SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa systemu do audytu i monitorowania zdarzeń bezpieczeństwa wraz z 36 miesięcznym wsparciem producenta

1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa systemu służącego do centralnego audytu, monitorowania, raportowania i analizy zdarzeń bezpieczeństwa w środowisku usług katalogowych oraz systemów operacyjnych, wraz z udzieleniem bezterminowej (wieczystej) licencji na korzystanie z systemu oraz zapewnieniem wsparcia technicznego producenta przez okres 36 miesięcy.

2. Zakres zamówienia

- Dostawa systemu służącego do centralnego audytu, monitorowania, raportowania i analizy zdarzeń bezpieczeństwa w środowisku usług katalogowych.
- Wdrożenie - instalację i konfigurację systemu oraz wspieranej bazy danych.
- Konfigurację pobierania, normalizacji, korelacji i przechowywania danych z kontrolerów domeny oraz innych źródeł
- Konfigurację raportów, alertów, retencji, archiwizacji, ról dostępowych, uwierzytelniania wieloskładnikowego.
- Przeprowadzenie warsztatów powdrożeniowych dla administratorów i operatorów.
- Przekazanie dokumentacji powykonawczej oraz zapewnienie wsparcia technicznego i aktualizacji przez wymagany okres.

3. Warunki licencyjne

- Licencja musi mieć charakter bezterminowy, zwany również licencją wieczystą.
- Wykonawca musi dostarczyć wszystkie licencje, subskrypcje, dodatki, konektory, instancje zapasowe i inne prawa niezbędne do realizacji całego zakresu funkcjonalnego oprogramowania.
- Po zakończeniu okresu wsparcia technicznego Zamawiający musi zachować prawo do bezterminowego korzystania z ostatniej wersji oprogramowania, do której uzyskał uprawnienia w okresie obowiązywania wsparcia.
- Wygaśnięcie lub nieprzedłużenie wsparcia technicznego nie może powodować zablokowania oprogramowania, ograniczenia wcześniej nabytej funkcjonalności, utraty dostępu do zgromadzonych danych, uniemożliwienia generowania raportów z wcześniej zgromadzonych danych, przejścia oprogramowania do wersji bezpłatnej, demonstracyjnej albo wersji o ograniczonej funkcjonalności ani obowiązku ponownego zakupu licencji podstawowej.
- Licencja musi umożliwiać użytkowanie oprogramowania na potrzeby wewnętrzne Zamawiającego, zgodnie z zakresem ilościowym wskazanym w dokumentach zamówienia.
- Licencja nie może być uzależniona od cyklicznego uiszczania opłat subskrypcyjnych warunkujących dalsze działanie podstawowej funkcjonalności oprogramowania.
- Zamawiający musi posiadać możliwość przeniesienia instalacji oprogramowania na inny serwer lub środowisko w ramach tej samej jednostki organizacyjnej, w szczególności w przypadku wymiany sprzętu, awarii, migracji, odtworzenia środowiska albo zmiany architektury technicznej.

- Licencja musi pochodzić z legalnego i autoryzowanego kanału dystrybucji oraz umożliwiać Zamawiającemu korzystanie ze wsparcia technicznego producenta.
- Zamawiający wymaga, aby licencja bazowa na komponent audytu środowiska Active Directory oraz obiektów Group Policy (GPO) była kalkulowana i dostarczona **wyłącznie w oparciu o liczbę audytowanych Kontrolerów Domeny (DC), bez limitowania liczby aktywnych lub nieaktywnych kont użytkowników (Unlimited Users).** Niedopuszczalne jest oferowanie rozwiązania, którego licencja bazowa posiada progi lub limity licencyjne ograniczające maksymalną liczbę użytkowników/pracowników w organizacji lub wymaga dokupienia licencji klienckich (CAL/User) dla dostępu do podstawowych funkcji audytowych.

