

### **Opis przedmiotu zamówienia**

Dotyczy wniosku na:

#### **Zakup i wdrożenie centralnego Systemu ochrony dla urządzeń końcowych funkcjonujących w PGL LP**

(nazwa wskazana we wniosku o udzielenie zamówienia)

#### **I. Skrótowy opis przedmiotu zamówienia:**

1. Wdrożenie w Państwowym Gospodarstwie Leśnym Lasy Państwowe (PGL LP) Systemu klasy EDR/XDR (Extended/Endpoint Detection and Response – zaawansowane oprogramowanie do ochrony stacji roboczych, serwerów przed zagrożeniami cybernetycznymi), dalej zwany Systemem, z konsolą zarządzającą w formie usługi chmurowej (SaaS), który ma zapewniać:
  - 1.1. aktywną ochronę stacji końcowych i serwerów przed działaniem złośliwego oprogramowania i innych zaawansowanych cyberzagrożeń;
  - 1.2. detekcję zagrożeń, identyfikację działań cyberprzestępców oraz zdarzeń z kategorii APT (Advanced Persistent Threats);
  - 1.3. aktywną reakcję i odpowiedzi na wykryte zdarzenia oraz incydenty;
  - 1.4. realizację działań proaktywnych, w tym aktywnego wyszukiwania intruzów w infrastrukturze informatycznej.– dostarczone rozwiązanie musi zapewniać obsługę 25 000 szt. urządzeń końcowych
2. Dostawa licencji oprogramowania w ramach zamówienia obligatoryjnego wraz ze wsparciem Producenta przez okres 36 miesięcy od dnia podpisania końcowego protokołu odbioru zadania ZN-4 liczbie sztuk:
  - 2.1. 10678 szt.. dla stacji roboczych z systemem Microsoft Windows;
  - 2.2. 561 szt. dla serwerów z systemem Microsoft Windows Server/Linux;
  - 2.3. 39 szt. dla stacji roboczych z systemem Linux.
3. Zapewnienie usług wsparcia Wykonawcy w języku polskim w okresie obowiązywania umowy.
4. Organizacja i realizacja szkoleń.
5. Realizacja prawa opcji dla jednostek organizacyjnych PGL LP w maksymalnym wymiarze:
  - 5.1. dostawy do 10 000 szt. licencji dla roboczych z systemem Microsoft Windows;
  - 5.2. dostawy do 1100 szt. licencji dla serwerów z systemem Microsoft Windows Server/Linux;
  - 5.3. dostawy do 100 szt. licencji dla stacji roboczych z systemem Linux.

## **II. Szczegółowy opis przedmiotu zamówienia (zamówienie obligatoryjne).**

### **1. Wymagania w zakresie wdrażanego rozwiązania.**

1.1. System musi być sklasyfikowany przez niezależne instytucje badające rynek rozwiązań EDR/XDR i spełniać przynajmniej jeden warunek:

- 1.1.1. sklasyfikowanie jako „Strong Performers” lub „Leader” w raporcie Forrester Wave for EDR Providers Q2 2024;
- 1.1.2. sklasyfikowanie jako „Leader” w raporcie 2024 Gartner Magic Quadrant for Endpoint Protection Platforms

1.2. W ramach przedmiotu zamówienia Wykonawca musi zrealizować następujące zadania:

#### **1.2.1. ZN-1 Procedura zarządzania projektem.**

Wykonawca w porozumieniu z Zamawiającym przygotowuje procedurę zarządzania projektem. Przedmiotowa procedura wymaga zgłoszenia do odbioru. Zamawiający wymaga minimum jednego spotkania roboczego koordynatorów w celu omówienia przygotowania niniejszej procedury. Procedura będzie zawierała co najmniej:

