPM Cache: min. 256 MB Średni czas między awariami: min 2.000.000 h Gwarancja: 5 lat	
Ilość	4 szt.	

10. Oprogramowanie menadżer haseł.

Nazwa	Minimalne wymagania
<p>Wymagania funkcjonalne</p>	<p>Aplikacja do zarządzania hasłami – menadżer haseł</p> <p>W ramach dostawy Wykonawca zobowiązany jest do dostarczenia oprogramowania menedżera haseł o minimalnych wymaganiach:</p> <p>Minimalne wymagania ogólne:</p> <ol style="list-style-type: none"> 1. Oprogramowanie musi umożliwiać zarządzanie danymi dostępowymi do zewnętrznych usług w postaci minimum loginu i hasła oraz adresu URL strony. 2. Licencja powinna pozwalać na bezterminowe korzystanie z oprogramowania. 3. Oprogramowanie musi umożliwić przechowywanie nieograniczonej ilości wpisów z danymi dostępowymi. 4. Oprogramowanie musi udostępniać opcję dedykowanej pomocy technicznej w języku polskim z możliwością zgłaszania problemów wewnątrz portalu poprzez wypełnienie formularza, składającego się min. z tytułu, treści oraz ewentualnych załączników. 5. Oprogramowanie musi posiadać wsparcie techniczne producenta do minimum 30.06.2026r. 6. Oprogramowanie musi być dostępne minimum w języku polskim z możliwością zmiany języka z poziomu indywidualnego użytkownika. 7. Oprogramowanie musi posiadać ocenę A+ pod względem ustawionych nagłówków HTTP względem strony https://securityheaders.com/, tj. ustawiony nagłówek Strict-Transport-Security, X-Frame-Options, X-Content-Type-Options, Refferer-Policy, Permission-Policy oraz Content-Security-Policy. 8. Oprogramowanie musi posiadać architekturę klient/serwer z umożliwieniem uruchomienia jej w opcji on-premise uruchomionym w infrastrukturze Zamawiającego. 9. Oprogramowanie musi spełniać normy dostępności treści internetowych dla osób niepełnosprawnych min. w zakresie wyboru kroju czcionki, wyboru rozmiaru czcionki oraz możliwości czytania tekstu. <p>Minimalne wymagania dotyczące przechowywania danych:</p>

-
1. Oprogramowanie musi umożliwić tworzenie, modyfikowanie i usuwanie wpisów z danymi dostępowymi składającymi się z minimum:
 - a. Tytułu,
 - b. Loginu,
 - c. Hasła,
 - d. Adresu URL strony,
 - e. Daty wygaśnięcia,
 - f. Notatki.
 2. Oprogramowanie musi umożliwiać tworzenie, modyfikowanie i usuwanie wpisów dedykowanych do przechowywania notatek składających się z minimum:
 - a. Tytułu,
 - b. Treści notatki.
 3. Oprogramowanie musi umożliwić dodawanie wpisów z danymi dostępowymi bez konieczności podawania wszystkich pól wymienionych w punktach 1-3.
 4. Oprogramowanie musi umożliwić nadawanie etykiet na wpisy, umożliwiając przy tym wizualną identyfikację przynależności do danej etykiety.
 5. Oprogramowanie musi umożliwić dodawanie załączników do wpisów w formie plików z możliwością zdefiniowania dozwolonych rozszerzeń i rozmiarów w licencji.
 6. Oprogramowanie musi umożliwić tworzenie grup dostępowych, szyfrowanych w myśl zasady zero-knowledge, tj. zaszyfrowanych na każdym etapie transferu danych z serwera do użytkownika i na odwrót i możliwych do odszyfrowania jedynie przez użytkownika lub odbiorcę.
 7. Oprogramowanie musi umożliwić dostosowywanie grup dostępowych poprzez nazwy oraz ikony.
 8. Oprogramowanie musi umożliwić możliwość tworzenia grup prywatnych, do których dostęp ma jedynie właściciel.
 9. Oprogramowanie musi umożliwić tworzenie grup współdzielonych, do których dostęp ma właściciel i wszyscy uprawnieni użytkownicy wskazani przez właściciela.
 10. Oprogramowanie musi mieć możliwość wyszukiwania wpisów po tytule.
 11. Oprogramowanie musi posiadać wbudowany generator haseł umożliwiający definiowanie złożonych haseł o określonej długości z możliwością dostosowania występowania wielkich liter, małych liter, cyfr oraz symboli i wykluczenia konkretnych znaków.
-

