Numer sprawy: Or.ZP.271.21.2024

Biała Piska, dnia 25 października 2024 r.

Gmina Biała Piska
ul. Plac Adama Mickiewicza 25
12-230 Biała Piska

Szczegółowy Opis Przedmiotu Zamówienia

Zakup sprzętu i oprogramowania informatycznego związany z realizacją projektu w ramach grantu Cyberbezpieczny Samorząd

Spis treści

1. Zestawienie ilościowe.

Część nr 1 – Zakup sprzętu i oprogramowania informatycznego.

Lp.	Nazwa	Ilość
1.	Zakup klastra serwerowego	1 szt.
2.	Zakup usług wdrożenia klastra serwerowego	1 szt.
3.	Zakup oprogramowania serwerowego systemu operacyjnego	1 szt.
4.	Zakup UPS	1 szt.
5.	Zakup UPS do stacji roboczych	30 szt.

Część nr 2 – Zakup oprogramowania do cyberbezpieczeństwa.

Lp.	Nazwa	Ilość
1.	Zakup licencji i wdrożenie oprogramowania SIEM	1 szt.
2.	Rozbudowa oprogramowania antywirusowego o funkcje EDR i wykrywanie podatności	1 szt.

2. Szczegółowy opis przedmiotu zamówienia dla części nr 1.

2.1. Wymagania ogólne w zakresie dostawy sprzętu i oprogramowania.

1. Dostarczony sprzęt i oprogramowanie muszą być wolne od wad prawnych i fizycznych oraz nienoszący oznak użytkowania.
2. Dostarczony sprzęt i oprogramowanie muszą być fabrycznie nowe (tzn. wyprodukowane nie wcześniej, niż na 9 miesięcy przed ich dostarczeniem), muszą pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski, pochodzić z seryjnej produkcji z uwzględnieniem opcji konfiguracyjnych przewidzianych przez producenta dla oferowanego modelu sprzętu i oprogramowania.
3. Niedopuszczalne są produkty prototypowe, nie dopuszcza się urządzeń długotrwale magazynowanych oraz pochodzących z programów wyprzedażowych producenta. Urządzenia nie mogą znajdować się na liście „end-of-sale", „end-of-support", „end-of-life" producenta.
4. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy) jakichkolwiek portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, itp., niedopuszczalne jest zastosowanie jakichkolwiek zewnętrznych przejściówek czy konwerterów.
5. Wszystkie urządzenia będą zasilane bezpośrednio z sieci 230V.
6. Wykonawca zapewni dostawę do każdej wskazanej przez Zamawiającego lokalizacji.
7. Wykonawca jest odpowiedzialny za skonfigurowanie połączeń fizycznych, logicznych, podłączenie i skonfigurowanie urządzeń do działania, pozwalające na rozpoczęcie pracy oraz dostarczenie

odpowiedniej ilości kabli zasilających, połączeniowych w celu przygotowania zamawianego sprzętu do działania.

8. Wykonawca zobowiązany jest do skonfigurowania zamawianego sprzętu w uzgodnieniu z Zamawiającym.
9. Prace instalacyjne będzie można realizować wyłącznie w terminach uzgodnionych z Zamawiającym.
10. W ramach prac konfiguracyjnych klastra serwerowego Zamawiający oczekuje wdrożenie klastra, w tym minimum wymaga: zaprojektowania schematu logicznego LAN dla dostarczanej infrastruktury wraz z uwzględnieniem istniejącej infrastruktury; opracowania założeń optymalizacji ruchu i zapewnienia bezpieczeństwa implementacji i separacji sieci; instalacji urządzeń w szafie RACK; podłączenia urządzeń kablami zasilającymi do gniazd UPS, wykonania aktualizacji oprogramowania i firmware'ów na urządzeniach; skonfigurowania połączeń sieciowych na urządzeniach zgodnie z wcześniej zaprojektowanym schematem logicznym; migracja maszyn wirtualnych, wykonanie testów akceptacyjnych polegających na weryfikacji poprawności pracy dostarczonych urządzeń; opracowanie i przekazanie Zamawiającemu dokumentacji powykonawczej zainstalowanych urządzeń oraz wykonanych prac instalacyjno-konfiguracyjnych.
11. W ramach zamówienia Wykonawca jest zobowiązany do dostarczenia urządzeń i oprogramowania oraz konfiguracji klastra HA w zakresie oprogramowania dla trzech serwerów serwerowego systemu operacyjnego Microsoft Windows Serwer 2022 Standard lub równoważnego zgodnie z kryteriami równoważności określonymi poniżej dla każdego serwera wraz z licencjami dostępowymi umożliwiającymi korzystanie z zasobów klastra dla 50 użytkowników.
12. Wykonawca będzie zobowiązany do złożenia dokumentacji powykonawczej, zawierającej w szczególności wszystkie dane dostępu do urządzeń i oprogramowania, które będą wykorzystywane podczas instalacji i konfiguracji sprzętu i oprogramowania.
13. Dla dostaw sprzętu informatycznego z oprogramowaniem Zamawiający wymaga fabrycznie nowego oprogramowania (nieużywanego nigdy wcześniej), w wersji z certyfikatem autentyczności dla każdej licencji, o ile producent oferowanego oprogramowania stosuje certyfikaty autentyczności. Wykonawca zobowiązany jest do dostarczenia fabrycznie nowego oprogramowania (w tym systemu operacyjnego) nieużywanego oraz nigdy wcześniej nieaktywowanego na innym urządzeniu oraz pochodzącego z legalnego źródła sprzedaży. W przypadku oprogramowania naklejka hologramowa winna być zabezpieczona przed możliwością odczytania klucza za pomocą zabezpieczeń stosowanych przez producenta, o ile producent oferowanego oprogramowania stosuje takie zabezpieczenia. Zamawiający zastrzega możliwość weryfikacji dostarczonego oprogramowania na etapie oceny ofert jak i na etapie dostawy pod kątem legalności oprogramowania bezpośrednio u producenta oprogramowania. Zamawiający zastrzega możliwość żądania od Wykonawcy na etapie dostawy przedstawienia dokumentów dotyczących zakupu oprogramowania (faktury, rachunki) w autoryzowanym kanale dystrybucyjnym producenta oprogramowania.

2.2. Zasada równoważności rozwiązań i neutralności technologicznej.

1. Za równoważne do wyspecyfikowanego rozwiązania Zamawiający uzna rozwiązanie o tym samym przeznaczeniu, cechach technicznych, jakościowych i funkcjonalnych odpowiadających cechom

technicznym, jakościowym i funkcjonalnym wskazanych w opisie przedmiotu zamówienia, lub lepszych, oznaczonych innym znakiem towarowym, patentem lub pochodzeniem.

2. Rozwiązanie równoważne musi pozwalać na zrealizowanie zakładanego przez Zamawiającego celu poprzez parametry wydajnościowe i funkcjonalne, mające wpływ na skuteczność działania, takie same lub lepsze od wskazanych wymagań minimalnych.
3. Użycie w opisie przedmiotu zamówienia nazw rozwiązań służy ustaleniu minimalnego standardu wykonania i określenia właściwości i wymogów technicznych założonych w dokumentacji technicznej dla projektowanych rozwiązań lub też stosowane jest w celu wskazania aktualnie użytkowanego środowiska Zamawiającego, z którym rozwiązanie równoważne powinno być kompatybilne.
4. Wykonawca zobligowany jest do wykazania, że oferowane rozwiązania równoważne spełnią zakładane wymagania minimalne. Wykonawca, który złoży ofertę na produkty równoważne musi do oferty załączyć dokumenty zawierające dokładny opis oferowanych produktów, z którego wynikać będzie zachowanie warunków równoważności. Wykonawca, który posługuje się równoważnymi certyfikatami musi je załączyć do oferty. Przez certyfikat równoważny Zamawiający rozumie certyfikat analogiczny co do zakresu z certyfikatami wskazanymi z nazwy, który potwierdza spełnianie normy charakteryzującej się cechami właściwymi dla normy wymienionej przez Zamawiającego, wystawiony przez niezależny podmiot uprawniony do wystawiania certyfikatów.
5. Brak określenia „minimum" oznacza wymaganie na poziomie minimalnym, a Wykonawca może zaoferować rozwiązanie o lepszych parametrach.
6. 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 lub jest lepsze od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym.
7. 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.
8. Przez bardzo zbliżoną (podobną) 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.
9. W przypadku wskazania przez Zamawiającego określonych testów wydajności Zamawiający zastrzega, iż w celu sprawdzenia poprawności przeprowadzonych testów może wezwać Wykonawcę do przedstawienia wskazanego przez Zamawiającego oprogramowania testującego wraz z testowanym urządzeniem i/lub oprogramowaniem. Wszystkie testy wydajnościowe wykonawca musi przeprowadzić w oferowanej konfiguracji, przy automatycznych ustawieniach konfiguratora oprogramowania testującego i natywnej rozdzielczości wyświetlacza oraz

włączonych wszystkich urządzaniach. Nie dopuszcza się stosowania overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację), jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). Zamawiający dopuszcza prowadzenie testów wydajnościowych w oparciu o dowolny system operacyjny zainstalowany na urządzeniu.

