Załącznik 2 do Zapytania o cenę

ZAMAWIAJĄCY:

BIURO RZECZNIKA PRAW PACJENTA

UL. PŁOCKA 11/13; 01-231 WARSZAWA

OPIS PRZEDMIOTU SZACOWANIA

ZINTEGROWANE WDROŻENIE ARCHITEKTURY CYBERBEZPIECZEŃSTWA I KOMPETENCJI W BIURZE RZECZNIKA PRAW PACJENTA

SPIS TREŚCI

CZEŚĆ NR 1 OBSZAR KOMPETENCYJNY

1. SZKOLENIE Z ZAKRESU CYBERBEZPIECZEŃSTWA - PRACOWNICY

1.1. Wykonawca przeprowadzi szkolenie o charakterze podstawowym (świadomościowym) z zakresu cyberbezpieczeństwa i ochrony informacji, ukierunkowane na praktyczne zachowania ograniczające ryzyka adekwatne dla prowadzonej przez Zamawiającego działalności.

1.2. Wykonawca dostosuje przykłady i scenariusze do realiów organizacji Zamawiającego, bez wymagania ujawniania informacji wrażliwych.

1.3. Wykonawca zapewni, aby szkolenie miało charakter praktyczny i było ukierunkowane na ograniczanie ryzyk związanych z pracą z pocztą elektroniczną, dokumentami, systemami IT oraz komunikacją zewnętrzną.

1.4. Wykonawca uwzględni w szkoleniu omówienie podstawowych pojęć i odpowiedzialności pracownika, w tym znaczenia poufności, integralności i dostępności informacji w ujęciu praktycznym.

1.5. Wykonawca omówi w szkoleniu konsekwencje typowych incydentów i błędów użytkowników, w tym skutki finansowe, organizacyjne i prawne.

1.6. Wykonawca uwzględni w szkoleniu zasady identyfikacji i ochrony informacji wrażliwych w pracy biurowej, w tym danych klientów, danych pracowników, dokumentów finansowych, umów i korespondencji.

1.7. Wykonawca omówi podstawowe zasady ochrony danych osobowych w zakresie niezbędnym dla pracownika biurowego, w tym minimalizację danych i zasadę potrzeby wiedzy.

1.8. Wykonawca omówi bezpieczne udostępnianie informacji i danych, w tym zasady doboru adresatów, stosowania DW i UDW, ograniczania grona odbiorców oraz weryfikacji właściwego adresata przed wysyłką.

1.9. Wykonawca omówi bezpieczne przekazywanie plików i dokumentów, w tym stosowanie uprawnień do linków, ograniczeń czasowych, szyfrowania plików oraz przekazywania haseł innym kanałem komunikacji.

1.10. Wykonawca omówi bezpieczne przechowywanie i przetwarzanie dokumentów, w tym zasady przechowywania na nośnikach i w systemach służbowych oraz ryzyka związane z kopiowaniem na nośniki prywatne.

1.11. Wykonawca przedstawi możliwości portalu bezpiecznedane.gov.pl oraz innych serwisów np. havibeenpawn.com w zakresie ustalania wycieku własnych haseł, danych osobistych.

1.12. Wykonawca przedstawi różnice między http a https i umiejętność ich rozpoznawania, weryfikacji prawidłowości certyfikatów, przykłady nadużyć związanych z certyfikatami stron.

1.13. Wykonawca przedstawi zagrożenia hybrydowe dotyczące cyberprzestrzeni, w szczególności zagadnienia dezinformacji, ataków hybrydowych, wykorzystywania kont społecznościowych.

1.14. Wykonawca przedstawi zagadnienia ochrony sieci Wi-Fi w domu i pracy – bezpieczne hasła, szyfrowanie, konieczność aktualizacji urządzeń sieciowych.

1.15. Wykonawca przedstawi zagadnienie podatności urządzeń, zarządzania podatnościami, zasad aktualizacji sprzętu i oprogramowania i konsekwencji wynikających z zaniechań aktualizacji bezpieczeństwa.

1.16. Wykonawca przedstawi zagrożenia wynikające z publikowania danych o infrastrukturze w BIP, zamówieniach publicznych, zdjęć w portalach Internetowych.

1.17. Wykonawca omówi zasady bezpiecznego drukowania i przechowywania wydruków oraz zasady niszczenia dokumentów i utylizacji nośników informacji.

1.18. Wykonawca uwzględni w szkoleniu rozpoznawanie zagrożeń socjotechnicznych i phishingu w kanałach e-mail, SMS, telefonicznych i komunikatorach.

1.19. Wykonawca przedstawi zagrożenia wynikające z wykorzystania bezpłatnych Rozwiązań chmurowych, mailowych czy modeli językowych AI, które wykorzystują do dalszej analizy dane, które tam przechowujemy – w kontekście zagrożeń utraty prywatności, danych chronionych.

1.20. Wykonawca przedstawi zagrożenia wynikające z instalacji aplikacji na telefony komórkowe.

1.21. Wykonawca zaprezentuje metody weryfikacji aplikacji instalowanych na telefonach komórkowych – pod katem ich uprawnień.

1.22. Wykonawca przedstawi cechy prób wyłudzeń typu podszywanie się pod osobę publiczną, instytucję lub przełożonego, w tym scenariusze „pilny przelew", „zmiana numeru rachunku" oraz „pilna prośba przełożonego" wraz z zasadami ich weryfikacji.

1.23. Wykonawca omówi zasady bezpiecznego postępowania z linkami, załącznikami oraz kodami QR, w tym typowe mechanizmy infekcji i wyłudzeń.

1.24. Wykonawca omówi wymagania bezpiecznego uwierzytelniania, w tym zasady tworzenia haseł, stosowania menedżerów haseł oraz uwierzytelniania wieloskładnikowego, o ile jest dostępne u Zamawiającego.

1.25. Wykonawca omówi zasady ochrony kont użytkowników przed przejęciem, w tym rozpoznawanie nietypowych logowań, podejrzanych powiadomień i prób wymuszeń potwierdzeń.

1.26. Wykonawca omówi zasady bezpiecznego korzystania ze sprzętu służbowego, w tym blokadę ekranu, aktualizacje oraz bezpieczne korzystanie z przeglądarki i aplikacji biurowych w ujęciu użytkownika.

1.27. Wykonawca omówi ryzyka związane z nośnikami USB i plikami z nieznanych źródeł oraz zasady postępowania ograniczające ryzyko infekcji.

1.28. Wykonawca uwzględni w szkoleniu zasady bezpiecznej pracy zdalnej i mobilnej, w tym ryzyka Wi-Fi publicznych, hotspotów, pracy na urządzeniach prywatnych oraz zasady ochrony ekranu w miejscach publicznych.

1.29. Wykonawca omówi podstawowe zasady korzystania z firmowych kanałów dostępu zdalnego, w tym VPN, jeżeli stosowany oraz ryzyka związane z obchodzeniem przyjętych zasad.

1.30. Wykonawca omówi rozpoznawanie objawów złośliwego oprogramowania i ransomware w ujęciu użytkownika, w tym typowe symptomy oraz podstawowe zasady pierwszych działań.

1.31. Wykonawca wskaże czynności niedopuszczalne w przypadku podejrzenia incydentu, w tym samodzielne „czyszczenie", ukrywanie zdarzenia, chaotyczne resetowanie lub przenoszenie danych na prywatne nośniki.

1.32. Wykonawca omówi minimalne zasady zgłaszania incydentów, w tym co należy zgłaszać, w jakim czasie i jakim kanałem zgodnie z procedurami Zamawiającego lub przyjętym modelem zgłoszeń.

1.33. Wykonawca wskaże minimalny zestaw informacji, który uczestnik powinien przekazać przy zgłoszeniu incydentu, w tym czas zdarzenia, użyte urządzenie, konto, opis objawów oraz dostępne zrzuty ekranu.

1.34. Wykonawca uwzględni w programie zasady klasyfikacji i ochrony informacji, w tym informacji wrażliwych z perspektywy IT.

1.35. Wykonawca omówi podstawowe obowiązki i dobre praktyki w zakresie ochrony danych osobowych w zakresie niezbędnym dla użytkownika systemów, w tym bezpieczne udostępnianie, przechowywanie oraz przekazywanie informacji.

1.36. Wykonawca omówi zasady bezpiecznego uwierzytelniania i zarządzania dostępem, w tym: hasła, MFA, menedżer haseł, zasadę najmniejszych uprawnień, rozdzielenie kont uprzywilejowanych od kont użytkownika.

1.37. Wykonawca omówi ryzyka związane z kontami serwisowymi i współdzielonymi oraz minimalne praktyki ograniczające nadużycia.

1.38. Wykonawca omówi mechanizmy socjotechniki i phishingu (e-mail, SMS, telefon, komunikatory), w tym rozpoznawanie cech prób wyłudzeń.

1.39. Wykonawca przedstawi scenariusze typowe dla IT, w szczególności podszywanie się pod dostawcę/serwis oraz presję „pilnej awarii" i żądania zdalnego dostępu, przekazania konfiguracji lub danych uwierzytelniających.

1.40. Wykonawca przedstawi zasady niezależnej weryfikacji próśb i poleceń (oddzwanianie, drugi kanał, zatwierdzenie przez osobę uprawnioną).

1.41. Wykonawca omówi ryzyka stałych dostępów serwisowych oraz stosowania niezatwierdzonych narzędzi zdalnych i „obejść" procedur (w ujęciu świadomościowym).

1.42. Wykonawca omówi typowy przebieg incydentu ransomware i jego skutki operacyjne w IT.

1.43. Wykonawca wskaże zachowania pracowników, które ograniczają straty (wczesne zgłoszenie, nieukrywanie incydentu, niepodejmowanie niekontrolowanych działań), oraz podstawowe zasady postępowania z nośnikami i plikami w sytuacji podejrzenia incydentu.

1.44. Wykonawca omówi sygnały ostrzegawcze incydentów w IT na poziomie podstawowym (np. nietypowe logowania, prośby o ponowne MFA, anomalie trendów/alertów, nieoczekiwane restarty, utrata komunikacji).

1.45. Wykonawca zapewni elementy praktyczne obejmujące co najmniej trzy ćwiczenia z udziałem uczestników: identyfikację phishingu, analizę ryzyk w wiadomości (link/załącznik/QR) oraz scenariusz weryfikacji „pilnej prośby" dotyczącej płatności lub danych.

1.46. Wykonawca zapewni materiały szkoleniowe dla każdego uczestnika obejmujące co najmniej listę podstawowych zasad bezpiecznej pracy, listę „czerwonych flag" dla prób wyłudzeń oraz instrukcję zgłaszania incydentów.

1.47. Wykonawca przeprowadzi po szkoleniu krótką weryfikację wiedzy w formie testu lub quizu sytuacyjnego.

1.48. Wykonawca przekaże Zamawiającemu zbiorcze podsumowanie wyników weryfikacji wiedzy oraz obszarów wymagających wzmocnienia, bez identyfikacji uczestników.

1.49. Szkoleniem objętych zostanie łącznie maksymalnie **130** pracowników Zamawiającego.

1.50. Szkolenie dla pracowników niebędących informatykami musi zostać zrealizowane w formie **5 grup szkoleniowych po ok. 26 osób.**

1.51. Szkolenie będzie realizowane stacjonarnie w siedzibie Zamawiającego.

1.52. Czas trwania szkolenia dla każdej grupy nie może być krótszy niż 8 godzin zegarowych (nie dydaktycznych), realizowanych w jednym dniu lub w uzgodnionym harmonogramie.

1.53. Szkolenie musi być prowadzone w języku polskim.

1.54. Po zakończeniu szkolenia Wykonawca przekaże Zamawiającemu dokumentację potwierdzającą realizację szkolenia (np. lista obecności, agenda).

1.55. Szkolenie musi być zgodne z obowiązującymi przepisami prawa, w szczególności RODO, KRI, ustawą o krajowym systemie cyberbezpieczeństwa oraz dobrymi praktykami cyberbezpieczeństwa oraz najnowszym stanem wiedzy technicznej.

2. SZKOLENIE SPECJALISTYCZNE DLA KADRY ZARZĄDZAJĄCEJ I INFORMATYKÓW

2.1. Przedmiotem zadania jest kompleksowa organizacja i przeprowadzenie jednego, jednodniowego szkolenia stacjonarnego w formie warsztatu dla kadry kierowniczej Zamawiającego.

2.2. Celem szkolenia jest podniesienie świadomości kadry kierowniczej wynikającej zagrożeń w cyberprzestrzeni i ataków hybrydowych a także w zakresie obowiązków podmiotów publicznych w zakresie cyberbezpieczeństwa.

2.3. Wykonawca jest zobowiązany zrealizować szkolenie obejmujące co najmniej następujące moduły tematyczne:

2.3.1. Zakres przedmiotowy i podmiotowy obowiązywania przepisów dotyczących cyberbezpieczeństwa

2.3.2. Obowiązki podmiotów publicznych

2.3.3. Struktura krajowego systemy cyberbezpieczeństwa

2.3.4. Zadania i rola CSIRT, rodzaje CSIRT w Polsce

2.3.5. Wymagania prawne i znaczenie SZBI, SZCD w organizacji

2.3.6. Odpowiedzialność kierowników jednostek

2.3.7. Definicje i przykłady incydentów

2.3.8. Zasady obsługi incydentów bezpieczeństwa, w tym obowiązki prawne.

2.3.9. Przykłady ataków na urzędy publiczne w Polsce i na świecie.

2.3.10. Techniki i taktyki atakujących.

2.3.11. Znaczenie publikowania informacji w BIP, mediach społecznościowych, portalach GIS.

2.3.12. Ochrona informacji niejawnych w Polsce.

2.3.13. Omówienie znaczenia i egzekwowania polityki bezpieczeństwa informacji oraz odpowiedzialności kadry za jej wdrażanie i utrzymanie.

2.3.14. Omówienie roli kadry w procesie reagowania na incydenty, eskalacji zdarzeń, podejmowania decyzji kryzysowych oraz komunikacji.

2.3.15. Omówienie powiązań między cyberbezpieczeństwem a ciągłością działania, w tym odpowiedzialności kadry za uruchamianie i nadzorowanie planów ciągłości działania.

2.3.16. Projekty zmian do ustawy o krajowym systemie cyberbezpieczeństwa (implementacja NIS2).

2.3.17. zastosowane i planowane do zastosowania środki bezpieczeństwa w ramach realizacji Przedmiotu zamówienia.

2.3.18. Zasady korzystania z MFA

2.3.19. omówienie technologii NGFW, SIEM, SOAR, XDR, IAM, PAM, kopi zapasowej

2.4. Szkolenie powinno uwzględniać wymagania norm ISO/IEC 27001, ISO/IEC 27002, ISO 22301 lub równoważnych pokrywających zakres tych norm oraz dobre praktyki cyberbezpieczeństwa.

2.5. Wykonawca zapewni materiały szkoleniowe dostosowane do poziomu kadry kierowniczej, w tym podsumowania decyzyjne i rekomendacje.

3. SZKOLENIE AUDYTOR WIODĄCY SZBI WG ISO/IEC 27001

3.1. Wykonawca przeprowadzi szkolenie przygotowujące jednego pracownika Zamawiającego do pełnienia roli Audytora Wiodącego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w formie stacjonarnej lub zdalnej na terenie m.st. Warszawy.

3.2. Celem szkolenia jest nabycie przez uczestnika wiedzy i umiejętności umożliwiających planowanie, prowadzenie, nadzorowanie i raportowanie audytów SZBI oraz kierowanie zespołem audytowym.

3.3. Wykonawca zrealizuje szkolenie obejmujące co najmniej:

3.3.1. Podstawy zarządzania bezpieczeństwem informacji i podejścia procesowego w SZBI.

3.3.2. Wymagania normy ISO/IEC 27001 (aktualne wydanie obowiązujące w dniu realizacji) – interpretacja wymagań, typowe dowody audytowe.

3.3.3. Powiązania i kontekst normatywny (co najmniej): ISO/IEC 27002 (kontrole), ISO 19011 (wytyczne audytowania) – w zakresie niezbędnym do audytu SZBI.

3.3.4. Kontekst organizacji, strony zainteresowane, zakres SZBI, mapa procesów i zasoby informacyjne – typowe ryzyka i błędy wdrożeniowe.

3.3.5. Podejście oparte o ryzyko w SZBI: metodyka oceny ryzyka, plan postępowania z ryzykiem, kryteria akceptacji, spójność dokumentacji i praktyki.

3.3.6. Projektowanie i ocena skuteczności zabezpieczeń (kontrole) oraz mierniki/monitorowanie skuteczności SZBI.

3.3.7. Program audytu: planowanie roczne i plan audytu, kryteria, zakres, próbki, metody zbierania dowodów.

3.4. Po zakończeniu szkolenia Wykonawca zapewni przeprowadzenie egzaminu certyfikującego potwierdzającego kompetencje Audytora Wiodącego SZBI.

4. SZKOLENIE POWIĄZANE Z TESTAMI SOCJOTECHNICZNYMI

4.1. Przedmiotem zadania jest przeprowadzenie oraz podsumowanie szkoleń z zakresu cyberbezpieczeństwa, powiązanych z praktycznymi testami socjotechnicznymi, weryfikującymi świadomość zagrożeń oraz reakcje personelu Zamawiającego.

4.2. W ramach szkolenia wykonawca przeprowadzi co najmniej 10 kampanii symulowanych ataków socjotechniczny na pracowników Zamawiającego.

4.3. Wykonawca przeprowadzi kontrolowane testy socjotechniczne, których celem jest sprawdzenie reakcji personelu na próby manipulacji i wyłudzeń informacji.

4.4. Testy muszą obejmować co najmniej:

4.4.1. symulacje phishingu (e-mail),

4.4.2. vishing (telefoniczne próby manipulacji),

4.4.3. smishing (SMS),

4.4.4. Testy muszą weryfikować:

4.4.5. rozpoznawanie prób socjotechnicznych,

4.4.6. właściwe reakcje użytkowników,

4.4.7. zgodność działań z obowiązującymi procedurami SZBI,

4.4.8. skuteczność zgłaszania incydentów.

4.5. Po każdej kampanii ataków wykonawca przeprowadzi kampanię awarness dla pracowników w celu podniesienia umiejętności wykrywania technik i taktyk użytych do ataku oraz wskazania popełnionych błędów w wykryciu ataku.

4.6. Wykonawca opracuje scenariusze testów socjotechnicznych dostosowane do profilu działalności Zamawiającego.

4.7. Po zakończeniu działań Wykonawca przekaże raport zawierający:

4.7.1. opis przeprowadzonych testów,

4.7.2. wyniki i statystyki,

4.7.3. ocenę świadomości personelu,

4.7.4. rekomendacje działań korygujących i doskonalących.

4.8. Testy socjotechniczne muszą być realizowane w sposób etyczny, kontrolowany i niepowodujący zakłóceń w pracy Zamawiającego.

CZĘŚĆ NR 2 WDROŻENIE ROZWIĄZAŃ CYBERBEZPIECZEŃSTWA

1. WYMAGANIA OGÓLNE

1.1. Przedmiotem Zamówienia jest dostawa kompletnych i spójnych **Rozwiązań bezpieczeństwa** (zwanymi dalej „Rozwiązaniami") do siedziby Zamawiającego oraz ich wdrożenie w pełnym zakresie funkcjonalnym a także przeszkolenie wybranych pracowników technicznych z wdrożonych Rozwiązań.

1.2. Docelowa architektura cyberbezpieczeństwa Zamawiającego ma stanowić spójny ekosystem Rozwiązań bezpieczeństwa, w którym każdy komponent ma jednoznacznie określoną rolę, a integracje pomiędzy komponentami zapewniają ciągły przepływ danych telemetrycznych, zdarzeń i kontekstu oraz umożliwiają koordynację działań detekcyjnych, analitycznych i reakcyjnych:

1.3. W ramach architektury wszystkie Rozwiązania muszą być wdrożone i skonfigurowane jako wzajemnie współpracujący ekosystem, w którym SIEM jest centralnym repozytorium i punktem raportowania.

1.4. Architektura musi zapewniać spójne zarządzanie czasem (NTP – serwer GUM) oraz ujednolicenie stref czasowych w logach dla wszystkich komponentów, aby umożliwić korelację zdarzeń i rzetelne raportowanie incydentów w SIEM.

1.5. Przez producenta Zamawiający rozumie podmiot odpowiedzialny za rozwój, utrzymanie, usuwanie podatności bezpieczeństwa oraz dostarczanie aktualizacji oferowanego rozwiązania.

1.6. Wykonawca jest zobowiązany do wykonania Analizy Przedwdrożeniowej oraz sporządzenia Projektu Technicznego przedkładanego do akceptacji Zamawiającego.

1.7. Wykonawca określi w Analizie Przedwdrożeniowej zalecaną specyfikację i optymalną konfigurację środowiska adekwatną do potrzeb Zamawiającego.

1.8. Wykonawca opracuje Projekt Techniczny zawierający:

1.8.1. Architekturę Rozwiązań i ekosystemu

1.8.2. Wersję oprogramowania wchodzące w skład Rozwiązania

1.8.3. Konfigurację Systemu

1.8.4. Zastosowane licencje.

1.9. Zamawiający wymaga, aby Wykonawca w ramach wdrożenia wykonał instalację, konfigurację i integrację Rozwiązań z systemami Zamawiającego, konfiguracja Rozwiązań musi uwzględniać:

1.9.1. Utworzenie kont użytkowników i grup zgodnie z wymaganiami Zamawiającego;

1.9.2. Integracji uwierzytelniania i autoryzacji użytkowników z Active Directory Zamawiającego;

1.10. Wykonawca określi kluczowe mierniki odnośnie do wydajności i dostępności Rozwiązań oraz określi wartości progowe dla tych liczników, dzięki którym możliwe będzie proaktywne monitorowanie systemów. W szczególności określone zostaną przez Wykonawcę dopuszczalne wartości wskaźników wydajnościowych wszystkich składników Rozwiązań w warunkach normalnych oraz ich wartości progowe, których przekroczenie będzie uznawane za sytuację alarmową i sytuację krytyczną.

1.11. Zamawiający wymaga, aby Wykonawca zapewnił wdrożenie najlepszych praktyk optymalnego wdrożenia i konfiguracji Rozwiązań.

1.12. Wykonawca sporządzi i dostarczy Zamawiającemu Dokumentację Powykonawczą. Dokumentacja musi być sporządzona w języku polskim lub angielskim.

1.13. Zawartość merytoryczna Dokumentacji musi obejmować:

1.13.1. Schemat infrastruktury i architekturę Rozwiązania wraz z opisem.

1.13.2. Zasady licencjonowania dostarczonych elementów infrastruktury.

1.13.3. Konfigurację sprzętową i logiczną elementów infrastruktury.

1.13.4. Procedurę instalacji i konfiguracji wszystkich elementów Rozwiązania.

1.13.5. Procedury uruchamiania, zatrzymywania oraz elementów infrastruktury.

1.13.6. Procedury wykonywania odtworzenia Rozwiązania z kopii zapasowej.

1.13.7. Procedury opisujące standardowe działania administracyjne.

1.13.8. Procedury odzyskania Rozwiązania po awarii.

1.13.9. Wytyczne (dobre praktyki) dla administratorów.

1.13.10. Spis dokumentacji zewnętrznej do której odwołuje się Dokumentacja Powykonawcza.

1.14. Wszelkie działania Wykonawcy muszą zostać przeprowadzone w taki sposób, aby nie nastąpiły przerwy w dostępie do systemów Zamawiającego.

1.15. W odniesieniu do każdego z Rozwiązania Wykonawca w obecności Zamawiającego przeprowadzi Testy Odbiorcze.

1.16. Wykonawca przygotowuje scenariusze testowe dla każdego rodzaju Rozwiązania zgodnie z szablonem uzgodnionym z Zamawiającym, przy czym minimalnie muszą zawierać:

1.16.1. uruchamianie i zatrzymywanie Rozwiązania

1.16.2. testy funkcjonalne

1.16.3. spójność i integralność Rozwiązań

1.16.4. potwierdzenie konfiguracji z dokumentacją powykonawczą

1.16.5. poprawność zainstalowanego sprzętu.

1.17. W przypadku negatywnych wyników testów odbiorczych wykonawca jest zobowiązany usunąć nieprawidłowości i spostrzeżenia Zamawiającego.

2. WYMAGANIA PODSTAWOWE DO ROZWIĄZAŃ BEZPIECZEŃSTWA

2.1. Oprogramowanie musi być dostarczone w aktualnej, stabilnej wersji produkcyjnej, rekomendowanej przez producenta do wdrożeń produkcyjnych, wraz z wszystkimi niezbędnymi licencjami, subskrypcjami oraz wszelkimi innymi elementami wymaganymi przez producenta, w ilości, parametrach zapewniających spełnienie wszystkich wymagań Zamawiającego określonych w OPZ.

2.2. Zamawiający wymaga, aby wszystkie Rozwiązania objęte zamówieniem zostały wdrożone, skonfigurowane i zintegrowane z systemami informatycznymi Zamawiającego jako spójny, wzajemnie współpracujący ekosystem bezpieczeństwa.

2.3. Wykonawca zobowiązany jest do dostarczenia sprzętu i oprogramowania niezbędnego do prawidłowego, pełnego i wydajnego funkcjonowania oferowanych Rozwiązań, bez konieczności ponoszenia przez Zamawiającego dodatkowych kosztów.

2.4. Zamawiający wymaga wykonania hardeningu wszystkich wdrażanych Rozwiązań zgodnie z wytycznymi producenta oraz powszechnie uznanymi najlepszymi praktykami bezpieczeństwa, w szczególności w oparciu o wzorcowe standardy konfiguracji (np. CIS Benchmark), o ile są one dostępne dla danego Rozwiązania, lub równoważne, powszechnie stosowane standardy bezpieczeństwa.

2.5. Wszystkie dostarczone Rozwiązania muszą pochodzić z oficjalnego kanału dystrybucji producenta, zapewniającego realizację warunków gwarancyjnych i serwisowych.

2.6. Przedmiot zamówienia musi być fabrycznie nowy, nieużywany, pochodzący z legalnego kanału dystrybucji, dopuszczony do obrotu na terytorium Unii Europejskiej oraz spełniający obowiązujące normy, w tym wymagania oznaczenia CE.

2.7. Zamawiający wymaga, aby oferowane urządzenia oraz oprogramowanie były Rozwiązaniami stabilnymi i sprawdzonymi w praktyce rynkowej, tj. oficjalnie

dostępne w sprzedaży i objęte wsparciem producenta co najmniej 6 miesięcy przed terminem składania ofert; niedopuszczalne jest oferowanie Rozwiązań w wersjach testowych, pilotażowych, beta lub równoważnych.

2.8. Oferowane Rozwiązania muszą być dostępne w sprzedaży oraz serwisowane przez producenta lub jego autoryzowanego przedstawiciela serwisowego na terenie Polski i nie mogą znajdować się, na dzień składania oferty, w fazie wycofania ze sprzedaży lub wsparcia (End-of-Sale, End-of-Life lub równoważne).

2.9. Poszczególne elementy Rozwiązań mogą być realizowane jako odrębne platformy sprzętowe; w przypadku implementacji programowej Wykonawca zobowiązany jest zapewnić odpowiednie platformy sprzętowe wraz z właściwie zabezpieczonym systemem operacyjnym.

2.10. **Dopuszcza się dostawę i wdrożenie zintegrowanych platform obejmujących niżej wymienione wymagania w jednym produkcie, jeżeli usprawni to Zamawiającemu proces obsługi.**

2.11. **Jeżeli spełnienie wymagań OPZ wymaga zastosowania dodatkowego oprogramowania, licencji lub subskrypcji, Wykonawca zobowiązany jest je jednoznacznie wskazać oraz dostarczyć w ramach przedmiotu zamówienia (dotyczy również środowiska wirtualizacji, przy czym środowisko to powinno być licencjonowane wieczyście lub w oparciu o rozwiązanie opensource np. Proxmox).**

2.12. **Jeżeli spełnienie wymagań OPZ wymaga dostarczenia dodatkowego Sprzętu, akcesoriów lub doposażenia istniejącej infrastruktury, Wykonawca zobowiązany jest je wskazać oraz dostarczyć w ramach przedmiotu zamówienia.**

2.13. **W ramach realizacji zamówienia Wykonawca zobowiązany jest dostarczyć i wdrożyć sprzęt niezbędny do prawidłowego funkcjonowania wszystkich Rozwiązań bezpieczeństwa w pełnym zakresie funkcjonalnym i wydajnościowym, zgodnie z wynikami Analizy Przedwdrożeniowej wykonanej w ramach realizacji zamówienia lub przekazanej przez Zamawiającego.**

2.14. **Sprzęt serwerowy musi być dostarczony wraz z wszystkimi niezbędnymi licencjami na systemy operacyjne, oprogramowanie wirtualizacje, bazy danych oraz inne komponenty wymagane do prawidłowego funkcjonowania Rozwiązań.**

2.15. **Rozwiązania muszą zapewniać wydajność umożliwiającą przetwarzanie danych, obsługę zdarzeń oraz realizację funkcji bezpieczeństwa w czasie rzeczywistym lub z opóźnieniem nieprzekraczającym wartości granicznych określonych przez**

producenta, przy obciążeniu odpowiadającym co najmniej docelowemu wolumenowi użytkowników, systemów i zdarzeń Zamawiającego.

2.16. **Wydajność systemu nie może ulegać degradacji w sposób wpływający na ciągłość działania, skuteczność mechanizmów bezpieczeństwa ani dostępność usług przy jednoczesnym wystąpieniu maksymalnego przewidywanego obciążenia.**

2.17. Oferowany sprzęt musi być przeznaczony do profesjonalnego użytku korporacyjnego.

2.18. Zamawiający wymaga zapewnienia dostępu do poprawek i aktualizacji, w tym aktualizacji bezpieczeństwa:

2.18.1. a) w odniesieniu do sprzętu – przez okres co najmniej 36 miesięcy od dnia dostawy,

2.18.2. b) w odniesieniu do oprogramowania – przez okres co najmniej 36 miesięcy od dnia dostawy.

3. GWARANCJA

3.1. Wykonawca zobowiązany jest udzielić lub zapewnić udzielenie co najmniej 36-miesięcznej gwarancji na dostarczone i wdrożone Rozwiązania, rozumiane jako całość obejmującą sprzęt, oprogramowanie oraz wykonane czynności wdrożeniowe i konfiguracyjne, na warunkach określonych w dokumentach gwarancyjnych dostarczonych przez Producentów, spełniających co najmniej warunki określone w Umowie oraz OPZ.