- 1) informacje organizacyjne, w tym dane kontaktowe, zasady korzystania i ingerowania w zasoby informatyczne PGL LP, w tym przekazanie danych dostępowych oraz innych, niezbędnych do realizacji Umowy;
- 2) harmonogram ramowy realizacji Umowy;
- 3) informację na temat sposobu weryfikacji liczby dostarczonych licencji i wsparcia Producenta w okresie obowiązywania umowy. Sposób weryfikacji musi zapewniać Zamawiającemu możliwość:
  - a) określenia daty dostawy
  - b) okresu obowiązywania wsparcia Producenta dla dostarczanych licencji
  - c) liczby dostarczonych licencji wraz ze wsparciem
  - d) identyfikację jednostki organizacyjnej PGL LP, na której rzecz była realizowana dostawa
  - e) informacje na temat liczby licencji wraz ze wsparciem Producenta dostarczonych w ramach „prawa opcji”
  - f) informacja musi być aktualizowana nie rzadziej niż 1 raz w miesiącu.
- 4) informacje o uzasadnionych wymaganiach technicznych względem zadań Wykonawcy określonych w Umowie, które to wymagania powinien spełnić Zamawiający, aby realizacja przedmiotu Umowy nie była zagrożona;
- 5) informacje o procedurach działania w sytuacjach kryzysowych (sposób zgłaszania awarii, zagrożeń, dane osób uprawnionych do podejmowania decyzji kierunkowych po stronie Wykonawcy, Zamawiającego i DGLP);
- 6) dostarczenie dokumentacji związanej z oferowanym produktem;
- 7) dostarczenie informacji o nieprawidłowych interakcjach dostarczanego Systemu z oprogramowaniem firm trzecich nie wskazanym w OPZ (jeżeli są mu znane).

#### 1.2.2. ZN-2 Przygotowanie wersji testowej Systemu

Wykonawca przygotowuje wersję testową Systemu. W ramach Zadania Wykonawca:

- 1) przygotowuje dokumentację projektową wdrożenia testowego (obejmujący między innymi: zasady synchronizacji z Active Directory Zamawiającego, sposoby komunikacji z SIEM, wymagania dotyczące komunikacji modułu SOAR z systemami Zamawiającego, polityki dotyczące stacji roboczych, serwerów z systemem Windows w tym kontrolerów Active Directory, serwerów z systemem Linux, opis komunikacji pomiędzy środowiskiem Zamawiającego a usługą chmurową Producenta, wykonania kopii bezpieczeństwa konfiguracji Systemu oraz procedur jej odtworzenia);
- 2) dokumentacja musi być przygotowana w języku polskim oraz w pełni odzwierciedlać instalację Zamawiającego nie może zawierać odwołań do stron, linków itp.;
- 3) wykreuje tenant/instancję z dedykowaną konsolą;
- 4) dostarczy licencje testowe w ilości 200 sztuk;
- 5) zainstaluje agenta Systemu przy współpracy z Zamawiającym na wybranej grupie stacji roboczych i serwerów;
- 6) wykona wstępną analizę środowiska i dostosuje polityki bezpieczeństwa i konfigurację Systemu zgodnie z wymaganiami opisanymi w OPZ.

#### 1.2.3. ZN-3 Wykonanie dokumentacji wdrożeniowej Systemu

Wykonawca wykona dokumentację wdrożeniową Systemu. Dokumentacja musi być przygotowana w języku polskim, w pełni odzwierciedlająca instalację Zamawiającego nie może zawierać odwołań do stron, linków itp. Ponadto dokumentacja będzie zawierała w szczególności:

- 1) szczegółowy opis architektury wybranego rozwiązania dostosowany zgodnie z wymaganiami Producenta i zapisami OPZ;
- 2) opis funkcjonalny Systemu oraz wykaz wymaganych komponentów Systemu, sposobu ich konfiguracji i wdrożenia;
- 3) wykaz licencji niezbędnych dla działania Systemu jako całości;
- 4) procedury i instrukcje dotyczące instalacji i deinstalacji agentów Systemu na stacjach roboczych, opis wyjątków i wykluczeń w konfiguracji Systemu mogących powodować konflikty z istniejącym oprogramowaniem na stacjach roboczych.