-
12. Oprogramowanie powinno oceniać poziom bezpieczeństwa wygenerowanego hasła oraz zawierać wyjaśnienie czynników wpływających na jego siłę.
 13. Oprogramowanie musi umożliwiać udostępnianie haseł w obrębie organizacji wykorzystując mechanizm grup współdzielonych.
 14. Oprogramowanie musi umożliwiać jednorazowe udostępnianie haseł dla użytkowników spoza organizacji za pomocą tymczasowych linków z ważnością czasową.
 15. Oprogramowanie musi umożliwiać import haseł z innych menedżerów haseł, minimum:
 - a. Google Chrome,
 - b. Mozilla Firefox,
 - c. Apple Safari,
 - d. Opera,
 - e. KeePass.
 16. Podczas importu należy zachować podział na grupy i foldery zgodnie ze strukturą pliku źródłowego. W przypadku zagnieżdżonych grup lub folderów dopuszcza się spłaszczenie ich struktury.
 17. Oprogramowanie musi udostępniać możliwość przeglądania załączników do haseł za pomocą dedykowanego widoku na portalu.
 18. Oprogramowanie musi automatycznie weryfikować i oznaczać hasła, które pojawiły się w publicznych bazach wycieków danych. Wycieknięte hasła muszą być wyraźnie oznaczone umożliwiając ich identyfikację oraz natychmiastową zmianę.
 19. Oprogramowanie musi udostępniać ogólny wskaźnik siły haseł dla administratorów.
 20. Oprogramowanie musi umożliwiać nadawanie miękkich (nieblokujących możliwości dodawania / edycji wpisów) wymagań na hasła z grup współdzielonych oraz wyświetlać ewentualne naruszenia w panelu administratora.
 21. Minimalne wymagania dotyczące zarządzania użytkownikami i przywilejami:
 22. Oprogramowanie musi umożliwiać zarządzanie użytkownikami w ramach licencji w formie tworzenia, edycji oraz usuwania.
 23. Oprogramowanie musi udostępniać konto organizacji, kierowników oraz użytkowników.
-

-
24. Oprogramowanie wdrożone w środowisku informatycznym Zamawiającego musi umożliwiać integrację z Active Directory.
 25. Oprogramowanie musi umożliwiać nadawanie dostępu do całych grup współdzielonych w formie opcji zarządzania, zarządzania z możliwością dalszego udostępniania lub read-only (tylko do odczytu).
 26. Oprogramowanie musi umożliwiać nadawanie dostępu do poszczególnych wpisów w grupach współdzielonych w formie opcji zarządzania, zarządzania z możliwością dalszego udostępniania lub read-only (tylko do odczytu).
 27. Oprogramowanie musi umożliwiać dostęp do danych na temat aktywności użytkowników.
 28. Oprogramowanie musi umożliwiać dostęp do raportów o ujawnionych hasłach w wyniku wycieków danych logowania.
 29. Oprogramowanie musi umożliwiać nadawanie i odbieranie przywilejów do tworzenia grup współdzielonych i/lub personalnych dla użytkowników.
 30. Oprogramowanie musi umożliwiać dostęp do logów systemowych, zbierających informacje o aktywności użytkowników w zakresie minimum:
 - a. Aktywacji konta,
 - b. Zmiany danych dostępowych konta,
 - c. Udanych oraz nieudanych prób logowania,
 - d. Tworzenia/modyfikacji/usuwania grup/wpisów,
 - e. Momentu otrzymania / utraty dostępu do grupy wpisów.
 - f. Zdarzeń dotyczących administrowania użytkownikami,
 - g. Udostępniania grup oraz wpisów wewnątrz oraz na zewnątrz organizacji
 31. Oprogramowanie musi umożliwiać przesyłanie logów systemowych do zewnętrznego systemu zarządzania logami z wykorzystaniem protokołu Syslog.
 32. Logi systemowe muszą jednoznacznie identyfikować użytkownika oraz urządzenie, z którego wykonywane są zdarzenia, poprzez zapisanie nazwy użytkownika, nazwy urządzenia oraz adresu IP.
 33. Oprogramowanie musi umożliwiać eksport logów do formatu minimum .csv z możliwością definicji zakresu czasowego, typu logów czy użytkownika, którego dotyczą.
-

34. Oprogramowanie musi umożliwiać monitorowanie i zarządzanie aktywnymi sesjami użytkownika, a także pozwalać na zamknięcie wszystkich istniejących.