3.2. Okres gwarancji biegnie od dnia podpisania przez obie Strony, bez zastrzeżeń, Protokołu Odbioru Końcowego.

3.3. Wykonawca oświadcza, że dostarczone i wdrożone w ramach przedmiotu zamówienia Rozwiązania jako całość są wolne od wad fizycznych, rozumianych jako niezgodność Rozwiązań z Opisem Przedmiotu Zamówienia, oraz wad prawnych, pochodzą z legalnego kanału dystrybucji, a dokumenty licencyjne, gwarancyjne oraz inne dokumenty uprawniające do korzystania z Rozwiązań umożliwiają Zamawiającemu korzystanie z dostarczonego sprzętu i oprogramowania w sposób zgodny z powszechnie obowiązującym prawem oraz warunkami producentów.

3.4. Odpowiedzialność z tytułu gwarancji obejmuje zarówno wady istniejące w chwili odbioru Rozwiązania przez Zamawiającego, jak i wszelkie inne wady fizyczne ujawnione w okresie obowiązywania gwarancji, w tym wady wynikające z błędów

wdrożeniowych, konfiguracyjnych lub integracyjnych, o ile powstały z przyczyn, za które odpowiedzialność ponosi Wykonawca.

3.5. Wykonawca gwarantuje, że w okresie co najmniej 36 miesięcy od dnia podpisania Protokołu Odbioru Końcowego Rozwiązanie jako całość będzie spełniało wszystkie wymagania funkcjonalne i wydajnościowe określone w Opisie Przedmiotu Zamówienia w sposób ciągły, bez konieczności ponoszenia przez Zamawiającego dodatkowych kosztów, w tym w szczególności kosztów licencyjnych, sprzętowych, modernizacyjnych lub rozbudowy infrastruktury, z zastrzeżeniem przypadków zmiany zakresu Zamówienia dokonanych na podstawie odrębnych uzgodnień Stron.

3.6. Wykonawca jest odpowiedzialny względem Zamawiającego za to, że jest uprawniony do wprowadzenia do obrotu Rozwiązań oraz że Zamawiający, wskutek zawarcia Umowy, będzie upoważniony do korzystania z Rozwiązań jako całości w sposób zgodny z ich charakterem, przeznaczeniem oraz przyjętymi zwyczajami.

3.7. W ramach gwarancji Zamawiający jest uprawniony do żądania usunięcia Awarii oraz wad Rozwiązań, które wystąpią w trakcie okresu obowiązywania gwarancji.

3.8. Zgłoszenie konieczności świadczenia usług w ramach gwarancji, w tym zgłoszenie konieczności usunięcia Awarii, dokonywane będzie bezpośrednio do Wykonawcy telefonicznie pod polskim numerem telefonicznym lub na adres poczty elektronicznej wskazane przez Wykonawcę.

3.9. Zgłoszenia przyjmowane będą 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku.

3.10. Usługi w ramach gwarancji, w tym usuwanie Awarii, będą realizowane zgodnie z następującymi zasadami i terminami:

3.10.1. czas reakcji – nie później niż w ciągu 3 godzin od momentu zgłoszenia wady Rozwiązania lub Awarii do momentu potwierdzenia przyjęcia zgłoszenia, przesłanego na adres poczty elektronicznej Zamawiającego;

3.10.2. czas usunięcia wady Rozwiązania lub Awarii – nie później niż w ciągu 24 godzin od momentu zgłoszenia do momentu potwierdzenia jej usunięcia; w przypadku uznania przez Zamawiającego, że wada lub Awaria nie została skutecznie usunięta, Zamawiający jest uprawniony do ponownego zgłoszenia, przy czym czas jej trwania liczony jest jako kontynuacja pierwotnego zgłoszenia;

3.10.3. w przypadku braku możliwości trwałego usunięcia wady lub Awarii w terminie 24 godzin Zamawiający dopuszcza zastosowanie Rozwiązania tymczasowego

wyłącznie po jego uprzedniej akceptacji, przy czym rozwiązanie docelowe musi zostać dostarczone i wdrożone w terminie 30 dni od dnia następującego po dniu wdrożenia Rozwiązania tymczasowego.

3.11. Zamawiający może wykonywać uprawnienia z tytułu gwarancji niezależnie od uprawnień z tytułu rękojmi i zachowuje prawo do korzystania z uprawnień z tytułu rękojmi przez cały okres obowiązywania gwarancji.

4. USŁUGA WSPARCIA TECHNICZNEGO

4.1. Wykonawca zobowiązany jest do świadczenia na rzecz Zamawiającego usług wsparcia technicznego na zasadach określonych w dokumentach dostarczonych przez Wykonawcę, spełniających na warunkach nie gorszych niż określone w Umowie oraz OPZ.

4.2. Usługa wsparcia technicznego Wykonawcy będzie świadczona przez okres 36 miesięcy, licząc od dnia podpisania bez zastrzeżeń przez obie Strony Protokołu Odbioru Końcowego.

4.3. Zakres usług wsparcia technicznego Wykonawcy obejmuje:

4.3.1. doradztwo i pomoc w zakresie obsługi Rozwiązania;

4.3.2. analizę i rozwiązywanie problemów związanych z Rozwiązaniem oraz zaistniałych na styku pomiędzy oprogramowaniem a sprzętem i innym oprogramowaniem użytkowanym przez Zamawiającego;

4.3.3. zapewnienie dostępu (za pośrednictwem strony internetowej) i możliwości korzystania z aktualizacji, poprawek bezpieczeństwa, nowych wersji oprogramowania, oraz dokumentacji administracyjnej i technicznej dotyczącej Rozwiązania;

4.3.4. informowanie o znanych problemach z Rozwiązaniem i sposobach ich Rozwiązania drogą telefoniczną - kontakt na polski numer telefonu lub poprzez pocztę elektroniczną, kontakt na adres poczty elektronicznej.

4.4. W sytuacji, gdy pomoc Wykonawcy realizowana w ramach wsparcia technicznego, okaże się niewystarczająca dla Zamawiającego, Wykonawca zobowiązuje do świadczenia na wniosek Zamawiającego dodatkowych usług wsparcia technicznego w wymiarze maksymalnym **120 godzin**, polegających na osobistym (bezpośrednim) wsparciu Zamawiającego w miejscu aktualnej lokalizacji Rozwiązania przez wykwalifikowanych polskojęzycznych inżynierów w pełnym zakresie, w tym:

4.4.1.1. usuwaniu Awarii na zasadach wskazanych OPZ oraz Umowie.

4.4.1.2. aktualizacji wersji wszystkich komponentów oraz przeprowadzania odpowiednich testów poprawnego funkcjonowania po ww. aktualizacjach;

4.4.1.3. wdrażania nowych funkcjonalności Rozwiązania wynikających z ww. aktualizacji;

4.4.1.4. pełnej instalacji i konfiguracji Rozwiązania;

4.4.1.5. oraz innych prac serwisowych dla Rozwiązania, na życzenie Zamawiającego.

4.5. Zamawiający może wyrazić zgodę, aby usługa była świadczona w formie zdalnej.

5. USŁUGA WSPARCIA PRODUCENTA

5.1. Wykonawca zapewni rozszerzoną usługę wsparcia technicznego producenta Rozwiązania świadczoną na zasadach określonych przez producenta Rozwiązania, opisanych w dokumentach przekazanych przez Wykonawcę, spełniających co najmniej warunki określone w Umowie oraz OPZ.

5.2. Usługa wsparcia technicznego producenta Rozwiązania będzie świadczona przez okres 36 miesięcy, licząc od dnia podpisania bez zastrzeżeń przez obie Strony Protokołu Odbioru Końcowego.

5.3. W ramach wsparcia technicznego producenta Rozwiązania Zamawiający będzie posiadać możliwość zgłaszania Awarii drogą telefoniczną lub elektroniczną za pośrednictwem poczty email lub strony WWW producenta Rozwiązania.

5.4. W ramach wsparcia technicznego producenta Rozwiązania Wykonawca zobowiązuje się do zapewnienia w szczególności:

5.5. dostępu do nowych wersji, aktualizacji i poprawek dla Rozwiązania;

5.6. udzielenia licencji na użytkowanie i kopiowanie nowych wersji, aktualizacji i poprawek dla Rozwiązania;

5.7. dostępu do elektronicznych kanałów informacji i usług wsparcia (bazy wiedzy, bibliotek dokumentacji, opisów produktów, specyfikacji, literatury technicznej i innych materiałów).

5.8. Zgłoszenia w ramach usługi wsparcia technicznego producenta Rozwiązania będą przyjmowane co najmniej w trybie 8 x 5 (NBD).

5.9. Rozwiązania muszą zostać objęte rozszerzonym wsparciem gwarancyjnym w przypadku awarii polegającym na dostarczeniu na drugi dzień roboczy Rozwiązania zastępczego na czas naprawy o takich samych parametrach.

5.10. Wykonawca zobowiązuje się pośredniczyć w przypadku konieczności uzyskania bezpośredniego wsparcia technicznego ze strony producenta Rozwiązania.

6. ROZWIĄZANIE PAM

6.1. Przedmiotem zamówienia jest dostawa wraz z kompleksowym wdrożeniem systemu zarządzania dostępem uprzywilejowanym oraz przeszkolenie personelu Zamawiającego.

6.2. Zamawiający wymaga, aby System PAM został wdrożony i zintegrowany z systemami informatycznymi Zamawiającego.

6.3. Zamawiający wymaga, aby System PAM był rozwiązaniem bez agentowym, umożliwiającym uwierzytelnianie wieloskładnikowe i obsługujące wiele platform i systemów operacyjnych. System PAM ma zabezpieczać maszyny fizyczne, wirtualne, sprzęt sieciowy m.in. routery, przełączniki, zapory sieciowe, aplikacje, bazy danych itp.

6.4. Zamawiający wymaga, aby Wykonawca przeprowadził Analizę Przedwdrożeniową z zakresu:

6.4.1. systemów Zamawiającego

6.4.2. wymagań Zamawiającego

6.4.3. uprzywilejowanych kont w systemach Zamawiającego.

6.5. Wykonawca określi w Analizie przedwdrożeniowej zalecaną specyfikację i optymalną konfigurację środowiska dla Systemu PAM m.in. pamięć, liczbę procesorów, ilość i wielkość dysków. Wynik Analizy Przedwdrożeniowej zostanie zawarty w Projekcie Technicznym a określone wymagania dostarczone w ramach niniejszego zamówienia.

6.6. Wykonawca dostarczy i wdroży niezbędny sprzęt o parametrach określonych w analizie przedwdrożeniowej. Zamawiający zapewni miejsce w szafie RACK.

6.7. Zamawiający nie dopuszcza możliwość instalacji Systemu PAM w posiadanej infrastrukturze wirtualnej. Wykonawca jest zobowiązany zapewnić środowisko wirtualizacji.

6.8. Zamawiający wymaga, aby Wykonawca w ramach wdrożenia wykonał instalację, konfigurację i integrację Systemu PAM z Systemem Informatycznym Zamawiającego, konfiguracja Systemu PAM musi uwzględniać:

6.8.1. Utworzenie kont użytkowników i grup Systemu PAM zgodnie z wymaganiami Zamawiającego;

6.8.2. Integracja uwierzytelniania i autoryzacji użytkowników Systemu PAM z Active Directory Zamawiającego;

6.8.3. Utworzenie kont systemów docelowych w Systemie PAM zgodnie z wymaganiami Zamawiającego;

6.8.4. Utworzenie polityk związanych ze złożonością hasła zgodnie z wymaganiami Zamawiającego;

6.8.5. Utworzenie harmonogramów zmiany hasła zgodnie z wymaganiami Zamawiającego;

6.8.6. Utworzenie schematów wnioskowania o dostęp do hasła i/lub sesji zgodnie z wymaganiami Zamawiającego;

6.8.7. Hardening Systemu PAM.

6.9. System PAM musi realizować dostęp do minimum 10 systemów chronionych z możliwością licencyjnej rozbudowy do 30 i więcej systemów.

6.10. System PAM musi zostać dostarczony z kompletem licencji dla co najmniej 8 administratorów z możliwością rozszerzenia, którzy będą korzystali z Systemu PAM, minimum dla następującej liczby funkcjonalności:

6.10.1. Ochrona kont uprzywilejowanych,

6.10.2. Zarządzanie i monitorowanie sesji uprzywilejowanych,

6.10.3. Ochrona kluczy SSH,

6.10.4. Raportowanie wykorzystania kont uprzywilejowanych,

6.10.5. Rejestrowanie sesji uprzywilejowanych.

6.11. Dostarczone licencje na System PAM do ochrony kont uprzywilejowanych nie mogą mieć ograniczeń czasowych. Dostarczone licencje będą udzielone bezterminowo.

6.12. System PAM musi zapewniać możliwość zarządzania (w szczególności):

6.12.1. Użytkownikami na systemach operacyjnych: Windows, Unix/Linux,

6.12.2. Kontami domenowymi: MS Active Directory,

6.12.3. Kontami lokalnymi: VMware ESX/ESXi / vSphere,

6.12.4. Kontami na urządzeniach m.in.: Juniper, PaloAlto, Fortigate, Cisco,

6.12.5. Kontami do zarządzania macierzami: Hitachi.

6.12.6. Kontami baz danych: Microsoft SQL, Oracle, MySQL,

6.12.7. Kontami do zarządzania i monitorowania serwerów: m.in. iLO, iDRAC, xClarity.

6.12.8. Kontami w innych niewymienionych systemach/urządzeniach do których dostęp odbywa się po protokołach: SSH, RDP,VNC, TELNET, HTTP/HTTPS.

6.13. System PAM musi umożliwiać usługę pośredniczenia w dostępie do systemów i urządzeń dla użytkowników domenowych oraz użytkowników zewnętrznych,

rejestrując obsługiwane sesje, oraz obsługując minimum następujące protokoły: SSH, RDP,VNC, TELNET, HTTP/HTTPS.

6.14. System PAM musi wspierać minimum następujące mechanizmy uwierzytelniania: LDAP, RADIUS, Active Directory.

6.15. System PAM musi obsługiwać monitorowanie i ochronę nawet kilkudziesięciu jednoczesnych połączeń od jednego użytkownika końcowego, do różnych systemów poprzez wiele lub jedno konto uprzywilejowane.

6.16. System PAM nie może wymagać instalacji żadnego dodatkowego agenta na systemie docelowym.

6.17. System PAM musi umożliwiać dostęp użytkowników do systemu docelowego następującymi narzędziami:

6.17.1. przeglądarka internetowa,

6.17.2. klient RDP,

6.17.3. klient protokołu SSH/Telnet.

6.18. System PAM musi posiadać możliwość automatycznego uwzględniania zmian zachodzących w organizacji w systemie AD/LDAP.

6.19. System PAM musi umożliwiać realizację operacji masowych, edycji lub dodawania atrybutów do wskazanych kont w tym samym czasie.

6.20. System PAM musi ograniczać administratorowi możliwość dostępu do haseł lub ograniczać podgląd do haseł uprzywilejowanych.

6.21. System PAM powinien zapewniać możliwość dwuskładnikowego uwierzytelniania.

6.22. System PAM musi umożliwiać budowanie polityk kontroli dostępu w oparciu o role, np. na podstawie przynależności do grup AD/LDAP.

6.23. System PAM musi wykorzystywać szyfrowanie przy komunikacji pomiędzy wszystkimi komponentami.

6.24. System PAM musi zapewniać ochronę kryptograficzną wszystkich zapisanych danych.

6.25. System PAM musi posiadać log dla wszystkich zdarzeń systemowych.

6.26. System PAM musi zapewnić możliwość oddzielenia ról: użytkownika (operator lub administrator danego systemu docelowego), administratora (zarządzający dostępem do danej grupy kont systemów docelowych), audytora (uprawniony do monitoringu i przeglądania sesji i logów).

6.27. System PAM musi umożliwiać wskazanie kont użytkowników, które realizowały logowanie do stacji/serwera.

6.28. System PAM musi umożliwiać wyświetlenie aktywności danego konta ze szczególnym uwzględnieniem zmian hasła oraz aktywności sesji.

6.29. System PAM musi umożliwiać zdefiniowanie harmonogramu generowania raportów.

6.30. System PAM musi umożliwiać raportowanie wszystkich zmian wprowadzonych przez administratorów.

6.31. System PAM musi umożliwiać raportowanie wszystkich logowań do systemu.

6.32. System PAM musi umożliwiać ograniczenie dostępu do raportów dla wskazanej grupy użytkowników lub administratorów.

6.33. System PAM musi umożliwiać wysyłanie powiadomień o wygenerowanych raportach przez email.

6.34. System PAM musi zapewniać możliwość dwuskładnikowego uwierzytelniania.

6.35. System PAM musi mieć możliwość zmiany wartości hasła na systemie docelowym zgodnie z ustawioną polityką m.in.:

6.35.1. umożliwiać zdefiniowanie wymagań na: długość hasła, znaki w haśle (małe i duże litery, cyfry, znaki specjalne),

6.35.2. generować automatycznie hasła kont systemów docelowych w sposób pseudolosowy,

6.35.3. generować unikalne hasła dla konta systemów docelowych,

6.35.4. zapewnić ręczną zmianę hasła na wskazanych kontach systemów docelowych,

6.35.5. zapewnić zdefiniowanie minimum następujących częstości: brak zmiany hasła, codziennie o wskazanej godzinie, cotygodniowo we wskazanym dniu tygodnia, comiesięcznie we wskazanym dniu miesiąca itp.

6.36. System PAM musi umożliwiać zmianę haseł na pojedynczym systemie docelowym, grupie systemów docelowych oraz wszystkich systemach docelowych jednocześnie, zgodnie z przyjętym kryterium.

6.37. System PAM musi umożliwiać generowanie haseł jednokrotnego użycia dla przechowywanych w systemie kont uprzywilejowanych.

6.38. System PAM musi umożliwiać transparentne połączenie do systemu docelowego, bez konieczności podawania przez użytkownika hasła konta uprzywilejowanego.

6.39. System PAM musi umożliwiać ograniczanie dostępu do systemów docelowych oraz tworzenie białych i czarnych list poleceń wykonywanych.

6.40. System PAM musi umożliwiać nagrywanie sesji wraz z podglądem sesji aktywnej oraz możliwość jej przerwania.

6.41. Nagrywanie sesji nie może mieć żadnego wpływu na wydajność systemu docelowego.

6.42. System PAM musi wykorzystywać mechanizmy indeksowania nagrań umożliwiające szybkie przeszukiwanie nagranych i monitorowanych sesji pod kątem występowania wskazanych słów kluczowych.

6.43. System PAM musi umożliwiać odtworzenie zarejestrowanych nagrań sesji.

6.44. System PAM musi posiadać funkcje rejestrowania wszystkich znaków wpisywanych z klawiatury użytkownika.

6.45. Oprogramowanie dostarczone w ramach realizacji zamówienia musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski. W przypadku zaproponowania Rozwiązania z innego kanału dystrybucji Wykonawca musi przedstawić dokument potwierdzający, iż zaoferowany produkt posiada wsparcie producenta na terenie Polski.

6.46. System PAM musi umożliwić poprawę bezpieczeństwa informacji kontrolując dostęp do danych, systemów, sieci, aplikacji, nie może wpłynąć to na opóźnienia transmisji lub znaczną złożoność operacyjną.

6.47. System PAM musi umożliwić egzekwowanie zgodności z politykami instytucji i raportowania.

6.48. System PAM musi umożliwić bezproblemową integrację z istniejącymi systemami (Active Directory) i narzędziami bezpieczeństwa SIEM, SOAR.

6.49. System PAM musi umożliwić, zapewnić scentralizowany, oparty na rolach i skuteczny system zarządzania, który powinien umożliwić wdrażanie, przeglądanie i kontrolowanie całej aktywność za pomocą pojedynczego punktu dostępu.

6.50. System PAM musi być kompletny i pozwalać na uruchomienie minimum następujących funkcjonalności:

6.50.1. zarządzać kontami uprzywilejowanymi w ramach organizacji,

6.50.2. monitorować wykorzystanie kont uprzywilejowanych,

6.50.3. nagrywać i archiwizować sesje zdalne,

6.50.4. gwarantować skalowalność Rozwiązania w przypadku dodawania nowych zasobów oraz nowych usług,

6.51. System PAM musi umożliwić usługę pośredniczenia w dostępie do systemów i urządzeń dla użytkowników domenowych, rejestrując obsługiwane sesje, oraz obsługując minimum następujące protokoły: SSH, RDP, VNC, TELNET, HTTP/HTTPS.

6.52. System PAM w trakcie rejestracji sesji, w których pośredniczy, musi zapewniać minimum następujące funkcjonalności:

6.52.1. rejestracja sesji w formie zapisu wideo,

6.52.2. indeksowanie sesji,

6.52.3. możliwość przeglądania nagranych sesji,

6.52.4. możliwość wyszukiwania kontekstowego wśród nagranych sesji.

6.53. Zamawiający wymaga od Wykonawcy przeprowadzenia szkolenia z Systemu PAM dla co najmniej 2 administratorów, które odbędzie się w siedzibie Zamawiającego, a jeśli nie będzie takiej możliwości – za zgodą Zamawiającego – w innej lokalizacji na terenie Warszawy. Za organizację szkolenia poza siedzibą Zamawiającego odpowiedzialny jest Wykonawca.

6.54. Zamawiający wymaga, aby szkolenie zostało przeprowadzone w dni robocze (od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy) i trwało minimum 16 godzin (minimum 2 dni robocze).

6.55. Zamawiający wymaga, aby szkolenie składało się z dwóch części: teoretycznej oraz warsztatowej. Część warsztatowa musi mieć udział nie mniejszy niż 25% (minimum 4 godziny) czasu przewidzianego na całe szkolenie.

6.56. Zakres szkolenia musi obejmować:

6.56.1. Ogólną architekturę Systemu PAM

6.56.2. Bezpieczeństwo Systemu PAM

6.56.3. Konfiguracje kont systemów docelowych w Systemie PAM

6.56.4. Zarządzanie użytkownikami w Systemie PAM i integracja z innymi mechanizmami uwierzytelnienia i autoryzacji

6.56.5. Polityki złożoności hasła, harmonogram zmian haseł, walidacja poprawności zmiany hasła

6.56.6. Zarządzanie sesjami w Systemie PAM

6.56.7. Zarządzanie schematami wnioskowania i akceptacji dostępu hasła i/lub sesji w Systemie PAM

6.56.8. Audyt i raportowanie w Systemie PAM

6.56.9. Procedurę aktualizacji systemu PAM

6.56.10. Rozwiązywanie problemów (troubleshooting)

7. ROZWIĄZANIE IAM

7.1. Zakres zadania obejmuje dostawę, konfigurację, wdrożenie oraz uruchomienie centralnego systemu zarządzania tożsamościami i dostępami (IAM), realizującego procesy zarządzania dostępami użytkowników do systemów i zasobów Zamawiającego, obejmujące w szczególności obsługę cyklu życia dostępów, procesy wnioskowania i akceptacji, mechanizmy uwierzytelniania i autoryzacji oraz integrację z istniejącą infrastrukturą teleinformatyczną Zamawiającego.

7.2. Rozwiązanie musi być rozwiązaniem onprem z licencją perpetual, działające lokalnie w środowisku Zamawiającego.

7.3. Konsola administracyjna w formie w pełni funkcjonalnej aplikacji webowej, umożliwiająca kompleksowe zarządzanie systemem, w tym przeglądanie, edycję, modyfikację, usuwanie oraz analizę danych, a także wyposażona w wbudowane mechanizmy generowania i prezentacji raportów.

7.4. System musi zawierać moduł obsługi żądań zmian oraz moduł zarządzania uprawnieniami, obejmujący składanie i obsługę wniosków o uprawnienia (w tym nowe wnioski, zwroty, listy wniosków, wnioski BO oraz podgląd bieżących uprawnień), weryfikację uprawnień formalnych i faktycznych, definiowanie uprawnień i szablonów zatwierdzeń, obsługę powodów odrzucenia, kartoteki użytkowników, obsługę skryptów, mechanizmy nieobecności i zastępstw oraz panel pracownika.

7.5. System musi zapewniać automatyczną aktualizację konsoli administracyjnej, bazy danych, słowników, raportów oraz pozostałych komponentów za pośrednictwem bezpiecznego połączenia z serwerami aktualizacji producenta, realizowaną nie później niż w ciągu 24 godzin od udostępnienia nowej wersji. W przypadku braku dostępu do serwerów aktualizacji producenta system musi umożliwiać przeprowadzenie aktualizacji w trybie manualnym poprzez pobranie ze strony producenta jednej paczki aktualizacyjnej zawierającej kompletną aktualizację systemu.

7.6. System musi umożliwiać logowanie do konsoli administracyjnej zarówno z sieci lokalnych, jak i rozległych, zapewniać stabilną i niezakłóconą obsługę co najmniej 250 jednocześnie zalogowanych administratorów i użytkowników,

7.7. System musi umożliwiać instalację w środowiskach Windows oraz Linux,

7.8. System musi umożliwiać realizację procesów zgodnie z metodyką ITIL v4

7.9. System musi zapewniać integrację z systemem zarządzania zasobami IT.

7.10. System musi być możliwy do zainstalowania i uruchomienia na systemach operacyjnych Ubuntu (20.04 LTS, 22.04 LTS, 24.04 LTS), Debian (11, 12), Red Hat Enterprise Linux (8, 9), CentOS Stream (8, 9) oraz Windows Server (2019, 2022, 2025).

7.11. System musi umożliwiać cykliczny, realizowany zgodnie z harmonogramem lub na żądanie, import użytkowników oraz struktury organizacyjnej – w całości lub w zakresie wybranego kontenera – z usługi Microsoft Active Directory, przy czym importowana struktura organizacyjna musi być umieszczana w wskazanym miejscu struktury organizacyjnej zdefiniowanej w systemie.

7.12. Import obiektów z usługi Microsoft Active Directory musi być odporny na zmiany nazw obiektów, takich jak użytkownicy czy elementy struktury organizacyjnej, a w trakcie importu zmodyfikowane dane muszą być aktualizowane na podstawie jednoznacznego identyfikatora UUID.

7.13. System musi umożliwiać import danych z zewnętrznych źródeł, w tym z plików CSV i Excel oraz z baz danych Microsoft SQL Server, MySQL, PostgreSQL i Oracle.

7.14. System musi posiadać wbudowany interfejs importu danych w pełni konfigurowalny przez administratora, umożliwiający jednorazowe lub harmonogramowe pobieranie danych z dowolnych źródeł i o dowolnej strukturze z wykorzystaniem sterownika ODBC, w tym m.in. z plików tekstowych, XLS oraz XML, przy czym mechanizm importu musi umożliwiać aktualizację danych wcześniej zaimportowanych do systemu.

7.15. Moduł akcji i skryptów musi zapewniać obsługę skryptów realizujących nadawanie oraz odbieranie uprawnień, a także umożliwiać administratorowi definiowanie akcji poprzez określenie nazwy akcji, jej statusu, typu polecenia (Windows Command Line lub Windows PowerShell), treści polecenia oraz parametrów, w tym nazwy parametru i sposobu jego przekazywania, jako parametr skryptu lub zmienna środowiskowa.

7.16. Moduł musi umożliwiać aktualizację oprogramowania z pliku oraz zapewniać dostęp do informacji o aktualnie zainstalowanej wersji oprogramowania.

7.17. System musi zapewniać widok zestawienia użytkowników obejmujący wszystkich użytkowników systemu, w tym osoby logujące się do systemu, pracowników obszarów, wykonawców oraz serwisantów.

7.18. Moduł musi umożliwiać administratorowi przypisywanie użytkownikom odpowiednich grup uprawnień.

7.19. Moduł musi umożliwiać wielokrotny import użytkowników oraz struktury organizacyjnej z usługi Microsoft Active Directory, realizowany zgodnie z harmonogramem lub na żądanie, w całości lub w zakresie wybranego kontenera, przy czym importowana struktura organizacyjna musi być umieszczana w wskazanym miejscu struktury organizacyjnej zdefiniowanej w systemie.

7.20. Import obiektów z usługi Microsoft Active Directory musi być odporny na zmiany nazw obiektów, takich jak użytkownicy lub elementy struktury organizacyjnej, a zmodyfikowane dane muszą być aktualizowane w systemie na podstawie klucza UUID.

7.21. Moduł musi umożliwiać import danych z zewnętrznych źródeł, w tym z plików CSV i Excel oraz z baz danych Microsoft SQL Server, MySQL, PostgreSQL i Oracle.

7.22. Widok listy użytkowników musi być podzielony na odrębne widoki obejmujące wszystkich użytkowników, pracowników obszarów, pracowników wykonawców oraz pracowników grup wsparcia.

7.23. Widok listy użytkowników musi umożliwiać tworzenie indywidualnych filtrów widoku.

7.24. Moduł musi umożliwiać przypisywanie indywidualnych uprawnień wybranym użytkownikom.

7.25. Moduł musi umożliwiać przypisywanie uprawnień do odczytu, zapisu i usuwania w zakresie menu systemowego, raportów, wniosków o uprawnienia z uwzględnieniem jednostek organizacyjnych oraz akcji i skryptów.

7.26. Widok użytkownika musi prezentować historię działań użytkownika, zawierającą co najmniej datę zdarzenia, autora zmiany, element oraz jego wartość.

7.27. System musi zapewniać centralne zarządzanie tożsamościami użytkowników, w tym kontami pracowników, administratorów oraz kontami technicznymi, z wykorzystaniem danych pochodzących z systemów źródłowych.

7.28. System musi obsługiwać pełny cykl życia dostępów użytkownika do systemów i zasobów, obejmujący nadawanie, modyfikację, zawieszanie oraz odbieranie uprawnień.

7.29. System musi wspierać współpracę z mechanizmami uwierzytelniania jedno- i wieloskładnikowego (MFA), realizowanymi natywnie lub przez systemy katalogowe albo zewnętrznych dostawców tożsamości.

7.30. System musi umożliwiać autoryzację opartą o role (RBAC) oraz definiowanie uprawnień szczegółowych, w tym ról technicznych i ról biznesowych.