10. W przypadku wskazania przez Zamawiającego określonych testów wydajności Zamawiający dopuszcza równoważne im testy wydajnościowe umożliwiające potwierdzenie zakładanych poziomów wydajności. W przypadku użycia przez Wykonawcę równoważnych testów wydajności Zamawiający zastrzega, iż w celu sprawdzenia równoważności przeprowadzonych testów Wykonawca może zostać wezwany do dostarczenia Zamawiającemu wskazanego przez Zamawiającego oprogramowania testującego i równoważnego do niego oprogramowania testującego wraz z testowanym urządzeniem i/lub oprogramowaniem. Wszystkie testy wydajnościowe wykonawca musi przeprowadzić w oferowanej konfiguracji, przy automatycznych ustawieniach konfiguratora oprogramowania testującego i natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowania overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację), jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). Zamawiający dopuszcza prowadzenie testów wydajnościowych w oparciu o dowolny system operacyjny zainstalowany na urządzeniu.
11. Dodatkowo, wszędzie tam, gdzie zostało wskazane pochodzenie (marka, znak towarowy, producent, dostawca itp.) materiałów lub normy, aprobaty, specyfikacje i systemy, o których mowa w ustawie Prawo Zamówień Publicznych (zwana dalej ustawą), Zamawiający dopuszcza oferowanie sprzętu lub rozwiązań równoważnych pod warunkiem, że zapewnią uzyskanie parametrów technicznych takich samych lub lepszych niż wymagane przez Zamawiającego w dokumentacji przetargowej. Zamawiający dopuszcza oferowanie materiałów lub urządzeń równoważnych. Materiały lub urządzenia pochodzące od konkretnych producentów określają minimalne parametry jakościowe i cechy użytkowe, a także jakościowe (m.in.: wymiary, skład, zastosowany materiał, kolor, odcień, przeznaczenie materiałów i urządzeń, estetyka itp.) jakim muszą odpowiadać materiały lub urządzenia oferowane przez Wykonawcę, aby zostały spełnione wymagania stawiane przez Zamawiającego. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Posługiwanie się nazwami producentów / produktów ma wyłącznie charakter przykładowy. Zamawiający, wskazując oznaczenie konkretnego producenta (dostawcy), konkretny produkt lub materiały przy opisie przedmiotu zamówienia, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych lub lepszych parametrach. Zamawiający opisując przedmiot zamówienia przy pomocy określonych norm, aprobat czy specyfikacji technicznych i systemów odniesienia dopuszcza rozwiązania równoważne opisywanym. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy spełniają wymagania określone przez Zamawiającego. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów uwiarygodniających te rozwiązania.

2.3. Zakup klastra serwerowego (1 szt.).

Minimalne parametry techniczne klastra serwerowego:

1. System musi zostać dostarczony w modelu hiperkonwergentnym tzn. z wykorzystaniem serwerów z zainstalowanymi procesorami, posiadającymi dyski wewnętrzne, które tworzą warstwę zasobów przechowywania danych.
2. Zamawiający wymaga dostarczenia jednego klastra składającego się z 3 serwerów, z możliwością rozbudowy do 4 serwerów.
3. Każdy z serwerów w klastrze powinien posiadać:
    a. min. 2 procesory wielordzeniowe osiągające w teście wydajności CPU PassMark Performance Test (https://www.cpubenchmark.net) z wynikiem aktualnym w okresie 30 dni przed terminem składania ofert co najmniej wynik 28 000 punktów. Zamawiający żąda załączenia do oferty przedmiotowego środka dowodowego określonego w SWZ potwierdzającego spełnienie dla procesora dedykowanego do pracy z zaoferowanym serwerem żądanej przez Zamawiającego wydajności;
    b. min. 512 GB pamięci RAM z możliwością instalacji 16 kości pamięci RAM;
    c. min. 2 porty 10 GbE SFP+;
    d. min. 2 porty 25/10 GbE SFP28;
    e. min. 4 dyski SSD o pojemności 3.84 TB z możliwością rozbudowy do 6 dysków;
4. Cały klaster powinien posiadać redundantne zasilacze.
5. Klaster powinien stanowić rozwiązanie składające się ze sprzętu serwerowego, wirtualizatora, pamięci masowej zdefiniowanej programowo umożliwiające ochronę i zabezpieczenie danych i umożliwiające zintegrowane zarządzanie.
6. Wszystkie komponenty rozwiązania muszą być zarządzane z jednego miejsca, za pomocą wbudowanego i zintegrowanego narzędzia.
7. Rozwiązanie musi być niezależne od sprzętu, tj. nie może być ograniczone do określonego dostawcy sprzętu. Wymagana jest możliwość przenoszenia zaoferowanej licencji lub subskrypcji pomiędzy wszystkimi wspieranymi platformami w dowolnym momencie ich obowiązywania.
8. Klaster musi posiadać możliwość wykonywania i monitorowania aktualizacji wszystkich komponentów rozwiązania za pomocą pojedynczego narzędzia zarządzania. Narzędzie musi wykonywać automatyczną weryfikację kompatybilności wersji oprogramowania.
9. Klaster musi utrzymywać określony poziom odporności na awarie oraz stałą wydajność w przypadku awarii, bez konieczności interwencji administratora. Musi także przywrócić odporność tak szybko jak tylko możliwe.
10. Rozwiązanie musi być niezależne od sieci, nie może wymagać określonego sprzętu sieciowego.
11. Rozwiązanie musi zapewniać wbudowaną funkcję udostępniania usług pamięci masowej dla maszyn wirtualnych i kontenerów blokowe zasoby iSCSI; plikowe zasoby – poprzez protokoły NFS i SMB.
12. Rozwiązanie musi wspierać różne warstwy pamięci masowej minimum w zakresie: SSD i NVMe jako warstwa wydajnościowa oraz NL-SAS/SATA/SSD jako warstwa pojemnościowa.
13. Rozwiązanie musi zapewniać zautomatyzowane, działające w czasie rzeczywistym, wielowarstwowe składowanie danych (ang. tiering) pomiędzy nośnikami SSD/NVMe (warstwa buforująca i wydajnościowa) oraz HDD/SSD (warstwa pojemnościowa), w celu zapewnienia optymalnej wydajności.

14. W przypadku rozwiązania opartego o technologię cache'owania danych, wymagany współczynnik warstwy wydajnościowej do warstwy pojemnościowej to min. 30%.
15. W przypadku rozwiązania opartego o technologie cache'owania danych, Zamawiający wymaga odpowiedniej wydajności: minimum 140 000 zapisów/s oraz wytrzymałości na poziomie 20 000 TBW.
16. Rozwiązanie musi umożliwiać utworzenie kontenera danych bez współczynnika odporności tzw. RAID 0 lub Resiliance Factor 1, który będzie przeznaczony dla aplikacji i baz danych posiadające wewnętrzne mechanizmy replikacji danych.
17. Wszystkie węzły muszą być hiperkonwergentne, a lokalne (wewnętrzne) dyski wszystkich węzłów muszą stanowić klaster prezentowany jako pojedyncza i rozproszona pula zasobów dostępna dla wszystkich węzłów kontrolowanych przez wirtualizator.
18. Rozwiązanie musi umożliwiać dodawanie serwerów typu Storage Node, które powiększają sumaryczną pojemność klastra, lecz nie umożliwiają uruchomiania maszyn wirtualnych na tych serwerach.
19. Rozwiązanie musi zapewniać usługę kompresji danych, w trybie inline oraz post-process, w ramach dostarczonej licencji. Wymaganie dotyczy zarówno konfiguracji hybrydowych, jak i All-Flash.
20. Rozwiązanie musi posiadać funkcjonalność usuwania wielu nodów w klastra.
21. Poniższe usługi i parametry pamięci masowej muszą być konfigurowalne osobno dla każdej maszyny wirtualnej lub kontenera danych oraz muszą być zawarte w dostarczonej licencji: kompresja i deduplikacja.
22. Rozwiązanie musi zapewniać funkcję tworzenia kopii migawkowych oraz klonów maszyn wirtualnych, także z zapewnieniem spójności z punktu widzenia aplikacji (co najmniej dla systemów operacyjnych Windows oraz Linux) . Funkcja ta musi być wbudowana w platformę i realizowana na poziomie pamięci masowej.
23. W przypadku awarii pojedynczego serwera lub dysku, centralna konsola zarządzania system musi wskazywać przewidywany czas potrzeby do odbudowany danych.
24. Platforma musi zapewniać bliskość danych względem miejsca ich przetwarzania (ang. data locality). Oznacza to, że zastosowana architektura i wykorzystywane algorytmy rozkładania danych pomiędzy węzły platformy, muszą nieustannie zmierzać do umieszczenia danych należących do maszyny wirtualnej na lokalnych zasobach pamięci masowej węzła, na którym uruchomiona jest dana maszyna wirtualna.
25. System musi wspierać dyski SED.
26. System musi wspierać dwuskładnikowe uwierzytelnienie do Systemu.
27. System musi posiadać tak zwane zalecenia STIG (Security Technical Information Guides), regularnie aktualizowane i udostępniane przez producenta.
28. System musi posiadać mechanizm automatycznego wykrywania odchyleń od zaleceń STIG i automatycznie je naprawiać, zarówno w warstwie wirtualizacji jak i storage.
29. System musi być odporny na awarię dysku lub serwera, dowolnych komponentów Systemu, nie powodując przerwy w pracy Systemu.
30. System musi umożliwiać konfigurację polityki replikacji per maszyna wirtualna.
31. Zarządzanie Systemem musi odbywać się z pojedynczej konsoli za pomocą HTML5, CLI oraz RESTAPI
32. System musi umożliwiać bezprzerwową rozbudowę klastra, poprzez dołożenie kolejnych węzłów. System musi automatycznie rozłożyć równomiernie dane w klastrze, bez ingerencji administratora.