#### 1.2.4. ZN-4 Wdrożenie i dostawa licencji (obligatoryjnych)

Wykonawca w terminie zgodnym z umową zrealizuje wdrożenie Systemu i dostarczy licencje zgodnie z niniejszym OPZ oraz poniższymi zapisami:

- 1) wdrożenie zostanie zrealizowane w oparciu o środowisko testowe. Środowisko produkcyjne będzie wyskalowane do maksymalnej liczby urządzeń zgodnie z OPZ;
- 2) od dnia odbioru Zadania Nazwanego ZN-3, w okresie do 4 miesięcy, Wykonawca dostarczy licencje dla jednostek organizacyjnych PGL LP,

- wg szczegółowego zapotrzebowania i harmonogramu stanowiącego Załącznik do OPZ, w sumarycznej ilości nie mniejszej niż 11 278 szt.;
- 3) potwierdzeniem odbioru licencji dla jednostek organizacyjnych PGL LP będzie podpisany protokół odbioru, który będzie stanowił podstawę wystawienia faktury dla danej jednostki za zamówione licencje obligatoryjne;
  - 4) podpisane protokoły odbioru, ze wszystkich jednostek Zamawiającego, stanowią podstawę do dokonania ostatecznego odbioru wdrożenia Systemu;
  - 5) od daty podpisania ostatecznego protokołu odbioru wdrożenia Systemu Wykonawca zapewni 36 miesięcy wsparcia na wdrożone rozwiązanie oraz uruchomi wsparcie Producenta dla dostarczonych licencji.
  - 6) Wykonawca zobowiązany jest udokumentować, że dostarczone licencje zostały zarejestrowane na koncie Zamawiającego tj. ZILP u Producenta Systemu.

#### 1.2.5. ZN-5 Szkolenia

Wykonawca w ramach zamówienia przeprowadzi następujące szkolenia:

- 1) Dla Administratorów Centralnych Systemu wskazanych przez Zamawiającego przeprowadzane w terminie do 30 dni roboczych od dnia odbioru Zadania ZN-3.
  - a) wykonawca zapewni szkolenie lub szkolenia, prowadzone przez certyfikowanego instruktora (trenera) oferowanego rozwiązania w formie warsztatów, obejmujące swym zakresem: instalację i konfigurację Systemu, pełną obsługę i administrację Systemem, działania mające na celu zapewnienie jego utrzymania i rozwoju oraz analizę i reakcję na incydenty bezpieczeństwa;
  - b) szkolenie zostanie przeprowadzone w języku polskim;
  - c) liczba uczestników: 10 osób;
  - d) w minimalnym wymiarze 24 godzin;
  - e) Zamawiający dopuszcza, że szkolenie zostanie przeprowadzone na środowisku szkoleniowym przygotowanym przez autoryzowany ośrodek poza siedzibą Zamawiającego, lecz wymaga się aby odbyło się na terenie Polski;
  - f) wszyscy uczestnicy szkolenia muszą otrzymać materiały szkoleniowe w języku polskim lub angielskim, w formie papierowej lub elektronicznej;
  - g) wszyscy uczestnicy otrzymają zaświadczenia w formie certyfikatu potwierdzające ukończenie szkolenia;
  - h) koszty szkolenia i koszty związane z jego organizacją pokrywa Wykonawca.
- 2) Dla Administratorów Regionalnych przeprowadzane w terminie do 30 dni roboczych od dnia odbioru Zadania ZN-4.
  - a) Wykonawca przeprowadzi szkolenie powdrożeniowe obejmujące zakresem między innymi: podstawową konfigurację, obsługę

konsoli, rozwiązywanie problemów działania agenta, wgląd w monitoring zdarzeń z obsługą alertów dotyczących anomalii systemów operacyjnych, zarządzanie pamięciami zewnętrznymi USB na bazie wdrożonego Systemu u Zamawiającego;