7.31. System musi integrować się z usługami katalogowymi, w tym LDAP, Active Directory lub rozwiązaniami równoważnymi, w zakresie synchronizacji danych tożsamości oraz uprawnień.

7.32. System musi wspierać procesy dostępu do systemów i aplikacji Zamawiającego, w tym współpracę z mechanizmami logowania jednokrotnego (SSO), realizowanymi przez systemy zarządzania tożsamością.

7.33. System musi umożliwiać integrację z aplikacjami lokalnymi (on-premise) oraz chmurowymi Zamawiającego w zakresie zarządzania dostępami i uprawnieniami.

7.34. System musi umożliwiać integrację z systemami zarządzania tożsamością, usługami katalogowymi oraz innymi komponentami infrastruktury bezpieczeństwa Zamawiającego.

7.35. System musi rejestrować zdarzenia związane z procesami uwierzytelniania, autoryzacji, nadawania i odbierania uprawnień oraz decyzjami akceptacyjnymi.

7.36. System musi umożliwiać eksport logów i danych audytowych do zewnętrznych systemów monitorowania i analizy bezpieczeństwa, w tym systemów klasy SIEM.

7.37. System musi umożliwiać delegowanie uprawnień administracyjnych oraz udział przełożonych lub właścicieli zasobów w procesach decyzyjnych dotyczących dostępów.

7.38. System musi zapewniać egzekwowanie polityk bezpieczeństwa w zakresie dostępu, w tym zasad dotyczących haseł, ról i uprawnień, zgodnych z dobrymi praktykami bezpieczeństwa.

7.39. System musi zapewniać szyfrowanie komunikacji pomiędzy wszystkimi komponentami rozwiązania.

7.40. System musi zapewniać bezpieczne przechowywanie danych związanych z tożsamościami i procesami uwierzytelniania.

7.41. System musi umożliwiać egzekwowanie zasady najmniejszych uprawnień w procesach nadawania i utrzymywania dostępów.

7.42. System musi umożliwiać realizację okresowych przeglądów oraz recertyfikacji uprawnień użytkowników, z udziałem przełożonych lub właścicieli zasobów oraz z rejestrowaniem wyników tych przeglądów.

7.43. System musi wspierać mechanizmy ograniczające ryzyko nadużyć w procesach uwierzytelniania i dostępu, w tym ochronę przed podstawowymi atakami na konta użytkowników.

7.44. Wykonawca przeprowadzi analizę środowiska Zamawiającego w zakresie tożsamości, dostępów oraz istniejących systemów źródłowych.

7.45. Wykonawca opracuje projekt wdrożenia systemu IAM, obejmujący architekturę rozwiązania, integracje oraz model ról i uprawnień.

7.46. Wykonawca zainstaluje i skonfiguruje system IAM w środowisku Zamawiającego.

7.47. Wykonawca zintegruje system IAM z systemami i aplikacjami wskazanymi przez Zamawiającego w zakresie zarządzania dostępami.

7.48. Wykonawca skonfiguruje role, polityki bezpieczeństwa, procesy wnioskowania i akceptacji oraz mechanizmy nadawania i odbierania uprawnień.

7.49. Wykonawca przeprowadzi testy poprawności działania systemu, w tym testy procesów nadawania, odbierania i recertyfikacji dostępów.

7.50. Wykonawca dostarczy dokumentację powdrożeniową obejmującą architekturę, konfigurację, integracje oraz procedury operacyjne.

7.51. Wykonawca przeprowadzi szkolenie administratorów systemu IAM.

7.52. Dopuszcza się rozwiązania równoważne, w tym rozwiązania typu open source, pod warunkiem spełnienia wszystkich wymagań funkcjonalnych i bezpieczeństwa.

8. ROZWIĄZANIE NGFW

8.1. Przedmiotem zamówienia jest zakup, dostawa oraz wdrożenie klastra HA urządzeń NGFW (Next Generation Firewall - NGFW) ze wsparciem gwarancyjnym, dalej określanym zamiennie jako „System NGFW" lub „System", „Rozwiązaniem".

8.2. Przedmiot zamówienia musi być fabrycznie nowy, nigdy wcześniej nie używany, pochodzący z legalnego kanału dystrybucyjnego, dopuszczony do obrotu na terytorium UE, spełniający normy CE.

8.3. Zamawiający wymaga, aby w ramach realizacji przedmiotu umowy wszystkie dostarczane urządzenia i pakiety oprogramowania były sprawdzone w praktyce rynkowej. Oznacza to, iż oprogramowanie (w tym także firmware urządzeń) realizujące wszystkie wymagane funkcje jak też same urządzenia muszą być oficjalnie dostępne na rynku od co najmniej 6 miesięcy przed terminem składania ofert.

8.4. Urządzenia i powiązane z nimi oprogramowanie systemowe muszą być objęte pełnym serwisem producenta (niedopuszczalne jest proponowanie oprogramowania lub urządzenia np. w wersji testowej, Beta itp.).

8.5. Zamawiający wymaga, aby zaoferowane urządzenia były dostępne i serwisowane przez producenta lub autoryzowanego przedstawiciela serwisowego producenta oraz nie będą przez producenta przewidziane do wycofania ze sprzedaży i

wsparcia (brak na listach End-of-Sale lub End-of-Life lub równoważne) – na dzień składania oferty.

8.6. Dodatkowe systemy zewnętrzne.

8.7. Zamawiający dopuszcza, aby całościowy system NGFW był zbudowany w oparciu o wymagane komponenty opisane w OPZ wraz z elementami dodatkowymi, których zastosowanie jest opcjonalne i dobrowolne. Decyzja o ich zastosowaniu leży w gestii Wykonawcy – jeżeli uzna on, iż dla osiągnięcia opisanych wymagań niezbędne są dodatkowe systemy zewnętrzne, to Zamawiający zezwala na ich zastosowanie pod warunkami opisanymi poniżej:

8.7.1. stosowanie dodatkowych systemów nie może dotyczyć funkcji ochronnych NGFW (np. wykrywania aplikacji, obsługi IPS, AV czy NAT);

8.7.2. stosowanie dodatkowych systemów nie może powodować ominięcia reguł bezpieczeństwa

8.7.3. Przykładowo stosowanie dodatkowych systemów jest dopuszczalne, gdy są one konieczne np. dla:

8.7.3.1. weryfikacji tożsamości użytkowników – system uwierzytelniania;

8.7.3.2. realizacji funkcji zarządzania firewallem i uprawnieniami administratorów;

8.7.3.3. zatwierdzania zmian w konfiguracji;

8.7.3.4. realizacji funkcji inspekcji ruchu SSL;

8.7.3.5. realizacji zaawansowanych funkcji ochrony wymagających pobierania danych z chmury Threat Intelligence producenta oferowanego rozwiązania.

8.8. Systemy wspomagające muszą być zaoferowane w pełnym wsparciem producenta co oznacza wymóg zaoferowania wszystkich pakietów serwisowych dostępnych dla danego rozwiązania,

8.9. W przypadku stosowania systemów wspomagających dla systemu firewall Zamawiający wymaga, aby system firewall oraz wszystkie systemy wspomagające były objęte jednolitym modelem wsparcia technicznego producenta, obejmującym jeden punkt przyjmowania zgłoszeń serwisowych, jeden spójny proces eskalacji incydentów i podatności bezpieczeństwa, jedno SLA dla całości rozwiązania oraz pełną odpowiedzialność producenta za poprawne, bezpieczne i wydajne działanie systemu firewall wraz z systemami wspomagającymi.

8.10. Stosowanie dodatkowych systemów jest możliwe tylko przy założeniu zapewnienia ich wysokiej dostępności. Oznacza to, że należy dostarczyć każdy taki system jako dedykowane rozwiązanie (urządzenie z dedykowanym dla niego oprogramowaniem serwisowane w całości przez jednego producenta); system

musi być dostarczony jako klaster niezawodnościowy – tzn. 2 identyczne urządzenia pracujące równolegle w modelu 1+1 lub N+1, wyposażone w redundantne zasilacze z możliwością ich wymiany „na gorąco" (hot-swap). Dodatkowe systemy muszą zostać zaoferowane w konfiguracji sprzętowej „analogicznej" dla konfiguracji urządzeń NGFW.

8.11. Zamawiający wymaga również, aby wszystkie dostarczane systemy wspomagające były sprawdzone w praktyce rynkowej i spełniały wymagania w tym obszarze analogicznie do firewalli, oznacza to, iż oprogramowanie systemowe realizujące wszystkie wymagane funkcje jak też samo urządzenie musiało być dostępne na rynku co najmniej 6 miesięcy przed terminem składania ofert.

8.12. Zapewnienie redundancji nie jest wymagane dla usług realizowanych z chmury Threat Intelligence producenta oferowanego rozwiązania.

8.13. Wymagania ogólne dla NGFW

8.14. 9,4 Gbps przepustowości Firewall/kontroli aplikacji;

8.15. 6 Gbps przepustowości Firewall/kontroli aplikacji/IPS/Antywirus/Antymalware;

8.16. 5,5 Gbps dla IPsec VPN;

8.17. 1 300 000 jednoczesnych sesji;

8.18. 130 000 nowych połączeń na sekundę;

8.19. 1 500 tuneli SSL VPN Remote Access z wykorzystaniem klienta VPN;

8.20. 10 wirtualnych routerów posiadających odrębne tabele routingu;

8.21. Możliwość licencyjnej rozbudowy do przynajmniej 5 wirtualnych instancji firewall (określanych jako kontekst/domena/system). Każda z instancji musi pozwalać na konfigurację niezależnych oraz odrębnych od innych instancji – polityk bezpieczeństwa (co najmniej dla IPS, AV i współpracy z sandboxem), tablicy routingu oraz realizacji zdalnego dostępu.

8.22. 100 stref bezpieczeństwa;

8.23. Lokalna przestrzeń pamięci co najmniej o pojemności 200GB przeznaczona na system operacyjny oraz dzienniki zdarzeń (logi)

8.24. Cechy urządzenia – minimalna wymagana ilość interfejsów, zasilanie:

8.24.1. Wysokość maksymalnie 1U wraz z zestawem montażowym do szafy RACK 19";

8.24.2. dwa redundantne zasilacze AC 230V z kompletami kabli;

8.24.3. 10 portów GigabitEthernet RJ45

8.24.4. 8 portów 10 GigabitEthernet SFP+ obsługujących moduły optyczne SR oraz LR

8.24.5. 2 porty 1 GigabitEthernet SFP

8.24.6. 1 port 1-GigabitEthernet RJ45 lub 10-GigabitEthernet RJ45 wyłącznie do celów zarządzania (dopuszcza się uzyskanie tego portu poprzez zastosowanie portów SFP / SFP+ obsadzonych modułami z RJ45, natomiast nie dopuszcza się wykorzystania do tego celu portów wymienionych w pozostałych punktach)

8.25. Urządzenie musi posiadać dedykowany/wydzielony port 2,5G lub 5G lub 10-GigabitEthernet lub szybszy dla celów połączenia urządzeń w klaster (high availability). Port ten musi być traktowany jako dodatkowy względem wymaganych przez Zamawiającego. Nie dopuszcza się wykorzystania do celu klastrowania portów opisanych w podstawowych wymaganiach.

8.26. Wymagania funkcjonalne dla rozwiązań NGFW: Wszystkie wymienione poniżej funkcje muszą być dostępne i realizowane przez firewall jednocześnie. Nie jest dopuszczalne, aby realizacja jakiejkolwiek funkcjonalności powodowała konieczność przełączenia urządzenia w inny tryb pracy ograniczający lub uniemożliwiający skorzystanie z innej wymaganej funkcji. Podobnie uruchomienie jakiekolwiek opisanej funkcji nie może spowodować wyłączenie lub ograniczenie działania innej funkcji wymaganej przez Zamawiającego. Jednocześnie Zamawiający zastrzega sobie prawo do wezwania Wykonawcy do złożenia wyjaśnień oraz prezentacji działania zaoferowanego urządzenia w przypadku powzięcia wątpliwości w tym zakresie.

8.27. Funkcjonalności NGFW

8.28. Rozpoznawanie aplikacji bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji nie może wymagać podania w konfiguracji NGFW numeru lub zakresu portów, na których jest ona dokonywana. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. NFGW musi wykrywać co najmniej 4000 aplikacji predefiniowanych przez Producenta.

8.29. Transparentne ustalenie tożsamości użytkowników

8.30. Realizowanie funkcjonalności na bazie profili przypisywanych na poziomie reguł bezpieczeństwa:

8.30.1. Intrusion Prevention System (IPS),

8.30.2. Antywirus (AV),

8.30.3. Anty-Spyware / Anty-Malware,

8.30.4. Kategoryzacja URL i filtracja URL

8.30.5. ochrona DNS,

8.30.6. sandboxingu do analizy złośliwego oprogramowania realizowaną w formie lokalnej lub chmurowej, zintegrowaną z systemem NGFW w sposób natywny, zapewniającą jednolity model aktualizacji, detekcji, eskalacji incydentów oraz wsparcia technicznego, a także pełną odpowiedzialność producenta za skuteczność działania sandboxingu w ramach całego rozwiązania NGFW.

8.31. Budowanie reguł bezpieczeństwa opierające się na podstawowych selektorach takich jak: strefy bezpieczeństwa źródłowe/docelowe, adresy IP źródłowe/docelowe, aplikacje (w warstwie L7 OSI), użytkownicy/grupy z Active Directory

8.32. System musi zapewniać możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji

8.33. Silniki detekcyjne i ochronne NGFW

8.34. Bazy sygnatur IPS, AV, Anty-Spyware (lub innego silnika, jeżeli obejmuje on ochronę przed Spyware) muszą być przechowywane na NGFW, regularnie aktualizowane w sposób automatyczny.

8.35. Aktualizacje sygnatur AV muszą odbywać się nie rzadziej niż raz na 24 godziny.

8.36. Musi być zapewniona możliwość tworzenia własnych sygnatur IPS bez wykorzystania zewnętrznych narzędzi (dopuszcza się tworzenie sygnatur z wykorzystaniem dostarczanego systemu zarządzania) czy wsparcia producenta.

8.37. Urządzenie NGFW musi umożliwiać elastyczną konfigurację AV i IPS w szczególności wyłączenia części sygnatur dla określonych grup użytkowników i/lub aplikacji. Urządzenie musi umożliwiać uruchomienie funkcji IPS i AV z dokładnością do reguły bezpieczeństwa. Nie dopuszcza się by IPS i AV był uruchamiany dla całego urządzenia lub dla interfejsu fizycznego albo logicznego, gdzie administrator nie ma możliwości konfiguracji jaka część ruchu będzie podlegała inspekcji i w jakim zakresie.

8.38. Wykrywanie aktywności sieci typu Botnet.

8.39. Możliwość blokowania transmisji plików, co najmniej następujących typów: bat, cab, pliki MS Office, rar, zip, exe, gzip, hta, pdf, tar, tif. Rozpoznawanie pliku na podstawie nagłówka i typu MIME.

8.40. Funkcja filtrowania ruchu URL w oparciu o automatycznie aktualizowaną bazę kategorii stron WWW i bazę reputacji tych stron.

8.41. Ocena strony musi obejmować określenie jej kategorii (np. finanse, zakupy, sport, itp)

8.42. Ocena strony musi obejmować określenie ryzyka do niej przypisanego (co najmniej wysokie, średnie, niskie).

8.43. Musi być zapewniona możliwość tworzenia własnych list stron (whitelist oraz blacklist) bez wykorzystania zewnętrznych narzędzi czy wsparcia producenta z możliwością konfiguracji, gdzie własne listy będą miały wyższy priorytet niż klasyfikacja na bazie kategorii dostarczanych przez producenta.

8.44. Funkcja ochrony przed zagrożeniami Zero Day oraz zapewnienie współpracy z sandboxem.

8.45. musi umożliwiać przesyłanie do systemu sandbox plików zdefiniowanych przez administratora, co najmniej w formatach: exe, dll, java, dokumenty MS Office oraz pdf, przy czym sandbox musi być funkcjonalnie i operacyjnie zintegrowany z systemem NGFW w sposób natywny, objęty tym samym modelem wsparcia technicznego, cyklem aktualizacji oraz odpowiedzialnością producenta za poprawne i skuteczne działanie tej funkcjonalności w ramach całego rozwiązania NGFW. Zamawiający dopuszcza by odbywało się to poprzez dedykowany mechanizm wbudowany w urządzenie lub przez jeden z wymaganych silników detekcyjnych przy czym funkcja ta musi mieć możliwość wskazania/wykluczania z filtrowania specyficznego ruchu sieciowego na podstawie zarówno kierunku transmisji (ruch wchodzący/wychodzący ze wskazanej strefy bezpieczeństwa), adresu źródłowego IP jak i adresu docelowego IP jak i rozpoznania aplikacji lub zdefiniowanych serwisów, np. poprzez numer portu, protokół transportowy

8.46. możliwość aktualizacji systemu firewall o nowo wykryte (w Sandbox) zagrożenia.

8.47. administrator musi posiadać dostęp do raportów z sandboxa dotyczących plików wysyłanych przez urządzenia, jak również posiadać możliwość manualnego wysłania pliku (np. poprzez upload przez stronę www) do sandboxa.

8.48. dopuszcza się zarówno realizację sandboxa w postaci chmury producenta jak i rozwiązania lokalnego. W tym drugim przypadku wymagane jest dostarczenie opisu współpracy proponowanej integracji z dostarczanym firewallem. W przypadku rozwiązania chmurowego analiza plików musi odbywać się na terenie Polski.

8.49. Bez względu na użyte rozwiązanie, wymaga się wydajności zapewniającej jednoczesną analizę minimum 20 plików/próbek w tzw. VM Sandboxing (rozumiana jako realizacja funkcjonalności sandbox polegająca na wykorzystaniu instancji maszyn wirtualnych z określonymi systemami operacyjnymi i zestawem zainstalowanych aplikacji do zdetonowania/uruchomienia, a następnie analizy

podejrzanego pliku pod kątem jego potencjalnie negatywnego wpływu na komputery klienckie lub serwery).

8.50. Jednoczesna analiza 20 próbek/plików musi być zapewniona bez względu na to czy pliki te będą wysyłane automatycznie przez firewall czy manualnie przez administratora czy też będzie to mieszana grupa plików pochodząca zarówno bezpośrednio z firewalla, jak też od administratorów 14) Podstawowa ochrona DNS co najmniej w zakresie:

8.50.1. wykrywanie zapytań do domen złośliwych.

8.50.2. możliwość skonfigurowania fałszowania odpowiedzi na zapytania DNS zaklasyfikowane jako niebezpieczne (tzw. DNS sinkholing)

8.51. Deszyfracja ruchu

8.52. Rozwiązanie musi posiadać funkcjonalność deszyfracji wychodzących połączeń SSL/TLS na wszystkich portach, wskazanych w polityce deszyfracji oraz deszyfracji wychodzących połączeń typu STARTTLS (Wymagane wsparcie co najmniej dla TLSv1.1, TLSv1.2 i TLSv1.3).

8.53. Zaawansowana ochrona DNS w trybie rzeczywistym.

8.54. Dla każdego zapytania DNS przetwarzanego przez firewall musi zostać wykonana jego pełna analiza. Nie dopuszcza rozwiązania funkcjonującego tylko w oparciu o weryfikację zapytania DNS w bazie danych rozpoznanych zagrożeń danego producenta, ponieważ taka metoda nie zapewnia ochrony tzw. pacjenta zero, który wykonuje zapytanie DNS o unikalną nazwę domenową, która jeszcze nie znajduje się w bazie. Analiza każdego zapytania musi obejmować co najmniej zakres detekcji jak poniżej:

8.54.1. wykrywanie zapytań do domen złośliwych

8.54.2. możliwość skonfigurowania fałszowania odpowiedzi na zapytania DNS zaklasyfikowane jako niebezpieczne (tzw. DNS sinkholing)

8.54.3. wykrywanie domen generowanych dynamicznie przez złośliwe oprogramowanie w celu uniknięcia wykrycia kanałów komunikacyjnych (tzw. domeny DGA)

8.54.4. wykrywanie domen fast flux

8.54.5. wykrywanie domen dynamicznych Dynamic DNS

8.54.6. wykrywanie domen nowo rejestrowanych – Newly-registered-domain

8.54.7. wykrywanie domen strategically-aged-domain

8.54.8. wykrywanie domen stockpiled

8.54.9. wykrywanie nadużyć protokołu DNS w celu infiltracji i eksfiltracji danych

8.54.10. wykrywanie ataków DNS Tunneling, w tym ultra-slow DNS Tunneling

8.54.11. wykrywanie ataków na rekordy DNS, w tym CNAME cloaking, Wildcard DNS i Dangling DNS

8.54.12. wykrywanie ataków na protokół DNS

8.55. Obsługa VPN oraz funkcji sieciowych

8.56. Zestawianie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site.

8.57. Zestawianie tuneli SSL VPN w konfiguracji remote-access-VPN.

8.58. Wymagane jest zestawienie tuneli z wykorzystaniem klienta VPN dostarczanego przez producenta urządzenia NGFW- obsługa co najmniej 1500 tuneli/użytkowników.

8.59. Oprogramowanie klienta VPN musi być dostępne co najmniej dla Windows, MacOS, Linux, Android i iOS.

8.60. Oprogramowanie klienta VPN dla Windows i MacOS musi posiadać możliwość weryfikacji kondycji bezpieczeństwa stacji końcowej co najmniej w zakresie sprawdzenia:

8.61. czy zainstalowano oprogramowanie antywirusowe i czy posiada ono aktualne sygnatury,

8.62. czy włączony jest osobisty firewall,

8.63. czy włączone jest szyfrowanie dysku.

8.64. Oprogramowanie klienta VPN musi być objęte wsparciem producenta w okresie zgodnym z długością wsparcia firewalla.

8.65. Wymagane jest zestawienie tuneli bez konieczności zastosowania klienta VPN – tzw. praca w trybie

8.66. Clientless VPN – dla co najmniej 200 tuneli

8.67. Jeżeli oprogramowanie klienta jest dodatkowo licencjonowane przez producenta wówczas należy przewidzieć je dla 2000 użytkowników/urządzeń oraz zapewnić możliwość licencyjnej rozbudowy do 3000.

8.68. oprogramowanie klienta musi mieć możliwość zdalnej kontroli, minimum sprawdzenie wersji oraz zdalną instalację aktualizacji.

8.69. Obsługa protokołów routingu: OSPFv2 i OSPFv3, BGP4; 19) Obsługa 4094 VLAN zgodnych z 802.1q.

8.70. Obsługa tworzenia subinterfejsów na interfejsach pracujących w L2 i L3.

8.71. Obsługa stref bezpieczeństwa symbolizujących np. WAN, LAN, DMZ, interfejsy fizyczne, subinterfejsy L2 i L3 – jako nazwane strefy, na bazie których można budować polityki bezpieczeństwa przy regulacji ruchu pomiędzy strefami.

8.72. Translacja adresów IP (NAT) zarówno statyczna jak i dynamiczna. Reguły dotyczące NAT muszą być odrębne od reguł definiujących polityki bezpieczeństwa tak, aby reguły dotyczące translacji nie powodowały w żaden sposób zależności od konfiguracji tych polityk.

8.73. Zarządzanie pasmem sieci (QoS) w zakresie ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. Przydzielanie takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego.

8.74. Inspekcja szyfrowanej komunikacji SSH (Secure Shell) w celu wykrywania tunelowania innych protokołów w ramach usługi SSH).

8.75. Uwierzytelnienie i ustalanie tożsamości użytkowników

8.76. Transparentne ustalenie tożsamości w oparciu o:

8.76.1. integrację z kontrolerem domeny Active Directory;

8.76.2. integrację z serwerami LDAP;

8.76.3. integrację z serwerami terminalowymi;

8.76.4. integrację bazującą na informacji z logów SYSLOG lub RADIUS pozwalającej na uwierzytelnienie użytkowników korzystających z systemów UNIX;

8.77. Firewall musi posiadać możliwość wymuszenia w procesie uwierzytelniania użytkownika podania przez niego drugiego czynnika uwierzytelniającego (tzw. MFA) w celu ochrony kluczowych systemów przed kradzieżą poświadczeń.

8.78. Uwierzytelnianie administratorów NGFW za pomocą:

8.78.1. bazy lokalnej;

8.78.2. zewnętrznej usługi katalogowej dostępnej po LDAPS;

8.78.3. RADIUS lub TACACS+.

8.79. Zarządzenie urządzeniami NGFW

8.80. Monitorowanie oraz podstawowe zarządzanie muszą być możliwe z linii poleceń (CLI) oraz przez Interfejs graficzny (GUI) realizowany przez przeglądarkę lub dedykowanego klienta instalowanego na stacji roboczej administratora – bez konieczności korzystania z centralnych narzędzi zarządzania.

8.81. Eksportowanie logów do zewnętrznych serwerów zgodnych z protokołem Syslog.

8.82. Praca na NGFW odbywa się na konfiguracji kandydackiej, a nie aktywnej. Zmiany w całości konfiguracji aktywnej odbywają się poprzez zatwierdzanie zmian (ang. Commit). Przed zatwierdzaniem zmian musi być możliwość przejrzenia zmian, które zostały wykonane na konfiguracji kandydackiej. Musi istnieć możliwość porównania zmian (m.in. polityk, konfiguracji interfejsów, routingu itp.), ze wcześniejszymi wersjami konfiguracji. Funkcja ta musi być dostępna z CLI i z GUI.

8.83. Interpretacja parametrów wydajnościowych NGFW

8.84. Interpretacja parametrów wydajnościowych dla Firewall/kontroli aplikacji - rozwiązanie pozwoli na:

8.84.1. wykrycie aplikacji,

8.84.2. przydzielenie do niej polityki bezpieczeństwa w tym przypisanie uprawnień użytkownikom do korzystania z określonych aplikacji sieciowych.

8.85. Interpretacja parametrów wydajnościowych dla Firewall/kontroli aplikacji/IPS/Antywirus/Antymalware - rozwiązanie pozwoli na:

8.85.1. wykrycie aplikacji,

8.85.2. przydzielenie do niej polityki bezpieczeństwa obejmującej przypisanie uprawnień użytkownikom do korzystania z określonych aplikacji sieciowych,

8.85.3. inspekcje IPS całego ruchu,

8.85.4. inspekcję antywirusową całego ruchu,

8.85.5. inspekcję antymalware/AntySpyware całego ruchu,

8.85.6. przesyłanie plików do sandboxa lokalnego i/lub chmurowego,

8.85.7. przechwytywanie i blokowanie plików określonego typu.

8.86. Logowanie zdarzeń

8.87. Scenariusz ten musi być realizowany z włączonym pełnym zakresem ochrony tj. z włączonymi wszystkimi dostępnymi dla rozwiązania sygnaturami IPS oraz z wszystkimi funkcjami dostępnymi w urządzeniu dla silników antywirus i antyspyware/antymalware. Inspekcjom bezpieczeństwa musi podlegać cały ruch – sprawdzeniu musi podlegać każdy bajt danych przesyłany przez urządzenie. Zamawiający wymaga, aby podana została przepustowość urządzenia dla pełnego zakresu ochrony oferowanego przez urządzenie – jeżeli urządzenie pozwala na pracę w wielu trybach to należy podać przepustowość dla trybu z największą liczbą dostępnych inspekcji dla silników IPS, antywirus, antymalware/antyspyware.

8.88. Wymagania licencyjne

8.89. Całość rozwiązania będzie pochodziła od jednego producenta.

8.90. W przypadku, kiedy jakakolwiek funkcjonalność lub parametr ilościowy wymagają licencji, Zamawiający wymaga ich dostarczenia w celu zapewnienia pełni wymaganych właściwości przez okres 36 miesięcy.

8.91. Dla systemu firewall należy dostarczyć usługi abonamentowe (subskrypcje) obejmujące aktualizacje sygnatur dla następujących funkcji:

8.91.1. Aktualizacje bazy aplikacji;

8.91.2. Aktualizacje baz sygnatur IPS;

8.91.3. Aktualizacje baz sygnatur AV;

8.91.4. Dostęp do bazy URL zapewniającej informacje o kategoryzacji strony i powiązanym z nią poziomie ryzyka

8.91.5. Możliwość współpracy z systemem sandbox

8.91.6. Aktualizacji baz dla ochrony DNS;

8.91.7. realizację sieci VPN w trybie site-to-site i client-to-site (wraz z oprogramowaniem klienta VPN);

8.92. Wymagania wdrożeniowe

8.93. W ramach wdrożenia Wykonawca przed przekazaniem Zamawiającemu urządzeń wstępnie je przygotuje, tak aby pracowały w trybie klastra HA na brzegu sieci.

8.94. Wykonawca przeniesie wszystkie dotychczas stosowane polityki na urządzeniach Palo Alto Networks PA-440 użytkowanych przez Zamawiającego.

8.95. Obecnie stosowane urządzenia PA-440 zostaną przekonfigurowane przez Wykonawcę do działania w innym segmencie sieci Zamawiającego.

8.96. Zamawiający przewiduje w ramach wdrożenia utworzenie użytkowników administratorów Zamawiającego (do 5 osób), integrację z Active Directory, która umożliwi identyfikację ruchu sieciowego generowanego przez użytkowników AD, dodatkowo uruchomienie bramy dla VPN dla pracowników korzystających z pracy zdalnej z wykorzystaniem MFA, również z wykorzystaniem urządzeń mobilnych.

8.97. Zamawiający przewiduje przy wdrożeniu utworzenie ok. 400 reguł (polis) zabezpieczeń ruchu sieciowego oraz utworzenie ok. 18 stref (zone).

9. ROZWIĄZANIE DO ZARZĄDZANIA I ORKIESTRACJI

9.1. Przedmiotem zamówienia jest dostawa i wdrożenia oprogramowania do centralnego zarządzania oraz logowania i raportowania, przystosowanego do współpracy z systemem NGFW typu Network Security Policy Management & Orchestration.

9.2. System musi umożliwiać centralne zarządzanie, logowanie i raportowanie zdarzeń bezpieczeństwa dla oferowanych urządzeń NGFW.

9.3. Zamawiający użytkuje obecnie urządzenia Palo Alto Networks PA-440 i oczekuje, aby NGFW był możliwy do zarządzania w pełnym zakresie funkcjonalnym wraz z ww. urządzeniami za pomocą jednej konsoli zarządzającej w formie oprogramowania instalowanego na maszynie wirtualnej działającej w infrastrukturze Zamawiającego.