33. Konsola zarządzania Systemem musi umożliwiać uaktualnianie wersji Systemu (sterowniki serwerów, hypervisor, podsystem storage) bez przerwy w pracy Systemu dla dostarczonego rozwiązania serwerowego
34. System musi automatycznie sprawdzać kompatybilność podnoszonych elementów Systemu (sterowniki serwerów, hypervisor, podsystem storage) eliminując możliwość omyłkowego podniesienia jednego z komponentów do niewłaściwej wersji. System musi udostępniać szczegółowe informacje na temat maszyn wirtualnych: wydajność maszyn wirtualnych (utylizacja CPU/RAM/IOPS oraz opóźnienie/latency.
35. System musi wspierać REST API dla całej platformy.
36. System musi posiadać wbudowany Self Service Portal, z możliwością wydzielania zasobów CPU/RAM/storage dla konkretnych użytkowników bądź grup użytkowników, uwierzytelnionych przez Active Directory.
37. Do zaproponowanego systemu należy dostarczyć licencje na oprogramowanie wirtualizacyjne na każdy dostarczony serwer.
38. Oprogramowanie wirtualizacyjne musi zapewniać mechanizmy przenoszenia maszyn wirtualnych bezprzerwowo pomiędzy węzłami w klastrze.
39. Oprogramowanie wirtualizacyjne musi zapewniać mechanizmy HA w obrębię pojedynczego klastra
40. Oprogramowanie wirtualizacyjne musi posiadać mechanizm inteligentnego umiejscowienia nowych maszyn wirtualnych na serwerach o najmniejszym obciążeniu.
41. Oprogramowanie wirtualizacyjne musi posiadać mechanizm Affinity Rules.
42. Oprogramowanie wirtualizacyjne musi umożliwiać tworzenie i zarządzanie wirtualnymi sieciami.
43. Oprogramowanie wirtualizacyjne musi automatycznie przenosić bezprzerwowo maszyny wirtualne pomiędzy węzłami w klastrze w zależności od ich obciążenia.
44. Oprogramowanie wirtualizacyjne musi posiadać mechanizmy klonowania maszyn wirtualnych. Klonowanie maszyn wirtualnych musi integrować się z podsystem dyskowym w celu szybkiego wykonywania klonów.
45. Oprogramowanie wirtualizacyjne musi posiadać wirtualny przełącznik sieciowy, umożliwiający konfigurację ustawień sieci per klaster.
46. Oprogramowanie wirtualizacyjne musi wspierać UEFI dla maszyn wirtualnych.
47. Oprogramowanie wirtualizacyjne musi wspierać karty GPU.
48. Deduplikacja i kompresja muszą być od siebie niezależne. Oznacza to, że musi być możliwość włączenia tylko kompresji lub tylko deduplikacji, włączenia obydwu mechanizmów jednocześnie lub wyłączenie obydwu. Powyższe ustawienia muszą być konfigurowalne osobno dla poszczególnych maszyn wirtualnych.
49. Zamawiający wymaga aby dostarczone rozwiązanie było w pełni redundantne i kompletne, jeżeli do spełnienia wymagań, wymagane są dodatkowe licencje lub komponenty należy je dostarczyć.
50. Deklaracja zgodności CE lub inny równoważny dokument poświadczający, że oferowany klaster spełnia wszystkie zasadnicze wymagania zawarte w poszczególnych dyrektywach nowego podejścia przewidujących oznakowanie CE. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany klaster w zakresie określonym powyżej.
51. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci deklaracji RoHS dla produktu lub oświadczenia producenta klastra lub innego dokumentu potwierdzającego spełnienie

kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany klaster w zakresie określonym powyżej.

52. Wykonawca zapewni dostęp do wsparcia producenta umożliwiającego serwis oprogramowania 24 godziny x 7 dni w tygodniu x 365 dni w roku, rozwiązywanie problemów ze sprzętem i oprogramowaniem Systemu oraz z dostarczonym wirtualizatorem, dostęp do poprawek (patch, hotfix, update) i nowych wersji oprogramowania do dnia 25.03.2026 r.
53. Wykonawca udzieli lub zapewni udzielenie gwarancji na cały system na okres min. 36 miesięcy obejmującej wymianę uszkodzonych podzespołów sprzętowych na następny dzień roboczy od momentu potwierdzenia usterki.

2.4. Zakup usług wdrożenia klastra serwerowego (1 szt.).

1. Wykonawca przygotuje projekt techniczny realizacji koncepcji, uwzględniający dobre praktyki i rekomendacje eksploatacyjne, po wykonaniu analizy istniejącego u Zamawiającego rozwiązania wraz z koncepcją uruchomienia produkcyjnego klastra serwerowego, migracji maszyn wirtualnych, migracji baz danych SQL, Firebird, PostgreSQL, aktualizacji systemów operacyjnych Windows Serwer 2021 i 2019 uwzględniając obecne u Zamawiającego uwarunkowania organizacyjne i sprzętowe, łącznie zwane dalej projektem technicznym. W projekcie technicznym muszą być zawarte:
    a. opis koncepcji realizacji prac przy wykorzystaniu dostarczonego oprogramowania i sprzętu, opis migracji maszyn wirtualnych, migracji baz danych SQL, Firebird, PostgreSQL, aktualizacji systemów operacyjnych Windows Serwer 2021 i 2019 w zakresie wskazanym przez Zamawiającego,
    b. scenariusze testowe, procedury oraz wzory raportów testów,
    c. szczegółowy harmonogram realizacji prac wdrożeniowych i migracyjnych, uwzględniający specyfikę organizacji Zamawiającego,
    d. zalecenia przedwdrożeniowe dla Zamawiającego, jeżeli będą wymagane.
2. Akceptacja projektu technicznego wraz z procedurami oraz wzorami raportów z testów będzie podlegała następującej procedurze:
    a. Wykonawca przekaże do akceptacji Zamawiającego, drogą elektroniczną projekt techniczny wraz z procedurami oraz wzorami raportów z testów, w terminie nie dłuższym niż 30 dni kalendarzowych od dnia zawarcia umowy,
    b. Zamawiający w terminie nie dłuższym niż 7 dni roboczych od dnia dostarczenia przez Wykonawcę kompletnych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,
    c. wszystkie uwagi do dokumentów zgłoszone przez Zamawiającego zostaną wprowadzone przez Wykonawcę, w terminie nie dłuższym niż 5 dni roboczych od dnia ich otrzymania,
    d. Zamawiający w terminie 5 dni roboczych od dnia powtórnego dostarczenia przez Wykonawcę poprawionych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,

e. w przypadku nieuwzględnienia uwag Zamawiającego, Zamawiający zastrzega sobie prawo do wskazania ostatecznego terminu dostarczenia projektu technicznego wraz z procedurami oraz wzorami raportów z testów,
f. zatwierdzony projekt techniczny wraz procedurami zostaną przekazane Zamawiającemu w 1 egzemplarzu oraz w formie elektronicznej na pendrive, w postaci plików do edycji i PDF.

3. Wykonawca zrealizuje wdrożenie klastra serwerowego, wykona migracje maszyn wirtualnych zgodnie z zakresem prac i projektem technicznym, w tym Wykonawca przeniesie wszystkie wskazane maszyny wirtualne na oferowany klaster wraz z podniesieniem wersji zainstalowanego systemu operacyjnego do najnowszej w dniu składania oferty. Klaster zostanie tak skonfigurowany, aby można było nim zdalnie zarządzać i zostanie uruchomione dwuskładnikowe uwierzytelnianie na klastrze. Klaster zostanie tak skonfigurowany, aby jak najbardziej automatycznie zgłaszał problemy dla administratora pocztą email oraz automatycznie naprawiał błędy z wbudowanymi dyskami lub serwerami, i w przypadku problemów z serwerem, drugi serwer automatycznie przejmował pracę serwera uszkodzonego.
4. Wykonawca przeprowadzi testy akceptacyjne wdrożonych rozwiązań.
5. Wykonawca opracuje i przedstawi raport z testów. W przypadku zrealizowania scenariusza testowego z wynikiem negatywnym, Wykonawca przedstawi nowe rozwiązanie wadliwego elementu systemu i przeprowadzi ponowny test wg scenariusza, w terminie wyznaczonym przez Zamawiającego, dochowując terminu wykonania Umowy. Raport z testów powinien zawierać listę przeprowadzonych testów wraz z ich wynikiem.
6. Wykonawca opracuje dokumentację powykonawczą oraz procedury administracyjne i eksploatacyjne w zakresie uzgodnionym z Zamawiającym, w tym: dokumentację wdrożeniową, procedury operacyjne, procedury „Disaster Recovery". Akceptacja dokumentacji powykonawczej będzie przebiegała zgodnie z zasadami określonymi dla akceptacji projektu technicznego.

<u>Instruktaże.</u>

1. Instruktaże stanowiskowe będą prowadzone w języku polskim w siedzibie Zamawiającego i obejmą zakresem m.in.: użytkowane oprogramowanie; budowę, architekturę i konfigurację rozwiązania; administrowanie wdrożonym rozwiązaniem.
2. Instruktaże stanowiskowe zostaną przeprowadzone przez osoby prowadzące prace wdrożeniowe w ramach niniejszego zamówienia.
3. Instruktaże powinny trwać minimum 16 godzin lekcyjnych (45 minut) i będą przeprowadzone dla wskazanej przez Zamawiającego liczby osób (maksymalnie 4 osoby).
4. Zamawiający nie dopuszcza przeprowadzenia instruktaży w trybie zdalnym (online).
5. Administratorzy rozwiązania po zakończeniu Instruktaży stanowiskowych muszą w szczególności umieć wykonywać czynności administracyjne związane z obsługą, utrzymaniem i monitoringiem klastra serwerowego, znać i umieć realizować procedury backupu. Ponadto powinni znać typowe zagrożenia i problemy związane z funkcjonowaniem rozwiązania, a także sposoby ich przeciwdziałania, wykrywania i usuwania. Powinni umieć instalować, konfigurować, rekonfigurować, monitorować i prawidłowo eksploatować wdrożone rozwiązanie, jak również znać jego wdrożoną konfigurację.