4. Wymagania dotyczące bezpieczeństwa

- System musi umożliwiać pracę z zastosowaniem zasady minimalnych niezbędnych uprawnień.
- Wykonawca musi dostarczyć dokumentację zawierającą wykaz uprawnień wymaganych do działania oprogramowania.
- Konsola musi działać z użyciem HTTPS. Wykonawca skonfiguruje certyfikat wskazany przez Zamawiającego i wyłączy nieszyfrowany dostęp HTTP, jeżeli pozwala na to architektura.
- System musi umożliwiać wymuszenie TLS 1.2 lub nowszego dla konsoli webowej i integracji, w zakresie wspieranym przez komponenty.
- Komunikacja katalogowa musi umożliwiać użycie LDAPS.
- System musi obsługiwać uwierzytelnianie kontami Active Directory oraz kontami lokalnymi systemu.
- System musi obsługiwać uwierzytelnianie wieloskładnikowe przy użyciu co najmniej jednego standardowego mechanizmu: TOTP, RADIUS, dostawca tożsamości, e-mail albo SMS.
- System musi posiadać kontrolę dostępu opartą na rolach, umożliwiającą rozdzielenie co najmniej roli administratora i operatora lub audytora.
- System musi umożliwiać tworzenie niestandardowych ról albo ograniczanie dostępu do raportów, domen i funkcji administracyjnych.
- System musi umożliwiać ograniczenie dostępu do repozytorium danych oraz audytować działania administratorów i techników systemu.
- Archiwa oraz eksportowane lub harmonogramowane raporty muszą mieć możliwość zabezpieczenia hasłem albo równoważnym mechanizmem ochrony, jeżeli zawierają dane wrażliwe.
- System musi zapewniać audyt zmian własnej konfiguracji i działań administracyjnych wykonywanych w konsoli.
- Hasła i sekrety przechowywane przez system muszą być chronione silnym mechanizmem kryptograficznym, co najmniej AES-256 lub rozwiązaniem zapewniającym równoważny poziom bezpieczeństwa.
- System nie może wymagać przekazywania danych audytowych poza infrastrukturę Zamawiającego.
- System musi umożliwiać aktualizację do wersji usuwających ujawnione podatności bezpieczeństwa przez cały okres obowiązywania wsparcia technicznego.
- Producent musi publikować informacje o aktualizacjach, poprawkach lub nowych wersjach oprogramowania.
- System musi być dostarczony w aktualnej, stabilnej i wspieranej przez producenta wersji, przeznaczonej do użytkowania produkcyjnego.

- System nie może być wersją demonstracyjną, testową, czasową, edukacyjną, nieprzeznaczoną do zastosowań produkcyjnych ani wersją o funkcjonalności ograniczonej czasowo.

5. Wymagania dotyczące działania systemu

- System musi być dostarczony jako rozwiązanie instalowane lokalnie w infrastrukturze Zamawiającego. Dane nie mogą być przekazywane do chmury producenta.
- Zapewnienie jednej, centralnej konsoli umożliwiającej wyszukiwanie, analizę, raportowanie i konfigurację audytu dla wszystkich objętych zamówieniem domen, lasów oraz dodatkowych źródeł.
- System musi przechowywać surowe i/lub znormalizowane dane w centralnym, wspieranym przez producenta repozytorium audytowym.
- System musi centralnie pobierać, filtrować, normalizować, korelować i przechowywać zdarzenia pochodzące z audytowanych źródeł.
- Umożliwienie ustalenia wartości istotnych atrybutów i uprawnień przed zmianą i po zmianie, jeżeli dane są dostępne w audytowanym środowisku.
- Zapewnienie mechanizmów alertowania o zdarzeniach krytycznych, nadużyciach, anomaliach i utracie ciągłości zbierania danych.
- Zapewnienie retencji bieżącej i archiwalnej oraz możliwości ponownego użycia danych archiwalnych do analiz i raportów.
- Zapewnienie kontroli dostępu opartej na rolach, uwierzytelniania wieloskładnikowego oraz audytu działań administratorów systemu.
- System musi umożliwiać bezagentowe pobieranie danych z kontrolerów domeny oraz opcjonalne użycie agentów lub kolektorów w środowiskach rozproszonych, WAN albo o dużej liczbie urządzeń.
- System musi umożliwiać centralną obsługę wielu domen i lasów z jednej konsoli, w zakresie dostarczonych licencji.
- System musi umożliwiać rozbudowę o audyt dodatkowych źródeł to jest: Audyt serwerów członkowskich Windows, Audyt stacji roboczych, Audyt serwerów plików Windows i urządzeń NAS, bez konieczności wdrażania niezależnego systemu zarządzanego z odrębnej konsoli.
- System musi umożliwiać przekazywanie zdarzeń i alertów do SIEM lub odbiornika Syslog w czasie rzeczywistym, co najmniej przez TCP albo UDP.
- System musi umożliwiać zabezpieczenie komunikacji pomiędzy komponentami oprogramowania;
- System musi umożliwiać tworzenie kopii zapasowej konfiguracji oprogramowania oraz jej odtworzenie.
- System musi być dostarczony z obsługiwaną bazą danych albo umożliwiać użycie zewnętrznego, wspieranego systemu bazodanowego. Zastosowany wariant musi zapewniać backup, odtwarzanie, kontrolę dostępu i obsługę zakładanej skali (rozmiaru bazy danych).
- System musi posiadać natywnie zintegrowaną, wbudowaną relacyjną bazę danych (silnik embedded, typu open source), instalowaną automatycznie w ramach jednego pakietu instalacyjnego systemu, która **nie wymaga instalacji i licencjonowania zewnętrznych komercyjnych serwerów bazodanowych** (np. takich jak Microsoft SQL Server). Jednocześnie system musi oferować opcję migracji do zewnętrznej bazy.
- System musi jednocześnie umożliwiać migrację danych do zewnętrznej bazy danych oraz dalszą pracę systemu z wykorzystaniem takiej bazy, zgodnie z listą silników bazodanowych wspieranych przez producenta.