- b) szkolenie zostanie przeprowadzone w języku polskim;
- c) liczba uczestników - 40 osób;
- d) w minimalnym wymiarze 8 godzin;
- e) szkolenie zostanie przeprowadzone i omówione na środowisku produkcyjnym w formie on-line;
- f) Zamawiający zastrzega sobie możliwość utrwalenia szkolenia w formie audio-wideo (rejestracja prezentacji).
- g) Wykonawca pokryje wszelkie koszty związane z dojazdem, pobytem oraz wyżywieniem i zakwaterowaniem wykładowców, którzy będą prowadzili szkolenie;
- h) wszyscy uczestnicy szkolenia muszą otrzymać materiały szkoleniowe w języku polskim lub angielskim, w formie papierowej lub elektronicznej;
- i) Wykonawca w ramach prowadzonych szkoleń zobowiązany jest przekazać Zamawiającemu listę obecności, materiały szkoleniowe (prezentacja, ewentualne materiały instruktażowe, itp.), listę wydanych zaświadczeń dla wszystkich uczestników, którzy ukończą szkolenie;
- j) na co najmniej 7 dni roboczych przed rozpoczęciem szkolenia Wykonawca przedstawi Zamawiającemu do akceptacji – harmonogram szkoleń przygotowany w porozumieniu z Zamawiającym obejmujący:
  - programy szkoleń zawierające szczegółowe informacje o zakresie i tematyce oraz rozkładzie zajęć dla poszczególnych szkoleń;
  - metodę oraz formę prowadzenia szkoleń.

#### 1.2.6. ZN-6 Wsparcie Wykonawcy

Wykonawca będzie świadczył usługi wsparcia na zasadach określonych w Rozdziale II punkt 4 OPZ.

## 2. Wymagania techniczne dotyczące oferowanego rozwiązania.

- 2.1. System musi być dostarczony w formie SaaS (Software as a Service). Producent Systemu musi posiadać certyfikację SOC 2 minimum type 2 lub ISO/IEC 27001 oraz gwarantować dostępność usługi w ramach SLA (Service Level Agreement) co najmniej na poziomie minimum 99,9%.
- 2.2. Fizyczna infrastruktura, na której uruchomiony będzie serwer Systemu EDR/XDR MUSI być umiejscowiona na terenie Unii Europejskiej.
- 2.3. Dokumentacja Producenta oferowanego Systemu, o której mowa w punkcie 1.2.1 ppkt 6) MUSI być opublikowana przez Producenta na jego stronie internetowej co najmniej w języku angielskim lub MUSI zostać dostarczona przez Wykonawcę w formie elektronicznej.

- 2.4. System MUSI umożliwiać zarządzanie przez pojedynczy graficzny interfejs z wykorzystaniem przeglądarki internetowej. Połączenie musi być szyfrowane. Zamawiający nie dopuszcza, aby webowy interfejs graficzny korzystał z technologii: flash, silverlight lub java.
- 2.5. Wszystkie składniki Systemu MUSZA być konfigurowalne i zarządzane przez jedną spójną konsolę. Nie dopuszcza się, aby składniki Systemu posiadały oddzielne pulpity/konsole do zarządzania konkretnymi funkcjami Systemu.
- 2.6. System MUSI pozwalać na instalację agenta na systemach operacyjnych co najmniej:
  - 1) Microsoft Windows 10 i nowszych;
  - 2) Linux (co najmniej dystrybucji CentOS, Debian, Red Hat Enterprise, SUSE, Ubuntu), mające aktualne wsparcie wydawców na dzień podpisania umowy;
  - 3) Microsoft Windows Server 2016 i nowszych oraz Windows Server Core 2016 i nowszych.
- 2.7. System MUSI szyfrować dane w trakcie transmisji i w trakcie przechowywania za pomocą protokołów i algorytmów kryptograficznych uznanych za powszechnie bezpieczne. Producent Systemu MUSI zagwarantować, że dostęp do przechowywanych danych posiada tylko i wyłącznie Producent i że dostęp do danych nie jest możliwy dla żadnej ze stron trzecich.
- 2.8. 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>.
- 2.9. System MUSI posiadać możliwość ograniczenia logowania do Systemu tylko ze wskazanych publicznych adresów IP lub za pośrednictwem szyfrowanego połączenia VPN Site-to-Site.
- 2.10. System MUSI umożliwić odzwierciedlenie trójstopniowej struktury podziału stacji roboczych i serwerów w PGL LP.
  - 1) Poziom najwyższy - widoczność wszystkich stacji i serwerów;
  - 2) Poziom pośredni - widoczność stacji i serwerów w obrębie regionu;
  - 3) Poziom najniższy - widoczność stacji i serwerów w obrębie podstawowej jednostki.
- 2.11. Odzwierciedlenie struktury organizacyjnej Zamawiającego zgodne z punktem 2.10 MUSI być osiągnięte za pomocą automatycznej synchronizacji Microsoft Active Directory Zamawiającego lub za pomocą grup dynamicznych filtrujących stacje robocze i serwery np. po ich nazwie, lub innych automatycznych metod synchronizacji.
- 2.12. System MUSI umożliwić konfigurację kont administratorów w oparciu o konta zaimportowane/zsynchronizowane z Microsoft Active Directory Zamawiającego lub utworzone bezpośrednio w Systemie oraz ich przypisanie do danego poziomu struktury Zamawiającego z punktu 2.10.
- 2.13. System MUSI umożliwić stworzenie ról (grup uprawnień) z określonymi prawami w Systemie oraz ich przypisanie do administratorów z punktu 2.14.
- 2.14. Role (grupy uprawnień) powinny obejmować:
  - 1) rola administratora centralnego - pełen dostęp do wszystkich funkcji Systemu (zgodnie z punktem 2.10.1));