2.5. Zakup oprogramowania serwerowego systemu operacyjnego (1 szt.).

Wykonawca dostarczy oprogramowanie serwerowego systemu operacyjnego na każdy serwer pracujący w klastrze klasy Microsoft Windows Serwer Standard w najnowszej wersji oprogramowania oferowanej przez producenta oprogramowania wraz z 55 licencjami dostępowymi umożliwiającymi korzystanie przez 55 użytkowników z zasobów klastra lub równoważnego systemu zgodnie z poniżej określonymi warunkami równoważności.

Warunki równoważności dla dostawy oprogramowania Microsoft Windows Serwer w najnowszej wersji oprogramowania oferowanej przez producenta oprogramowania wraz z 55 licencjami dostępowymi Microsoft Windows Server CAL User:

1) Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowiskach serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji oraz dostępu do serwerowego systemu operacyjnego dla minimum 55 użytkowników.
2) Możliwość wykorzystywania 240 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny.
3) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
4) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
5) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
6) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
7) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
8) Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading;
9) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
10) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
11) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.
12) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
13) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
14) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.

15) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 2 języków poprzez wybór z listy dostępnych lokalizacji.
16) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
17) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
18) Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).
19) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
20) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.

2.6. Zakup UPS (1 szt.).

Minimalne parametry techniczne urządzenia:

1. Typ obudowy: RACK, max 4U, Wykonawca jest zobowiązany dostarczyć szyny do montażu UPS w szafie RACK.
2. Moc pozorna: min. 6000 VA.
3. Moc rzeczywista: min. 6000 W.
4. Architektura UPSa: line-interactive lub online.
5. Typ przebiegu: sinusoidalny.
6. Liczba i rodzaj gniazdek z utrzymaniem zasilania: 10 x IEC320.
7. Typ gniazda wejściowego: C14 lub C20.
8. Czas podtrzymania dla obciążenia 100%: min. 3 min.
9. Czas podtrzymania przy obciążeniu 50%: min. 10 min.
10. Zabezpieczenia: przeciwprzepięciowe, przeciwzwarciowe, przeciwprzeciążeniowe.
11. Wyświetlacz LCD lub diody LED sygnalizujące stan pracy urządzenia.
12. Alarmy dźwiękowe urządzenia sygnalizujące stan pracy urządzenia w zakresie określonych przez producenta zdarzeń.
13. Interfejsy: min. 1 x USB, 1 x RJ45.
14. Deklaracja zgodności CE lub inny równoważny dokument poświadczający, ze oferowany UPS spełnia wszystkie zasadnicze wymagania zawarte w poszczególnych dyrektywach nowego podejścia przewidujących oznakowanie CE. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany UPS w zakresie określonym powyżej.
15. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci deklaracji RoHS dla produktu lub oświadczenia producenta UPS lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany UPS w zakresie określonym powyżej.
16. Gwarancja producenta: min. 24 miesiące.

2.7. Zakup UPS do stacji roboczych (30 szt.).

Minimalne parametry techniczne urządzenia:

1. Typ obudowy: wolnostojąca.
2. Rozmiar obudowy: suma wymiarów obudowy (szerokość + wysokość+ głębokość), nie większa niż 65 cm łącznie.
3. Moc wyjściowa: min. 500 W.
4. Napicie wejściowe: 230 V.
5. Czas przełączania: max. 10 ms.
6. Architektura UPS: line interactive lub on-line.
7. Ilość gniazd sieciowych: min. 4 typu Schuko.
8. Porty: min. 1 x USB, min. 1x Ethernet.
9. Alarmy i informacje dźwiękowe i wizualne w zależności od rodzaju zdarzenia.
10. Zabezpieczenia: wbudowany moduł regulacji napięcia AVR, zabezpieczenie przeciwprzepięciowe.
11. Czas podtrzymania przy obciążeniu 80 % - min. 1 min.
12. Czas podtrzymania przy obciążeniu 50 % - min. 6 min.
13. Przewód zasilający nie krótszy niż 1 metr.
14. Deklaracja zgodności CE lub inny równoważny dokument poświadczający, ze oferowany UPS spełnia wszystkie zasadnicze wymagania zawarte w poszczególnych dyrektywach nowego podejścia przewidujących oznakowanie CE. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany UPS w zakresie określonym powyżej.
15. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci deklaracji RoHS dla produktu lub oświadczenia producenta UPS lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany UPS w zakresie określonym powyżej.
16. Co najmniej 24 miesiące gwarancji producenta.

3. Szczegółowy opis przedmiotu zamówienia dla części nr 2.

3.1. Wymagania ogólne w zakresie dostawy oprogramowania.

1. Dostarczone oprogramowanie musi być wolne od wad prawnych i fizycznych oraz wcześniej nieużytkowane.
2. Dostarczone oprogramowanie musi być fabrycznie nowe, musi pochodzić z oficjalnego kanału sprzedaży producenta, pochodzić z seryjnej produkcji z uwzględnieniem opcji konfiguracyjnych przewidzianych przez producenta oferowanego oprogramowania.
3. Niedopuszczalne są produkty prototypowe oraz pochodzących z programów wyprzedażowych producenta. Oferowane oprogramowanie nie może znajdować się na liście „end-of-sale", „end-of-live oraz „end-of-support" producenta.
4. Wykonawca zapewni dostawę oprogramowania do wskazanej lokalizacji w siedzibie Zamawiającego.
5. Wykonawca jest odpowiedzialny za skonfigurowanie w porozumieniu z Zamawiającym oprogramowania w celu przygotowania zamawianego oprogramowania do działania.
6. Prace instalacyjne będzie można realizować wyłącznie w terminach uzgodnionych z Zamawiającym.

7. Wykonawca będzie zobowiązany do złożenia dokumentacji powykonawczej, zawierającej w szczególności wszystkie dane dostępu do oprogramowania, które będą wykorzystywane podczas instalacji i konfiguracji oprogramowania.
8. Dla dostaw oprogramowania Zamawiający wymaga fabrycznie nowego oprogramowania (nieużywanego nigdy wcześniej), w wersji z certyfikatem autentyczności dla każdej licencji, o ile producent oferowanego oprogramowania stosuje certyfikaty autentyczności. Wykonawca zobowiązany jest do dostarczenia fabrycznie nowego oprogramowania, nieużywanego oraz nigdy wcześniej nieaktywowanego oraz pochodzącego z legalnego źródła sprzedaży. W przypadku oprogramowania posiadającego fizyczny nośnik naklejka hologramowa winna być zabezpieczona przed możliwością odczytania klucza za pomocą zabezpieczeń stosowanych przez producenta, o ile producent oferowanego oprogramowania stosuje takie zabezpieczenia. Zamawiający zastrzega możliwość weryfikacji dostarczonego oprogramowania na etapie oceny ofert jak i na etapie dostawy pod kątem legalności oprogramowania bezpośrednio u producenta oprogramowania. Zamawiający zastrzega możliwość żądania od Wykonawcy na etapie dostawy przedstawienia dokumentów dotyczących zakupu oprogramowania w autoryzowanym kanale dystrybucyjnym producenta oprogramowania.
9. Wymagania instalacyjne i wdrożeniowe dla dostarczonego oprogramowania:
    a. Instalacja ma odbyć się na komputerach oraz serwerach wskazanych przez Zamawiającego, a w przypadku jeżeli dostarczone oprogramowanie działa w modelu rozwiązania chmurowego to Wykonawca jest zobligowany do konfiguracji oprogramowania w chmurze Wykonawcy bądź Producenta oferowanego oprogramowania.
    b. Zamawiający dopuszcza instalację i wdrożenie zdalne przy wykorzystaniu narzędzia Wykonawcy, z zastrzeżeniem, że Wykonawca jest zobowiązany dostarczyć oprogramowanie do zdalnej pracy umożliwiające szyfrowanie połączeń oraz nagrywanie sesji serwisowych.
    c. W przypadku jeżeli dotyczy, Wykonawca wykona wdrożenie na wybranym serwerze/maszynie wirtualnej wskazanym przez Zamawiającego oraz na stanowiskach wskazanych przez Zamawiającego.
    d. Wykonawca, pomimo zapewnienia serwisu producenta zobowiązany będzie do udzielania pomocy technicznej Zamawiającemu przez okres gwarancji.
    e. Usługa wsparcia wdrożenia obejmuje:
        i. przeprowadzenie analizy przedwdrożeniowej,
        ii. pomoc przy instalacji silnika bazy danych – jeżeli będzie wymagana instalacja,
        iii. rejestracja produktu – jeżeli wymagana,
        iv. instalację oprogramowania: na stacji roboczej lub serwerze – jeżeli dotyczy,
        v. dystrybucję oprogramowania na wybranych stacjach roboczych – jeżeli dotyczy,
        vi. konfigurację oprogramowania,
        vii. optymalizację ustawień pod wymogi sieciowe i sprzętowe Zamawiającego,
        viii. szkolenie administratorów z zakresu pracy z programem,
        ix. w uzgodnionym terminie z Zamawiającym zostanie przeprowadzane kontrolne połącznie zdalne w celu weryfikacji ustawień oraz poprawienia konfiguracji.
10. Proces współpracy między Wykonawcą a Zamawiającym w celu wdrożenia oprogramowania – wymagania minimalne:
    a. Wykonawca przygotuje projekt techniczny realizacji koncepcji, uwzględniający dobre praktyki i rekomendacje eksploatacyjne publikowane przez producentów wdrażanego oprogramowania, po wykonaniu analizy istniejącego u Zamawiającego rozwiązania wraz

z koncepcją uwzględniające obecne u Zamawiającego uwarunkowania organizacyjne i sprzętowe, łącznie zwane dalej projektem technicznym. W projekcie technicznym muszą być zawarte:

i. scenariusze testowe, procedury oraz wzory raportów testów,
ii. szczegółowy harmonogram realizacji prac wdrożeniowych i migracyjnych, uwzględniający specyfikę organizacji Zamawiającego,
iii. opis koncepcji realizacji prac,
iv. zalecenia przedwdrożeniowe dla Zamawiającego, jeżeli będą wymagane.