- Integracja SIEM musi umożliwiać wybór kategorii danych przekazywanych do systemu zewnętrznego.

6. Minimalne wymagania funkcjonalne

a) Audyt usług katalogowych

- Rejestrowanie utworzenia, usunięcia, modyfikacji, przeniesienia, zmiany nazwy oraz przywrócenia obiektów Active Directory.
- Audyt użytkowników, grup, komputerów, jednostek organizacyjnych, kontaktów, obiektów zasad grupy oraz innych klas obiektów katalogowych.
- Audyt włączenia, wyłączenia, odblokowania, zablokowania, wygaśnięcia i usunięcia konta użytkownika.
- Audyt zmian haseł, resetów haseł, zmian flag konta i ustawień uwierzytelniania.
- Audyt zmian dotyczących grup i kont uprzywilejowanych oraz możliwość oznaczania obiektów krytycznych.
- Audyt operacji związanych z replikacją, konfiguracją domeny oraz kontrolerami domeny.
- Audyt prób dokonania zmian zakończonych niepowodzeniem, o ile odpowiednie zdarzenia są udostępniane przez monitorowany system.
- Audyt zmian delegacji i list kontroli dostępu obiektów Active Directory.
- Audyt zmian schematu Active Directory, partycji Configuration oraz ról FSMO.
- Audyt zmian obiektów i stref DNS wraz z prezentacją wartości przed i po zmianie, o ile są dostępne.
- Audyt usług certyfikatów Active Directory, jeśli są używane przez Zamawiającego i objęte zakresem.
- Audyt operacji związanych z LAPS, w szczególności odczytu lub zmian dotyczących zarządzanych haseł lokalnych kont, w zakresie wspieranym przez środowisko Microsoft.
- Prezentowanie starych i nowych wartości zmienionych atrybutów, a nie wyłącznie informacji o samym fakcie modyfikacji.
- Dla każdego zarejestrowanego zdarzenia oprogramowanie powinno prezentować, o ile dane są dostępne w źródle, co najmniej: datę i czas zdarzenia; rodzaj wykonanej operacji; nazwę lub identyfikator obiektu; dane użytkownika albo konta wykonującego operację; nazwę urządzenia lub systemu źródłowego; poprzednią i nową wartość zmienionego parametru; rezultat operacji; adres sieciowy urządzenia źródłowego.
- Możliwość tworzenia niestandardowych raportów i filtrów według obiektów, użytkowników, OU, domen, operacji i zakresu czasu.

b) Audyt obiektów i ustawień Group Policy

- Audyt utworzenia, usunięcia, modyfikacji, zmiany nazwy, kopiowania oraz powiązania obiektów GPO.
- Audyt zmian ustawień GPO, a nie wyłącznie zmian metadanych samego obiektu.
- Prezentowanie użytkownika, czasu i źródła zmiany oraz wartości ustawienia przed zmianą i po zmianie.
- Audyt zmian ustawień konfiguracji komputera i użytkownika.
- Audyt zmian zasad haseł i blokady kont.
- Audyt zmian powiązań GPO z OU lub domeną, wymuszania, blokowania dziedziczenia oraz filtrów bezpieczeństwa.