- 2) rola administratora regionalnego (zgodnie z punktem 2.10.2)) - poziom operacyjny ograniczony do jednostek organizacyjnych danego regionu, pozwalający przynajmniej na: instalację i deinstalację agentów, podgląd stanu systemu operacyjnego, zarządzanie zdalne hostem, dodawanie wyjątków umożliwiających użycie pamięci USB;
  - 3) rola administratora jednostki (zgodnie z punktem 2.10.3)) – poziom operacyjny ograniczony tylko do danej jednostki organizacyjnej pozwalający przynajmniej na: instalację agentów, podgląd stanu systemu operacyjnego, dodawanie wyjątków umożliwiających użycie pamięci USB.
- 2.15. System MUSI umożliwiać definiowanie pojedynczych wskaźników kompromitacji IOC w formie: MD5, SHA256, nazwy domenowej, adresu IPv4, adresu IPv6 oraz oznaczenia okresu wygaśnięcia znacznika. MUSI istnieć możliwość dodania znacznika ręcznie, zaimportowania znaczników z pliku i poprzez API. System musi umożliwić dodanie co najmniej 50 000 rekordów wskaźników IOC przez Zamawiającego.
  - 2.16. System MUSI umożliwiać definiowanie własnych dashboard'ów z wykorzystaniem predefiniowanych widget'ów oraz kontrolki definiowanych samodzielnie poprzez kwerendy do danych telemetrycznych.
  - 2.17. System MUSI przechowywać informacje o alarmach i incydentach co najmniej przez okres 90 dni.
  - 2.18. System MUSI przechowywać szczegółowe dane telemetryczne z wszystkich zabezpieczonych agentem systemów przez co najmniej 180 dni. Musi istnieć możliwość przeszukiwania tych danych za cały okres retencji zarówno za pośrednictwem konsoli oraz API systemu, a ich przeszukiwanie nie może posiadać żadnych wymogów licencyjnych ani pociągać dodatkowych kosztów.
  - 2.19. System MUSI co najmniej przez 365 dni przechowywać logi audytowe dokumentujące wszystkie akcje podejmowane przez użytkowników zalogowanych do Systemu.
  - 2.20. Wykonawca zapewni Zamawiającemu dostęp do informacji, o których mowa w punktach 2.18 i 2.19 przez okres 6 miesięcy od dnia zakończenia obowiązywania Umowy, tj. Umowa będzie wiązać Strony przez ww. okres po zakończeniu wsparcia Producenta.
  - 2.21. System MUSI posiadać możliwość eksportu wybranych danych do systemu SIEM Zamawiającego za pośrednictwem protokołu syslog lub udostępniać możliwość pobrania tych danych przez system SIEM Zamawiającego za pośrednictwem API Systemu. Jeśli do eksportu danych System wykorzystuje syslog, to w dokumentacji powykonawczej Systemu MUSI być wskazany adres IP lub zakres adresów IP, z których nawiązywane będzie połączenie do serwerów Zamawiającego.
  - 2.22. System MUSI posiadać możliwość alarmowania o wskazanych zdarzeniach poprzez wysłanie korespondencji mailowej na wskazane skrzynki poczty elektronicznej.
  - 2.23. System MUSI umożliwiać wygenerowanie i pobranie pakietu instalacyjnego:
    - 1) w formacie msi lub exe dla systemów Windows; wygenerowane pakiety dla systemów Microsoft Windows muszą mieć możliwość instalacji w trybie

cichym oraz zawierać wstępną konfigurację umożliwiającą połączenie się klienta z serwerem.