9.4. System musi rejestrować zdarzenia ze wszystkich modułów sieciowych i bezpieczeństwa zarządzanych firewalli.

9.5. System musi być dostarczony w postaci maszyny wirtualnej (virtual appliance) działającej w środowisku VMware ESXi lub Microsoft Hyper-V lub KVM (Linux).

9.6. System musi być rozwiązaniem natywnie zintegrowanym z oferowanymi urządzeniami NGFW, objętym tym samym modelem wsparcia technicznego, cyklem aktualizacji, jednym SLA oraz pełną odpowiedzialnością producenta za poprawne, bezpieczne i wydajne działanie systemu zarządzania oraz zarządzanych urządzeń NGFW w ramach jednego rozwiązania

9.7. System musi umożliwiać zarządzanie łącznie co najmniej 10 fizycznymi urządzeniami NGFW i co najmniej 50 firewallami wirtualnymi rozumianymi jako wirtualny firewalli/system/domena/kontekst.

9.8. Zamawiający dopuszcza możliwość zastąpienia WebGUI, wyłącznie w momencie, gdy:

9.8.1. zapewni wszystkie niezbędne licencje i komponenty, przy czym licencje te muszą być nieodwołalne i nie mogą powodować powstania po stronie zamawiającego obowiązku wnoszenia dodatkowych opłat, wynagrodzenia, honorariów etc., Licencje muszą być zapewnione co najmniej na czas trwania wsparcia technicznego zaoferowanego przez dostawcę,

9.8.2. rozwiązanie to będzie umożliwiało dostęp dla co najmniej 10 osób jednocześnie,

9.8.3. w przypadku konieczności łączenia się do komponentu zarządczego za pośrednictwem oprogramowania nie działającego na systemach operacyjnych z rodziny GNU/LINUX wykonawca musi dostarczyć licencję na system obsługujący to oprogramowanie wraz z licencją i oprogramowaniem umożliwiającym pracę zdalną na tym systemie co najmniej 10 administratorom, umożliwiając im równoległe zarządzanie Systemem, z możliwością niezależnej pracy. Licencje muszą być zapewnione co najmniej na czas trwania wsparcia technicznego zaoferowanego przez dostawcę,

9.8.4. gwarancja i wsparcie na rozwiązanie zastępujące WebGUI musi trwać przez cały okres gwarancyjny Systemu,

9.9. System musi umożliwiać zdefiniowanie co najmniej 10 lokalnych kont administracyjnych z możliwością określenia praw dostępu.

9.10. System musi dawać możliwość pełnej konfiguracji urządzeń, ze wszystkimi ich funkcjami składowymi.

9.11. Zarządza obiektami używanymi przez wszystkie firewalle w jednym, centralnym repozytorium.

9.12. Zapewnia dystrybucję i zdalną instalację nowych sygnatur oraz wersji oprogramowania systemowego.

9.13. Przechowuje różne wersje konfiguracji zarządzanych NGFW.

9.14. Pozwala na tworzenie raportów na podstawie zbudowanych grup NGFW.

9.15. System musi dawać możliwość zbierania logów (dzienników zdarzeń) z zarządzanych urządzeń, ze wszystkimi ich funkcjami składowymi.

9.16. Zbiera logi zdarzeń z oferowanych NGFW co najmniej o ruchu sieciowym, użytkownikach, aplikacjach, zagrożeniach i filtrowanych stronach WWW.

9.17. Umożliwia korelację logów zdarzeń z zarządzanych firewalli.

9.18. Umożliwia tworzenie, zapisywanie i ponowne wykorzystywanie filtrów służących do wyszukiwania informacji w logach zebranych z zarządzanych NGFW.

9.19. Pozwala na tworzenie raportów na podstawie gromadzonych w logach informacji.

9.20. Pozwala na zapisywanie stworzonych raportów, uruchamianie ich w sposób manualny lub automatyczny w określonych przedziałach czasu oraz eksport do formatu tekstowego.

9.21. System musi być w stanie zarządzać wersjami baz sygnatur na urządzeniach oraz zdalnymi uaktualnieniami.

9.22. Graficzny interfejs Systemu (Web GUI) musi być dostępny po protokole HTTPS przez przeglądarkę WWW w HTML5, bez wykorzystania technologii Java czy Flash.

9.23. Komponent zarządczy powinien pozwalać na obsługę co najmniej:

9.23.1. Logi użytkowników

9.23.2. 5000 logów na sekundę

9.23.3. Przyrost dzienny nie mniej niż 150GB

9.23.4. 16TB użytecznej przestrzeni dyskowej

9.23.5. Retencja danych nie mniej niż 100 dni

9.23.6. Logi Administracyjne

9.23.7. 100 logów na sekundę

9.23.8. Przyrost dzienny nie mniej niż 2GB

9.23.9. 4TB użytecznej przestrzeni dyskowej

9.23.10. Logi administracyjne przechowywane przez okres minimum 3 lat.

9.24. System może zostać zbudowany w oparciu o dwie osobne maszyny wirtualne pochodzące od tego samego producenta (i jednocześnie producenta Systemu), współpracujące pomiędzy sobą, gdzie:

9.24.1. Jedna maszyna jest dedykowana dla centralnego logowania zdarzeń i raportowania, obsługująca logi inspekcyjne

9.24.2. Druga maszyna jest dedykowana dla zarządzania urządzeniami, kontami administratorów i obsługująca logi administracyjne

9.25. Obie maszyny (jako każda z osobna) muszą spełniać wymagania w zakresie:

9.25.1. liczby zarządzanych firewalli

9.25.2. liczby docelowo zarządzanych firewalli

9.25.3. możliwości pracy autonomicznej w szczególności nie dopuszcza się, aby spełnienie wymagań odbywało się przez współdzielenie zasobów przez poszczególne maszyny (awaria pojedynczej maszyny nie może wpływać na drugą). Dlatego też wymagane jest spełnienie wymagań do obu maszyn niezależnie. Do oferty należy dołączyć dodatkową dokumentację potwierdzającą spełnienie tych wymagań.

9.26. System może być alternatywnie dostarczony w postaci sprzętowej - w postaci dedykowanego urządzenia. W przypadku, jeżeli System będzie oferowany w postaci sprzętowej muszą zostać spełnione następujące warunki:

9.27. System musi być dostarczony w postaci dedykowanych urządzeń - jako dedykowane rozwiązanie (urządzenie z dedykowanym dla niego oprogramowaniem serwisowane w całości przez jednego producenta).

9.28. Każdy z komponentów systemu musi posiadać minimum 2 interfejsy 10GE;

9.29. Użyteczna przestrzeń dyskowa zapewniana przez sprzętowy komponent zarządczy musi zostać zrealizowana w RAID-1;

9.30. Każdy z komponentów systemu musi posiadać redundantne zasilacze AC

9.31. W przypadku gdy komponent zarządczy będzie składał się z dwóch komponentów oba te komponenty muszą zostać dostarczone w postaci sprzętowej oraz spełniać wszystkie opisane wcześniej wymagania dla systemu zarządzania składającego się z dwóch komponentów

10. ROZWIĄZANIE SIEM

10.1. Przedmiotem zamówienia jest dostawa i wdrożenie w pełnym zakresie funkcjonalnym systemu typu SIEM wraz z niezbędną infrastrukturą oraz przeszkoleniem personelu Zamawiającego.

10.2. Wykonawca wdroży rozwiązanie klasy SIEM obejmujące centralizację logów, korelację zdarzeń, reguły detekcji, alertowanie, raportowanie oraz wsparcie reakcji na incydenty, w środowisku Zamawiającego.

10.3. Wykonawca zapewni pełną gotowość produkcyjną: stabilne zbieranie logów, mierzalne pokrycie źródeł, działające przypadki użycia, procedury operacyjne oraz dokumentację utrzymaniową.

10.4. Wykonawca wykona analizę stanu obecnego (inwentaryzacja źródeł logów, wolumen, formaty, retencja, wymagania prawne/organizacyjne, uprawnienia, sieć, dostępność).

10.5. Wykonawca opracuje projekt architektury SIEM co najmniej w zakresie:

10.5.1. topologii (kolektory/forwardery, transport, warstwa korelacji, warstwa składowania),

10.5.2. segmentacji i zasad dostępu administracyjnego,

10.5.3. modelu danych/logów (normalizacja, mapowanie pól), czasu (NTP), tożsamości (konta, role),

10.5.4. wymagań zasobowych (CPU/RAM/dysk/IOPS), licencjonowania (EPS/GB/dzień) oraz rozbudowy

10.6. Wykonawca przygotuje środowiska: testowe oraz produkcyjne (minimum), z rozdzieleniem uprawnień i danymi testowymi.

10.7. Wykonawca zapewni synchronizację czasu dla wszystkich komponentów (NTP) oraz ujednolici strefy czasowe w logach.

10.8. System musi zapewniać skalowalne składowanie i wyszukiwanie danych w architekturze umożliwiającej obsługę wolumenu wskazanego w OPZ, z możliwością rozbudowy horyzontalnej

10.9. Rozwiązanie musi być rozwiązaniem on-prem, działające lokalnie w środowisku Zamawiającego.

10.10. System musi mieć możliwość centralnego zbierania i zarządzania logami.

10.11. System działać w trybie zbliżonym do rzeczywistego.

10.12. System musi mieć możliwość działania jako niezależne instancje zainstalowane w oddziałach Zamawiającego wraz z możliwość centralnego dostępu.

10.13. Instancje systemu muszą mieć możliwość działania w przypadku odłączenia scentralizowanego dostępu.

10.14. System musi zapewniać efektywną obsługę co najmniej **3000 EPS lub 100 GB** danych dziennie.

10.15. System musi zapewniać retencję danych w okresie minimum 365 dni.

10.16. Oferowana licencja nie może ograniczać ilości zarejestrowanych lub jednoczesnych użytkowników systemu.

10.17. System musi umożliwiać rozbudowę bez potrzeby wyłączania lub restartu środowiska.

10.18. Architektura Rozwiązania musi umożliwiać rozdzielenie ról systemu pomiędzy osobne komponenty (serwery/maszyny wirtualne). Należy przewidzieć rozdzielenie przynajmniej 3 typów ról: Agregacja, Prezentacja, Retencja.

10.19. Dołączenie nowego węzła przetwarzania, prezentacji lub przechowywania pozwalającego na skalowanie wydajności. Rozszerzenie takie powinno odbywać się bez konieczności restartu działającego systemu.

10.20. System musi zapewniać wysoką dostępność na poziomie Agregacji i Retencji

10.21. System musi zapewniać buforowanie agregowanych danych na okres minimum 2 dni w przypadku awarii któregokolwiek z komponentów oraz ich uzupełnienie w po przywróceniu pełnej sprawności systemu.

10.22. Komunikacja pomiędzy wszystkim komponentami musi być szyfrowana z wykorzystaniem protokołu TLS w wersji minimum 1.2.

10.23. Szyfrowanie komunikacji z przeglądarką internetową użytkownika musi wykorzystywać protokołów TLS w wersji minimum 1.3.

10.24. System musi posiadać interfejs graficzny dostępny z poziomu przeglądarki internetowej min. Firefox, Chrome, Edge.

10.25. Interfejs musi posiadać angielską lub polską wersję językową.

10.26. System powinien być tworzony zgodnie z zaleceniami standardu OWASP Testing Guide, a w szczególności OWASP - TOP 10 (Open Web Application Security Project). Projektowany System powinna spełniać wymagania standardu OWASP ASVS (Application Security Verification Standard) w wersji 4.0 co najmniej na poziomie pierwszym (L1).

10.27. Dostęp do systemu musi być zabezpieczany hasłem lub certyfikatem.

10.28. Autoryzacja do systemu musi być zintegrowana z:

10.28.1. Microsoft AD,

10.28.2. LDAP,

10.28.3. Radius

10.29. Hasła typu Windows AD bind muszą być przechowywane w postaci zaszyfrowanej.

10.30. System musi wspierać mechanizm logowania typu Single Sign On.

10.31. System musi umożliwiać zarządzanie czasem automatycznego wygasania sesji użytkowników.

10.32. System musi posiadać dedykowany widok zarządzania użytkownikami i rolami.

10.33. System powinien umożliwiać zarządzenie uprawnieniami do modyfikacji wytworzonych w systemie obiektów tj. wyszukiwania, wizualizacje, dashboardy. Dla utworzonych ról musi istnieć możliwość przypisania wspomnianych obiektów w podziale na dostęp typu „read only" oraz „pełny". Obiekty, do których grupa nie ma dostępu, nie mogą być widoczne dla użytkownika.

10.34. System musi zapewniać pełen audyt aktywności jego użytkowników, w tym: udanych/nieudanych logowaniach, pełnej historię operacji, realizowanych zapytań, zmian uprawnień.

10.35. System musi umożliwiać ręczne ustawianie poziomu szczegółowości gromadzonych danych audytowych.

10.36. System musi posiadać autoryzowane przez producenta narzędzie/moduł do kontroli wydajności dostarczonego systemu. Wsparcie producenta musi obejmować zakresem również to narzędzie.

10.37. System musi zapewniać mechanizmy umożliwiające pracę w trybie multitenant.

10.38. System musi pozwalać na tworzenie parserów z poziomu GUI

10.39. System musi zapewniać budowę modeli prognostycznych w oparciu o metody matematyczne i statystyczne tzw. Machine Learning.

10.40. System musi zapewniać wizualizację danych w postaci, oryginalnych logów, list, wykresów i diagramów.

10.41. System musi umożliwiać graficzną wizualizację zidentyfikowanych połączeń sieciowych pomiędzy adresami IP.

10.42. Wizualizacja danych powinna być również możliwa dla wartości tekstowych jak i liczbowych przekazywanych w logach.

10.43. System musi umożliwiać funkcjonalność eksportu danych o Zdarzeniach i Incydentach do formatu CSV i HTML m.in. w celu analizy wyników działania reguł korelacyjnych.

10.44. System musi zapewniać parsowanie spływających do niego wiadomości w formatach:

10.44.1. Syslog,

10.44.2. WEF,

10.44.3. Flat file,

10.44.4. Event log,

10.44.5. WMI,

10.44.6. SNMP trap,

10.44.7. XML,

10.44.8. JSON,

10.44.9. JDBC/ODBC

10.44.10. CSV,

10.44.11. Email,

10.44.12. musi pozwalać na implementację innych formatów w przypadku zaistnienia takiej potrzeby ze strony Zamawiającego.

10.45. System musi zbierać logi z Rozwiązań chmurowych opartych minimum o AWS oraz Microsoft Azure.

10.46. System musi umożliwiać prezentację logu o zdarzeniu w interfejsie użytkownika w takiej formie w jakiej ten log został przesłany do Systemu tj. wyświetlenie logu w postaci surowej (RAW) przed parsowaniem.

10.47. System musi do przyjmowania zdarzeń wykorzystywać zarówno mechanizmy agentowe jak i bezagentowe.

10.48. System musi umożliwiać definiowanie parserów dla niestandardowych formatów logów w oparciu o składnię wyrażeń regularnych oraz formatów wymiany danych dla wszystkich obsługiwanych formatów.

10.49. Interfejs musi umożliwić parsowanie warunkowe na podstawie dopasowania wartości pól. Po dopasowaniu wzorca dalsze parsowanie powinno być konfigurowalne w celu wyboru optymalnej metody parsowania, np.: REGEX, JSON, XML oraz umożliwiać zastosowanie innego parsera.

10.50. System musi posiadać predefiniowany zestaw parserów zdarzeń.

10.51. System musi umożliwiać weryfikację reputacji adresów IP/URL/domen na podstawie źródeł reputacyjnych, w tym co najmniej jednego źródła dostarczonego wraz z rozwiązaniem oraz źródeł zewnętrznych integrowanych przez API/feedm.

10.52. System musi wspierać geolokalizację zdarzeń na bazie adresów IP.

10.53. System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, np. dzięki zmianie wartości tych pól oraz wzbogacaniu tych danych o dodatkowe pola bazując na całych wartościach lub wzorcach wyszukiwania.

10.54. System musi umożliwiać przeszukiwanie Danych Wejściowych z uwzględnieniem filtracji po sparsowanych polach.

10.55. Proces parsowania musi umożliwiać wzbogacanie treści obieranych Wiadomości poprzez matematyczne operacje wykonywane na innych polach.

10.56. Proces parsowania musi umożliwiać anonimizację Danych Wejściowych celem ukrycia fragmentów informacji, których składowanie nie jest konieczne lub narusza wewnętrzny procedury bezpieczeństwa.

10.57. System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych

10.58. System powinien pozwalać na rozpoznanie formatów czasu i daty oraz normalizowanie ich do jednego wspólnego formatu.

10.59. Incydent, który powstał w wyniku korelacji, musi dać się wyszukiwać korzystając ze standardowego dostępnego w systemie mechanizmu wyszukiwania. System musi umożliwiać budowanie na jego podstawie kolejnych reguł korelacyjnych lub generowania alarmów.

10.60. System musi posiadać funkcjonalność korelacji danych w czasie rzeczywistym.

10.61. System musi umożliwiać tworzenie nowych reguł korelacyjnych oraz modyfikowanie istniejących.

10.62. System musi umożliwiać tworzenie własnych reguł korelacyjnych na bazie reguł odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie, w tym:

10.62.1. Wykrycia dowolnej treści w logach,

10.62.2. Wykrycia wystąpienia wartości pola na wybranej liście,

10.62.3. Wykrycia niewystępowania wartości pola na wybranej liście,

10.62.4. Wykrycia zmiany jednego z kilku pól,

10.62.5. Wykrycia zdarzeń występujących z zadaną częstotliwością,

10.62.6. Wykrycia zdarzeń, których liczba zmienia się w wskazany sposób względem czasu poprzedniego,

10.62.7. Wykrycia zaniku Wiadomości,

10.62.8. Wykrycia nowej wartości pola w zadanym okresie,

10.62.9. Wykrycia incydentu będącego pochodną zdarzeń występujących w określonej kolejności

10.63. System musi pozwalać na tworzenie własnych algorytmów ewaluacji Incydentów

10.64. Reguły korelacji oraz algorytmy ewaluacji incydentów muszą być możliwe do dodawania lub modyfikacji z poziomów zarówno GUI jak i API.

10.65. System musi pozwolić na określenie okna czasowego oraz warunków dla zdarzeń, które mają zostać poddane regułom korelacyjnym.

10.66. System musi pozwalać na realizację zapytań obejmujących całą historię gromadzonych w nim danych

10.67. System musi umożliwić korelację Zdarzeń pochodzących z różnych źródeł informacji z anomaliami wykrywanymi m.in. w. Netflow oraz wykrytymi podatnościami zidentyfikowanymi przez skaner podatności

10.68. System musi zapewnić mechanizmy obsługi incydentów i wymiany informacji pomiędzy, operatorami systemu w tym przypisanie incydentu do operatora i zmiana jego statusu.

10.69. System musi posiadać funkcjonalność tworzenia scenariuszy obsługi incydentu tzw. Playbook

10.70. System musi automatycznie podpowiadać odpowiednie scenariusze obsługi incydentów.

10.71. Scenariusze muszą mieć możliwość ich symulacji i weryfikacji, m.in. na przykładowym zasobie IT.

10.72. System musi pozwalać na tworzenie własnych scenariuszy obsługi oraz edycję istniejących.

10.73. Rozwiązanie musi posiadać funkcjonalność wysyłania powiadomień o Incydentach do innych systemów bądź zdefiniowanych użytkowników (co najmniej: powiadamianie email, opcjonalnie SMS, czat).

10.74. System musi umożliwiać testowanie reguł korelacyjnych i alertów na etapie ich tworzenia. Wynik testu nie może tworzyć wpisu o sytuacji alarmowej i ewentualnego incydentu.

10.75. System musi pozwalać na zautomatyzowane szacowanie ryzyka dla dowolnych kryteriów w ramach przetwarzanych zdarzeń. W rozwiązaniu musi być obecna funkcjonalność. kategoryzacji obiektów (adresy IP, loginy i inne pola), dla których mechanizm szacowania ryzyka uwzględni podane wagi.

10.76. System umożliwia konfiguracje automatycznych akcji, które są wykonywane na monitorowanych systemach w przypadku detekcji zagrożenia wskazanego w regule

10.77. Tworzone incydenty będące wynikiem pracy reguł bezpieczeństwa muszą posiadać wbudowany poziom istotności. Musi istnieć możliwość modyfikacji poziomu istotności dla każdej reguły.

10.78. System musi zapewniać funkcjonalność generowania raportów z dowolnych danych gromadzonych w systemie.

10.79. Raporty muszą być generowane ręcznie oraz automatycznie według zdefiniowanego harmonogramu.

10.80. System musi generować raporty do formatów minimum PDF oraz JPEG z jednoczesną możliwością opatrywania dokumentu logo Zamawiającego oraz komentarzami.

10.81. System musi zapewniać wbudowany mechanizm archiwizacji danych w postaci plików płaskich oraz ich zarządzaniem z poziomu konsoli użytkownika.

10.82. Mechanizm archiwizacji musi posiadać funkcjonalność przesyłania danych online do archiwum według zadanych kryteriów w sposób automatyczny lub ręczny.

10.83. Mechanizm archiwizacji musi umożliwiać pozwalać na przywracanie danych do systemu celem analizy online.

10.84. Mechanizm archiwizacji musi zapewniać funkcjonalność wyszukiwania w spakowanych danych bez potrzeby ich wcześniejszego rozpakowania.

10.85. System musi umożliwiać zbieranie i analizę pełnego ruchu sieciowego (warstwy modelu ISO OSI od L2 do L7) oraz analizy formatu Netflow w wersji min. V5, v9 oraz IPFIX z wykorzystaniem oficjalnych modułów dostarczanych przez producenta.

10.86. System musi umożliwiać analizę ruchu sieciowego pod kątem występowania opóźnień, retransmisji, Jitter, Server Response Time oraz Round Trip Time.

10.87. System musi umożliwiać zakup licencji wieczystych wraz ze wsparciem producenta na okres 2lat.

10.88. Oferowana licencja nie może ograniczać ilości urządzeń będących źródłem logów.

10.89. System musi umożliwiać czasowe przyjęcie zwiększonej ilości danych o minimum 30% bez potrzeby zwiększania zasobów sprzętowych lub licencyjnych.

10.90. Wsparcie producenta musi być realizowane w języku polskim przez dedykowanych inżynierów.

10.91. Wsparcie producenta musi być świadczony w formule minimum 8/5.

10.92. Wsparcie nie może być limitowane ilością zgłoszeń i musi być realizowane zdalnie oraz z siedzibie Zamawiającego.

10.93. Musi istnieć możliwość automatycznego importu informacji IoC (ang. Indicator Of Compromise), a następnie automatyczne przeszukiwanie wśród zgromadzonych zdarzeń w wyznaczonym czasie.

10.94. System musi posiadać natywną integrację z bazą MISP min. Adresy IP, hash zainfekowanych plików, adresy domen, adresy URL.

10.95. System musi umożliwiać integrację z Mitre ATT@CK.

10.96. System musi zbierać i korelować logi z następujących źródeł:

10.96.1. infrastruktura sieciowa (firewall, router/switch, VPN, proxy, DNS/DHCP),

10.96.2. systemy i serwery (Windows – w tym AD, Linux/UNIX, wirtualizacja),
10.96.3. stacje robocze i EDR/XDR (jeśli występuje),
10.96.4. usługi katalogowe/IAM (AD/LDAP/SSO), poczta, aplikacje kluczowe,
10.96.5. usługi chmurowe (0365) – logi dostępu, konfiguracji i zdarzeń bezpieczeństwa,
10.96.6. kopie zapasowe (zdarzenia wykonania backupów i błędów),

10.97. Reguły korelacyjne, alerty i obsługa incydentów

10.98. System musi posiadać bazę minimum 700 predefiniowanych reguł korelacyjnych
10.99. System musi dostarczać funkcjonalność badania integralności plików i rejestrach na monitorowanych hostach, w tym: monitorowanie zmian na zawartości plików i katalogów, zmiany uprawnień dostępu do pliku, zmiany w atrybutach plików oraz zmian na sumach kontrolnych MD5 i SHA1.
10.100. System musi posiadać funkcjonalność monitorowania konfiguracji systemów oraz aplikacji w celu zapewnienia zgodności z politykami i standardami bezpieczeństwa oraz praktykami dotyczącymi hardeningu, takimi jak CIS Benchmark.
10.101. System musi posiadać gotowe wizualizacje i polityki zgodności z GDPR, PCI-DSS, NIST.
10.102. System musi posiadać możliwość skanowania środowiska pod kątem detekcji rootkit'u i wykrywania ukrytych procesów, plików, portów
10.103. System musi posiadać funkcjonalności skanowania podatności dla aplikacji oraz systemów operacyjnych Linux i Windows
10.104. System musi posiadać funkcjonalność ciągłego śledzenia polityk OpenSCAP
10.105. Wykonawca wdroży zestaw reguł detekcji i korelacji minimum dla:
10.106. prób nieautoryzowanego dostępu i nadużyć kont (w tym AD),
10.107. eskalacji uprawnień, lateral movement, podejrzanych logowań,
10.108. złośliwego oprogramowania/IOC (jeśli dostępne dane),
10.109. anomalii ruchu sieciowego i komunikacji do nietypowych lokalizacji,
10.110. zmian konfiguracji krytycznych systemów i urządzeń,
10.111. prób wyłączenia zabezpieczeń/logowania.
10.112. Wykonawca zapewni strojenie (tuning) reguł:
10.112.1. redukcję false positives,
10.112.2. progi,
10.112.3. whitelisting/blacklisting,
10.112.4. okna czasowe,
10.112.5. zależności.

10.113. Wykonawca zapewni mapowanie zdarzeń do taksonomii (np. MITRE ATT&CK) oraz klasyfikację incydentów (severity/impact/priority) według uzgodnionych zasad

10.114. Wykonawca skonfiguruje alertowanie (kanały, eskalacje, dyżury – jeśli dotyczy) oraz minimalny workflow obsługi incydentu.

10.115. Wykonawca zapewni integrację z systemem zgłoszeń/ticketing lub wdroży minimalny rejestr incydentów (np. wbudowany).

10.116. Wykonawca dostarczy playbooki operacyjne co najmniej dla najważniejszych alertów (co sprawdzić, jakie logi/artefakty, jak eskalować, jak dokumentować).

10.117. Wykonawca przygotuje dashboardy operacyjne (SOC/IT) oraz zarządcze (KPI/KRI), obejmujące co najmniej:

10.117.1. status ingestu (EPS/GB, błędy kolektorów), pokrycie źródeł,

10.117.2. trendy incydentów i alertów, top zdarzenia, top konta/hosty,

10.117.3. zgodność z retencją i integralnością logów.

10.118. Wykonawca wykona testy obciążeniowe lub testy wydajnościowe ingestu (na uzgodnionych próbkach/źródłach) i przedstawi wyniki

10.119. Wykonawca wdroży mechanizmy backupu konfiguracji SIEM

10.120. Wykonawca dostarczy kompletną dokumentację w języku polskim, obejmującą co najmniej:

10.120.1. architekturę (diagramy), konfigurację, konta/role, integracje,

10.120.2. listę źródeł logów i parametry kolekcji (format, transport, retencja),

10.120.3. katalog use cases i reguł (opis, logika, wymagane źródła, tuning),

10.120.4. dashboardy/raporty, procedury operacyjne i playbooki,

10.120.5. procedury backup/restore, aktualizacji, zarządzania certyfikatami TLS, NTP.

10.121. Wykonawca przekaże pliki konfiguracyjne/eksporty ustawień w formie umożliwiającej odtworzenie środowiska.

10.122. Wykonawca przeprowadzi szkolenie administratorów i użytkowników operacyjnych, obejmujące:

10.122.1. obsługę alertów i dochodzenie (investigation),

10.122.2. tworzenie/edycję reguł i dashboardów,

10.122.3. utrzymanie, aktualizacje, rozwiązywanie problemów z ingestem.

10.123. Wykonawca zapewni warsztat praktyczny na danych Zamawiającego (minimum kilka scenariuszy „od alertu do wniosku”).

11. ROZWIĄZANIE SOAR

11.1. Przedmiotem zamówienia jest dostawa i wdrożenie systemu typu SOAR wraz z niezbędną infrastrukturą sprzętową i przeszkolenie pracowników Zamawiającego.

11.2. Oprogramowanie musi wspomagać pracę zespołu reagowania IT Zamawiającego tj. wspomagać procesy: monitorowania bezpieczeństwa teleinformatycznego, reagowania na incydenty, zarządzania podatnościami, gdzie głównym celem jest standaryzacja i automatyzacja działań analityków cyberbezpieczeństwa.

11.3. Oprogramowanie SOAR musi posiadać udokumentowaną i wspieraną przez producenta integrację z systemem klasy SIEM dostarczanym w ramach Przedmiotu Zamówienia, realizowaną co najmniej poprzez gotowy konektor lub API, umożliwiającą dwukierunkową wymianę danych (alerty, incydenty, komentarze, statusy) oraz automatyczne wyzwalanie scenariuszy.

11.4. Rozwiązanie musi działać jako rozwiązanie onprem w infrastrukturze Zamawiającego.

11.5. Wykonawca uruchomi i skonfiguruje platformę SOAR oraz zintegruje ją z SIEM, systemem zgłoszeń (ITSM) i kluczowymi narzędziami bezpieczeństwa (np. XDR, firewall, poczta, AD/IAM), aby automatycznie przyjmować i wzbogacać alerty oraz tworzyć/aktualizować zgłoszenia. Następnie przygotuje i przetestuje playbooki dla uzgodnionych typów incydentów (np. phishing, malware, podejrzane logowanie), ustali które akcje wykonują się automatycznie a które po akceptacji, przeszkoli zespół i przekaże dokumentację oraz wsparcie stabilizacyjne po uruchomieniu produkcyjnym.

11.6. Oprogramowanie musi umożliwiać automatyczne tworzenie incydentów wymagających obsłużenia na podstawie powiadomień z systemu klasy SIEM, zgłoszeń przekazywanych przez użytkowników na dedykowany adres e-mail, zgłoszeń przypisanych w systemie typu helpdesk do odpowiedniej grupy, przez co najmniej system RTIR (Request Tracker Incident Response) lub Jira. Ponadto rozwiązanie musi umożliwiać automatyczne zamykanie obsłużonego zgłoszenia w systemie typu helpdesk, przynajmniej dla Rozwiązania RTIR (Request Tracker Incident Response) lub Jira.