- Alertowanie w czasie zbliżonym do rzeczywistego o krytycznych zmianach wskazanych polityk i ustawień.

c) Monitorowanie logowań i analiza blokad kont

- Raportowanie udanych i nieudanych logowań domenowych z informacją o użytkowniku, czasie, komputerze źródłowym, adresie IP, kontrolerze domeny, typie logowania i wyniku.
- Analiza przyczyn nieudanych logowań i prezentowanie komunikatu lub zrozumiałej przyczyny błędu.
- Analiza blokad kont z identyfikacją urządzenia, usługi lub innego źródła powodującego blokadę.
- Korelacja blokady konta z wcześniejszymi błędnymi próbami uwierzytelnienia pochodzącymi z wielu komponentów środowiska Windows.
- Alertowanie o blokadzie konta, powtarzających się błędach logowania oraz przekroczeniu zdefiniowanych progów.
- Raportowanie logowań poza zdefiniowanymi godzinami, logowań na wielu komputerach oraz aktywności z nietypowych źródeł.
- Możliwość rozszerzenia zakresu o aktywność RADIUS/NPS i ADFS.
- Monitorowanie wylogowań użytkowników.
- Wykrywanie nietypowej aktywności logowania na podstawie zdefiniowanych reguł, progów, harmonogramów lub mechanizmów analitycznych.
- Generowanie alertów dotyczących zdarzeń logowania i uwierzytelniania.

d) Monitoring kont uprzywilejowanych i wykrywanie zagrożeń

- Prowadzenie skonsolidowanego śladu audytowego działań kont uprzywilejowanych na użytkownikach, grupach, OU, GPO, schemacie i konfiguracji Active Directory.
- Wykrywanie pierwszego, nietypowego lub niezgodnego z przyjętym profilem użycia uprawnień oraz prób eskalacji uprawnień.
- Budowanie charakterystyki typowej aktywności użytkowników albo stosowanie równoważnego mechanizmu identyfikacji odchyleń i anomalii.
- Wykrywanie zdarzeń lub sekwencji zdarzeń mogących wskazywać na próby pozyskania lub wykorzystania biletów Kerberos, nieautoryzowaną replikację danych katalogowych, użycie podrobionych albo przejętych poświadczeń, masowe próby uwierzytelnienia lub eskalację uprawnień.
- Wykrywanie nietypowych lub masowych zmian, nieoczekiwanej aktywności uprzywilejowanej, powtarzających się błędów uwierzytelnienia i prób dostępu do dużej liczby zasobów.
- Alertowanie o wyczyszczeniu dziennika, wyłączeniu lub zmianie audytu, zatrzymaniu mechanizmu zbierania danych albo utracie komunikacji ze źródłem.
- Możliwość uruchomienia zdefiniowanego skryptu, polecenia albo równoważnej akcji reakcji po wystąpieniu wybranego alertu.

e) Raportowanie i wyszukiwanie

- Posiadać zestaw predefiniowanych raportów dotyczących monitorowanych obszarów;
- Umożliwiać tworzenie raportów własnych na podstawie dostępnych danych audytowych;

- Umożliwiać filtrowanie raportów co najmniej według zakresu dat i czasu, użytkownika lub konta, rodzaju zdarzenia, monitorowanego urządzenia lub systemu, obiektu, pliku, folderu albo zasobu oraz wyniku operacji;
- Umożliwiać zapisywanie zdefiniowanych filtrów i raportów;
- Umożliwiać cykliczne generowanie raportów według harmonogramu;
- Umożliwiać automatyczne przekazywanie raportów do wskazanych odbiorców;
- Umożliwiać eksport raportów co najmniej do jednego powszechnie stosowanego formatu dokumentowego oraz jednego formatu umożliwiającego dalsze przetwarzanie danych, w szczególności PDF, CSV, XLSX lub równoważnego;
- Umożliwiać prezentację danych w formie tabelarycznej oraz, dla wybranych raportów, graficznej;
- Umożliwiać wyszukiwanie informacji w zgromadzonych danych audytowych;
- Zapewniać możliwość uzyskania informacji pozwalających ustalić co najmniej: kto, kiedy, z jakiego urządzenia i jakiej zmiany dokonał.

f) Alertowanie i automatyzacja

- Definiowanie alertów według co najmniej: rodzaju zdarzenia, użytkownika, obiektu, źródła, czasu, liczby wystąpień i ustalonego progu.
- Dostarczanie powiadomień co najmniej pocztą elektroniczną.
- Możliwość oznaczenia krytycznych użytkowników, grup, obiektów i zdarzeń oraz tworzenia dla nich odrębnych profili alertów.
- Możliwość ograniczenia liczby powtarzalnych powiadomień przez progi, grupowanie, czas wyciszenia albo równoważny mechanizm.
- Rejestrowanie w systemie historii wygenerowanych alertów i wykonanych akcji reakcji.