b. Akceptacja projektu technicznego wraz z procedurami oraz wzorami raportów z testów będzie podlegała następującej procedurze:
   i. Wykonawca przekaże do akceptacji Zamawiającego, drogą elektroniczną projekt techniczny wraz z procedurami oraz wzorami raportów z testów, w terminie nie dłuższym niż 30 dni kalendarzowych od dnia zawarcia umowy,
   ii. Zamawiający w terminie nie dłuższym niż 7 dni roboczych od dnia dostarczenia przez Wykonawcę kompletnych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,
   iii. wszystkie uwagi do dokumentów zgłoszone przez Zamawiającego zostaną wprowadzone przez Wykonawcę, w terminie nie dłuższym niż 5 dni roboczych od dnia ich otrzymania,
   iv. Zamawiający w terminie 5 dni roboczych od dnia powtórnego dostarczenia przez Wykonawcę poprawionych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,
   v. w przypadku nieuwzględnienia uwag Zamawiającego, Zamawiający zastrzega sobie prawo do wskazania ostatecznego terminu dostarczenia projektu technicznego wraz z procedurami oraz wzorami raportów z testów,
   vi. zatwierdzony projekt techniczny wraz procedurami zostaną przekazane Zamawiającemu w 1 egzemplarzu oraz w formie elektronicznej na pendrive, w postaci plików do edycji i PDF.
c. Wykonawca zrealizuje wdrożenia i migracje zgodnie z zakresem prac i projektem technicznym.
d. Wykonawca przeprowadzi testy akceptacyjne wdrożonych rozwiązań.
e. Wykonawca opracuje i przedstawi raport z testów. W przypadku zrealizowania scenariusza testowego z wynikiem negatywnym, Wykonawca przedstawi nowe rozwiązanie wadliwego elementu systemu i przeprowadzi ponowny test wg scenariusza, w terminie wyznaczonym przez Zamawiającego, dochowując terminu wykonania Umowy. Raport z testów powinien zawierać listę przeprowadzonych testów wraz z ich wynikiem.
f. Wykonawca opracuje dokumentację powykonawczą oraz procedury administracyjne i eksploatacyjne w zakresie uzgodnionym z Zamawiającym, w tym: dokumentację wdrożeniową, procedury operacyjne, procedury „Disaster Recovery". Akceptacja dokumentacji powykonawczej będzie przebiegała zgodnie z zasadami określonymi dla akceptacji projektu technicznego.

11. Instruktaże w zakresie dostarczonego oprogramowania – wymagania minimalne.
    a. Instruktaże stanowiskowe będą prowadzone w języku polskim w siedzibie Zamawiającego i obejmą zakresem m.in.: użytkowane oprogramowanie; budowę, architekturę i konfigurację rozwiązania; administrowanie wdrożonym rozwiązaniem.

b. Instruktaże stanowiskowe zostaną przeprowadzone przez osoby prowadzące prace wdrożeniowe w ramach niniejszego zamówienia.
c. Instruktaże powinny trwać minimum 8 godzin lekcyjnych (45 minut) i będą przeprowadzone dla wskazanej przez Zamawiającego liczby osób (maksymalnie 4 osoby).
d. Zamawiający dopuszcza przeprowadzenia instruktaży w trybie zdalnym (online).
e. Administratorzy rozwiązania po zakończeniu Instruktaży stanowiskowych muszą w szczególności umieć wykonywać czynności administracyjne, a także instalacji oprogramowania, znać i umieć realizować procedury backupu. Ponadto powinni znać typowe zagrożenia i problemy związane z funkcjonowaniem rozwiązania, a także sposoby ich przeciwdziałania, wykrywania i usuwania. Powinni umieć instalować, konfigurować, rekonfigurować, monitorować i prawidłowo eksploatować wdrożone rozwiązanie, jak również znać jego wdrożoną konfigurację.

12. Wymagania licencyjne dla dostarczonego oprogramowania:
    a. Licencjobiorcą wszystkich licencji będzie Gmina Biała Piska i ma zapewnić wykorzystanie z 70 użytkowników/urządzeń końcowych.
    b. Zamawiający dopuszcza udzielenie licencji w wersji papierowej i/lub elektronicznej. W przypadku jeżeli producent oprogramowania nie wystawia licencji w zakresie oferowanego oprogramowania Wykonawca powinien dostarczyć stosowne oświadczenie producenta oprogramowania bądź jego dystrybutora.
    c. Licencje muszą obowiązywać do dnia 25.03.2026 r. niezależnie od modeli dystrybucji poszczególnych producentów oferowanego oprogramowania.
    d. Oferowane licencje muszą pozwalać na użytkowanie oprogramowania zgodnie z przepisami prawa.
    e. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do przeniesienia oprogramowania na inny serwer/komputer.
    f. Licencja na oprogramowanie nie może w żaden sposób ograniczać sposobu pracy użytkowników końcowych (np. praca w sieci LAN, praca zdalna poprzez Internet). Użytkownik może pracować w dowolny dostępny technologicznie sposób.
    g. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do wykonania kopii bezpieczeństwa oprogramowania w ilości, którą uzna za stosowną.
    h. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do instalacji użytkowania oprogramowania na serwerach zapasowych uruchamianych w przypadku awarii serwerów podstawowych.
    i. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do korzystania z oprogramowania na dowolnym urządzeniu klienckim (licencja nie może być przypisana do komputera/urządzenia).
    j. Licencja oprogramowania nie może limitować wielkości przechowywanych danych oraz możliwości wyszukiwania informacji ze zgromadzonych danych.
    k. Wykonawca zapewni gwarancję producenta oprogramowania, która obejmie gwarancję aktualizacji oprogramowania do najnowszej wersji oprogramowania w okresie objętym gwarancją.
13. Wymagania gwarancyjne i serwisowe dla dostarczonego oprogramowania:
    a. Gwarancja producenta musi zostać zapewniona przez Wykonawcę na oferowane oprogramowanie do dnia 25.03.2026 r

b. W ramach gwarancji Zamawiający ma prawo zgłaszać błędy w oprogramowaniu do serwisu producenta lub jego dystrybutora.
c. Serwis producenta musi zostać zapewniony przez Wykonawcę do dnia 25.03.2026 r
d. Serwis polega na świadczeniu usługi wsparcia technicznego udzielonego przez producenta lub autoryzowanego dystrybutora producenta w języku polskim i objąć musi minimum:
    i. dostęp do najnowszych wersji oprogramowania,
    ii. wsparcie telefoniczne w zakresie oferowanego oprogramowania zespołu inżynierów technicznych,
    iii. wsparcie w prawidłowym i zgodnym z wymaganiami producenta użytkowaniu oprogramowania,
    iv. przyjmowanie i realizacja zgłoszeń serwisowych,
    v. doradztwo techniczne w zakresie konfiguracji i optymalizacji oprogramowania,

    w przypadku jeżeli w dalszej części niniejszego dokumentu zdefiniowano wymogi serwisu lub gwarancji w innym zakresie powyższe wymogi są obowiązujące i należy potraktować jako podstawowe, precyzowane przez dodatkowe wymagania opisane w dalszej części dokumentu.

14. W poniżej wskazanych wymaganiach Zamawiający posługuje się terminami „musi", „powinien", „możliwość" określając w ten sposób wymaganą funkcjonalność oprogramowania.

3.2. Zakup licencji i wdrożenie oprogramowania SIEM (1 szt.).

Przedmiotem zamówienia jest dostawa licencji i wdrożenie systemu SIEM – systemu przeciwdziałania cyberzagrożeniom oferującym możliwości wykrywania i obsługi zdarzeń, incydentów oraz podatności przy wsparciu mechanizmów uczenia maszynowego oraz zapewniającego automatyzację obsługi.