Minimalne wymagania dotyczące szyfrowania:

1. Oprogramowanie musi umożliwiać nadanie dwóch haseł użytkownika, jedno do konta, drugie do szyfrowania/odszyfrowania danych.
2. Oprogramowanie musi umożliwiać zmianę i reset hasła do konta.
3. Oprogramowanie musi umożliwiać zmianę hasła wykorzystywanego do szyfrowania/odszyfrowania danych.
4. Oprogramowanie musi stosować minimum funkcję PBKDF2 na poziomie minimum 800000 iteracji.
5. Oprogramowanie musi stosować szyfrowanie symetryczne oraz asymetryczne w procesie zabezpieczania wpisów z hasłami, wykorzystując klucze min. RSA o długości minimum 2048 bitów oraz szyfrowania min. AES w trybie GCM.
6. Oprogramowanie musi umożliwić użytkownikowi nadania sobie weryfikacji dwuetapowej w postaci minimum:
 - a. Kodu SMS,
 - b. Kodu e-mail,
 - c. Kodu w aplikacji zewnętrznego dostawcy (np. Google Authenticator, Microsoft Authenticator),
 - d. Sprzętowych kluczy zabezpieczających.

Minimalne wymagania dotyczące wtyczki do przeglądarki:

1. Oprogramowanie musi umożliwić pobranie i uruchomienie wtyczki w przeglądarkach minimum:
 - a. Google Chrome,
 - b. Mozilla Firefox,
 - c. Apple Safari.
 2. Oprogramowanie w postaci wtyczki musi obsługiwać logowanie za pomocą tych samych kont co na portalu WWW.
 3. Oprogramowanie musi umożliwiać obsługę weryfikacji dwuetapowej 2FA.
 4. Oprogramowanie musi umożliwiać dodawanie wpisów wewnątrz wtyczki.
 5. Oprogramowanie musi umożliwiać otworzenie wtyczki w nowym oknie.
 6. Oprogramowanie musi umożliwiać automatyczne proponowanie dodawania wpisów w przypadku wykrycia logowania na nowym portalu.
-

7. Oprogramowanie musi umożliwiać przeglądanie posiadanych wpisów wraz z możliwością kopiowania poszczególnych danych.

8. Oprogramowanie musi posiadać wbudowany generator haseł umożliwiający definiowanie złożonych haseł o określonej długości z możliwością dostosowania występowania wielkich liter, małych liter, cyfr oraz symboli i wykluczenia konkretnych znaków.

9. Oprogramowanie musi umożliwiać aktualizację wpisów w przypadku wykrycia zmiany hasła na portalu.

10. Oprogramowanie musi umożliwiać funkcjonalność automatycznego wypełniania pól formularza logowania za pomocą nakładki loginem i hasłem dodanym wcześniej do banku haseł.

Minimalne wymagania dotyczące aplikacji mobilnej:

1. Oprogramowanie musi umożliwić pobranie i uruchomienie aplikacji minimum na systemach mobilnych w sklepach:

a. Google Play na urządzenia mobilne z systemem Android,

b. Apple AppStore na urządzenia mobilne z systemem iOS.

2. Oprogramowanie w postaci aplikacji mobilnej musi obsługiwać logowanie za pomocą tych samych kont co na portalu WWW.

3. Oprogramowanie musi umożliwiać obsługę weryfikacji dwuetapowej 2FA.

4. Oprogramowanie musi umożliwiać dodawanie wpisów wewnątrz aplikacji mobilnej.

5. Oprogramowanie musi umożliwiać przeglądanie i edycję posiadanych wpisów wraz z możliwością kopiowania poszczególnych danych.