11.7. Oprogramowanie musi umożliwiać ręczne utworzenie incydentu.

11.8. Oprogramowanie musi posiadać możliwość automatycznej oraz ręcznej klasyfikacji incydentów ze względu na ich krytyczność.

11.9. Oprogramowanie musi umożliwiać tworzenie własnych definicji klasyfikacji incydentów i ich krytyczności. W ramach wdrożenia Wykonawca wraz z zamawiającym ustali oraz zaimplementuje właściwą klasyfikację incydentów w systemie.

11.10. Oprogramowanie musi umożliwiać śledzenie czasu oraz podjętych działań w ramach utworzonego incydentu oraz raportowanie czasów: Time-to-detect oraz czasów: Time-to-mitigate.

11.11. Oprogramowanie musi umożliwiać łączenie utworzonych incydentów, w tym inteligentne łączenie automatyczne.

11.12. Oprogramowanie musi umożliwiać automatyczne przydzielanie predefiniowanych zadań dla danych typów incydentów.

11.13. Oprogramowanie musi umożliwiać tworzenie i edytowanie procedur reagowania na incydenty w postaci graficznej. System musi umożliwiać stosowanie podstawowych operatorów logicznych i matematycznych przy definicji procedur.

11.14. Oprogramowanie musi umożliwiać automatyczne oraz ręczne przydzielanie incydentów wymagających obsłużenia do pracowników obsługujących system.

11.15. Oprogramowanie musi umożliwiać automatyczną oraz ręczną weryfikację w wewnętrznych oraz zewnętrznych źródłach informacji, charakterystycznych dla danego incydentów atrybutów.

11.16. Oprogramowanie musi umożliwiać zaprojektowanie oraz wdrożenie automatycznych działań reagowania na dane typy incydentów.

11.17. Oprogramowanie musi umożliwiać edycję kodu źródłowego automatycznych działań reagowania.

11.18. Oprogramowanie musi umożliwiać tworzenie zbiorczych raportów z utworzonych oraz obsłużonych incydentów.

11.19. Oprogramowanie musi integrować się przynajmniej z następującymi systemami:

11.19.1.1. Office 365 / Microsoft Exchange (pobranie lub wysłanie maili)

11.19.1.2. Slack (wysyłka komunikatów)

11.19.1.3. Mattermost

11.19.1.4. SIEM

11.20. Oprogramowanie musi umożliwiać łatwą integrację z pozostałymi systemami klasy threat intel/threat hunting/threat share za pomocą API.

11.21. System musi posiadać możliwość generowania dashboardów security z danych znajdujących się w SOAR, między innymi statystyk, w tym system musi posiadać

możliwość tworzenia i konfiguracji widoków głównych na główny ekran dyspozycyjny w pomieszczeniu SOC.

11.22. Umożliwiać dwustronną komunikację z użytkownikami systemu (np. w celu zebrania dodatkowych informacji od osób związanych z incydentem) oraz operatorami systemu SOAR, na przykład poprzez zastosowanie interaktywnych formularzy.

11.23. Zapewniać zestaw co najmniej 250 gotowych integracji pozwalających na szybką, dwustronną komunikację z zewnętrznymi systemami.

11.24. Automatyzować proces analizy otrzymanych danych, realizować funkcje informacyjne, jak również podejmować funkcje naprawcze (np. automatyczna analiza pliku w chmurze sandbox wybranego producenta, wysłanie wiadomości e-mail do użytkownika zainfekowanej stacji końcowej, aby nie otwierał załącznika i blokada na urządzeniu sieciowym dostępu do wskazanych usług dla wybranego użytkownika).

11.25. Posiadać wbudowaną bibliotekę minimum 5 typów incydentów, a także powinno dostarczać specjalizowane typy incydentów związane z integrowanymi systemami, pozwalając jednocześnie na ich edycję lub kopiowanie celem stworzenia własnej karty incydentu.

11.26. Umożliwić wykorzystanie w skryptach własnych bibliotek zewnętrznych oraz programów (np. poprzez umożliwienie uruchomienia skryptów we własnym kontenerze, zawierającym pożądane oprogramowanie).

11.27. Zapewniać możliwość wglądu w kod integracji oraz jego klonowanie pod kątem wprowadzania modyfikacji lub napisania własnej wersji integracji.

11.28. Pozwalać na kopiowanie oraz edycję już istniejących scenariuszy jak również dodawanie nowych.

11.29. Pozwalać na edycję i dodawanie nowych scenariuszy obsługi incydentu (tzw. playbook) za pomocą graficznego interfejsu użytkownika bez konieczności wykorzystania języków skryptowych lub znajomości języków programowania.

11.30. Pozwalać na tworzenie scenariuszy zagnieżdżonych, tzn. scenariusz nadrzędny może zawierać scenariusze podrzędne uruchamiane na zasadzie pod-scenariuszy. Edycja/zmiana pod-scenariusza wpływa automatycznie na wszystkie scenariusze, które go wykorzystują, co ułatwia administrację.

11.31. Pozwalać na tworzenie scenariuszy zawierających:

11.31.1. zadania ręczne

11.31.2. zadania zautomatyzowane

11.31.3. zadania warunkowe automatyczne

11.31.4. zadania warunkowe ręczne

11.31.5. akwizycję danych przy użyciu formularzy

11.31.6. filtry danych

11.31.7. pod-scenariusze.

11.32. Pozwalać na automatyczne i ręczne wykonywanie dostępnych scenariuszy.

11.33. Pozwalać na automatyczne dokumentowanie uruchomionych scenariuszy wraz z wynikami jego działania

11.34. Umożliwiać wizualizacje przebiegu wykonania scenariusza (wizualizacje rezultatu wszystkich wykonanych oraz pominiętych zadań, operacji warunkowych, decyzji itp.).

11.35. Pozwalać na sterowanie wykonaniem scenariusza przez operatora (zadania warunkowe ręczne) drogą korespondencyjną (m.in. z poziomu wiadomości email oraz wiadomości w komunikatorze takim jak np. Microsoft Teams, Slack, Mattermost itp.).

11.36. Pozwalać na uruchomienie scenariusza w trybie krokowym w celu analizy jego poprawności i usunięcia ewentualnych błędów.

11.37. Pozwalać na ponowne uruchomienie scenariusza na konkretnym incydencie, jeżeli zajdzie taka potrzeba.

11.38. Pozwalać na zatrzymanie scenariusza w trakcie jego wykonania.

11.39. Pozwalać na doraźne wykonanie dowolnego zadania automatyzacyjnego przez operatora, bez konieczności tworzenia nowych / modyfikacji istniejących scenariuszy (np. przy użyciu wiersza poleceń).

11.40. Pozwalać na proste monitorowanie stanu wykonania scenariuszy powiązanych z incydentami. Ponadto, w przypadku wystąpienia jakichkolwiek anomalii w trakcie wykonania scenariusza, osoby odpowiedzialne za incydent powinny zostać natychmiast o tym poinformowane.

11.41. Pozwalać na przydzielanie zadań pojedynczego scenariusza różnym członkom zespołu SOC.

11.42. Pozwalać na przekazywanie parametrów pomiędzy zadaniami pojedynczego scenariusza.

11.43. Pozwalać na odczytywanie wyników analizy i wykorzystaniu ich w kolejnych zadaniach uruchomionego scenariusza.

11.44. Pozwalać na sprawdzenie historycznych danych na temat uruchomionych scenariuszy/zadań.

11.45. Pozwalać na okresowe uruchamianie scenariuszy w zdefiniowanym czasie i wedle harmonogramu.

11.46. Pozwalać na sprawdzenie, które incydenty nie zostały obsłużone.

11.47. Pozwalać na tworzenie własnych:

11.47.1. Typów incydentów

11.47.2. Pól/etykiet incydentów

11.47.3. Typów wskaźników (ang. indicator)

11.47.4. Pól/etykiet wskaźników (ang. indicator)

11.47.5. Raportów

11.47.6. Dashboardów.

11.48. Pozwalać na automatyczne wypełnianie pól incydentu bazując na typie incydentu lub jego atrybutach.

11.49. Pozwalać na delegowanie zadań innym członkom zespołu Zamawiającego w ramach oceny danego incydentu.

11.50. Pozwalać na współpracę pomiędzy członkami zespołu Zamawiającego (np. rozmowa między członkami zespołu a temat incydentu).

11.51. Pozwalać na zapisywanie historycznych incydentów wraz z pełną informacją na temat podjętych akcji obsługi/Rozwiązania w celu szkolenia/transferu wiedzy pomiędzy członkami zespołu Zamawiającego (Na historię incydentu składają się wyniki działania automatycznych i ręcznych zadań określonych w playbooku, komentarze analityków pracujących nad incydentem, indykatory zagrożenia IOC (IP, URL, domeny, itd.) wyciągane automatycznie i wskazywane ręcznie w czasie obsługi incydentu, elementy analizy oznaczone przez analityków jako dowód w sprawie (np. zrzuty ekranu z widokiem podejrzanych stron web), pliki dodawane do historii obsługi incydentu przez analityków, itp.).

11.52. Pozwalać na export wskaźników kompromitacji do serwerów MISP.

11.53. Pozwalać na import zdarzeń z serwerów MISP.

11.54. Pozwalać na eksport incydentów w formatach STIX 1/2, CSV, PDF.

11.55. Pozwalać na tworzenie wielu instancji integracji tego samego typu do Rozwiązań firm trzecich (przykładowo dwie integracje z serwerami IMAP lub zaczytujące dane threat intel z dwóch źródeł w formacie JSON).

11.56. Pozwalać na rozszerzenie możliwości systemu w zakresie tworzenia i edycji scenariuszy poprzez dodanie własnych skryptów realizujących niestandardową logikę operacji warunkowych, filtracji danych, modyfikacji danych, a także

skryptów realizujących niestandardową prezentację danych w dashboardach, zadania wykonywane po zakończeniu obsługi incydentu itp.

11.57. Pozwalać na proste wprowadzenie globalnych zestawów poświadczeń w celu ułatwienia użycia wspólnego konta technicznego w wielu integracjach z systemami trzecimi.

11.58. Posiadać zestaw przygotowanych raportów takich jak:

11.58.1. Raport na temat incydentów: dzienny, 7- i 30-dniowy

11.58.2. Raport na temat średniego czasu Rozwiązania incydentu

11.59. Pozwalać na tworzenie własnych raportów oraz dashboardów za pomocą predefiniowanych komponentów umożliwiających wizualizację pożądanych danych (np. wykres kołowy, słupkowy, liniowy, tabela itp.).

11.60. Pozwalać na proste wyszukiwanie incydentów na podstawie ich cech (np. przy użyciu dedykowanego języka zapytań) oraz podobieństwa do innych incydentów (related incidents).

11.61. Pozwalać na wizualizację zależności pomiędzy podobnymi incydentami na poziomie wystąpień identycznych indykatorów.

11.62. Pozwalać na eksport raportów w formacie, co najmniej PDF.

11.63. Mieć możliwość działania jako platforma SOAR dla wielu instytucji/klientów z całkowitą separacją zasobów i przetwarzanych danych (tzw. wsparcie dla trybu multi-tenant).

11.64. Posiadać repozytorium wskaźników (ang. indicators), które kolekcjonuje i koreluje wskaźniki w ramach wszystkich incydentów, alertów i feedów dostarczanych do Rozwiązania.

11.65. Posiadać możliwość wykonywania scenariuszy na podstawie zestawu wskaźników (ang. indicators) określonych przez użytkownika.

11.66. Być w stanie obsługiwać formaty strukturalne, takie jak JSON, CSV, STIX 1.X i STIX 2.X itp. w ramach integracji ze źródłami wskaźników (ang. indicators).

11.67. Wspierać minimum następujące typy wskaźników (ang. indicators):

11.67.1. numery kart płatniczych

11.67.2. IBAN

11.67.3. adres email

11.67.4. konto użytkownika

11.67.5. wyniki CVE

11.67.6. domena

11.67.7. FQDN

11.67.8. nazwy hosta

11.67.9. IP (v4 oraz v6)

11.67.10. klucz i ścieżka rejestru

11.67.11. URL

11.67.12. CIDR.

11.67.13. Umożliwiać własną definicję wskaźników, jego pól oraz skryptów reputacyjnych.

11.67.14. Zapewniać użytkownikom możliwość automatycznej weryfikacji wskaźników (tzw. enrichment), wykonując odpowiedni scenariusz lub uruchamiając sprawdzanie na podstawie typu wskaźnika (ang. indicator).

11.68. System musi posiadać natywną integrację z MITRE ATT&CK i przypisywać do incydentów odpowiednie techniki i taktyki

11.69. System musi być rozwiązaniem opartym o licencję wieczystą.

12. ROZWIAZANIE KOMPLEKSOWEJ KOPII ZAPASOWEJ

12.1. Przedmiotem zamówienia jest dostawa oraz wdrożenie kompleksowego sprzętowego Rozwiązania kopii zapasowej, obejmującego co najmniej oprogramowanie do realizacji kopii zapasowych, dedykowane urządzenie sprzętowe oraz bibliotekę taśmową w technologii LTO, stanowiących spójne i zintegrowane rozwiązanie.

12.2. Zakres wdrożenia obejmuje wykonanie wszelkich czynności niezbędnych do uruchomienia Rozwiązania w środowisku produkcyjnym, w szczególności instalację, konfigurację, integrację z istniejącą infrastrukturą Zamawiającego, konfigurację polityk kopii zapasowych i odtwarzania danych, testy poprawności działania, dokumentację powdrożeniową oraz przekazanie Rozwiązania do eksploatacji i przeszkolenie personelu Zamawiającego.

12.3. Rozwiązanie musi zapewnić za pomocą jednej platformy oprogramowania realizację backupu dla serwerów, kontenerów, maszyn wirtualnych oraz stacji roboczych.

12.4. Rozwiązanie musi stanowić dedykowane rozwiązanie do wykonywania kopii zapasowych i odtwarzania danych.

12.5. Rozwiązanie musi odpowiadać za przechowywanie danych kopii zapasowych, zarządzanie repozytoriami danych oraz udostępnianie interfejsu API.

12.6. Rozwiązanie musi umożliwiać wykonywanie kopii zapasowych z hostów działających pod kontrolą nowoczesnych dystrybucji Linux.

12.7. Rozwiązanie musi umożliwiać szyfrowanie danych.

12.8. Rozwiązanie musi realizować kopie zapasowe w trybie przyrostowym.

12.9. Rozwiązanie musi przesyłać wyłącznie zmienione bloki danych pomiędzy kolejnymi kopiami zapasowymi.

12.10. Rozwiązanie musi realizować deduplikację danych.

12.11. Rozwiązanie musi obsługiwać deduplikację opartą o bloki o stałym oraz zmiennym rozmiarze.

12.12. Rozwiązanie musi wykorzystywać sumy kontrolne do identyfikacji identycznych bloków danych.

12.13. Rozwiązanie musi zapewniać weryfikację integralności danych przy użyciu algorytmu SHA-256.

12.14. Rozwiązanie musi umożliwiać weryfikację kopii zapasowych w celu wykrywania uszkodzeń danych.

12.15. Szyfrowanie musi być realizowane z użyciem co najmniej algorytmu AES-256.

12.16. Rozwiązanie musi umożliwiać generowanie klucza głównego w postaci pary kluczy RSA do bezpiecznego przechowywania kluczy szyfrujących kopie zapasowe.

12.17. Rozwiązanie musi umożliwiać odzyskanie kluczy szyfrujących niezależnie od systemu serwerowego.

12.18. Rozwiązanie musi zapewniać mechanizmy zarządzania użytkownikami, rolami oraz uprawnieniami.

12.19. Rozwiązanie musi umożliwiać precyzyjne przypisywanie uprawnień do zasobów i operacji.

12.20. Rozwiązanie musi umożliwiać synchronizację repozytoriów danych pomiędzy różnymi lokalizacjami.

12.21. Rozwiązanie musi umożliwiać definiowanie zadań synchronizacji (Sync Jobs) uruchamianych ręcznie lub cyklicznie.

12.22. Synchronizacji muszą podlegać wyłącznie zmiany od ostatniego uruchomienia zadania.

12.23. Rozwiązanie musi wspierać strategię ochrony przed ransomware poprzez:

12.23.1. kontrolę dostępu,

12.23.2. weryfikację integralności danych,

12.23.3. możliwość wykonywania kopii zapasowych poza główną lokalizacją.

12.24. Rozwiązanie musi umożliwiać szybkie odtwarzanie danych po incydencie.

12.25. Rozwiązanie musi umożliwiać szybkie i precyzyjne odtwarzanie danych.

12.26. Rozwiązanie musi umożliwiać:

12.26.1. odtwarzanie całych maszyn wirtualnych,

12.26.2. odtwarzanie archiwów,

12.26.3. odtwarzanie pojedynczych plików i katalogów.

12.27. Rozwiązanie musi udostępniać katalog snapshotów umożliwiający przegląd zawartości kopii zapasowych.

12.28. Rozwiązanie musi udostępniać interaktywną powłokę odzyskiwania plików.

12.29. Rozwiązanie musi posiadać zintegrowany, webowy interfejs administracyjny.

12.30. Interfejs webowy musi umożliwiać:

12.30.1. monitorowanie stanu systemu,

12.30.2. zarządzanie repozytoriami danych,

12.30.3. przegląd i odtwarzanie kopii zapasowych,

12.30.4. zarządzanie użytkownikami i uprawnieniami,

12.30.5. zarządzanie synchronizacją zdalną,

12.30.6. monitorowanie zadań, logów i wykorzystania zasobów.

12.31. Rozwiązanie musi udostępniać wbudowaną konsolę GUI.

12.32. Rozwiązanie musi udostępniać interfejs wiersza poleceń (CLI) z dokumentacją typu man.

12.33. Rozwiązanie musi udostępniać REST API.

12.34. Rozwiązanie musi umożliwiać integrację z platformą wirtualizacji Proxmox VE oraz HyperV

12.35. Rozwiązanie musi wspierać wykonywanie kopii zapasowych maszyn wirtualnych oraz kontenerów.

12.36. Rozwiązanie musi umożliwiać odtwarzanie pojedynczych plików z kopii maszyn wirtualnych.

12.37. Rozwiązanie musi zapewniać bezpieczeństwo integracji przy użyciu odcisku certyfikatu.

12.38. Rozwiązanie musi umożliwiać wykonywanie kopii zapasowych na nośniki taśmowe.

12.39. Rozwiązanie musi obsługiwać napędy LTO-8 i nowsze, z obsługą sprzętowego szyfrowania.

12.40. Rozwiązanie musi umożliwiać definiowanie polityk retencji taśm.

12.41. Rozwiązanie musi umożliwiać konfigurację obsługi bibliotek taśmowych z poziomu interfejsu webowego.

12.42. Rozwiązanie musi umożliwiać generowanie etykiet kodów kreskowych dla taśm LTO.

12.43. Urządzenia muszą zostać objęte rozszerzonym wsparciem gwarancyjnym w przypadku awarii polegającym na dostarczeniu na drugi dzień roboczy Rozwiązania zastępczego na czas naprawy o takich samych parametrach.

12.43.1. Urządzenie musi być przystosowane do montażu w szafie rack 19” i zajmować nie więcej jak 2U.

12.43.2. Redundantne zasilanie i chłodzenie.

12.43.3. Musi zapewniać funkcje deduplikacji.

12.43.4. Rozwiązanie musi posiadać co najmniej 100 TB pojemności masowej netto po RAID.

12.43.5. Dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID-6.

12.43.6. Musi zapewniać możliwość pracy przy utracie co najmniej 3 dysków.

12.43.7. Urządzenie musi zapewniać wydajność umożliwiającą realizację jednoczesnych procesów tworzenia i odtwarzania kopii zapasowych dla wielu systemów, w sposób zapewniający zakończenie operacji backupu w założonych oknach czasowych Zamawiającego.

12.43.8. Urządzenie musi zapewniać integralność danych end-to-end poprzez ciągłą weryfikację poprawności zapisu i odczytu danych oraz automatyczne wykrywanie i naprawę przekłamań danych w locie, realizowaną na poziomie systemu plików lub mechanizmów RAID, przy czym Zamawiający dopuszcza rozwiązanie równoważne oparte na zaawansowanej korekcji błędów pamięci RAM oraz obsłudze standardu T10-PI (Protection Information).

12.43.9. Urządzenie musi być wyposażone w co najmniej dwa porty sieciowe 25 Gb/s w standardzie SFP28 oraz cztery porty sieciowe 1 Gb/s w standardzie RJ-45, przeznaczone do pracy w sieci Ethernet.

12.43.10. Urządzenie do wykonywania kopii zapasowych musi zapewniać kompatybilność z heterogenicznymi środowiskami IT, w tym platformami wirtualizacji, środowiskami kontenerowymi, infrastrukturą chmurową oraz systemami fizycznymi, umożliwiając realizację kopii zapasowych i odzyskiwania danych dla obciążeń wirtualnych, fizycznych, chmurowych i kontenerowych w sposób scentralizowany z jednego urządzenia, bez uzależnienia od konkretnego producenta lub platformy.

12.43.11. Urządzenie do wykonywania kopii zapasowych musi być wyposażone w zaawansowane mechanizmy bezpieczeństwa, zapewniając ochronę danych przed zaawansowanymi zagrożeniami cybernetycznymi oraz skutkami błędów ludzkich obejmujące co najmniej:

12.43.11.1. szyfrowanie danych,

12.43.11.2. obsługę niezmiennych kopii zapasowych (immutable backup),

12.43.11.3. możliwość realizacji kopii zapasowych w modelu air-gap, z

12.43.11.4. zarządzanie dostępem oparte na rolach (RBAC)

12.43.11.5. uwierzytelnianie wieloskładnikowe (MFA),

12.43.12. Urządzenie do wykonywania kopii zapasowych musi umożliwiać pełne odzyskiwanie maszyn wirtualnych, selektywne odzyskiwanie pojedynczych plików oraz przywracanie danych na poziomie aplikacji, zapewniając elastyczne scenariusze odtwarzania adekwatne do charakteru incydentu lub awarii.

12.43.13. Rozwiązanie musi rejestrować działania administracyjne oraz operacyjne użytkowników, w tym operacje konfiguracji, usuwania i odtwarzania kopii zapasowych, z możliwością eksportu logów do zewnętrznych systemów monitorowania lub SIEM.

12.44. Minimalne wymagania dla biblioteki taśmowej

12.44.1. Biblioteka nie może przekraczać 3U w dostarczonej konfiguracji.

12.44.2. Montaż w przemysłowej szafie RACK 19”.

12.44.3. Biblioteka musi skalować się do min. 8 modułów, 3U każdy, 24U łącznie. Niedopuszczalne jest stosowanie jakiegokolwiek okablowania zewnętrznego (np. łączników SCSI) do wykonania rozbudowy, wszelka komunikacja musi odbywać się połączeniami wewnętrznymi.

12.44.4. Biblioteka taśmowa musi być wyposażona w min. 2 napędy taśmowe LTO8 o natywnym interfejsie SAS, połowy wysokości (Half Height)

12.44.5. Biblioteka powinna umożliwiać wymianę napędów bez przerywania pracy (napędy typu „hot swap”).

12.44.6. Biblioteka musi posiadać możliwość zautomatyzowanego kalibrowania nośników LTO9 z poziomu panelu zarządzania biblioteką taśmową.

12.44.7. Biblioteka musi mieć możliwość rozbudowy do 24 napędów taśmowych LTO9 (o natywnym interfejsie SAS lub i FC, połowy wysokości (Half Height)), łącznie.

12.44.8. Musi być możliwość mieszania napędów różnych technologii LTO (od min. LTO-8) oraz różnych interfejsów.

12.44.9. Biblioteka musi mieć możliwość sprzętowego szyfrowania kopii zapasowych z wykorzystaniem napędów taśmowych. Klucze szyfrujące muszą być przechowywane w aplikacji backup. Licencja musi być dostarczona wraz z biblioteką.

12.44.10. Biblioteka musi mieć możliwość sprzętowego szyfrowania kopii zapasowych z wykorzystaniem napędów taśmowych. Klucze szyfrujące muszą być przechowywane w SafeNet KeySecure (KMIP), Thales keyAuthority (KMIP) lub IBM TKLM/SKLM (non-KMIP), przy czym Zamawiający nie wymaga dostarczenia licencji na ww. funkcjonalność.

12.44.11. Biblioteka musi mieć min. (fizycznie oraz licencjonowanych do dowolnego użytku) 25 kieszeni na nośniki taśmowe.

12.44.12. Biblioteka musi mieć możliwość rozbudowy do min. (fizycznie oraz licencjonowanych do dowolnego użytku) 800 kieszeni na nośniki taśmowe.

12.44.13. Biblioteka musi mieć możliwość zdefiniowania do 25 kieszeni typu „mail slot" w odstępach co 5 (licząc od 0).

12.44.14. Biblioteka musi mieć możliwość stworzenia bezpiecznej partycji dla nośników taśmowych w celu ochrony przed ransomware. Partycja musi być skonfigurowana na dostępnych slotach w bibliotece nawet w przypadku, kiedy nie są one za licencjonowane oraz bez możliwości dołączenia do niej napędu taśmowego. Biblioteka taśmowa musi przechwytywać operację eksportu nośników taśmowych wykonywanych przez aplikację backup i umieszczać te nośniki w bezpiecznym miejscu a nie w slotach typu "mail".

12.44.15. Biblioteka musi mieć możliwość definiowania tzw. "logical lock", który uniemożliwi użytkownikowi administracyjnemu przesunięcie nośnika taśmowego w inny slot lub napęd biblioteki taśmowej.

12.44.16. Biblioteka musi mieć możliwość zainstalowanego tzw. "hardware lock", który uniemożliwi fizyczną ingerencję w bibliotekę taśmową (np. serwisowe wysunięcie magazynków z nośnikami taśmowymi) ale zapewni możliwość skanowania tak zabezpieczonych nośników taśmowych w celach np. inwentaryzacji.

12.44.17. „Hardware Lock" musi mieć możliwość zdefiniowania po jakiej liczbie nośników taśmowych magazynek ma zostać automatycznie wysunięty.

12.44.18. Biblioteka taśmowa musi mieć możliwość włączenia adresacji logicznej dla modułu kontrolnego (numer seryjny) oraz napędów taśmowych (WWN).

12.44.19. Biblioteka musi zarządzana z poziomu panelu dotykowego zabezpieczonego hasłem lub/i numerem PIN oraz zdalnego modułu zarządzania przez panel WWW.

12.44.20. Musi być możliwość tworzenia użytkowników lokalnych oraz integracji z systemem usług katalogowych – Microsoft Active Directory (które Zamawiający obecnie używa). Biblioteka musi wspierać Multi-Factor Authentication (MFA) dla min. użytkowników lokalnych.

12.44.21. Biblioteka musi udostępniać funkcje monitorowania stanu napędów i robota.

12.44.22. Biblioteka taśmowa powinna mieć również możliwość zdalnego monitorowania stanu urządzenia i wychwytywania błędów bezpośrednio przez inżynierów producenta za pomocą odpowiedniego oprogramowania, dostarczonego razem z biblioteką taśmową. Nie jest dopuszczalne instalowanie żadnych dodatkowych systemów (wirtualnych czy fizycznych) w celu osiągnięcia tej funkcjonalności.

12.44.23. Obsługa SNMP, Syslog, proxy, definiowanie access list dla adresów IP.

12.44.24. Biblioteka musi posiadać min. 2 redundantne interfejsy 1GbE do zarządzania. Interfejsy muszą być zlokalizowane na module zarządzania biblioteką oraz posiadać wszystkie mechanizmy zarządzania na obu portach.

12.44.25. Biblioteka powinna być wykonana w technologii umożliwiającej sprzętowy podział na mniejsze biblioteki „logiczne", a następnie podłączane do różnych serwerów, korzystających z różnego oprogramowania do wykonywania kopii zapasowych i archiwizacji.

12.44.26. Biblioteka musi wspierać do 24 logicznych bibliotek.

12.44.27. Biblioteka musi być wyposażona w czytnik kodów kreskowych a czas jej inwentaryzacji nie powinien przekraczać 5 minut dla pełnej konfiguracji.

12.44.28. Musi posiadać w pełni redundantne zasilanie dla wszystkich modułów posiadających napędy taśmowe.

12.44.29. Biblioteka powinna mieć możliwość raportowania ad-hoc oraz zgodnie z harmonogramem:

12.44.29.1. Zużycia/wykorzystania nośników taśmowych,

12.44.29.2. Spójności danych taśm (informacja o błędach),

12.44.29.3. Utylizacja napędów taśmowych,

12.44.29.4. Informacji nt. zewnętrznej ingerencji (np. usunięcie nośnika taśmowego w trakcie działania biblioteki lub między rebootami).

12.44.30. Musi być możliwość definiowania grup odbiorców dla powyższych raportów. Funkcjonalność musi być realizowana bezpośrednio przez oprogramowanie wewnętrzne biblioteki lub przez dedykowany system producenta biblioteki taśmowej uruchomiony jako maszyna wirtualna.

12.44.31. Sprzęt musi być dostarczony wraz z 20 taśmami co najmniej LTO-8 oraz 2 taśmami czyszczącymi.

12.44.32. Jeśli do jakiejkolwiek wyżej opisanej funkcjonalności lub rozbudowy fizycznej wymagane jest dostarczenie licencji ta licencje musi być dostarczona w ramach tego postępowania.

13. ROZWIĄZANIE MONITOROWANIA INFASTRUKTURY

13.1. Przedmiotem zamówienia jest dostawa i wdrożenie systemu monitoringu wydajnością i dostępnością w zakresie komponentów tj.:

13.1.1.1. serwery,

13.1.1.2. urządzenia sieciowe,

13.1.1.3. bazy danych,

13.1.1.4. aplikacje.

13.2. Zakres wdrożenia obejmuje wykonanie przez Wykonawcę wszelkich czynności niezbędnych do uruchomienia produkcyjnego systemu monitoringu wydajności i dostępności infrastruktury IT Zamawiającego.

13.3. Wykonawca przeprowadzi instalację systemu monitoringu na infrastrukturze Zamawiającego oraz dokona jego podstawowej konfiguracji, w tym konfiguracji komponentów serwerowych, bazodanowych oraz interfejsu użytkownika.