Minimalne parametry funkcjonalne oprogramowania:

1. System musi umożliwić odbieranie logów z urządzeń sieciowych oraz wygenerowanych przez systemy zabezpieczeń, systemy sieciowe, systemy operacyjne i aplikacje minimum następującymi protokołami: Syslog, TLS syslog, NetFlow, Windows Event Forwarding.
2. System musi zapewnić agentów na stacje końcowe umożliwiających im pobieranie pełnych danych hostów, których chronią i przesłanie tych danych do systemu centralnego w celu dalszej korelacji i analizy behawioralnej. W przypadku wykrycia zagrożenia agenci muszą umożliwiać automatyczną i dostosowaną do kontekstu reakcje, m.in. blokowanie bądź izolację sieciową złośliwego oprogramowania.
    2.1. Agent musi posiadać możliwość dodawania i usuwania reguł wbudowanego firewalla obejmując m.in. blokowanie i odblokowywanie poszczególnych procesów bądź reguł dotyczących ruchu sieciowego stanowiące reakcję na wykryte zagrożenie.
    2.2. Agent musi pobierać oraz aktualizować na bieżąco listę zainstalowanego oprogramowania.
    2.3. System w przypadku wykrycia techniki ataku ukierunkowanego na podatną aplikację w celu zablokowania ataku musi umożliwiać zatrzymanie procesu aplikacji oraz zapewnić dostęp do danych dowodowych obejmujących nazwę chronionego systemu, system operacyjny, tożsamość użytkownika, nazwę procesu, dokładną komendę uruchamiającą złośliwy proces wraz parametrami i znacznik czasowy.

2.4. System musi obsługiwać scenariusz uwzględniający ocenę prawdopodobieństwa materializacji się wykrytego zagrożenia, gdzie w przypadku, gdy wyliczone przez system prawdopodobieństwo ataku jest wysokie proces zostanie zablokowany, natomiast w pozostałych przypadkach, gdy jest ono średnie bądź niskie zostanie on zamrożony z możliwością ponownego wznowienia przez operatora.

2.5. System musi posiadać możliwość dostosowania reakcji na zagrożenie w zależności od rodzaju zasobu, który chroni, przykładowo, jeżeli zagrożenie dotyczyć będzie procesu na stacji roboczej proces zostanie automatycznie zablokowany, jednakże w przypadku, gdy to samo zagrożenie dotyczyć będzie serwera świadczącego usługi w sieci publicznej proces pozostanie uruchomiony z jednoczesną blokadą publicznego ruchu przychodzącego.

3. 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.
4. System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych.
5. System musi być wyposażony w mechanizmy normalizacji (parsowania) pozyskanych zdarzeń umożliwiający ich podział na poszczególne pola, na podstawie których może odbywać się dalsze przetwarzanie oraz wyszukiwanie ich w systemie.
6. System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, obejmującą zmianie 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.
7. 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.
8. Normalizacja musi umożliwiać automatyczne nadawanie kategorii zdarzeń w formie nowych pól, np.: logowanie, wylogowanie, zmiana uprawnień, błąd konfiguracji, wykryte skanowanie systemu czy zablokowany malware.
9. Normalizacja logów musi posiadać mechanizm geolokalizacyjny, pozwalający na wzbogacenie pól o nazwę lub kod kraju korzystając z wbudowanej w produkt bazy.
10. 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.
11. 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.
12. 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.
13. System musi rejestrować i przechowywać pozyskane logi w postaci surowej (RAW) oraz znormalizowanej.

14. System musi być wyposażony w graficzny interfejs umożliwiający określenie miejsca składowania logów (wskazania właściwego repozytorium logów) w zależności od zwartości 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.
15. 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.
16. 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.
17. Ze względu na możliwość wygenerowania dużej ilości danych przez algorytmy uczenia maszynowego system musi mieć możliwość rozdzielenia ich składowania na osobny serwer i dedykowane zasoby dyskowe.
18. System musi umożliwiać automatyczną archiwizację danych na zewnętrzne repozytoria danych w postaci skompresowanej.
19. System musi zapewnić mechanizmy bezpieczeństwa dla danych przechowywanych w repozytoriach uniemożliwiające ich nieautoryzowaną modyfikację oraz zapewnić operatorom mechanizmy weryfikacyjne integralność danych.
20. 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.
21. 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.
22. 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.
23. Elektroniczna dokumentacja musi posiadać możliwość wizualizacji, gdzie widoczne będą urządzenia zabezpieczeń, strefy bezpieczeństwa oraz połączenia sieciowe wskazujące jakie mechanizmy zabezpieczeń chronią poszczególne strefy bezpieczeństwa. Wybór na dowolny z obiektów musi pozwolić na podgląd oraz edycję parametrów tego obiektu.
24. System musi umożliwiać prezentację danych zgromadzonych w elektronicznej dokumentacji również w formie tabelarycznej.
25. System musi pozwalać na definiowanie własnych parametrów dla wszystkich typów obiektów zgromadzonych w elektronicznej dokumentacji sieci.
26. 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.

27. 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.
28. 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 minimum 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.
29. System musi umożliwiać uwiarygodnianie uzyskiwanych informacji na bazie wartości progowych osiągniętych w zadanej jednostce czasu i dopiero po ich uwiarygodnieniu uzupełniać automatycznie elektroniczną dokumentację.
30. System powinien posiadać zestaw predefiniowanych reguł do automatycznego uzupełniania elektronicznej dokumentacji, których uruchomienie będzie automatycznie aktualizować elektroniczną dokumentację bez ingerencji operatora.
31. Interfejs graficzny musi posiadać mechanizm definiowania dozwolonej komunikacji sieciowej dla każdego zasobu IT który został zdefiniowany w elektronicznej dokumentacji oraz nazwę usługi, której ta komunikacja dotyczy.
32. 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 minimum 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.
33. 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/).
34. System musi umożliwiać definiowanie list referencyjnych zarówno z jedną wartością jak i łączących unikalne wartości w pojedynczym wierszu.
35. Listy referencyjne muszą mieć możliwość synchronizacji z listami publikowanymi publicznie (np.: „Malicious IPs”, „Malicious domain” czy „Tor Exit Nodes”).
36. 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.

37. System powinien umożliwiać zdefiniowanie struktury organizacyjnej oraz zapewniać możliwość jej synchronizacji z usługą katalogową Microsoft Active Directory.
38. System musi umożliwiać analizę konfiguracji systemów IT poprzez ich skanowanie bezpośrednio w ramach mechanizmów dostępnych w samym rozwiązaniu oraz poprzez integrację ze skanerami podatności.
39. System powinien posiadać zestaw predefiniowanych reguł weryfikacji konfiguracji zasobów IT.
40. 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.
41. 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 zakresie minimum:
    a. id techniki,
    b. taktykę,
    c. platformy których dotyczy,
    d. potencjalne źródła,
    e. opis zagrożenia,
    f. mityzację,
    g. sposób detekcji,
    h. referencje.
42. System w swoim działaniu musi korzystać z wbudowanych algorytmów uczenia maszynowego dla celów zbudowania i utrzymywania modelu danych użytkowników i komputerów.
43. 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).
44. 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.
45. System uczenia maszynowego musi posiadać wbudowane mechanizmy niewymagające żadnej dodatkowej konfiguracji, które po zakończeniu procesu nauki umożliwią detekcję anomalii zachowania użytkowników oraz zasobów (UEBA).

46. 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.
47. System musi zapewniać kontrolę dostępu do systemu i oferowanych przez niego funkcjonalności w oparciu o zdefiniowane role.
48. 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.
49. 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 minimum:
    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®.
50. Reguły korelacyjne bazujące na sparsowanych polach i ich wartościach muszą umożliwić minimum:
    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,
    e. wykrycie incydentu będącego pochodną zdarzeń występujących w określonej kolejności,
    f. wykrycie zdefiniowanej ilości przesłanych danych w zadanym okresie,
    g. wykrycie chwilowego wzrostu ilości przesłanych danych (tzw. peek) w stosunku do całkowitej ilości przesłanych danych w zadanym okresie,
    h. wykrycie sumarycznego wzrostu przesłanych danych w zdefiniowanej strefie bezpieczeństwa,
    i. wykrycie zdefiniowanej ilości przesyłanych pakietów w zadanym okresie,
    j. wykrycie chwilowego wzrostu (tzw. peek) w stosunku do ilości przesyłanych pakietów w zadanym okresie,
    k. wykrycie sumarycznego wzrostu ilości pakietów przesyłanych w zdefiniowanej strefie bezpieczeństwa,
    l. wykrycie ilości uruchomionych procesów w zadanym okresie,
    m. wykrycie skanowania portów.
51. Reguły korelacyjne bazujące na listach referencyjnych muszą umożliwić minimum:
    a. wykrycie wystąpienia wartości pola na wybranej liście,
    b. wykrycie niewystępowania wartości pola na wybranej liście,
    c. wykrycie wystąpienia pary wartości na wybranej liście (np.: proces i obraz pliku, z którego

został uruchomiony),
   d. wykrycie niewystąpienia pary wartości na wybranej liście.
52. Reguły korelacyjne wykorzystujące atrybuty użytkowników z Active Directory muszą umożliwić minimum:
   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.
53. Reguły korelacyjne wykorzystujące atrybuty komputerów z Active Directory muszą umożliwić minimum:
   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.
54. Reguły korelacyjne wykorzystujące bazę wskaźników kompromitacji (IOC) muszą umożliwić minimum:
   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.
55. 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.
56. Reguły korelacyjne wykorzystujące anomalie w zachowaniu użytkowników (UBA) muszą umożliwić minimum:
   a. wykrycie anomalii ilościowej związanej z kontem użytkownika wskazującej na potencjalny atak DDoS 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 przejecie konta użytkownika przez cyberprzestępcę lub złośliwe oprogramowanie,
   d. wykrycie anomalii związanych z logowaniami użytkowników w ramach sesji VPN.
57. Reguły korelacyjne wykorzystujące anomalie w zachowaniu zasobów (EBA) muszą umożliwić

minimum:

a. wykrycie anomalii ilościowej związanej z komputerem wskazującej na potencjalny atak DDoS 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 przejecie komputera przez cyberprzestępcę lub złośliwe oprogramowanie,
d. wykrycie anomalii związanych z procesami uruchamianymi na serwerach.