6. Oprogramowanie musi posiadać wbudowany generator haseł umożliwiający definiowanie złożonych haseł o określonej długości z możliwością dostosowania występowania wielkich liter, małych liter, cyfr oraz symboli i wykluczenia konkretnych znaków.

7. Oprogramowanie musi umożliwiać obsługę kodów TOTP poprzez generowanie jednorazowych kodów, skanowanie kodów QR oraz manualne wprowadzanie kodów sekret.



8. Oprogramowanie musi powiadamiać użytkownika o nowych dostępach udostępnionych dla niego przez innych użytkowników.

9. Oprogramowanie musi umożliwiać udostępnianie grup oraz pojedynczych wpisów.

Minimalne wymagania dotyczące wdrożenia i obsługi:

Wykonawca zapewni bezpłatne szkolenia w zakresie użytkowania i administrowania wdrożonego systemu. Szkolenie ma zostać przeprowadzone dla maksymalnie 2 osób i muszą być zakończone przyznaniem certyfikatu, potwierdzającego wspomniane umiejętności wydanym przez producenta systemu. Szkolenia mogą odbyć się w formie zdalnej.

Licencja

Na 4 stanowiska komputerowe. Dostarczone rozwiązanie musi być w formie licencji wieczystej oraz być objęte wsparciem producenta lub producentów do 30.06.2026 roku.

11. Serwerowy system operacyjny

Nazwa	Minimalne wymagania dla oprogramowania
Typ	Serwerowy system operacyjny
Wymagania ogólne	<p>Licencja musi uprawniać do uruchamiania Serwerowego Systemu Operacyjnego (SSO) w środowisku fizycznym i minimum 4 wirtualnych środowisk serwerowych systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. oraz minimum 35 szt. licencji dostępowych do zasobów serwera dla użytkownika.</p> <p>Serwerowy System Operacyjny (SSO) musi posiadać następujące, wbudowane cechy.</p> <ol style="list-style-type: none"> 1. Możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym 2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny. 3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych. 4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 9. Wbudowane wsparcie instalacji i pracy na wolumenach, które: <ol style="list-style-type: none"> a. pozwalają na zmianę rozmiaru w czasie pracy systemu, b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).

10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
12. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET
13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilkoma serwerami.
14. Wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15. Graficzny interfejs użytkownika.
16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
18. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
19. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
20. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
21. Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).
22. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
 - a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
 - b. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
 - Podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
 - Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
 - Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
 - c. Zdalna dystrybucja oprogramowania na stacje robocze.

- d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
 - e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
 - Dystrybucję certyfikatów poprzez http
 - Konsolidację CA dla wielu lasów domeny,
 - Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen.
 - f. Szyfrowanie plików i folderów.
 - g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
 - h. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
 - i. Serwis udostępniania stron WWW.
 - j. Wsparcie dla protokołu IP w wersji 6 (IPv6),
 - k. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
 - l. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
 - Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
 - Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
 - Obsługi 4-KB sektorów dysków
 - Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
 - Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
 - Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model)
23. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
24. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).



25.Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.

26.Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.

27.Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

Wymagania dotyczące licencji i wsparcia	System operacyjny musi być nowy, nigdy wcześniej nie aktywowany w najnowszej dostępnej na rynku wersji.
Ilość	1 szt.

12. Serwerowy system operacyjny

Nazwa	Minimalne wymagania dla oprogramowania
Typ	Serwerowy system operacyjny
Wymagania ogólne	<p>Licencja musi uprawniać do uruchamiania Serwerowego Systemu Operacyjnego (SSO) w środowisku fizycznym i minimum 2 wirtualnych środowisk serwerowych systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. oraz minimum 10 szt. licencji dostępowych do zasobów serwera dla użytkownika.</p> <p>Serwerowy System Operacyjny (SSO) musi posiadać następujące, wbudowane cechy.</p> <ol style="list-style-type: none"> 1. Możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym 2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny. 3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych. 4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 9. Wbudowane wsparcie instalacji i pracy na wolumenach, które: <ol style="list-style-type: none"> b. pozwalają na zmianę rozmiaru w czasie pracy systemu, c. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, d. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, e. umożliwiają zdefiniowanie list kontroli dostępu (ACL).