13.4. Wykonawca zintegruje system monitoringu z istniejącą infrastrukturą Zamawiającego, obejmującą co najmniej serwery, urządzenia sieciowe, bazy danych, aplikacje oraz systemy operacyjne, zgodnie z wymaganiami określonymi w OPZ.

13.5. Wykonawca skonfiguruje zestaw podstawowych metryk wydajnościowych i dostępności, progów ostrzegawczych i krytycznych oraz mechanizmów alertowania, uwzględniając charakter monitorowanych komponentów i dobre praktyki administracyjne.

13.6. Wykonawca skonfiguruje panele wizualizacyjne (kokpity) oraz mapy infrastruktury umożliwiające bieżący nadzór nad stanem monitorowanych komponentów i usług.

13.7. Wykonawca przeprowadzi szkolenie dla administratorów Zamawiającego w zakresie obsługi, konfiguracji i utrzymania systemu monitoringu.

13.8. System monitoringu musi być oparty na architekturze serwer–agent lub serwer–sonda, z możliwością rozszerzania funkcjonalności poprzez mechanizmy wtyczek, szablonów monitoringu lub własnych definicji metryk, bez konieczności modyfikacji kodu źródłowego systemu.

13.9. System musi być oparty o licencję open source np. Zabbix lub licencję wieczystą, niewymagającą cyklicznych opłat za monitorowanie liczby hostów, usług, metryk ani liczby użytkowników systemu, działającym wewnątrz infrastruktury Zamawiającego.

13.10. System musi umożliwiać monitorowanie w trybie agentowym oraz bezagentowym, w szczególności z wykorzystaniem protokołów sieciowych, mechanizmów zdalnego wykonywania testów oraz standardowych interfejsów systemowych.

13.11. System musi umożliwiać definiowanie progów ostrzegawczych i krytycznych, reguł eskalacji alertów oraz zależności pomiędzy monitorowanymi komponentami w celu ograniczenia liczby alertów kaskadowych.

13.12. System musi umożliwiać tworzenie, importowanie oraz wielokrotne wykorzystanie szablonów monitoringu dla grup zasobów IT.

13.13. System musi umożliwiać monitorowanie dostępności i czasu odpowiedzi usług sieciowych oraz witryn WWW, wraz z raportowaniem poziomu dostępności (SLA).

13.14. System musi umożliwiać analizę trendów oraz wykrywanie anomalii w oparciu o historyczne dane monitoringowe, linie bazowe lub reguły progowe.

13.15. System musi wspomagać administrowanie w proaktywnym zarządzaniu kondycją infrastruktury IT identyfikując potencjalne problemy i awarie, zanim wpłyną one negatywnie na działanie.

13.16. System musi umożliwiać monitorowanie agentowe co najmniej systemów:

13.16.1.1. Microsoft Windows,

13.16.1.2. Linux (dowolna dystrybucja),

13.17. System musi posiadać możliwość monitorowanie bezagentowego dostępności i wydajności dowolnej witryny WWW (SLA).

13.18. System musi być dostarczony na licencji umożliwiającej na monitorowanie dowolnej liczby komponentów IT i pracę dowolnej liczby operatorów.

13.19. System musi posiadać narzędzia do zbierania danych o wydajności i dostępności usług.

13.20. System musi umożliwiać konfigurację interwałów i częstotliwości monitoringu poszczególnych komponentów lub grup komponentów.

13.21. System musi posiadać narzędzia umożliwiające wizualizację danych w postaci wykresów.

13.22. System musi umożliwiać budowanie map infrastruktury sieci oraz osadzania komponentów na mapach.

13.23. System musi posiadać mechanizm alertów z możliwością ich wysyłki co najmniej przez e-mail.

13.24. System musi posiadać API umożliwiającego integrację z innymi narzędziami.

13.25. System musi posiadać funkcję wykrywania anomalii oraz monitorowania trendów.

13.26. System musi posiadać możliwość definiowania i zamawiania okresowych raportów dotyczących kondycji środowiska.

13.27. Komunikacja pomiędzy wszystkimi komponentami systemu musi odbywać się z wykorzystaniem bezpiecznych i szyfrowanych połączeń.

14. ROZWIĄZANIE ZARZĄDZANIA INFRASTRUKTURĄ IT

14.1. Przedmiotem zadania jest dostawa, wdrożenie i uruchomienie Rozwiązania informatycznego umożliwiającego centralne zarządzanie infrastrukturą IT oraz prowadzenie inwentaryzacji sprzętu i oprogramowania Zamawiającego.

14.2. System musi zapewniać obsługę co **najmniej 250 stacji roboczych i użytkowników**.

14.3. Konsola administracyjna systemu musi działać w sposób w pełni responsywny, niezależnie od rozmiaru oraz rozdzielczości ekranu urządzenia, na którym jest wyświetlana, oraz być dostępna za pośrednictwem dowolnej przeglądarki internetowej zgodnej ze standardem HTML5, w tym m.in. Internet Explorer 11, Mozilla Firefox, Google Chrome oraz Opera.

14.4. Komponent Klienta musi obsługiwać systemy operacyjne w architekturze 32- i 64-bitowej, w tym Windows Server, Windows, macOS oraz Linux, w szczególności dystrybucje Ubuntu, Debian, Red Hat, CentOS oraz Fedora.

14.5. Klient systemu musi wspierać monitorowanie aktywności użytkowników w sieci internetowej w przeglądarkach Opera, Google Chrome oraz Mozilla Firefox.

14.6. Komponent serwerowy systemu musi działać na systemach operacyjnych w architekturze 64-bitowej, w szczególności Windows Server oraz Windows.

14.7. Serwer WWW systemu musi być oparty na platformie Microsoft w architekturze 64-bitowej, obejmującej systemy Windows Server lub Windows 10, oraz wykorzystywać środowisko Java 8 w wersji JRE lub JDK wraz z serwerem aplikacyjnym Apache Tomcat.

14.8. Baza danych systemu musi działać w oparciu o silnik Microsoft SQL Server w wersji 64-bitowej, zarówno w edycjach komercyjnych, jak i bezpłatnych, w tym Microsoft SQL Server Express Edition. Wykonawca zapewnia odpowiednie licencje.

14.9. System musi umożliwiać pracę w środowiskach wirtualnych opartych o platformy Microsoft Hyper-V oraz Vmware i Proxmox.

14.10. Architektura systemu musi obejmować komponent Klienta, który odpowiada za zarządzanie komputerem, gromadzenie danych oraz ich bezpieczne przesyłanie do serwera, przy czym Klient musi działać w trybie usługi systemowej.

14.11. System musi zawierać konsolę administracyjną przeznaczoną do zarządzania całością rozwiązania, udostępnioną w postaci w pełni funkcjonalnej aplikacji webowej.

14.12. System musi udostępniać panel pracownika w formie aplikacji webowej niewymagającej dodatkowego procesu logowania, przeznaczonej dla pracowników, zapewniającej dostęp do wybranych informacji z konsoli administracyjnej oraz umożliwiającej interakcję z pracownikiem w określonych obszarach funkcjonalnych.

14.13. System musi zawierać komponent serwerowy odpowiedzialny za utrzymywanie komunikacji oraz wymianę danych pomiędzy serwerem a Klientami.

14.14. Komponenty systemu, w tym Klient, konsola administracyjna, serwer oraz baza danych, muszą być aktualizowane automatycznie z wykorzystaniem bezpiecznego połączenia.

14.15. System musi posiadać mechanizmy automatycznej konserwacji realizowanej zgodnie z ustalonym harmonogramem.

14.16. System musi umożliwiać pełne zdalne zarządzanie komponentem Klienta, obejmujące jego uruchamianie i zatrzymywanie, zmianę konfiguracji, inicjowanie skanowań oraz wykonywanie poleceń systemowych. Klient musi prezentować komunikaty w formacie HTML wraz z informacją o czasie ich wyświetlenia oraz identyfikacją użytkownika.

14.17. Konsola administracyjna systemu musi obsługiwać co najmniej dwa języki – polski oraz angielski – oraz udostępniać intuicyjny interfejs użytkownika zapewniający pełny zakres operacji administracyjnych, w tym dodawanie, edycję oraz usuwanie obiektów systemowych.

14.18. Konsola administracyjna musi zawierać nie mniej niż 140 predefiniowanych dashboardów, w tym dashboardy użytkownika, prezentujących informacje dotyczące infrastruktury, sieci oraz bezpieczeństwa systemu.

14.19. Użytkownicy systemu muszą mieć możliwość samodzielnej konfiguracji dashboardów użytkownika, natomiast dashboardy sieciowe i bezpieczeństwa muszą prezentować szczegółowe widżety zawierające informacje o stanie usług oraz poziomie bezpieczeństwa.

14.20. Konsola administracyjna musi umożliwiać filtrowanie danych prezentowanych na dashboardach oraz personalizację interfejsu użytkownika, w tym definiowanie własnych pól, filtrów i widoków, z zachowaniem tych ustawień pomiędzy kolejnymi sesjami logowania.

14.21. System musi umożliwiać definiowanie poziomów uprawnień dla użytkowników oraz grup użytkowników, z obsługą mechanizmu dziedziczenia uprawnień oraz integracją z usługą Microsoft Active Directory w zakresie zarządzania dostępem.

14.22. Konsola administracyjna musi zapewniać zaawansowane funkcje zarządzania rekordami, w tym wykonywanie operacji jednocześnie na wielu rekordach oraz dostęp do szczegółowych informacji dotyczących pracy urządzeń.

14.23. Panel pracownika systemu musi uruchamiać się automatycznie i realizować proces autoryzacji w momencie logowania użytkownika do systemu.

14.24. Administrator systemu musi mieć możliwość definiowania zakresu informacji dostępnych w panelu pracownika dla poszczególnych grup użytkowników.

14.25. Panel kierownika musi agregować oraz analizować dane pochodzące z paneli pracowników.

14.26. Informacje prezentowane w panelach muszą być uporządkowane w logiczne sekcje, które administrator może włączać lub wyłączać indywidualnie albo grupowo.

14.27. System musi umożliwiać kompleksowe zarządzanie licencjami w różnych modelach licencyjnych oraz strukturach organizacyjnych, obejmujące audyty licencyjne, zarządzanie oprogramowaniem oraz oprogramowaniem niedozwolonym.

14.28. System musi umożliwiać przypisywanie, rozliczanie oraz ewidencjonowanie różnych typów licencji oraz przechowywać historię zmian licencyjnych.

14.29. System musi zapewniać funkcje inwentaryzacji oprogramowania oraz zdalnej dezinstalacji aplikacji.

14.30. System musi posiadać rozbudowaną bazę wzorców aplikacji i pakietów oprogramowania oraz umożliwiać definiowanie własnych wzorców przez administratora.

14.31. System musi automatycznie importować nowe wzorce aplikacji udostępniane przez producenta.

14.32. System musi dostarczać szczegółowe informacje dotyczące zainstalowanych pakietów oprogramowania oraz ich wykorzystania, w tym informacji o edycjach pakietu Microsoft Office.

14.33. System musi zapewniać zaawansowaną inwentaryzację sprzętu komputerowego realizowaną automatycznie zarówno w sieci lokalnej, jak i w trybie zdalnym.

14.34. Inwentaryzacja sprzętu musi obejmować szczegółowe informacje o komponentach, w tym pamięci RAM, monitorach, dyskach twardych oraz innych elementach konfiguracji.

14.35. System musi umożliwiać ewidencjonowanie zmian konfiguracji sprzętowej oraz identyfikację i klasyfikację urządzeń podłączanych do komputerów wraz z historią ich podłączeń.

14.36. System musi umożliwiać identyfikację oraz zarządzanie środowiskami wirtualizacji Hyper-V oraz VMware, a także urządzeniami sieciowymi.

14.37. System musi być wyposażony w skaner sieci oraz obsługę protokołu SNMP, umożliwiające automatyczne zbieranie danych, analizę jakości połączeń oraz identyfikację urządzeń w sieci.

14.38. System musi umożliwiać zdalną instalację Klientów oraz generowanie map sieci.

14.39. System musi umożliwiać inwentaryzację urządzeń innych niż komputery, w tym drukarek oraz urządzeń sieciowych.

14.40. System musi umożliwiać zarządzanie dokumentacją związaną z urządzeniami, monitorowanie ich przemieszczania oraz przypominanie o terminach gwarancji i umów utrzymaniowych.

14.41. System musi przechowywać historię użycia urządzeń zewnętrznych oraz umożliwiać definiowanie zasad dopuszczania urządzeń USB do użytkowania.

14.42. System musi zapewniać pełne szyfrowanie dysków wewnętrznych oraz zewnętrznych nośników USB z wykorzystaniem mechanizmu BitLocker oraz obsługą algorytmów szyfrowania XTS AES 256, XTS AES 128, AES 256 oraz AES 128.

14.43. System musi umożliwiać zdalne zarządzanie procesem szyfrowania i deszyfrowania dysków, w tym realizację operacji masowych na partycjach systemowych oraz niesystemowych, zarówno w sieci lokalnej, jak i poza siecią NAT.

14.44. Klucze szyfrujące muszą być przechowywane w konsoli administracyjnej systemu w sposób zabezpieczony i dostępne wyłącznie po poprawnym uwierzytelnieniu administratora.

14.45. Proces szyfrowania musi być realizowany w sposób niewidoczny dla użytkownika końcowego i nie może być przez niego przerywany, z wyjątkiem stanów hibernacji lub wyłączenia systemu, po których proces jest automatycznie wznawiany.

14.46. System musi umożliwiać zdalną administrację komputerami, obejmującą automatyczne wykonywanie poleceń systemowych związanych z zarządzaniem aplikacjami, plikami oraz rejestrem systemowym.

14.47. System musi umożliwiać definiowanie i zarządzanie zadaniami cyklicznymi z wykorzystaniem harmonogramu, w tym określanie warunków uruchamiania oraz zakończenia zadań.

14.48. System musi obsługiwać technologię Intel vPro w zakresie zdalnej konfiguracji i zarządzania komputerami.

14.49. System musi umożliwiać zdalne przejęcie kontroli nad komputerem użytkownika z wykorzystaniem technologii Ultra VNC, w tym obsługę wielu jednoczesnych sesji.

14.50. System musi umożliwiać jednoczesne operowanie na wielu pulpitach zdalnych oraz uruchomienie do sześciu sesji Ultra VNC w obrębie jednego ekranu.

14.51. System musi integrować mechanizmy skryptowe wspierane przez algorytmy sztucznej inteligencji w celu automatycznego generowania poleceń administracyjnych.

14.52. System musi umożliwiać tworzenie oraz zarządzanie zadaniami cyklicznymi z różnymi wariantami częstotliwości ich uruchamiania oraz warunkami zakończenia.

14.53. System musi zapewniać zdalne zarządzanie komputerami z wykorzystaniem technologii WebRTC, umożliwiając jednoczesne połączenia z wieloma urządzeniami.

14.54. System musi umożliwiać przejęcie kontroli nad pulpitami, zarządzanie plikami, uruchamianie aplikacji oraz instalację oprogramowania i aktualizacji w ramach sesji WebRTC.

14.55. System musi umożliwiać konfigurację połączeń WebRTC, w tym instalację i konfigurację niezbędnych serwerów oraz portów komunikacyjnych.

14.56. System musi obsługiwać różne tryby przejmowania sesji zdalnych, zarówno z wymaganą zgodą użytkownika, jak i bez jej wymogu.

14.57. System musi umożliwiać nagrywanie sesji zdalnych, wykonywanie zrzutów ekranu oraz zarządzanie historią połączeń.

14.58. System musi umożliwiać dostosowanie parametrów wyświetlania i jakości sesji oraz obsługiwać uruchomienie do dwunastu sesji zdalnych na jednym ekranie.

14.59. System musi umożliwiać wykonywanie zapytań WMI bez konieczności nawiązywania zdalnego połączenia z urządzeniem.

14.60. System musi umożliwiać edycję rejestru systemowego urządzeń bez wykorzystywania zdalnego pulpitu.

14.61. System musi umożliwiać zdalną instalację pakietów MSI oraz plików wykonywalnych EXE z wykorzystaniem mechanizmów WMI oraz usługi Klienta, bez konieczności użycia dodatkowych poświadczeń.

14.62. System musi umożliwiać korzystanie z lokalnych oraz sieciowych repozytoriów instalatorów oraz zarządzanie wersjami aplikacji i ich kategoryzacją.

14.63. System musi umożliwiać tworzenie grup instalacyjnych, definiowanie schematów instalacji oraz automatyzację procesu wdrażania oprogramowania na nowych urządzeniach.

14.64. System musi udostępniać kiosk aplikacji umożliwiający użytkownikom samodzielną instalację zatwierdzonego oprogramowania.

14.65. System musi rejestrować i raportować wszystkie procesy instalacyjne oraz umożliwiać ich przerwanie.

14.66. System musi zapewniać ciągłe monitorowanie stanu aktualizacji systemów operacyjnych oraz komponentów infrastruktury IT.

14.67. System musi identyfikować brakujące poprawki, umożliwiać ich pobieranie, klasyfikację oraz instalację w sposób niezakłócający pracy użytkowników.

14.68. System musi umożliwiać przeprowadzanie aktualizacji zbiorczych oraz indywidualnych oraz zapewniać możliwość szybkiego przywrócenia poprzedniego stanu systemu poprzez odinstalowanie poprawek.

14.69. System musi umożliwiać pomijanie wybranych aktualizacji oraz generować raporty dotyczące stanu aktualizacji i urządzeń wymagających restartu.

14.70. System musi umożliwiać centralne zdalne zarządzanie zaporą sieciową w całej infrastrukturze IT.

14.71. System musi zapewniać monitorowanie stanu zapory w czasie rzeczywistym oraz definiowanie zaawansowanych reguł zapory z poziomu konsoli administracyjnej.

14.72. System musi umożliwiać szybką identyfikację oraz reakcję na potencjalne zagrożenia sieciowe.

14.73. System musi umożliwiać definiowanie harmonogramów dla czynności konserwacyjnych, naprawczych oraz porządkujących, z możliwością określenia częstotliwości ich wykonywania, parametrów wejściowych oraz ręcznego uruchamiania i zatrzymywania zadań.

14.74. System musi posiadać mechanizmy automatyzacji obejmujące wykonywanie kopii zapasowych, identyfikację aplikacji i pakietów, porządkowanie bazy danych oraz usuwanie nadmiarowych lub nieaktualnych danych.

14.75. System musi generować alerty dotyczące zdarzeń istotnych dla infrastruktury IT, w tym pojawienia się nowych komputerów w bazie danych, braków licencyjnych oraz innych zdarzeń krytycznych.

14.76. System musi umożliwiać zarządzanie magazynem IT, w tym obsługę dowolnej liczby magazynów zlokalizowanych w różnych lokalizacjach organizacyjnych.

14.77. System musi obsługiwać dokumenty magazynowe, w szczególności typu PZ, RW, WZ oraz inne dokumenty ewidencyjne, z możliwością ich przeglądania i powiązania z zasobami systemu.

14.78. System musi prowadzić ewidencję materiałów magazynowych zgodnie z zasadą FIFO.

14.79. System musi umożliwiać automatyczne powiązanie dokumentów magazynowych z zasobami IT zarejestrowanymi w systemie.

14.80. Konsola administracyjna systemu musi być wyposażona w repozytorium dokumentów dowolnego typu, umożliwiające dodawanie, przechowywanie oraz wyszukiwanie dokumentów.

14.81. Repozytorium dokumentów musi umożliwiać definiowanie kontenerów logicznych w celu uporządkowania i zarządzania dokumentacją.

14.82. System musi wspierać obsługę kodów kreskowych jedno- i dwuwymiarowych.

14.83. System musi umożliwiać parametryzację kodów kreskowych w zakresie ich rozmiaru oraz atrybutów graficznych.

14.84. System musi umożliwiać podgląd oraz wydruk generowanych kodów kreskowych.

14.85. System musi udostępniać funkcję komunikatora umożliwiającego bezpośrednią wymianę wiadomości pomiędzy administratorem a użytkownikami systemu.

14.86. System musi umożliwiać administratorowi inicjowanie rozmów oraz przechowywać historię konwersacji.

14.87. System musi umożliwiać wysyłanie jednorazowych komunikatów typu ALERT oraz tworzenie szablonów wiadomości wielokrotnego użytku z możliwością określenia czasu ich wygaśnięcia.

14.88. System musi umożliwiać realizację szkoleń pracowników za pomocą komunikatów tekstowych, z możliwością definiowania treści szkoleniowych oraz ich automatycznej dystrybucji.

14.89. System musi umożliwiać eksport oraz import treści systemowych.

14.90. System musi umożliwiać monitorowanie i zarządzanie wydrukami realizowanymi z drukarek lokalnych oraz sieciowych.

14.91. System musi rejestrować szczegółowe informacje dotyczące każdego wydruku, w tym dane umożliwiające kalkulację kosztów na podstawie wbudowanego cennika.

14.92. System musi umożliwiać prognozowanie kosztów drukowania oraz zarządzanie drukarkami według ich statusu oraz poziomu materiałów eksploatacyjnych.

14.93. System musi umożliwiać monitorowanie aktywności użytkowników w Internecie w różnych przeglądarkach, w tym przy wykorzystaniu połączeń szyfrowanych HTTPS.

14.94. System musi rejestrować informacje dotyczące połączeń internetowych, w tym adresy IP oraz czas połączenia.

14.95. System musi umożliwiać analizę treści stron internetowych z wykorzystaniem algorytmów sztucznej inteligencji w celu klasyfikacji i kontroli treści.

14.96. System musi umożliwiać monitorowanie wskazanych serwerów WWW, prezentując informacje o ich dostępności, aktywności oraz czasie odpowiedzi.

14.97. System musi umożliwiać analizę treści stron serwerów WWW oraz graficzną prezentację danych historycznych dotyczących ich działania.

14.98. System musi umożliwiać monitorowanie dzienników zdarzeń komputerów z możliwością definiowania oraz filtrowania zdarzeń według kategorii.

14.99. System musi umożliwiać monitorowanie komunikatów przesyłanych za pomocą protokołu Syslog.

14.100. System musi monitorować pracę komputerów, w tym daty rozpoczęcia i zakończenia pracy oraz logowania użytkowników.

14.101. System musi umożliwiać zdalne monitorowanie sesji połączeń wraz z rejestracją adresów IP oraz danych użytkowników.

14.102. System musi umożliwiać skanowanie oraz monitorowanie uprawnień ACL wraz z generowaniem szczegółowych raportów oraz automatyczną aktualizacją danych.

14.103. System musi integrować monitoring warunków środowiskowych z wykorzystaniem sensorów komunikujących się poprzez protokół SNMP.

14.104. System musi umożliwiać graficzną prezentację danych z sensorów oraz generowanie alertów.

14.105. System musi zapewniać obsługę helpdesku, umożliwiając użytkownikom zgłaszanie problemów oraz administratorom ich obsługę.

14.106. System musi umożliwiać edycję zgłoszeń, nadawanie im priorytetów oraz konfigurację mechanizmów powiadomień.

14.107. System musi posiadać zintegrowane repozytorium CMDB umożliwiające zarządzanie zasobami IT.

14.108. Repozytorium CMDB musi przechowywać szczegółowe informacje o użytkownikach, urządzeniach, licencjach oraz oprogramowaniu wraz z możliwością importu i eksportu danych.

14.109. System musi umożliwiać monitorowanie oraz analizę czasu pracy użytkowników.

14.110. System musi umożliwiać definiowanie grup użytkowników przypisanych do przełożonych oraz prezentować dane o aktywności użytkowników w postaci widżetów oraz danych analitycznych.

14.111. Informacje dotyczące czasu pracy, sesji, aktywności w aplikacjach oraz produktywności muszą być dostępne w panelu pracownika.

14.112. System musi oferować zaawansowane mechanizmy raportowania oraz eksportu danych do formatów xls, csv, html oraz formatów graficznych.

14.113. System musi umożliwiać generowanie raportów wieloparametrycznych z zastosowaniem filtrów oraz obsługę wieloinstancyjności raportowania.

14.114. System musi umożliwiać definiowanie harmonogramów generowania raportów, ich automatyczne wysyłanie oraz zapisywanie w dowolnej lokalizacji, przy czym wynikiem harmonogramu musi być raport w formacie PDF.

14.115. System musi udostępniać rozbudowany interfejs API oparty o REST.

14.116. Interfejs API musi zapewniać szyfrowaną komunikację z wykorzystaniem protokołu TLS 1.3 oraz obsługę złożonych zapytań w formacie JSON.

14.117. System musi umożliwiać zarządzanie kluczami API, przy czym długość klucza musi wynosić co najmniej 32 znaki.

14.118. System musi umożliwiać generowanie powiadomień w konsoli administracyjnej, za pośrednictwem poczty e-mail oraz wiadomości SMS.

14.119. System musi umożliwiać edycję treści powiadomień oraz definiowanie grup odbiorców.

14.120. System musi integrować się z CMD oraz Windows PowerShell w zakresie automatycznego wywoływania zadań.

14.121. System musi zawierać co najmniej 30 predefiniowanych powiadomień oraz umożliwiać ich personalizację.

14.122. System musi umożliwiać definiowanie praw dostępu indywidualnie dla każdego użytkownika oraz dla grup użytkowników.

14.123. Kontrola dostępu musi być konfigurowalna niezależnie dla każdego rodzaju operacji, obejmując co najmniej odczyt, modyfikację, usuwanie oraz eksport danych.

14.124. System musi umożliwiać jednoczesną kontrolę dostępu na poziomie menu aplikacji, typów operacji (takich jak dodawanie, edycja, usuwanie i przeglądanie) oraz struktury organizacyjnej, w tym ograniczanie dostępu administratorów wyłącznie do zasobów przypisanych do określonych jednostek organizacyjnych.

14.125. System musi umożliwiać uwierzytelnianie użytkowników z wykorzystaniem imiennego konta użytkownika oraz hasła.

14.126. System musi umożliwiać uwierzytelnianie administratorów z wykorzystaniem imiennego konta administratora oraz hasła.

14.127. Hasła przechowywane w systemie oraz w bazach danych nie mogą być w żadnym przypadku przechowywane w postaci jawnej.

14.128. System musi obsługiwać jednokrotne uwierzytelnianie użytkowników (Single Sign-On) z wykorzystaniem usługi Microsoft Active Directory.

14.129. System musi obsługiwać jednokrotne uwierzytelnianie użytkowników z wykorzystaniem mechanizmu CAS.

14.130. System musi rejestrować i udostępniać historię korzystania z poszczególnych funkcji systemu przez administratorów.

14.131. System musi umożliwiać definiowanie polityki siły haseł użytkowników, obejmującej parametry takie jak minimalna długość hasła, liczba liter, cyfr, znaków specjalnych, wielkich i małych liter, znaki alfanumeryczne, listy dozwolonych oraz wykluczonych znaków specjalnych.

14.132. System musi zapewniać bezpieczne przechowywanie haseł administratorów w bazie danych z zastosowaniem mechanizmu kodowania Base64 oraz funkcji skrótu SHA-512 z użyciem soli, uwzględniającej login i hasło.

14.133. System musi posiadać wbudowany mechanizm automatycznej synchronizacji czasu pomiędzy agentami a serwerem systemu, przy czym synchronizacja ta nie może wpływać na czas systemowy komputerów, na których zainstalowano agentów.

14.134. System musi umożliwiać automatyczne wykonywanie kopii zapasowych w zdefiniowanych interwałach czasowych, zarówno w formie kopii pełnych, jak i przyrostowych.

14.135. System musi udostępniać informację o rezultacie wykonania operacji tworzenia kopii zapasowych.

14.136. System musi zapewniać pełne logowanie błędów systemowych, logów bezpieczeństwa oraz logów aktywności administratorów.

14.137. System musi umożliwiać przechowywanie oraz eksport logów systemowych i bezpieczeństwa.

14.138. System musi zapewniać mechanizmy gwarantujące integralność, poufność oraz dostępność przechowywanych danych.

14.139. System musi posiadać dokumentację pomocy użytkownika dostępną w języku polskim.

14.140. System musi udostępniać materiały pomocnicze w postaci filmów instruktażowych w języku polskim.

14.141. Wsparcie techniczne dla użytkowników systemu musi być świadczone w języku polskim.

14.142. Pomoc techniczna musi być dostępna w dni robocze w godzinach od 8:00 do 16:00.

15. ROZWIĄZANIE DLP

15.1. Przedmiotem zamówienia jest dostawa wraz z wdrożeniem i opracowaniem polityk ochronnych oprogramowania do zapobiegania wyciekowi danych chronionych (DLP) w środowisku Zamawiającego.

15.2. Do obowiązków Wykonawcy należy dostawa niezbędnego sprzętu w szczególności serwerowego wraz z oprogramowaniem, niezbędnymi licencjami w celu zapewnienia wydajnego działania oprogramowania DLP.

15.3. System musi działać w środowisku Zamawiającego i nie dopuszcza się wysyłki danych poza siedzibę Zamawiającego.

15.4. System musi umożliwiać kontrolę dostępu do urządzeń podłączanych do stacji roboczych, w tym urządzeń magazynujących dane oraz urządzeń komunikacyjnych.