g) Retencja, archiwizacja i analiza historyczna

- Przechowywanie danych audytowych w centralnym repozytorium;
- Konfigurowanie odrębnych okresów retencji dla danych bieżących i archiwalnych oraz, jeżeli rozwiązanie to umożliwia, dla poszczególnych kategorii danych.
- Obsługa co najmniej warstwy danych bieżących oraz skompresowanego lub zoptymalizowanego archiwum historycznego.
- Możliwość ponownego udostępnienia danych archiwalnych do wyszukiwania i raportowania bez utraty ich kontekstu audytowego.
- Możliwość bezterminowego przechowywania archiwum albo automatycznego usuwania danych po zdefiniowanym okresie.
- Możliwość umieszczenia archiwum poza katalogiem instalacyjnym, w tym na innym dysku, udziale sieciowym albo wskazanym serwerze plików.
- Zapewnienie procedury kopii zapasowej i odtwarzania konfiguracji oraz repozytorium danych zgodnie z dokumentacją producenta.

h) Audyt serwerów i stacji roboczych

- Monitorowanie zdarzeń bezpieczeństwa rejestrowanych przez system operacyjny;
- Monitorowanie zmian konfiguracji systemu istotnych z punktu widzenia bezpieczeństwa;
- Monitorowanie operacji dotyczących lokalnych użytkowników i grup;
- Monitorowanie zmian członkostwa w lokalnych grupach uprzywilejowanych;
- Monitorowanie uruchamiania i zatrzymywania usług systemowych;
- Monitorowanie zmian zasad zabezpieczeń;

- Monitorowanie operacji wykonywanych przez konta administracyjne;
- Monitorowanie zdarzeń logowania, wylogowania i blokowania sesji użytkowników;
- Monitorowanie zmian w harmonogramach zadań lub innych mechanizmach automatycznego wykonywania operacji - jeżeli informacje te są dostępne w monitorowanym systemie;
- Monitorowanie podłączania lub wykorzystywania urządzeń wymiennych - jeżeli funkcjonalność ta jest objęta oferowaną licencją.
- Audyt procesów PowerShell wraz z wykonanymi poleceniami, w zakresie udostępnianym przez konfigurację logowania.

i) Audyt systemów plików

- Monitorowanie operacji wykonywanych na plikach i folderach.
- Monitorowanie co najmniej następujących czynności: utworzenia, odczytu lub próby odczytu, modyfikacji, usunięcia, zmiany nazwy, przeniesienia, skopiowania - w zakresie umożliwianym przez monitorowany system, zmiany uprawnień oraz zmiany właściciela.
- Identyfikowanie użytkownika wykonującego operację.
- Identyfikowanie czasu, urządzenia źródłowego oraz ścieżki zasobu.
- Rejestrowanie udanych i nieudanych prób dostępu, o ile odpowiednie zdarzenia są udostępniane przez monitorowany system.
- Monitorowanie dostępu do wskazanych plików, folderów, udziałów lub kategorii danych.
- Definiowanie wykluczeń ograniczających gromadzenie zdarzeń nieistotnych.
- Generowanie alertów dla określonych operacji, użytkowników, zasobów lub zakresów czasowych.
- Raportowanie zmian uprawnień do plików, folderów i udziałów.
- Analizowanie aktywności użytkowników w odniesieniu do zasobów plikowych.
- Audyt zmian uprawnień NTFS i uprawnień udziałów wraz z wartościami przed i po zmianie.

8 Zakres monitorowanego środowiska

Poniższe dane stanowią podstawę do przygotowania architektury, oszacowania pojemności repozytorium, retencji i kosztu licencji.

Liczba lasów Active Directory	2
Liczba domen Active Directory	2
Liczba kontrolerów domeny objętych audytem	5
Liczba użytkowników w AD	1500
Liczba serwerów członkowskich Windows	66
Liczba serwerów plików Windows	2
Liczba urządzeń NAS i wymagane platformy	2
Liczba stacji roboczych Windows	1200
Wymagana retencja danych dostępnych bez odtwarzania archiwum	12 miesięcy
Wymagana retencja archiwalna	5 lat

9 Wdrożenie i konfiguracja

Zamawiający wymaga przygotowania przez Wykonawcę:

- Opracowanie projektu technicznego obejmującego serwer aplikacyjny, repozytorium danych, przepływy sieciowe, konta serwisowe, retencję, archiwum i integracje.
- Instalacja i aktualizacja oprogramowania do stabilnej wersji wspieranej przez producenta.
- Konfiguracja kont serwisowych zgodnie z zasadą minimalnych uprawnień.