10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
12. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET
13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilkoma serwerami.
14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15. Graficzny interfejs użytkownika.
16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
18. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
19. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
20. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
21. Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).
22. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
 - b. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
 - c. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
 - Podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
 - Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
 - Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
 - d. Zdalna dystrybucja oprogramowania na stacje robocze.

- e. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
 - f. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
 - Dystrybucję certyfikatów poprzez http
 - Konsolidację CA dla wielu lasów domeny,
 - Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen.
 - g. Szyfrowanie plików i folderów.
 - h. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
 - i. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
 - j. Serwis udostępniania stron WWW.
 - k. Wsparcie dla protokołu IP w wersji 6 (IPv6),
 - l. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
 - m. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
 - Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
 - Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
 - Obsługi 4-KB sektorów dysków
 - Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
 - Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
 - Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model)
23. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
24. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).



25.Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.

26.Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.

27.Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

Wymagania dotyczące licencji i wsparcia	System operacyjny musi być nowy, nigdy wcześniej nie aktywowany w najnowszej dostępnej na rynku wersji.
Ilość	2 szt.

**13. Szkolenia dla działu IT i dla pracowników spoza działu IT**

Nazwa	Minimalne wymagania dla szkolenia
Typ	Szkolenia socjotechniczne - phishing oraz szkolenie cyberbezpieczeństwa
Szkolenie socjotechniczne phishing	<p>W ramach realizacji przedmiotu zamówienia, Wykonawca zobowiązany jest do przeprowadzenia testów phishingowych (TP) wg poniższego zakresu minimalnego:</p> <ol style="list-style-type: none"> 1. Zamawiający wymaga ustalenia scenariusza w zakresie minimum: Opracowania i zatwierdzenie z Zamawiającym szczegółowego scenariusza ataku socjotechnicznego. Wyboru metod i narzędzi do jego realizacji. Szczegóły kampanii, w tym scenariusze socjotechniczne oraz harmonogram realizacji, muszą zostać ustalone i zatwierdzone przez Zamawiającego co najmniej 14 dni przed planowanym rozpoczęciem kampanii. 2. Zamawiający wymaga przeprowadzenia przygotowań ataku w zakresie minimum: <ul style="list-style-type: none"> • Projektowanie minimum jednego szablonu mailowego • Przygotowanie minimum jednej fałszywej domeny i konfiguracja hostingu. • Listy odbiorców • Finalizacja listy docelowych odbiorców w oparciu o informacje uzyskane od Zamawiającego. 3. Zamawiający wymaga przeprowadzenia startu realizacji ataku w zakresie minimum: <ul style="list-style-type: none"> • Rozpoczęcie kampanii phishingowej: kampania musi zostać przeprowadzona w ciągu minimum 3 dni, rozpoczynając się od wysyłki mailowej do wybranych odbiorców. 4. Zamawiający wymaga kontynuacji kampanii i monitorowania w zakresie minimum: <ul style="list-style-type: none"> • Dostosowania harmonogramu wysyłki do ustaleń przeprowadzonych z Zamawiającym na etapie ustalania scenariusza. • Czas trwania kampanii: minimum 3 dni robocze, liczba dni zostaje dostosowana w oparciu o ustalenia z Zamawiającym podczas pierwszego etapu jakim jest ustalenie scenariusza. • Kampania powinna być realizowana etapami, z wysyłkami dokonywanymi w określonych partiach i godzinach, aby zapewnić maksymalną skuteczność. • Bieżące śledzenie odpowiedzi i interakcji odbiorców z wysłanymi wiadomościami