15.5. System musi rejestrować informacje o wszystkich podłączanych urządzeniach oraz prowadzić historię ich użycia.

15.6. System musi wymuszać szyfrowanie plików przenoszonych na pamięci zewnętrzne typu USB.

15.7. System musi umożliwiać blokowanie podłączania nieautoryzowanych urządzeń.

15.8. System musi umożliwiać automatyczne odłączanie nieautoryzowanych urządzeń.

15.9. System musi umożliwiać definiowanie reguł dostępu do urządzeń z uwzględnieniem użytkowników i wyjątków.

15.10. System musi zapobiegać nieautoryzowanemu kopiowaniu danych z urządzeń końcowych.
15.11. System musi monitorować uruchamiane procesy i aplikacje na stacjach roboczych.
15.12. System musi umożliwiać blokowanie uruchamiania nieautoryzowanych aplikacji i procesów.
15.13. System musi monitorować użycie schowka systemowego.
15.14. System musi umożliwiać blokowanie operacji kopiowania danych za pośrednictwem schowka systemowego.
15.15. System musi monitorować próby wykonywania zrzutów ekranu.
15.16. System musi umożliwiać blokowanie wykonywania zrzutów ekranu.
15.17. System musi monitorować operacje wykonywane na plikach, w tym ich tworzenie, otwieranie, modyfikację, kopiowanie i usuwanie.
15.18. System musi umożliwiać blokowanie operacji na plikach, które mogą prowadzić do wycieku danych.
15.19. System musi monitorować przesyłanie danych do usług chmurowych.
15.20. System musi umożliwiać ograniczanie lub blokowanie przesyłania danych do usług chmurowych.
15.21. System musi monitorować komunikację e-mail, w tym treść wiadomości oraz załączniki.
15.22. System musi umożliwiać blokowanie wysyłania wiadomości e-mail lub załączników naruszających polityki DLP.
15.23. System musi realizować identyfikację dokumentów z wykorzystaniem mechanizmu fingerprint.
15.24. System musi umożliwiać automatyczne oznaczanie dokumentów zgodnie z polityką scheduled tagging.
15.25. System musi umożliwiać definiowanie i egzekwowanie polityk DLP obejmujących wszystkie obsługiwane obszary ochrony danych.
15.26. System musi umożliwiać definiowanie wyjątków od polityk DLP dla wybranych użytkowników lub zasobów.
15.27. System musi generować alerty o naruszeniach polityk DLP.
15.28. System musi rejestrować zdarzenia związane z naruszeniami polityk DLP.
15.29. System musi zapewniać monitorowanie działań użytkowników w czasie rzeczywistym w zakresie funkcji DLP.

16. ROZWIĄZANIE OCHRONY XDR

16.1. Przedmiotem zamówienia jest dostawa i wdrożenie systemu typu XDR wraz z niezbędną infrastrukturą sprzętową i przeszkolenie pracowników Zamawiającego.

16.2. Zakres wdrożenia obejmuje kompleksowe działania zmierzające do uruchomienia produkcyjnego w całej infrastrukturze Zamawiającego:

16.2.1. Analizę środowiska IT Zamawiającego w zakresie infrastruktury serwerowej, stacji roboczych, urządzeń mobilnych, sieci, usług chmurowych oraz systemów tożsamości.

16.2.2. Opracowanie architektury logicznej i technicznej Rozwiązania XDR wraz z projektem integracji z istniejącą infrastrukturą bezpieczeństwa.

16.2.3. Dostawę, instalację, konfigurację oraz uruchomienie centralnej platformy XDR.

16.2.4. Wdrożenie agentów bezpieczeństwa na stacjach roboczych, serwerach fizycznych i wirtualnych oraz innych wspieranych punktach końcowych.

16.2.5. Integrację XDR z systemami pocztowymi, systemami katalogowymi, infrastrukturą sieciową, zaporami sieciowymi, usługami VPN, systemami IAM oraz usługami chmurowymi.

16.2.6. Konfigurację mechanizmów detekcji zagrożeń w oparciu o analizę behawioralną, korelację zdarzeń, reguły heurystyczne oraz mechanizmy uczenia maszynowego.

16.2.7. Uruchomienie mechanizmów automatycznej reakcji na incydenty, w tym izolacji stacji roboczej, blokowania kont, zatrzymywania procesów, kwarantanny plików oraz blokowania komunikacji sieciowej.

16.2.8. Konfigurację centralnego gromadzenia, korelacji i analizy logów bezpieczeństwa.

16.2.9. Integrację z systemem SIEM.

16.2.10. Konfigurację dashboardów, raportów operacyjnych i menedżerskich oraz mechanizmów alertowania.

16.2.11. Wdrożenie polityk bezpieczeństwa, profili ochronnych oraz scenariuszy reagowania na incydenty.

16.2.12. Przeprowadzenie testów poprawności działania, testów bezpieczeństwa oraz symulacji incydentów.

16.2.13. Szkolenie administratorów oraz użytkowników technicznych w zakresie obsługi i eksploatacji systemu.

16.2.14. Opracowanie dokumentacji powdrożeniowej, w tym architektury, procedur operacyjnych, procedur reagowania na incydenty oraz zaleceń utrzymaniowych.

16.2.15. Wsparcie powdrożeniowe, stabilizację środowiska oraz asystę przy pierwszych rzeczywistych incydentach bezpieczeństwa.

16.3. Wymaga się, aby dane analizowane przez XDR były przechowywane i przetwarzane wyłącznie na terenie Rzeczypospolitej Polskiej.

16.4. Producent systemu musi posiadać certyfikację SOC 2 type 2 lub równoważną. Za spełniające wymaganie uznaje się także Rozwiązania, systemy zarządzania, certyfikaty lub raporty z audytów, które łącznie spełniają następujące warunki:

16.4.1. Potwierdzają istnienie oraz skuteczne funkcjonowanie systemu kontroli wewnętrznych w obszarze bezpieczeństwa informacji, dostępności, integralności przetwarzania, poufności oraz ochrony danych, w cyklu operacyjnym obejmującym co najmniej 6 miesięcy ciągłego działania.

16.4.2. Obejmują niezależny audyt przeprowadzony przez uprawniony, zewnętrzny podmiot audytorski, potwierdzający zarówno zaprojektowanie, jak i skuteczność działania mechanizmów kontrolnych w czasie.

16.4.3. Zapewniają poziom bezpieczeństwa, dojrzałości procesowej oraz zarządzania ryzykiem nie niższy niż wynikający z raportu SOC 2 Type II.

16.4.4. Są oparte na uznanych międzynarodowych normach, standardach lub ramach referencyjnych w zakresie zarządzania bezpieczeństwem informacji, ciągłości działania, kontroli wewnętrznej i ochrony danych.

16.4.5. Dokumentacja potwierdzająca spełnienie wymagań umożliwia Zamawiającemu jednoznaczną weryfikację zakresu, metodyki oraz wyników audytu.

16.5. Producent musi gwarantować dostępność usługi w ramach SLA co najmniej na poziomie 99,9%.

16.6. System XDR musi posiadać możliwość dynamicznej analizy plików wykonywalnych dla systemów Windows oraz Linux w środowisku sandbox, zintegrowanym z systemem XDR w sposób natywny, objętym tym samym modelem wsparcia technicznego, cyklem aktualizacji oraz odpowiedzialnością producenta za skuteczność analizy i detekcji w ramach całego rozwiązania XDR, przy czym system musi obsługiwać analizę plików o rozmiarze co najmniej 100 MB.

16.7. System musi umożliwiać pobranie raportu z analizy dynamicznej.

16.8. Wymaga się, aby system analizy typu sandbox był realizowany na terenie Rzeczypospolitej Polskiej

16.9. Wymagania dla systemu XDR

16.10. Oprogramowanie musi posiadać:

16.10.1. aktywną ochronę endpointów (stacji końcowych i serwerów) przed działaniem złośliwego oprogramowania i innych technik stosowanych przez cyberprzestępców

16.10.2. detekcję i triage'u zagrożeń z kategorii APT

16.10.3. odpowiedzi na wykryte zdarzenie

16.10.4. realizację threat hunting

16.11. System bezpieczeństwa XDR musi być dostarczony w formie SaaS.

16.12. Dokumentacja systemu musi być publikowana przez producenta na jego ogólnodostępnej (bez potrzeby rejestracji) stronie internetowej w języku polskim lub angielskim.

16.13. System musi obsługiwać następujący rodzaj endpointów w tym:

16.13.1. stacje robocze Windows 10/11 (w tym VDI)

16.13.2. stacje robocze macOS

16.13.3. serwery Linux

16.13.4. serwery Microsoft Server

16.13.5. urządzenia mobilne z Android

16.13.6. urządzenia mobilne z iOS

16.14. System musi przechowywać informacje o alarmach i incydentach co najmniej przez 180 dni.

16.15. System musi przechowywać szczegółowe dane telemetryczne z endpointów zabezpieczonych agentem przez co najmniej 30 dni.

16.16. System musi szyfrować dane w trakcie transmisji i w trakcie przechowywania za pomocą protokołów i algorytmów kryptograficznych uznanych powszechnie za bezpieczne. Dane w trakcie przechowywania muszą być szyfrowane algorytmem AES-256.

16.17. System musi umożliwiać zarządzania przez pojedynczy webowy interfejs graficzny z wykorzystaniem graficznej przeglądarki internetowej oraz przez REST API. Oba dostępne po https (co najmniej TLS 1.2). Nie dopuszcza się, aby webowy interfejs graficzny korzystał z technologii flash, silverlight lub java.

16.18. Wszystkie składniki systemu muszą być konfigurowalne i zarządzane przez jeden spójny interfejs. Nie dopuszcza się, aby składniki systemu posiadały oddzielne pulpity/konsole do zarządzania konkretnymi funkcjami bezpieczeństwa, a dostęp do nich realizowany jest przez pojedyncze logowanie (Single Sign-On).

16.19. Wymagana jest ocena na poziomie min „A+" dla wszystkich serwisów, z których korzysta oferowane rozwiązanie. Ocena będzie weryfikowana przy pomocy ogólnodostępnego narzędzia https://www.ssllabs.com

16.20. System musi posiadać możliwość ograniczenia logowania do systemu tylko ze wskazanych publicznych adresów IP.

16.21. System musi umożliwiać integrację z zewnętrznym katalogiem użytkownik via SAML 2.0 (ze wsparciem dla ADFS) oraz posiadać możliwość definiowania lokalnych użytkowników, których logowanie jest zabezpieczone hasłem oraz dodatkowym czynnikiem uwierzytelniającym w formie tokenu. System jako dodatkową metodę uwierzytelnienia musi wspierać co najmniej tokeny w formie jednorazowych kodów generowanych w aplikacji mobilnej wg. algorytmu Time-based One-Time Password algorithm (ang. TOTP-based). Wymaga się zastosowania Google Authenticator lub Microsoft Authenticator na platformy Android i iOS dla aplikacji mobilnej służącej jako dodatkowa metoda uwierzytelnienia.

16.22. System dla lokalnych kont podczas tworzenia haseł dla kont administracyjnych musi żądać stosowania się do przyjętej polityki, która wymaga ustawienia hasła spełniającego następujące kryteria: co najmniej 11 znaków, musi zawierać małe i duże litery łacińskie, cyfry i znaki specjalne. System musi posiadać mechanizmy blokowania konta po przy najmniej 5 niepoprawnych próbach podania hasła.

16.23. System musi umożliwiać przypisywanie użytkowników do grup użytkowników. Dodatkowo w przypadku użytkowników uwierzytelnionych via SAML 2.0 musi istnieć możliwość zmapowania grup SAML do lokalnie zdefiniowanych grup.

16.24. Każdy użytkownik systemu (administrator, operator, analityk) muszą posiadać indywidualne konta pozwalające na jego jednoznaczną identyfikację

16.25. System musi umożliwiać określenie zakresu dostępu z wykorzystaniem ról i ich przypisanie do użytkownika lub do grupy użytkowników. Rola musi definiować dostęp do określonego obszaru administracyjnego systemu, jego rodzaju (tylko do odczytu, pełen dostęp) oraz jego zakresu (wszystkie lub wybrane endpointy).

16.26. System w ramach roli musi umożliwiać określenie dostępu do co najmniej następujących obszarów:

16.27. Ustawienia systemu

16.28. Zarządzanie endpointami

16.29. Zarządzanie politykami

16.30. Zarządzanie regułami detekcyjnymi

16.31. Zarządzania wykluczeniami
16.32. Zarządzanie incydentami
16.33. Uruchamianie odpowiedzi na incydent
16.34. Nawiązywanie połączenia do linii poleceń
16.35. Uruchamianie skryptów python
16.36. Zarządzanie kwerendami do danych
16.37. Zarządzanie raportami
16.38. Zarządzenie dashboardami/kokpitami
16.39. System musi posiadać możliwość definiowania własnych dopasowanych do potrzeb ról.
16.40. System musi posiadać zestaw predefiniowanych dashboardów informujących co najmniej:
16.41. O liczbie i powadze incydentów
16.42. O liczbie incydentów przypisanych do analityków
16.43. O endpointach z największą liczbą incydentów
16.44. O liczbie agentów z rozbiciem na wersję agenta
16.45. O liczbie agentów z rozbiciem na agentów offline i online
16.46. O liczbie agentów z rozbiciem na wersję aktualizacji podsystemów bezpieczeństwa
16.47. O liczbie agentów z rozbiciem na status ochrony
16.48. System musi umożliwiać tworzenie własnych spersonalizowanych dashboardów z wykorzystaniem predefiniowanych kontrolek/widgetów oraz kontrolek definiowanych samodzielnie poprzez kwerendy do danych telemetrycznych.
16.49. System musi umożliwiać skonfigurowanie okresu, po którym użytkownik zostanie automatycznie wylogowany z systemu oraz możliwość automatycznego zawieszania kont użytkowników, którzy nie logowali się dłużej niż określona liczba dni.
16.50. System musi co najmniej przez 365 dni przechowywać logi audytowe dokumentujące wszystkie akcje podejmowane przez użytkowników zalogowanych do systemu oraz logi audytowe dotyczące funkcjonowania agentów.
16.51. System musi posiadać możliwość eksportu wybranych logów audytowych via syslog po ssl/tls w formacie CEF. W dokumentacji systemu musi być wskazany adres IP lub zakres adresów IP, z których nawiązywane będzie połączenie syslog.

16.52. System musi posiadać możliwość alarmowania o wskazanych zdarzeniach zapisanych w logach audytowych poprzez wysłanie emaila na wskazane skrzynki poczty elektronicznej.

16.53. System musi posiadać możliwość integracji z Microsoft Active Directory w zakresie synchronizacji struktury organizacyjnej katalogu AD zarówno z lokalnym AD jak również z Azure AD na potrzeby automatycznego wzbogacania informacji na temat endpointów i użytkowników oraz tworzenia dynamicznych grup endpointów celem różnicowania konfiguracji agentów.

16.54. System musi posiadać funkcjonalność wykrywania niezarządzanych endpointów w sieci w oparciu o skanowanie obiektów kont komputerów Active Directory.

16.55. System po integracji z Active Directory, musi mieć możliwość wyświetlenia widoku wszystkich komputerów obsługiwanych przez Active Directory Zamawiającego z możliwością filtrowania per OU. Konsola zarządzająca oferowanego Rozwiązania musi wykrywać serwery będące członkami domeny Active Directory, na których nie zainstalowano agenta Systemu EDR. Widok powinien być podzielony na maszyny chronione i nie chronione przez agenta. System co najmniej raz na dobę musi alarmować (co najmniej notyfikacja emailowa i via syslog), jeśli serwery w określonym OU nie są chronione przez agenta.

16.56. System musi posiadać możliwość określenia strefy czasowej wykorzystywanej do reprezentowania znaczników czasowych w interfejsie zarządzania oraz formatu tego znacznika co najmniej w takim zakresie, aby uwidaczniał on strefę czasową.

16.57. System musi posiadać oprogramowanie agenta co najmniej dla następujących systemów operacyjnych:

16.57.1. Windows 8, 10 i 11 (włącznie ze środowiskiem Persistent oraz Non-Persistent VDI)

16.57.2. Windows Server 2012 R2, 2016 standard i core, 2019 standard i core oraz 2022,

16.57.3. Linux

16.57.4. Red Hat Enterprise Linux 7, 8 i 9

16.57.5. Rocky Linux 8 i 9

16.57.6. SUSE Linux Enterprise Server 11, 12 i 15

16.57.7. Ubuntu 18.04 LTS, 20.04 LTS, 22.04 LTS, 24.04 LTS

16.57.8. Oracle Linux 6, 7, 8 i 9

16.57.9. CentOS 6,7, 8 i 9

16.57.10. Debian 9, 10, 11 i 12

16.57.11. Talos Linux 1.44, 1.83

16.57.12. macOS 11.x, 12.x i 13.x, 14.x, 15.x

16.57.13. Kubernetes

16.57.14. Android 10,11, 12, 13, 14, 15 i najnowsze

16.57.15. iOS 15.x i 16.x i najnowsze

16.58. System musi umożliwiać wygenerowanie i pobranie pakietu instalacyjnego:

16.58.1. W formacie msi dla systemów Windows

16.58.2. W formacie rpm, deb i sh dla systemów Linux

16.58.3. W formacie dpkg dla systemów macOS

16.58.4. W formacie helm dla klastrów kubernetes

16.59. Pakiet instalacyjny agenta dla systemów Windows, macOS, Linux i klastrów kubernetes musi posiadać możliwość:

16.59.1. Przypisanie do endpointa nieusuwalnego znacznika, który może być wykorzystany do tworzenia dynamicznych grup endpointów i określenia zakresu dostępu jaki posiada rola użytkownika.

16.59.2. Skonfigurowania komponentu pośredniczącego w komunikacji z systemem

16.59.3. Wyłączenia opcji wykonywania skryptów python

16.59.4. Wyłączenia opcji pobierania plików

16.59.5. Wyłączenia opcji dostępu do linii poleceń

16.60. Pakiet instalacyjny agenta dla systemów Windows musi posiadać możliwość wskazania lokalnej kopii aktualizacji podsystemów bezpieczeństwa.

16.61. Instalacja agenta i jego aktywacja w systemie nie może wymagać restartu systemu operacyjnego

16.62. Komunikacja pomiędzy agentem a systemem musi być zabezpieczona z wykorzystaniem https (co najmniej TLS 1.2) i w zależności od konfiguracji być realizowana w sposób bezpośredni lub pośredni via dedykowany komponent pośredniczący (dalej proxy) tego samego producenta, który:

16.62.1. musi umożliwiać uruchomienie w formie maszyny wirtualnej

16.62.2. musi obsługiwać funkcję proxy chaining dla http z uwierzytelnieniem

16.62.3. musi umożliwiać cache'owanie aktualizacji oprogramowania agenta i aktualizacji podsystemów bezpieczeństwa agenta

16.63. Komunikacja pomiędzy proxy a systemem musi być zabezpieczona z wykorzystaniem https (co najmniej TLS 1.2). Proxy musi posiadać możliwość manualnej lub automatycznej aktualizacji. System musi umożliwiać centralne zarządzanie ustawieniami proxy.

16.64. System musi obsługiwać co najmniej 3 proxy.

16.65. W dokumentacji systemu muszą być wskazane publiczne adresy IP oraz adresy URL niezbędne do zapewnienia poprawnej komunikacji między agentami i systemem oraz pomiędzy proxy a systemem. Komunikacja musi być zawsze nawiązywana w kierunku od agenta/proxy do systemu.

16.66. System musi posiadać możliwość skonfigurowania manualnej i automatycznej aktualizacji agenta dla wskazanych grup endpointów. Polityka automatycznej konfiguracji agenta musi umożliwiać określenie:

16.66.1. Dnia tygodnia i zakresu czasu, w którym wykonywana jest aktualizacja

16.66.2. Maksymalnej liczby równolegle aktualizowanych agentów

16.66.3. Zakresu: tylko minor release, tylko minor release w ramach wskazanego major release, najnowszy major. minor release, najnowszy przedostatni major. minor release

16.66.4. Opóźnienie aktualizacji o wskazaną liczbę dni od publikacji nowego release

16.66.5. Źródła: bezpośrednio z systemu, z komponentu pośredniczącego, peer-to-peer

16.67. System musi posiadać możliwość skonfigurowania manualnej i automatycznej różnicowej aktualizacji podsystemów bezpieczeństwa agenta dla wskazanych grup endpointów. Polityka automatycznej aktualizacji podsystemów bezpieczeństwa musi umożliwiać określenie:

16.67.1. Zakresu: tylko major release, najnowszy major. minor release

16.67.2. Opóźnienie aktualizacji o wskazaną liczbę dni od publikacji nowego release

16.67.3. Źródła: bezpośrednio z systemu, z komponentu pośredniczącego, peer-to-peer

16.67.4. Globalnego limitu na wykorzystanie pasma przy bezpośrednim pobieraniu z systemu

16.67.5. System musi umożliwiać alarmowanie w przypadku, gdy:

16.67.6. Podsystemy bezpieczeństwa agenta nie będą funkcjonowały poprawnie

16.67.7. Agent zostanie odinstalowany

16.67.8. Agent nie zgłosi się od systemu a równocześnie endpoint zaloguje się w domenie Active Directory (dotyczy systemów Windows)

16.68. System musi umożliwiać różnicowanie konfiguracji agenta i podsystemów bezpieczeństwa poprzez przypisanie różnych profili konfiguracyjnych do wybranych grup endpointów lub pojedynczych endpointów.

16.69. Wszystkie dane telemetryczne muszą być przechowywane przez system w centralnym i przeszukiwanym repozytorium danych.

16.70. System musi umożliwiać przeszukiwanie danych telemetrycznych przy pomocy kreatorów lub manualnie z wykorzystaniem kwerend. Kwerendy muszą

umożliwiać łączenie danych telemetrycznych z różnych źródeł, ich filtrowanie i przekształcanie wyników. Reguły tworzenia kwerend muszą być opisane w ogólnodostępnej (bez potrzeby rejestracji) dokumentacji systemu.

16.71. System musi umożliwiać zapisanie kwerendy do danych telemetrycznych do prywatnej biblioteki kwerend danego użytkownika lub do globalnej biblioteki kwerend dostępnej dla wszystkich innych użytkowników.

16.72. System musi umożliwiać zrealizowanie kwerendy do danych telemetrycznych i odczytanie jej wyników via REST API.

16.73. System musi umożliwiać eksport wyników kwerendy do danych telemetrycznych w formie pliku tekstowego.

16.74. System musi umożliwiać uruchamianie kwerendy cyklicznie zgodnie z podanym harmonogramem lub jeden raz o określonym czasie.

16.75. System musi umożliwiać wizualizację wyników kwerendy do danych telemetrycznych w formie tabelarycznej i w formie wykresu: liniowego, słupkowego i kołowego.

16.76. System musi umożliwiać wykorzystanie wyników kwerendy do tworzenia periodycznie generowanych raportów.

16.77. System musi umożliwiać wykorzystanie wyników kwerend do wizualizacji danych w dashboardach.

16.78. System musi umożliwiać przekształcenie kwerendy do danych telemetrycznych w uruchamianą zgodnie z zadanym harmonogramem regułę korelacyjną generującą alarmy, jeśli kwerenda zwróciła jakiekolwiek rekordy.

16.79. System musi umożliwiać analitykowi pobieranie plików z urządzenia końcowego za pośrednictwem agenta, z poziomu centralnej konsoli. Pliki pobierane w ten sposób muszą być zabezpieczane hasłem.

16.80. System musi umożliwiać definiowanie atomowych wskaźników kompromitacji w formie: SHA256, nazwy domenowej, adresu IPv4, adresu IPv6, ścieżki, nazwy pliku. Musi istnieć możliwość dodania znacznika ręcznie, zaimportowania znaczników z pliku i via REST API oraz oznaczenia reputacji, wiarygodności i okresu wygaśnięcia znacznika.

16.81. System musi umożliwiać definiowanie złożonych wskaźników kompromitacji opisujących zachowanie procesu co najmniej w zakresie: operacji plikowych, uruchamianych procesów i ich parametrów, operacji sieciowych i operacji na rejestrze (tylko Windows).

16.82. System dla każdego wprowadzonego atomowego i złożonego wskaźnika kompromitacji musi wygenerować alarm(-y):

16.82.1. jeśli znacznik został odszukany w historycznych danych telemetrycznych (zgromadzonych przed dodaniem wskaźnika)

16.82.2. jeśli znacznik zostanie odszukany w nowych danych telemetrycznych

16.83. System musi umożliwiać przekształcanie złożonych wskaźników kompromitacji w reguły prewencyjne co najmniej dla agenta dla Windows, macOS i Linux.

16.84. System musi umożliwiać integrację z VirusTotal.

16.85. System musi umożliwiać globalne blokowanie uruchamiania/ładowania plików binarnych o określonych SHA256.

16.86. System musi umożliwiać tworzenie, edytowanie oraz uruchamianie playbooków – wysokopoziomowych mechanizmów automatyzacji, które koordynują wykonywanie wielu zadań i akcji w ramach zdefiniowanego przepływu pracy. Playbooki muszą wspierać realizację ciągów operacji zawierających m.in.: zadania, warunki, automatyzacje, polecenia oraz pętle logiczne. Celem stosowania playbooków musi być zwiększenie efektywności oraz przyspieszenie procesu analizy i reakcji na incydenty.

16.87. System musi umożliwiać tworzenie i uruchamianie skryptów wykonujących określone akcje w ramach automatyzacji. Skrypty muszą umożliwiać wykorzystanie poleceń integracyjnych (integration commands), które mogą być wykorzystywane zarówno w zadaniach playbooków, jak i podczas ręcznego uruchamiania automatyzacji w konsoli operacyjnej systemu (War Room)

16.88. System musi udostępniać środowisko testowe typu Playground, które umożliwia bezpieczne testowanie oraz rozwój automatyzacji bez wpływu na środowisko produkcyjne. Playground musi pozwalać na uruchamianie poleceń oraz testowanie ich działania w izolowanym środowisku, a wyniki tych poleceń muszą być prezentowane w ustrukturyzowanym formacie JSON. Format ten musi umożliwiać łatwą analizę, udostępnianie wyników oraz ich integrację z innymi elementami przepływu pracy.

16.89. System musi zapewniać możliwość instalacji silnika integracyjnego wykorzystywanego w playbookach w co najmniej następujących formatach instalacyjnych: a) Shell c) Pakiet DEB d) Pakiet RPM e) ZIP

16.90. System w ramach odpowiedzi na incydent musi umożliwiać:

16.90.1. Remediację ze wskazaniem kroków, które mogą być podjęte automatycznie i kroków, które należy zrealizować manualnie. Musi istnieć możliwość wyboru kroków remediacyjnych, które zostaną wykonane automatycznie.

16.90.2. Uruchomienie skryptu python na endpointcie.

16.90.3. Nawiązanie interaktywnego połączenia do linii poleceń na endpoitcie.

16.90.4. Wstrzymanie procesu na endpointcie.

16.90.5. Wyłączenie procesu na endpointcie.

16.90.6. Izolację sieciową endpointa.

16.90.7. Dodanie adresu IP do listy publikowanej po https z uwierzytelnieniem w celu integracji z firewallami i innymi systemami bezpieczeństwa.

16.90.8. Dodanie nazwy domenowej do publikowanej po https z uwierzytelnieniem w celu integracji z firewallami i innymi systemami bezpieczeństwa.

16.90.9. Zmianę w rejestrze (tylko systemy Windows).

16.90.10. Usunięcie pliku na endointcie.

16.90.11. Przeniesienie pliku na endpointcie do kwarantanny.

16.90.12. Wyszukanie pliku na innych endpointach.

16.90.13. Zrzucenie pamięci procesu na endpointcie.

16.91. System musi obsługiwać co najmniej następujące poziomy krytyczności alarmów: informacyjny, niski, średni, wysoki i krytyczny.

16.92. System musi automatycznie grupować powiązane alarmy w celu przyspieszenia i ułatwienia triażu i analizy incydentu.

16.93. W ramach incydentu system musi grupować:

16.93.1. powiązanych z incydentem użytkowników

16.93.2. Endpointy

16.93.3. Pliki

16.93.4. Domeny

16.93.5. Adresy IP

16.94. System dla alarmów zgrupowanych w ramach incydentu musi automatycznie tworzyć łańcuchy przyczynowo skutkowe reprezentujące zależności pomiędzy procesami wykorzystywanymi w trakcie ataku i powiązane dane telemetryczne, tak aby analityk mógł w łatwy sposób przeanalizować wykorzystywane techniki, określić zakres ataku, ustalić potencjalny cel ataku i zweryfikować, czy cel został osiągnięty.

16.95. System musi umożliwiać wgląd w raport z sandbox dla plików powiązanych z incydentem i eksport raportu.

16.96. System musi umożliwiać zarządzanie incydentami co najmniej w następującym zakresie:

16.96.1. Przypisanie incydentu do analityka

16.96.2. Zmianę stanu incydentu: badany, false positives, true positive, duplikat, testy

16.96.3. Dodawanie notatek

16.96.4. Komunikacja z innymi analitykami

16.96.5. Raportowanie czasu MTTR

16.97. System musi mapować alarmy do matrycy technik i taktyk MITRE ATT&CK.

16.98. System musi umożliwić szyfrowanie danych przechowywanych w chmurowym repozytorium typu Data Lake przy użyciu kluczy szyfrujących dostarczonych i zarządzanych przez Zamawiającego (BYOK – Bring Your Own Key). Dostawca systemu nie może mieć dostępu do klucza szyfrującego Zamawiającego. Rozwiązanie musi umożliwiać Zamawiającemu pełną kontrolę nad generowaniem, rotacją oraz odwołaniem klucza szyfrującego.

16.99. System musi wskazywać natywną integrację (bez potrzeby stosowania zewnętrznych pośredników, skryptów lub dodatkowych narzędzi) z co najmniej następującymi systemami i usługami zewnętrznymi:

16.99.1. Atlassian Jira,

16.99.2. ServiceNow (w tym moduły: IAM oraz CMDB),

16.99.3. Microsoft Teams,

16.99.4. Microsoft Teams Management,

16.99.5. Microsoft Teams poprzez Webhook,

16.99.6. Slack IAM.

16.100. System musi oferować moduł zarządzania podatnościami, który zapewnia wgląd w podatności na punktach końcowych Linux i Windows, wraz z informacjami o poziomie ich istotności zgodnie z bazą danych NIST CVE.

16.101. System musi umożliwiać pełną inwentaryzację hostów, prezentując szczegółowe informacje o aplikacjach, usługach, sterownikach, autoruns, użytkownikach, grupach, udziałach oraz dyskach, co pozwala na szybkie identyfikowanie luk w zabezpieczeniach i przyspieszenie dochodzeń.

16.102. System musi zapewniać bazę wykrywanych podatności obejmującą co najmniej 280 000 unikalnych wpisów

16.103. System musi umożliwiać prezentację informacji o podatnościach (CVE), również w przypadkach, gdy dana podatność nie posiada przypisanego wyniku CVSS

16.104. Nie może wykorzystywać Oracle Java JRE/JDK.

16.105. System XDR musi umożliwiać korzystanie z wersji agenta, która posiada zapewnione wsparcie techniczne i aktualizacje treści przez okres co najmniej 24 miesięcy od momentu jej wydania.