- Konfiguracja polityk audytu i ustawień systemów Windows wymaganych do uzyskania kompletnego śladu audytowego.
- Dołączenie kontrolerów domeny i wszystkich objętych zamówieniem źródeł.
- Konfiguracja pobierania i przetwarzania zdarzeń.
- Konfiguracja repozytorium, kopii zapasowych i procedury odtwarzania.
- Konfiguracja retencji bieżącej i archiwalnej.
- Konfiguracja HTTPS, LDAPS, MFA, ról i uprawnień.
- Konfiguracja co najmniej 20 profili alertów dla zdarzeń krytycznych uzgodnionych z Zamawiającym.
- Konfiguracja co najmniej 10 harmonogramowanych raportów.
- Konfiguracja agentów lub kolektorów, jeżeli ich zastosowanie jest uzasadnione architekturą środowiska.

10 Testy odbiorowe

Wykonawca przygotuje plan testów, dane testowe i protokół wyników. Każdy scenariusz musi zostać wykonany w środowisku Zamawiającego albo w uzgodnionym środowisku demonstracyjnym.

Scenariusz odbioru:

- Wygenerowanie udanego i nieudanego logowania oraz sprawdzenie pełnego kontekstu zdarzenia.
- Wywołanie blokady konta i wskazanie źródła blokady.
- Wygenerowanie serii nieudanych logowań przekraczającej zdefiniowany próg i sprawdzenie alertu.
- Wyczyszczenie testowego dziennika albo zasymulowanie przerwania zbierania danych i potwierdzenie alertu.
- Utworzenie raportu niestandardowego, zapisanie filtra, eksport do PDF i CSV oraz harmonogram wysyłki.
- Przeniesienie lub wskazanie lokalizacji archiwum poza katalogiem instalacyjnym oraz ponowne użycie danych archiwalnych w raporcie.
- Weryfikacja uwierzytelniania kontem AD, MFA i rozdziału uprawnień administratora oraz audytora.
- Weryfikacja audytu zmian konfiguracji samego systemu.
- Weryfikacja raportu z zakresu plikowego – utworzenie, modyfikacja, usunięcie pliku oraz zmiana jego uprawnień.

11 Dokumentacja, szkolenie i wsparcie

a) Dokumentacja powykonawcza

- Architektura wdrożenia i diagram przepływów danych.
- Wykaz serwerów, komponentów, portów, certyfikatów i kont serwisowych.
- Konfiguracja źródeł danych, repozytorium, retencji i archiwum.
- Lista utworzonych raportów i alertów.
- Konfiguracja bezpieczeństwa, ról i uwierzytelniania wieloskładnikowego.
- Procedury aktualizacji, backupu, odtwarzania i – jeżeli dotyczy – przełączenia wysokiej dostępności.
- Instrukcja operacyjna dla administratorów i operatorów.
- Dokumentacja musi być w języku polskim.

b) Warsztaty powdrożeniowe

Warsztaty muszą obejmować administrację systemem, zarządzanie źródłami danych, tworzenie raportów i alertów, analizę blokad kont, obsługę archiwum, integrację SIEM, zarządzanie rolami oraz podstawowe czynności utrzymaniowe i diagnostyczne.

- Czas trwania warsztatów: co najmniej 10 godzin, podzielonych na min. 2 spotkania;
- Zajęcia muszą być przeprowadzone w języku polskim;
- Warsztaty mogą się odbyć w formie wideokonferencji w dni robocze w godzinach 9.00 – 14.00 lub stacjonarnej w siedzibie Zamawiającego;
- Uczestnikom zapewnione zostaną materiały dydaktyczne w formie elektronicznej w języku polskim lub angielskim;
- Liczba uczestników: 7;

c) Wsparcie i aktualizacje

- Dostęp do aktualizacji, poprawek bezpieczeństwa i nowych stabilnych wersji przez cały okres wsparcia.
- Możliwość zgłaszania incydentów technicznych pocztą elektroniczną, portalem i telefonicznie w języku polskim.
- Wsparcie producenta albo autoryzowanego partnera posiadającego kompetencje wdrożeniowe dla oferowanego rozwiązania w języku polskim.
- Przekazanie procedury eskalacji zgłoszeń i kontaktów serwisowych.
- Zdalna pomoc techniczna w języku polskim.
- Pomoc techniczną producenta systemu.
- Dostęp do polskiej bazy wiedzy.