	<ul style="list-style-type: none"> Analizy efektywności i w razie potrzeby, wprowadzanie zmian w strategii kampanii. <p>5. Zamawiający wymaga przeprowadzenia zakończenia kampanii i przygotowanie raportu w zakresie minimum:</p> <ul style="list-style-type: none"> Zebrania i dokonania pierwszej analizy zebranych danych na temat interakcji i reakcji na przeprowadzone działania. Przygotowania raportu końcowego dotyczącego skuteczności kampanii, zawierającego wszystkie zebrane dane, w zakresie minimum: opis wykorzystanych i skonfigurowanych domen opis szablonów oraz opis celu jaki stanowił podczas realizacji kampanii opis niebezpieczeństw związanych z dalszymi krokami prawdziwego ataku statystyki kampanii phishingowej, w tym: liczby wysłanych, otwartych maili, liczby kliknięć w link, liczby osób, które podały swoje dane. podsumowanie oraz rekomendacje.
Szkolenie cyberbezpieczeństwa	<p>Szkolenie musi zostać przeprowadzone w minimum 3 grupach.</p> <p>Szkolenie musi trwać minimum 1 h.</p> <p>Wymagane jest, aby szkolenie przeprowadzone było, w formie online.</p> <p>Szkolenie musi być zrealizowane w formie vouchera z możliwością zrealizowania w wybranym przez Zamawiającego terminie w przeciągu minimum 12 miesięcy od daty dostarczenia.</p> <p>Szkolenie musi obejmować w zakresie minimum:</p> <ul style="list-style-type: none"> Wycieki informacji – mechanizmy i skutki. Zarządzanie hasłami – dobre praktyki i narzędzia pomocnicze. Psychomanipulacja w sieci – zasady i zastosowania. Sfałszowane komunikaty i strony – identyfikacja zagrożeń. Ataki głosowe i podszywanie się pod identyfikator dzwoniącego (vishing) Archiwizacja internetowa – cyfrowy ślad nie znika. Mechanizmy śledzenia w sieci – rola i funkcja cookies. Niebezpieczeństwa ze strony nieautoryzowanego sprzętu. Ataki siłowe na hasła – jak nie dać się złamać. Wyłudzenie informacji przez celowane ataki phishingowe (spear phishing). Świadomość pracowników – kultura bezpieczeństwa w organizacji.
Wymagania dodatkowe	<p>Zamawiający wymaga, aby szkolenia dedykowane dla pracowników jednostki zorganizowane były przez jednostki posiadające stosowną wiedzę oraz m.in. 2 letnie doświadczenie w przygotowaniu</p>

	i przeprowadzeniu szkoleń budujących i wzmacniających świadomość cyberzagrożeń.
Ilość	1 szt.

Nazwa	Minimalne wymagania dla szkolenia
Typ	Szkolenia dla pracownika IT
Szkolenie	<p>W ramach realizacji przedmiotu zamówienia, Wykonawca zobowiązany jest dostarczyć Voucher uprawniający do skorzystania z określonego szkolenia autoryzowanego dotyczącego cyberbezpieczeństwa systemów operacyjnych, poruszającego tematy:</p> <ul style="list-style-type: none"> • analizy i skanowania w sieci • weryfikacji i wyszukiwania dostępnych exploitów na aplikacje wykorzystywane w organizacji • ataki na systemy operacyjne Windows oraz Linux • ataki na aplikacje w systemach operacyjnych • ataki na bazy danych • ataki na przeglądarki internetowe • szybkiej identyfikacji możliwych ataków na systemy Windows i ich uniemożliwianie • szybkiej identyfikacji możliwych ataków na systemy Linux i ich uniemożliwianie • podstawowy Port knocking-u
Wymagania dodatkowe	Zamawiający wymaga, aby szkolenie autoryzowane przeprowadzone było przez autoryzowane centrum szkoleniowe, świadczące usługi szkoleniowe przez okres min. 2 lat. Formuła szkolenia: on-line. Ważność vouchera 1 rok.
Ilość	1 szt.

Nazwa	Minimalne wymagania dla szkolenia
Typ	Szkolenia dla pracownika IT
Szkolenie	<p>W ramach realizacji przedmiotu zamówienia, Wykonawca zobowiązany jest dostarczyć Voucher uprawniający do skorzystania z określonego szkolenia autoryzowanego dotyczącego technik pozyskiwania informacji, ślady cyfrowe, poruszającego tematy:</p>



	<ul style="list-style-type: none">• fundamenty bezpieczeństwa operacyjnego (OPSEC)• przygotowanie i uruchomienie stanowiska OSINT• narzędzia OSINT klasyczne, wsparcie AI• Media społecznościowe (SOCMINT) oraz automatyzacja• Darknet OSINT
Wymagania dodatkowe	Zamawiający wymaga, aby szkolenie autoryzowane przeprowadzone było przez autoryzowane centrum szkoleniowe, świadczące usługi szkoleniowe przez okres min. 2 lat. Formuła szkolenia: on-line. Ważność vouchera 1 rok.
Ilość	1 szt.