16.106. Wymagania dla agenta:

16.107. Musi posiadać możliwość pobierania aktualizacji agenta i aktualizacji podsystemów bezpieczeństwa:

16.107.1. Bezpośrednio z systemu

16.107.2. Z komponentu pośredniczącego

16.107.3. Od innych endpointów w tej samej podsieci (peer-to-peer)

16.108. Musi posiadać mechanizm ochronny przed nieautoryzowanymi próbami wyłączenia agenta nawet przez użytkowników z uprawnieniami administratora. Wyłączenie podsystemów bezpieczeństwa i odinstalowanie agenta musi wymagać podania hasła, które może być skonfigurowane per grupa endpointów lub indywidualnie dla danego endpointa po stronie systemu. Nie dopuszcza się Rozwiązań, w których hasło jest statyczne i podawana w trakcie uruchamiania instalatora. Operacja deinstalacji agenta i wyłączenia podsystemów bezpieczeństwa musi zostać zapisana w dzienniku audytowym systemu.

16.109. Musi być procesem chronionym w trybie PPL dla oprogramowanie antymalware.

16.110. Musi posiadać sterownik ELAM (Early Launch Anti-Malware).

16.111. Musi umożliwiać:

16.111.1. Ukrycie ikony agenta w zasobniku systemowym

16.111.2. Wyłączenie powiadomień o zablokowanych zagrożeniach

16.111.3. Wyłączenie powiadomień o załączeniu i wyłączeniu izolacji sieciowej

16.111.4. Wyłączenie powiadomień o nawiązaniu zdalnego połączenia konsolowego

16.111.5. Spolszczenie komunikatów powiadomień

16.111.6. Zarządzanie host firewallem endpointa z wykorzystaniem Windows Filtering Platform

16.111.7. Kontrolę urządzeń pamięci masowej na porcie USB w zakresie dopuszczenia dostępu do pamięci, dostępu w trybie tylko do odczytu i pełnego dostępu

16.112. Weryfikację stanu szyfrowania dysków

16.113. Musi posiadać wbudowany runtime python 3.7 lub nowszy i możliwość uruchamiania wbudownych i własnych skryptów python z wykorzystaniem co najmniej następujących bibliotek: argparse, asyncio, base64, browserhistory, certifi, collections, contextlib, csv, ctypes, datetime, enum, fnmatch, functools, glob, globmatch, gzip, hashlib, icmplib, importlib, io, json, LnkParse3, locale,

logging, multiprocessing, netifaces, os, pathlib, pefile, platform, pprint, protobuf, psutil, pysftp, python_hosts, pythoncom, pytsk3, pywintypes, queue, random, re, Registry, requests, runpy, setuptools, shlex, shutil, signal, socket, sqlite_utils, sqlite3, ssl, stat, struct, subprocess, sys, threading, time, traceback, types, unicodecsv, uuid, websocket, win32api, win32com, win32con, win32evtlog, win32evtlogutil, win32file, win32net, win32netcon, win32process, win32security, win32service, win32serviceutil, win32timezone, winapps, winerror, winreg, wmi, xml, xmljson, yara, zipfile, zlib.

16.114. Musi posiadać możliwość wyszukania plików we wskazanej ścieżce przy pomocy filtrów yara.

16.115. Musi posiadać możliwość zrzucenia pamięci wskazanego procesu.

16.116. Musi integrować się z Windows Security Center.

16.117. System musi zapewniać gotowy do użycia mechanizm ochrony plików w trakcie zapisu (On-write File Protection) dla systemów operacyjnych Microsoft Windows. Mechanizm ten musi monitorować operacje zapisu plików i automatycznie podejmować działania w przypadku wykrycia plików złośliwych lub potencjalnie niebezpiecznych.

16.118. System musi zapewniać ochronę przed złośliwymi plikami typu ASP oraz ASPX

16.119. System musi umożliwiać zwiększenie bezpieczeństwa komunikacji pomiędzy agentem a systemem poprzez wymuszenie wykorzystania głównego urzędu certyfikacji (CA) dostarczanego przez producenta systemu. Certyfikat CA musi być wykorzystywany do uwierzytelniania oraz szyfrowania komunikacji agenta z systemem.

16.120. Musi posiadać możliwość blokowania uruchamiania programów z zewnętrznej pamięci masowej podłączonej na porcie USB i z napędów optycznych.

16.121. Musi posiadać możliwość blokowania uruchamiania programów ze wskazanych lokalizacji w systemie plików.

16.122. Musi posiadać możliwość blokowania uruchamiania programów z zasobów sieciowych poza wybranymi ścieżkami.

16.123. Do kolekcji danych telemetrycznych musi używać sterownika lub sterowników (działać w jądrze systemu operacyjnego).

16.124. Musi wykonywać:

16.125. monitoring zdarzeń w trybie kernela, aby uniemożliwić usunięcie hooków z poziomu programów działających w trybie użytkownika, co najmniej w następującym zakresie:

16.125.1. Pobieranie informacji o procesach (tworzenie procesu i otwieranie handlerów)
16.125.2. Pobieranie informacji o wątkach (tworzenie wątku i otwieranie handlerów)
16.125.3. Pobieranie informacji o ładowaniu bibliotek dll
16.125.4. Pobieranie informacji o próbach dostępu do rejestru
16.125.5. Pobieranie informacji o operacjach na systemie plików.
16.125.6. monitoring co najmniej następujących funkcje NT API:
16.125.7. VirtualAlloc i VirtualAllocEx
16.125.8. VirtualProtect i VirtualProtectEx
16.125.9. CreateThread, CreateRemoteThread i CreateRemoteThreadEx
16.125.10. NtAllocateVirtualMemory i ZwAllocateVirtualMemory
16.125.11. NtCreateThread, NtCreateThreadEx, ZwCreateThread i ZwCreateTheadEx
16.125.12. NtProtectVirtualMemory i ZwProtectVirtualMemory
16.125.13. NtSetInformationProcess i ZwSetInformationProcess
16.125.14. Monitoring zdarzeń ETW-TI (Event Tracing for Windows - Threat Intelligence) poprzez subskrypcję na zdarzenia Microsoft-Windows-Threat-Intelligence.
16.126. Musi zbierać co najmniej następujące dane telemetryczne:
16.126.1. Utworzenie nowego procesu i zakończenie procesu
16.126.2. Wszystkie operacje na plikach: tworzenie, zapisywanie, kasowanie, zmiana nazwy, przesunięcie, modyfikacja, link symboliczny
16.126.3. Ładowanie bibliotek DLL
16.126.4. Wstrzykiwanie do procesu
16.126.5. Wszystkie operacje na socketach sieciowych dla TCP i UDP: accept, connect, create, listen, close, bind
16.126.6. Statystyki połączeń sieciowych
16.126.7. Praca z rejestrem: skasowanie wartości, ustawienie wartości, utworzenie klucza, kasowanie klucza, zmiana nazwy klucza
16.126.8. Wywołania RPC (atrybuty: action_rpc_interface_uuid, action_rpc_interface_version_major, action_rpc_interface_version_minor, action_rpc_func_opnum, action_rpc_func_str_call_fields, action_rpc_func_int_call_fields,action_rpc_interface_name, action_rpc_func_name)
16.126.9. Wywołania systemowe (atrybuty: action_syscall_string_params, action_syscall_int_params, action_syscall_target_instance_id, action_syscall_target_image_path, action_syscall_target_image_name, action_syscall_target_os_pid, Action_syscall_target_thread_id, address_mapping)

16.126.10. Windows Event Log:

16.126.11. Security:

16.126.12. Successful logon (4624), Failed logon (4625), Logoff (4634), User initiated logoff (4647), Logon attempted, explicit credentials (4648), Replay attack (4649), Special privileges attempted login (4672), Kerberos TGT request (4768), Kerberos service ticket requested (4769), Kerberos service ticket renewal (4770), Kerberos pre-authentication failed (4771), Domain controller validation attempt (4776), Session was reconnected to a Windows station (4778), Workstation locked (4800), Workstation unlocked (4801), Screensaver was invoked (4802), Screensaver was dismissed (4803), A user account was created (4720), A user account was enabled (4722), An attempt was made to change an account's password (4723), An attempt was made to reset an account's password (4724), A user account was disabled (4725), A user account was deleted (4726), Group creations (4727, 4731, 4754), Group member additions (4728, 4732, 4756), Group member removals (4729, 4733, 4757), Group changes (4735, 4737, 4755, 4764), A user account was changed (4738), A user account was locked out (4740), A computer account was created (4741), A computer account was changed (4742), A computer account was deleted (4743), SID history (4765, 4766), A user account was unlocked (4767), ACL set on accounts (4780), Group membership enumeration (4799), System time was changed (4616), Kerberos service ticket was denied (4821), NTLM authentication failed (4822, 4823), Kerberos pre-authentication failed (4824), User denied access to Remote Desktop (4825), Key file operation (5058), Key migration operation (5059), A scheduled task was created (4698), A scheduled task was updated (4702), Certificate Services received a certificate request (4886), Certificate Services approved a certificate request (4887), A Certificate Services template was updated (4899), Certificate Services template security was updated (4900), A network share object was accessed (5140), Security Log cleared events (1102), CA Service Stopped (4880), CA Service Started (4881), CA DB row(s) deleted (4896), CA Template loaded (4898), Kerberos policy was changed (4713)

16.126.13. Microsoft-Windows-DNS-Client/Operational: DNS Query Completed (3008) without local machine name resolution events and without empty name resolution events

16.126.14. Microsoft-Windows-PowerShell/Operational: PowerShell executes block activity (4103), Remote Command (4104), Start Command (4105), Stop Command (4106)

16.127. Musi wysyłać zgromadzone dane telemetryczny do systemu nie rzadziej niż co 5 minut, przy czym wymagane jest, aby agent posiadał możliwość wymuszenia wysłania danych telemetrycznych na żądanie. Jeśli z powodu braku łączności sieciowej agent nie może wysłać danych telemetrycznych, to dane telemetryczne muszą zostać lokalnie przechowane (zcache'owane) i wysłane do systemu po przywróceniu łączności sieciowej.

16.128. Musi zapewniać ochronę przed znanymi i nieznanymi exploitami wykorzystującymi znane i nieznane luki bezpieczeństwa w oprogramowaniu poprzez wykrywanie prób wykorzystania co najmniej następujących technika eksploitacji:

16.128.1. Przekierowanie APC

16.128.2. Obejście Data Execution Prevention

16.128.3. DLL Hijacking

16.128.4. Exploit Kit Fingerprinting

16.128.5. JIT

16.128.6. Null Dereference

16.128.7. ROP

16.128.8. Structures exception handler hijackings

16.128.9. Heap Spray

16.128.10. Kernel Privilege Escalation

16.129. Musi zapewnić ochronę przed znanymi i nieznanymi złośliwymi plikami binarnymi umożliwiając skonfigurowanie co najmniej następujących mechanizmów:

16.129.1. Weryfikacja sha256 w bazie threat intelligence producenta systemu

16.129.2. Analiza dynamiczna w sandboxie chmurowym producenta systemu (nie dopuszcza się uruchomienia funkcji sandbox bezpośrednio na chronionym endpontcie)

16.129.3. Lokalna analiza statyczna

16.129.4. Weryfikacja podpisu pliku binarnego

16.129.5. Przeniesienie pliku binarnego do kwarantanny

16.129.6. Zablokowanie uruchomienia/załadowania złośliwego pliku binarnego

16.129.7. Zablokowanie uruchomienia pliku z przenośnej pamięci masowej USB

16.129.8. Zablokowanie uruchomienia pliku z innych lokalizacji sieciowych niż wskazane

16.129.9. Weryfikację i wykrycie groźnego zachowania procesu powstałego w wyniku uruchomienia/załadowania pliku binarnego

16.129.10. Wykrywanie shellcodu'u ładowanego do pamięci

16.129.11. Wykrycie i przerwanie próby szyfrowania plików na dysku (ochrona przeciw ransomware).

16.129.12. Musi wykrywać i blokować próbę wyłączenia Volume Shadow Copy Service (VSS).

16.130. Musi zapewnić ochronę przed znanymi i nieznanymi złośliwymi makrami co najmniej w plikach Microsoft Word i Microsoft Excel umożliwiając skonfigurowanie co najmniej następujące mechanizmy:

16.130.1. Weryfikacja sha256 w bazie threat intelligence producenta systemu

16.130.2. Analiza dynamiczna w sandboxie chmurowym producenta systemu (nie dopuszcza się uruchomienia funkcji sandbox bezpośrednio na chronionym endpontcie)

16.130.3. Lokalna analiza statyczna

16.131. Musi zapewnić ochronę przed atakami wykorzystującymi legalne narzędzia systemowe w groźny sposób poprzez analizę złożonych łańcuchów przyczynowo skutkowych i wykrywanie technik i taktyk stosowanych przez cyberprzestępców.

16.132. Musi umożliwiać zablokowanie całego ruchu sieciowego (izolacji sieciowej) poza połączeniem do systemu.

16.133. Musi posiadać możliwość manualnego wyłączenia izolacji sieciowej w przypadku, gdy agent utracił łączność z systemem. Wyłączenie izolacji sieciowej musi być zabezpieczone hasłem. Każdy endpoint musi posiadać własne hasło, tak aby można było je podać bezpiecznie użytkownikowi bez obawy, że inni użytkownicy zaczną wyłączać agenta. Hasło musi być automatycznie rotowane przez system nie rzadziej niż co dwa tygodnie.

16.134. System XDR musi umożliwiać ręczne (ad hoc) uruchamianie skanów bezpieczeństwa na wybranych punktach końcowych lub grupach urządzeń, niezależnie od zaplanowanego harmonogramu skanowania. Skan ad hoc musi być możliwy do uruchomienia z poziomu konsoli zarządzającej, zdalnie, bez konieczności fizycznego dostępu do urządzenia.

16.135. Agent dla systemów macOS

16.136. Musi posiadać możliwość pobierania aktualizacji agenta i aktualizacji podsystemów bezpieczeństwa:

16.136.1. Bezpośrednio z systemu

16.136.2. Z komponentu pośredniczącego

16.136.3. Od innych endpointów w tej samej podsieci (peer-to-peer)

16.137. Musi posiadać mechanizm ochronny przed nieautoryzowanymi próbami wyłączenia agenta nawet przez użytkowników z uprawnieniami administratora. Wyłączenie podsystemów bezpieczeństwa i odinstalowanie agenta musi

wymagać podania hasła, które może być skonfigurowane per grupa endpointów lub indywidualnie dla danego endpointa po stronie systemu. Nie dopuszcza się Rozwiązań, w których hasło jest statyczne i podawana w trakcie uruchamiania instalatora. Operacja deinstalacji agenta i wyłączenia podsystemów bezpieczeństwa musi zostać zapisana w dzienniku audytowym systemu.

16.138. Musi umożliwiać:

16.138.1. Ukrycie ikony agenta w zasobniku systemowym

16.138.2. Wyłączenie powiadomień o zablokowanych zagrożeniach

16.138.3. Wyłączenie powiadomień o załączeniu i wyłączeniu izolacji sieciowej

16.138.4. Wyłączenie powiadomień o nawiązaniu zdalnego połączenia konsolowego

16.138.5. Spolszczenie komunikatów powiadomień

16.138.6. Zarządzanie host firewallem endpointa

16.138.7. Kontrolę urządzeń pamięci masowej na porcie USB w zakresie dopuszczenia dostępu do pamięci, dostępu w trybie tylko do odczytu i pełnego dostępu

16.138.8. Weryfikację stanu szyfrowania dysków

16.139. Musi posiadać wbudowany runtime python 3.7 lub nowszy i możliwość uruchamiania wbudownych i własnych skryptów python z wykorzystaniem co najmniej następujących bibliotek: argparse, asyncio, base64, browserhistory, certifi, collections, contextlib, csv, ctypes, datetime, enum, fnmatch, functools, glob, globmatch, gzip, hashlib, icmplib, importlib, io, json, LnkParse3, locale, logging, multiprocessing, netifaces, os, pathlib, pefile, platform, pprint, protobuf, psutil, pysftp, python_hosts, pythoncom, pytsk3, pywintypes, queue, random, re, Registry, requests, runpy, setuptools, shlex, shutil, signal, socket, sqlite_utils, sqlite3, ssl, stat, struct, subprocess, sys, threading, time, traceback, types, unicodecsv, uuid, websocket, win32api, win32com, win32con, win32evtlog, win32evtlogutil, win32file, win32net, win32netcon, win32process, win32security, win32service, win32serviceutil, win32timezone, winapps, winerror, winreg, wmi, xml, xmljson, yara, zipfile, zlib

16.140. Musi posiadać możliwość wyszukania plików we wskazanej ścieżce przy pomocy filtrów yara.

16.141. Musi posiadać możliwość zrzucenia pamięci wskazanego procesu.

16.142. Musi zbierać co najmniej następujące dane telemetryczne:

16.143. Utworzenie nowego procesu i zakończenie procesu

16.144. Wszystkie operacje na plikach: tworzenie, zapisywanie, kasowanie, zmiana nazwy, przesunięcie, otwarcie

16.145. Wszystkie operacje na socketach sieciowych dla TCP i UDP: accept, connect, connect failure, disconnect, listen.

16.146. Statystyki połączeń sieciowych.

16.147. Zdarzenia z event logu dotyczącego uwierzytelnienia.

16.148. Musi wysyłać zgromadzone dane telemetryczny do systemu nie rzadziej niż co 5 minut, przy czym wymagane jest, aby agent posiadał możliwość wymuszenia wysłania danych telemetrycznych na żądanie. Jeśli z powodu braku łączności sieciowej agent nie może wysłać danych telemetrycznych, to dane telemetryczne muszą zostać lokalnie przechowane (zcache'owane) i wysłane do systemu po przywróceniu łączności sieciowej.

16.149. Musi zapewniać ochronę przed znanymi i nieznanymi exploitami wykorzystującymi znane i nieznane luki bezpieczeństwa w oprogramowaniu poprzez wykrywanie prób wykorzystania co najmniej następujących technika eksploitacji:

16.149.1. Dylib Hijacking

16.149.2. JIT

16.149.3. ROP

16.150. Musi zapewnić ochronę przed znanymi i nieznanymi złośliwymi plikami binarnymi wykorzystując co najmniej następujące mechanizmy:

16.150.1. Weryfikacja sha256 w bazie threat intelligence producenta systemu

16.150.2. Analiza dynamiczna w sandboxie chmurowym producenta systemu (nie dopuszcza się uruchomienia funkcji sandbox bezpośrednio na chronionym endpontcie)

16.150.3. Lokalna analiza statyczna.

16.150.4. Weryfikacja podpisu pliku binarnego.

16.150.5. Przeniesienie pliku binarnego do kwarantanny.

16.150.6. Weryfikację i wykrycie groźnego zachowania procesu powstałego w wyniku uruchomienia/załadowania pliku binarnego.

16.151. Musi zapewnić ochronę przed atakami wykorzystującymi legalne narzędzia systemowe w groźny sposób poprzez analizę złożonych łańcuchów przyczynowo-skutkowych i wykrywanie technik i taktyk stosowanych przez cyberprzestępców.

16.152. Musi umożliwiać zablokowanie całego ruchu sieciowego (izolacja sieciowa) poza połączeniem do systemu.

16.153. Musi posiadać możliwość manualnego wyłączenia izolacji sieciowej w przypadku, gdy agent utracił łączność z systemem. Wyłączenie izolacji sieciowej musi być zabezpieczone hasłem. Każdy endpoint musi posiadać własne hasło, tak aby

można było je podać bezpiecznie użytkownikowi bez obawy, że inni użytkownicy zaczną wyłączać agenta. Hasło musi być automatycznie rotowane przez system nie rzadziej niż co dwa tygodnie.

16.154. System XDR musi umożliwiać ręczne (ad hoc) uruchamianie skanów bezpieczeństwa na wybranych punktach końcowych lub grupach urządzeń, niezależnie od zaplanowanego harmonogramu skanowania. Skan ad hoc musi być możliwy do uruchomienia z poziomu konsoli zarządzającej, zdalnie, bez konieczności fizycznego dostępu do urządzenia.

16.155. Agent dla systemów Linux i klastrów kubernetes

16.156. Musi posiadać możliwość pobierania aktualizacji agenta i aktualizacji podsystemów bezpieczeństwa:

16.156.1. Bezpośrednio z systemu

16.156.2. Z komponentu pośredniczącego

16.156.3. Od innych endpointów w tej samej podsieci (peer-to-peer)

16.156.4. Operacja deinstalacji agenta i wyłączenia podsystemów bezpieczeństwa musi zostać zapisana w dzienniku audytowym systemu.

16.157. Musi posiadać wsparcie dla rozszerzenia eBPF.

16.158. Musi posiadać wbudowany runtime python 3.7 lub nowszy i możliwość uruchamiania wbudownych i własnych skryptów python z wykorzystaniem co najmniej następujących bibliotek: argparse, asyncio, base64, browserhistory, certifi, collections, contextlib, csv, ctypes, datetime, enum, fnmatch, functools, glob, globmatch, gzip, hashlib, icmplib, importlib, io, json, LnkParse3, locale, logging, multiprocessing, netifaces, os, pathlib, pefile, platform, pprint, protobuf, psutil, pysftp, python_hosts, pythoncom, pytsk3, pywintypes, queue, random, re, Registry, requests, runpy, setuptools, shlex, shutil, signal, socket, sqlite_utils, sqlite3, ssl, stat, struct, subprocess, sys, threading, time, traceback, types, unicodecsv, uuid, websocket, win32api, win32com, win32con, win32evtlog, win32evtlogutil, win32file, win32net, win32netcon, win32process, win32security, win32service, win32serviceutil, win32timezone, winapps, winerror, winreg, wmi, xml, xmljson, yara, zipfile, zlib

16.159. Musi posiadać możliwość wyszukania plików we wskazanej ścieżce przy pomocy filtrów yara

16.160. Musi posiadać możliwość zrzucenia pamięci wskazanego procesu

16.161. Musi zbierać co najmniej następujące dane telemetryczne:

16.161.1. Utworzenie nowego procesu i zakończenie procesu

16.161.2. Informacje o kontenerach (co najmniej docker i containerd)

16.161.3. Wszystkie operacje na plikach: tworzenie, otwarcie, zapisywanie, kasowanie, kopiowanie, zmiana nazwy, zmiana właściciela, zmiana atrybutów

16.161.4. Wszystkie operacje na socketach sieciowych dla TCP i UDP: listen, accept, connect, connect failure, disconnect.

16.161.5. Zdarzenia z event logu dotyczącego uwierzytelnienia.

16.162. Musi wysyłać zgromadzone dane telemetryczny do systemu nie rzadziej niż co 5 minut, przy czym wymagane jest, aby agent posiadał możliwość wymuszenia wysłania danych telemetrycznych na żądanie. Jeśli z powodu braku łączności sieciowej agent nie może wysłać danych telemetrycznych, to dane telemetryczne muszą zostać lokalnie przechowane (zcache'owane) i wysłane do systemu po przywróceniu łączności sieciowej.

16.163. Musi zapewniać ochronę przed znanymi i nieznanymi exploitami wykorzystującymi znane i nieznane luki bezpieczeństwa w oprogramowaniu poprzez wykrywanie prób wykorzystania co najmniej następujących technika eksploitacji:

16.164. Java Deserialization

16.165. SO Hijacking

16.166. Heap spray

16.167. ROP

16.168. Kernel Privilege Escalation

16.169. Musi zapewnić ochronę przed znanymi i nieznanymi złośliwymi plikami binarnymi wykorzystując co najmniej następujące mechanizmy:

16.169.1. Weryfikacja sha256 w bazie threat intelligence producenta systemu

16.169.2. Analiza dynamiczna w sandboxie chmurowym producenta systemu (nie dopuszcza się uruchomienia funkcji sandbox bezpośrednio na chronionym endpontcie).

16.169.3. Lokalna analiza statyczna.

16.169.4. Przeniesienie pliku binarnego do kwarantanny.

16.169.5. Weryfikację i wykrycie groźnego zachowania procesu powstałego w wyniku uruchomienia/załadowania pliku binarnego.

16.169.6. Wykrywanie webshelli.

16.170. Musi zapewnić ochronę przed atakami wykorzystującymi legalne narzędzia systemowe w groźny sposób poprzez analizę złożonych łańcuchów przyczynowo-skutkowych i wykrywanie technik i taktyk stosowanych przez cyberprzestępców.

16.171. Musi umożliwiać zablokowanie całego ruchu sieciowego (izolacji sieciowej) poza połączeniem do systemu.

16.172. Musi posiadać możliwość manualnego wyłączenia izolacji sieciowej w przypadku, gdy agent utracił łączność z systemem. Wyłączenie izolacji sieciowej musi być zabezpieczone hasłem. Każdy endpoint musi posiadać własne hasło, tak aby można było je podać bezpiecznie użytkownikowi bez obawy, że inni użytkownicy zaczną wyłączać agenta. Hasło musi być automatycznie rotowane przez system nie rzadziej niż co dwa tygodnie.

16.173. System XDR musi umożliwiać ręczne (ad hoc) uruchamianie skanów bezpieczeństwa na wybranych punktach końcowych lub grupach urządzeń, niezależnie od zaplanowanego harmonogramu skanowania. Skan ad hoc musi być możliwy do uruchomienia z poziomu konsoli zarządzającej, zdalnie, bez konieczności fizycznego dostępu do urządzenia.

16.174. Agent dla systemów Android

16.175. Musi umożliwiać automatyczną instalację via system MDM i manualną via Google Play.

16.176. Operacja deinstalacji agenta musi zostać zapisana w dzienniku audytowym systemu i wygenerować alarm.

16.177. Musi zapewnić ochronę przed znanymi i nieznanymi złośliwymi aplikacjami wykorzystując co najmniej następujące mechanizmy:

16.177.1. Weryfikacja sha256 w bazie threat intelligence producenta systemu

16.177.2. Analiza dynamiczna w sandboxie chmurowym producenta systemu

16.178. System XDR musi umożliwiać wykrywanie i generowanie alertów dotyczących urządzeń z systemem Android, na których stwierdzono uzyskanie uprawnień root.

16.179. Agent dla systemów iOS

16.180. Musi umożliwiać automatyczną instalację via system MDM i manualną via App Store.

16.181. Operacja deinstalacji agenta musi zostać zapisana w dzienniku audytowym systemu i wygenerować alarm.

16.182. Musi weryfikować i raportować integralność systemu operacyjnego (tzw. jail break).

16.183. Musi zapewniać ochronę przed groźnymi wiadomościami tekstowymi przez weryfikację linków url (ochrona przeciw smishingowa).

16.184. Musi zapewniać ochronę przed groźnymi połączeniami głosowymi (ochrona przeciw vishingowa).

16.185. Musi umożliwiać użytkownikowi raportowanie podejrzanych wiadomości tekstowych.

16.186. Musi mieć opcję okresowego przypominania o konieczności restartu telefonu.

16.187. System musi umożliwiać monitorowanie ruchu sieciowego przeglądarki Safari na urządzeniach z systemem iOS za pomocą dedykowanego modułu bezpieczeństwa przeglądarki. Dodatkowo, system musi pozwalać na konfigurację zasad w module bezpieczeństwa sieciowego w celu ograniczania lub blokowania ruchu sieciowego generowanego przez nieautoryzowane aplikacje na nadzorowanych urządzeniach iOS. Rozwiązanie musi umożliwiać proaktywną blokadę podejrzanych witryn oraz zapewniać granularną kontrolę nad ruchem sieciowym na poziomie aplikacji.

17. ROZWIĄZANIE MFA

17.1. Przedmiotem zadania jest wdrożenie w infrastrukturze Zamawiającego metody uwierzytelniania wieloczynnikowego MFA opartego w szczególności o klucze sprzętowe i inne czynniki uwierzytelniające wraz z dostawą niezbędnego sprzętu i oprogramowania.

17.2. Przez uwierzytelnianie co najmniej trzyskładnikowe Zamawiający rozumie zastosowanie czynników należących do co najmniej dwóch różnych kategorii, w szczególności:

17.2.1. czegoś co użytkownik posiada (np. klucz sprzętowy),

17.2.2. czegoś co użytkownik zna (np. PIN lub hasło),

17.2.3. cechy sprzętu użytkownika,

17.2.4. przy czym co najmniej jednym z czynników musi być sprzętowy klucz kryptograficzny.

17.3. Minimalny zakres wdrożenia MFA obejmuje:

17.3.1. dostępy do środowiska chmurowego O365, w szczególności poczty elektronicznej Zamawiającego,

17.3.2. uwierzytelniania do stacji roboczych, kont AD,

17.3.3. uwierzytelniania do systemów bezpieczeństwa wdrażanych w ramach Przedmiotu Zamówienia,

17.3.4. dostępów zdalnych typu VPN do infrastruktury Zamawiającego,

17.3.5. dostępów uprzywilejowanych, przy czym do tego rodzaju dostępów wymaga się co najmniej 3 składników uwierzytelniania.

17.4. W ramach dostawy Wykonawca dostarczy **450 kluczy sprzętowych**, które będą służyć do silnego uwierzytelniania użytkowników oraz administratorów systemów teleinformatycznych Zamawiającego.

17.5. Dostarczone klucze muszą spełniać poniższe wymagania:

17.5.1. muszą być zgodne ze standardami U2F oraz FIDO2/WebAuthn;

17.5.2. muszą zapewniać uwierzytelnianie odporne na phishing, przechwycenie haseł oraz ataki typu man-in-the-middle;

17.5.3. muszą umożliwiać uwierzytelnianie wieloskładnikowe (2FA/MFA) oraz bezhasłowe logowanie;

17.5.4. klucze prywatne muszą być generowane i przechowywane wyłącznie w bezpiecznym elemencie sprzętowym i nie mogą być eksportowane;

17.5.5. muszą posiadać interfejs USB-C oraz obsługę NFC;

17.5.6. nie mogą wymagać baterii ani zewnętrznego zasilania;

17.5.7. muszą posiadać fizyczny mechanizm potwierdzenia obecności użytkownika;

17.5.8. muszą być kompatybilne z systemami Windows, Linux i macOS oraz popularnymi przeglądarkami internetowymi;

17.5.9. musi istnieć możliwość rejestracji, przypisywania do użytkownika oraz unieważnienia klucza;

17.5.10. muszą być objęte co najmniej 12 miesięczną gwarancją producenta.

17.6. Wykonawca w ramach zadania dotyczącego wdrożenia wdroży system typu MFA z wykorzystaniem kluczy, skonfiguruje je dla każdego użytkownika.

17.7. Wykonawca opracuje regulamin korzystania z kluczy sprzętowych dla pracowników, w tym zasady wymiany i postępowania w sytuacji utraty.