58. Reguły korelacyjne wykorzystujące podatności na zasobach muszą umożliwić minimum:
    a. wykrycie skanowania portów z zasobu posiadającego krytyczne podatności,
    b. wykrycie wielokrotnych prób połączeń do zasobu posiadającego krytyczne podatności,
59. Reguły korelacyjne wykorzystujące wyniki analizy konfiguracji muszą pozwalać minimum na:
    a. wykrycie wielokrotnych prób nieudanego logowania do komputera,
    b. wykrycie wielokrotnych prób nieudanego logowania do komputera, który umożliwia tworzenie haseł niespełniających następujących kryteriów złożoności: duża litera, mała litera, liczba, znak specjalny.
60. Reguły korelacyjne wykorzystujące technikach MITRE ATT&CK® muszą umożliwić minimum:
    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.
61. Pojedyncza reguła korelacyjna musi mieć możliwość wzajemnej korelacji wszystkich powyższych mechanizmów umożliwiając minimum:
    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.
62. System przy wykorzystaniu reguł kwalifikacyjnych musi automatycznie selekcjonować zdarzenia wygenerowane przez reguły korelacyjne, wybierając do obsługi tylko zdarzenia spełniające zdefiniowane warunki.
63. Obsługiwane zdarzenia muszą posiadać zestaw predefiniowanych scenariuszy obsługi oraz pozwalać na tworzenie własnych scenariuszy obsługi oraz ich edycję z poziomu interfejsu graficznego.
64. System musi potrafić wczytywać informacje z innych systemów bezpieczeństwa i traktować je, jako elementy/dowody dla zdarzeń.
65. Zdarzenia muszą umożliwiać gromadzenie dodatkowych informacji wygenerowanych podczas ich obsługi oraz umożliwiać do nich dostęp bezpośrednio z poziomu tych zdarzeń, obejmujących minimum:
    a. wszystkie skorelowane zdarzenia,

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

66. 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 rozdzielenia 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.
67. 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 minimum następujące dane:
    a. identyfikacja celu i źródła zagrożenia,
    b. nazwa oraz adres IP źródła zagrożenia,
    c. rodzaj zasobu będący źródłem zagrożenia np.: urządzenie mobilne, stacja robocza,
    d. lokalizacja, z której pochodzi zagrożenie np.: Internet,
    e. strefa 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. nazwa oraz adres IP celu zagrożenia,
    i. zabezpieczenia lokalne chroniące cel zagrożenia,
    j. strefa bezpieczeństwa w której znajduje się cel zagrożenia.
68. 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.
69. Dla wyznaczonych w czasie obsługi wektorów zagrożeń przedstawiane wyniki szacowania prawdopodobieństwa muszą być zwizualizowane operatorowi w formie listy zagrożeń z oszacowanymi dla nich poziomami.
70. 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 zakresie minimum:
    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.
71. 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 minimum: 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.

72. Zdarzenia w obsłudze muszą obejmować statusy właściwe dla procesu obsługi zdarzeń w zakresie minimum:
    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. zdarzanie obsłużone – zdarzenie, które zostało obsłużone w systemie.
73. System musi także zapewniać możliwość edycji w zakresie dodawania 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".
74. 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.
75. 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.
76. Obsługiwane zdarzenia muszą zapewniać historyczność, obejmującą wszystkie aktywności realizowane w ramach poszczególnych statusów.
77. Dla każdego obsługiwanego zdarzenia system powinien udostępniać automatyczny raport obejmujący wszystkie podjęte działania wraz z komentarzami operatorów.
78. 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.
79. 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.
80. 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 rozszerzajcie 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,
    h. gotowe i proste w użyciu filtry rozszerzajcie 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.

81. Dla zdarzeń w obsłudze system musi być wyposażony w graficzny interfejs umożliwiający definiowanie własnych powiadomień obejmujących:
    a. warunki powiadomień, w tym:
        - 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 sklasyfikowane 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.
82. 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 zdarzania przez innego operatora,
    g. zamknięcia przydzielonego operatorowi zdarzania przez innego operatora,
    h. przejęcia przydzielonego operatorowi zdarzania przez innego operatora.
83. 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,
- określnej liczby raportów,

g. określenie odbiorców raportu.

84. System musi umożliwiać obsługę podatności w ramach scenariuszy obsługi.
85. 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 wyznaczą 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,
    f. usługi realizowane przez ten zasób,
    g. wartość parametrów CVSS dla podatności,
    h. poprawność konfiguracji zasobu, na którym została wykryta podatność,
    i. szacowane prawdopodobieństwo przełamania zabezpieczeń ze zdefiniowanej strefy, która jest autoryzowana do dostępu do tego zasobu.
86. 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 jaki i możliwość ich wyłączenia z obsługi w przypadku znikomego zagrożenia dla organizacji.
87. 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”.
88. 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,

89. 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 informację,
        - 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, 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.
90. 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.
91. 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.

92. System powinien w formie graficznej prezentować podsumowanie aktualnego stanu bezpieczeństwa organizacji umożliwiający dostosowanie zakresu i prezentacji danych do potrzeb zalogowanego użytkownika.
93. System musi pozwalać na tworzenie dedykowanych:
    a. zestawów wykresów dla bieżącego użytkownika,
    b. zestawów wykresów dla wybranego użytkownika,
    c. zestawów wykresów dla roli zdefiniowanej w systemie, np.: administratorzy systemu,
    d. zestawów wykresów dla wybranego zespołu obsługi, np.: operatorzy SOC (Security Operations Center).
94. System musi zapewniać predefiniowane zestawy wykresów obejmujących następujące wykresy:
    a. wykres przedstawiający status klasyfikacji zdarzeń,
    b. wykres przedstawiający skale zagrożeń,
    c. wykres przedstawiający źródła zagrożeń,
    d. wykres przedstawiający poziom zagrożeń,
    e. wykres przedstawiający czas obsługi zagrożeń,
    f. wykres przedstawiający zagrożone usługi,
    g. wykres przedstawiający skale podatności,
    h. wykres przedstawiający czas obsługi podatności,
    i. wykres przedstawiający wagę podatności, który uwzględnia:
95. Rozwiązanie może być dostarczone w ramach odrębnych rozwiązań, jednakże muszą być one zintegrowane w sposób umożliwiający spełnienie wszystkich wymagań z poziomu jednej konsoli.
96. 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.
97. Oferowana licencja nie może nakładać limitów w zakresie ilości danych przekazywanych do systemu, tj. EPS (Events Per Second).
98. System musi umożliwiać równoczesną pracę co najmniej 5 operatorów oraz obsługiwać co najmniej 200 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 funkcjonalności.
99. Dla wszystkich źródeł objętych licencją oraz stanowiących jednocześnie komputery bądź serwery licencja produktu musi uwzględniać możliwość wykorzystania dedykowanych agentów XDR.
100. System ma gwarantować możliwość elastycznej rozbudowy o kolejne źródła logów.
101. 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.
102. System musi umożliwiać instalację na jednej z platform systemowych: Microsoft Windows Server

(minimum Server 2016), Redhat/Oracle Linux (minimum 7.x).

Wdrożenie oprogramowania SIEM – wymagania minimalne:

1. Wykonawca przeprowadzi instalację i konfigurację systemów operacyjnych dla serwerów wirtualnych na potrzeby zaoferowanego systemu.
2. Instalacja oprogramowania systemu serwerowego wraz z niezbędnymi usługami oraz instalacja wszystkich niezbędnych kodów dostępowych oraz licencji (wszelkie procedury rejestracyjne powinno zostać wykonane na danych dostarczonych przez Zamawiającego).
3. Proces wdrożenia systemu określony powinien zostać zrealizowany zgodnie z opisanymi niżej wytycznymi oraz zatwierdzonym harmonogramem, umożliwiając efektywne wdrożenie rozwiązania w okresie 90 dni.
4. Proces wdrożeniowy powinien uwzględnić następujące obszary:
    a. Obszar Analizy, zakładający stworzenie elektronicznej dokumentacji organizacji wraz z podłączeniem i skonfigurowaniem mechanizmów szacowania ryzyka pod kątem kluczowych zasobów IT i procesów organizacji (budowa kontekstu organizacji).
    b. Obszar Detekcji, zakładający podłączenie i konfigurację narzędzi odpowiedzialnych za wykrywanie zdarzeń i incydentów bezpieczeństwa w ramach zainstalowania modułu SIEM.
    c. Obszar Reakcji, zakładający podłączenie i konfigurację mechanizmów wspomagających proces automatyzacji reakcji na wykryte zdarzenia, incydenty bezpieczeństwa i podatności w ramach zainstalowania modułu SOAR.

Obszar Analizy ma na celu identyfikację potencjalnych cyberzagrożeń oraz możliwych konsekwencji na jakie narażona jest organizacja. Zakres prac powinien uwzględniać minimum:

1. Pracę z konsultantem (w zakresie m.in. wprowadzenia do metodyki, uzupełnienia ankiety przedwdrożeniowej oraz przygotowania i zatwierdzenia harmonogramu prac).
2. Uruchomienie systemu w infrastrukturze zamawiającego, w tym:
    a. konsultacje w przygotowaniu infrastruktury Zamawiającego do instalacji systemu,
    b. przygotowanie przez Zamawiającego połączenia zdalnego,
    c. instalację lub import maszyny wirtualnej typu „software appliance”,
    d. aktywację licencji,
    e. wstępną konfigurację,
    f. import/wprowadzenie tabeli adresacji znaczących stref bezpieczeństwa, wymaganych przez mechanizmy wykrywania (np.: sieci serwerów, sieci DMZ, sieci LAN).
3. Podłączenie głównego źródła zdarzeń opisującego komunikację sieciową, w tym:
    a. przekierowanie logów opisujących transmisje sieciową (traffic) z zapór sieciowych (Firewall) na kolektor systemu,
    b. uruchomienie reguł wykrywania.
4. Prace audytowe, w tym:
    a. pasywną analizę transmisji sieciowej:
        i. o ruch z/do serwerów webowych i aplikacyjnych,
        ii. o ruch z/do serwerów baz danych,
        iii. o ruch z/do serwerów pocztowych,
        iv. o ruch z/do kontrolerów domenowych,
        v. o ruch z/do serwerów usług podstawowych (m.in. DNS/NTP),
        vi. o ruch z/do zasobów zidentyfikowanych na bazie charakterystyki i wolumenu ruchu

oraz możliwości identyfikacji aplikacji.
   b. konsultacje w ramach otrzymanych wyników,
   c. zebranie danych audytowych wymaganych do sporządzenia raportu.
5. Analizę podatności, w zakresie:
   a. integracji po API ze wskazanym przez zamawiającego komercyjnym skanerem/ skanerami podatności lub zainstalowanie skanera podatności typu open source,
   b. przygotowanie reguł priorytetów i importu krytycznych podatności.
6. Przygotowanie dynamicznego raportu audytowego w oparciu o dostępne w systemie narzędzia elektronicznej dokumentacji i szacowania ryzyka obejmującego analizę prawdopodobieństwa przełamania zabezpieczeń organizacji. Raport powinien zawierać:
   a. zidentyfikowane zagrożenia oraz prawdopodobieństwo ich wystąpienia,
   b. potencjalne wektory ataków dla wykrytych zagrożeń,
   c. wizualizacja graficzna wykrytych źródeł zagrożeń oraz wektorów ataków,
   d. rekomendacja zabezpieczeń,
   e. zidentyfikowane zagrożenia związane z podatnościami oraz prawdopodobieństwo wykorzystania ich do przełamania zabezpieczeń.

Obszar Detekcji ma na celu uruchomienie i dostrojenie mechanizmów wykrywania zagrożeń. Zakres prac powinien uwzględniać minimum:
1. Podłączenie (przekierowanie przez Zamawiającego do systemu) źródeł zdarzeń i ich dalszą konfigurację w systemie. Kluczowe źródła zdarzeń obejmują:
   a. zapory sieciowe w punkach styku z siecią Internet (Firewall brzegowy),
   b. sieciowe systemy bezpieczeństwa dedykowane do wykrywania incydentów bezpieczeństwa (np.: Sandbox, IDP/IPS, AntySpam),
   c. centralne systemy, dedykowane do kontroli złośliwego oprogramowania na stacjach końcowych/Serwerach, umożliwiające wykrywanie aktywności złośliwego oprogramowania (np.: AntyWirus, EDR),
   d. kontroler domenowy oraz system zarządzania dostępem uprzywilejowanym,
   e. systemy detekcji anomalii w przepływach lub zdarzeniach (np.: NBA),
   f. system SIEM,
   g. źródła, muszą zostać powiązane z parserami, pozwalającymi na detekcję zgodną z wbudowanymi w system regułami korelacji,
2. Adaptację reguł profilowych, pozwalających na dostosowanie zdarzeń do zasobów, których dotyczą.
3. Podłączenie reguł detekcji.
4. Podłączenie i konfiguracja mechanizmów UEBA:
   a. integracja z Active Directory,
   b. adaptacja profili użytkowników UBA,
   c. adaptacja profili hostów EBA,
   d. import reguł bezpieczeństwa UEBA, uruchomienie procesu uczenia.

Obszar Reakcji ma na celu uruchomienie i dostrojenie mechanizmów automatyzacji w działaniach reagowania na wykryte zagrożenia bezpieczeństwa. Zakres prac powinien uwzględniać minimum:
1. Import gotowych scenariuszy obsługi.
2. Konfigurację zespołów obsługi, celem właściwej adresacji podatności oraz zdarzeń wymagających

obsługi.

3. Konfigurację mechanizmów powiadamiania.
4. Usługa konsultacji powdrożeniowej, świadczona przez dedykowanego inżyniera w ramach okresu wsparcia musi w szczególności uwzględniać:
   a. przygotowanie i modyfikację formularzy raportów;
   b. tworzenie i edycję parserów;
   c. przygotowywanie nowych reguł bezpieczeństwa;
   d. modyfikację dostępnych reguł i ich dostrojenie;
   e. wsparcie w procesie aktualizacji systemu;
   f. tworzenie i edycję nowych scenariuszy reakcji.
5. 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.

3.3. Rozbudowa oprogramowania antywirusowego o funkcje EDR i wykrywanie podatności (1 szt.).

Aktualnie Zamawiający posiada licencję oprogramowania antywirusowego Bitdefender Endpoint Security Tool. Przedmiotem zamówienia jest rozbudowa oprogramowania do wersji Bitdefender GravityZone Business Security Enterprise (Ultra z EDR) w okresie do dnia 25.03.2026 r. obejmująca maksymalnie 70 użytkowników indywidualnych oraz 5 urządzeń serwerowych lub dostawa równoważnej platformy bezpieczeństwa zgodnie z funkcjonalnymi kryteriami równoważności określonymi poniżej.

Minimalne wymagania (kryteria równoważności) określone dla równoważnej platformy bezpieczeństwa:

<u>Administracja zdalna w chmurze.</u>

1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.
2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.
4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami,

zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.

9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.
10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
11. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.

Ochrona stacji roboczych.

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
2. Rozwiązanie musi wspierać architekturę ARM64.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
10. Rozwiązanie musi integrować się z Intel Threat Detection Technology.
11. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
13. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
14. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.

15. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
16. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
    a. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
    b. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
    c. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
    d. tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
    e. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
17. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
18. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
19. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
22. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.
23. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:
    a. tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
    b. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
    c. tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
    d. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
24. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
25. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
26. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
27. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.

28. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
29. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
30. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

Ochrona serwera.

1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7,8 i 9, CentOS 7, Ubuntu Server (SLES) 15, Oracle Linux 8 oraz Amazon Linux.
2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
   Dodatkowe wymagania dla ochrony serwerów Windows:
9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
13. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
14. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.
    Dodatkowe wymagania dla ochrony serwerów Linux:

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

Szyfrowanie.

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

Sandbox w chmurze.

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

c. Bardzo podejrzany,
d. Szkodliwy.

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

Moduł zarządzania podatnościami i aktualizacjami.

1. Rozwiązanie musi mieć możliwości wykrywania podatności w systemach operacyjnych (co najmniej Windows 10, Windows 11) oraz aplikacjach zainstalowanych na zarządzanych stacjach.
2. Baza wykrywanych podatności musi zawierać minimum 35000 CVE.
3. Rozwiązanie nie może wymagać instalacji dodatkowej konsoli, ani innych dodatkowych komponentów na stacjach końcowych.
4. Automatyczne wykrywanie podatności musi wykonywać się zgodnie z harmonogramem, nie częściej niż raz dziennie.
5. Moduł wykrywania podatności musi umożliwiać wyświetlanie szczegółów danej podatności zawierające minimum:
   a. nazwę aplikacji lub systemu operacyjnego;
   b. punktacje CVSS;
   c. opis wykrytej podatności;
   d. wartość ryzyka oceniona przez wewnętrzne mechanizmy producenta.
6. Moduł wykrywania podatności musi wykrywać podatności w minimum 700 aplikacjach.
7. Moduł zarządzania aktualizacjami musi umożliwiać wykonanie automatycznej aktualizacji dla minimum 150 popularnych aplikacji.
8. Moduł zarządzania aktualizacjami musi umożliwiać stworzenie białej listy aplikacji podlegających automatycznej aktualizacji. Automatyczne aktualizacje będą aplikowane tylko i wyłącznie dla wskazanych aplikacji w białej liście. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.
9. Moduł zarządzania aktualizacjami musi umożliwiać stworzenie czarnej listy aplikacji podlegających automatycznej aktualizacji. Automatyczne aktualizacje oprogramowania będą realizowane dla wszystkich - ponad 150 aplikacji, oprócz aplikacji wskazanych na czarnej liście. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.
10. Zarządzanie aktualizacjami aplikacji musi umożliwiać ręczne wdrażanie poprawek na wybranych stacjach.
11. Moduł zarządzania aktualizacjami oraz wykrywania podatności musi być zintegrowany bezpośrednio z programem antywirusowym tego samego producenta zainstalowanym na zarządzanym komputerze.
12. Stacja robocza posiadająca włączony moduł wykrywania podatności oraz zarządzania aktualizacjami musi być w odpowiedni sposób oznaczona w konsoli centralnego zarządzania.
13. Administrator konsoli musi mieć możliwość włączenia modułu wykrywania podatności i zarządzania aktualizacjami przy pomocy menu kontekstowego dostępnego w konsoli centralnego zarządzania.

14. Moduł wykrywania podatności ma umożliwiać wyłączenie powiadomień dla wybranej podatności.

Moduł EDR.

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