2) w formacie rpm, deb lub sh dla systemów Linux.

- 2.24. Zamawiający ze względów bezpieczeństwa i sposobu licencjonowania nie dopuszcza, aby agent wykorzystywał komponenty Oracle Java JRE/JDK.
- 2.25. System MUSI umożliwiać automatyczną aktualizację agentów bezpośrednio z Systemu. System MUSI posiadać mechanizm chroniący przed wysyceniem łącza sieciowego przy przeprowadzaniu aktualizacji agentów, np.: aktualizacja peer-to-peer, aktualizacja z lokalnego serwera cache'ującego, czy różnicowanie tempa propagacji aktualizacji.
- 2.26. Agent Systemu nie może wchodzić w interakcje powodujące nieprawidłowe działanie żadnych zainstalowanych aplikacji na systemach operacyjnych Zamawiającego w szczególności klienta VPN firmy CheckPoint i oprogramowania ActivClient firmy HID,
- 2.27. Agent Systemu nie może wchodzić w interakcje powodujące nieprawidłowe działanie m.in. takich usług serwerowych jak: kontrolerów Microsoft Active Directory, Microsoft SQL Server, serwerów DNS, serwerów DHCP, Microsoft Exchange
- 2.28. System MUSI umożliwiać różnicowanie konfiguracji agenta i polityk bezpieczeństwa poprzez przypisanie różnych profili konfiguracyjnych do wybranych grup hostów lub pojedynczych hostów.
- 2.29. System MUSI umożliwiać przeszukiwanie wszystkich danych telemetrycznych przy pomocy kreatorów lub manualnie z wykorzystaniem kwerend wykonywanych w konsoli i przez API Systemu. Kwerendy muszą pozwalać na filtrowanie oraz obsługę wyszukiwania dowolnego ciągu znaków (free text search) bez wskazywania konkretnego pola. Reguły tworzenia kwerend muszą być opisane w dokumentacji Systemu.
- 2.30. System MUSI umożliwiać zapisanie kwerendy do danych telemetrycznych do prywatnej biblioteki kwerend danego użytkownika lub do globalnej biblioteki kwerend dostępnej dla wszystkich innych użytkowników.
- 2.31. System MUSI umożliwiać wykorzystanie wyników kwerendy do tworzenia periodycznie generowanych raportów.
- 2.32. System MUSI umożliwiać przekształcenie kwerendy do danych telemetrycznych w uruchamianą zgodnie z zadaniem harmonogramem regułę generującą alarmy, jeśli kwerenda zwróciła jakiegokolwiek rekordy.
- 2.33. System w ramach odpowiedzi na incydent MUSI umożliwiać reakcję (remediację) polegającą na zabiciu groźnego procesu i innych procesów, które bezpośrednio i pośrednio doprowadziły do jego uruchomienia, na przeniesieniu groźnych plików do kwarantanny oraz na usunięciu mechanizmów persystencji.
- 2.34. System MUSI automatycznie grupować powiązane alerty w celu przyspieszenia i ułatwienia segregacji i analizy incydentu.
- 2.35. System dla alertów zgrupowanych w ramach incydentu MUSI automatycznie tworzyć łańcuchy przyczynowo skutkowe (w tym w formie graficznej) 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.
- 2.36. System MUSI mapować alerty do matrycy taktyk, technik i procedur w ramach frameworku (metodyki) MITRE ATT&CK bezpośrednio w konsoli alertu.
  - 2.37. System MUSI posiadać mechanizm ochronny przed nieautoryzowanymi próbami wyłączenia agenta nawet przez użytkowników z uprawnieniami administratora. Ręczne wyłączenie modułów bezpieczeństwa lub odinstalowanie agenta na stacji roboczej oraz na serwerach Windows i Linux MUSI wymagać dodatkowego potwierdzenia tej czynności.
  - 2.38. System MUSI umożliwiać połączenie do linii komend systemu operacyjnego wybranej stacji roboczej z zainstalowanym agentem z poziomu konsoli zarządzającej Systemu.
  - 2.39. System MUSI umożliwić wykonywanie skryptów w powershell lub python na zdefiniowanej grupie stacji roboczych i serwerów Windows z zainstalowanym agentem Systemu. Agent dla serwerów Linux musi umożliwiać wykonanie skryptów bash lub python.
  - 2.40. System MUSI mieć możliwość domyślnego blokowania użycia pamięci USB oraz dodawania ich do wyjątków umożliwiających ich użycie. Dodany wyjątek musi dać możliwość automatycznego używania pamięci USB na wszystkich stacjach roboczych z zainstalowanym agentem Systemu.
  - 2.41. System musi posiadać wbudowany moduł klasy ITDR (Identity Threat Detection and Response) zapewniający detekcję, analizę oraz reakcję na zagrożenia związane z kradzieżą tożsamości i nieautoryzowanym dostępem. Moduł ten musi funkcjonować co najmniej w środowiskach Active Directory oraz Entra ID, umożliwiając identyfikację anomalii w uwierzytelnieniu, wykrywanie prób eskalacji uprawnień oraz monitorowanie działań wskazujących na kompromitację kont użytkowników.
3. Opis wymagań dodatkowo punktowanych w ramach kryteriów oceny ofert:  
Wymagania określone w poniższych punktach stają się obowiązkowe dla Wykonawcy/Systemu w przypadku wskazania ich spełnienia w formularzu ofertowym.
- 3.1 **15 pkt** – uruchomienie modułu SOAR (ang. Security Orchestration, Automation and Response) w ramach dostarczonej licencji do wdrażanego Systemu, umożliwiającego: automatyczną obsługę alarmów, w tym m.in. zmianę konfiguracji (orkiestrację) innych systemów bezpieczeństwa oraz rozszerzenie kontekstu alarmu poprzez integrację z systemami trzecimi. Moduł SOAR musi umożliwiać tworzenie spersonalizowanych scenariuszy obsługi (tzw. playbooków) przy użyciu graficznego narzędzia, bez konieczności pisania kodu. Wbudowany moduł SOAR musi umożliwiać orkiestrację zarówno systemów bezpieczeństwa działających w infrastrukturze lokalnej Zamawiającego (on-premises), jak i systemów bezpieczeństwa dostarczanych w modelu chmurowym (SaaS). W szczególności moduł SOAR musi umożliwiać zrealizowanie co najmniej następujących scenariuszy:

- 1) wysłanie powiadomienia mailowego i np. via Microsoft Team, Cisco Webex, jeśli mechanizmy detekcyjno-prewencyjne agenta przestały funkcjonować poprawnie;
  - 2) włączenie skanowania hosta w odpowiedzi na alarm o wskazanej istotności;
  - 3) wysłanie powiadomienia mailowego do określonych adresatów w odpowiedzi na alarm o wskazanej istotności, potwierdzające zastosowanie izolacji sieciowej hosta;
  - 4) w odpowiedzi na alarm o określonej wartości, wskazujący na komunikację z zidentyfikowanymi złośliwymi publicznymi adresami IP, System musi dodać te adresy do listy blokowanych adresów IP na firewallu. Dodanie adresów IP wymaga akceptacji wyznaczonego operatora, który otrzyma powiadomienie o konieczności podjęcia decyzji za pośrednictwem wskazanego kanału np. Microsoft Teams, Cisco Webex lub drogą mailową;
  - 5) w odpowiedzi na alarm o określonej ważności, wygenerowany przez moduł ITDR, musi nastąpić reset hasła użytkownika, którego poświadczenia są powiązane z alarmem. Jeśli użytkownik należy do określonej grupy w katalogu Active Directory, reset hasła wymaga akceptacji wyznaczonego operatora. W przeciwnym przypadku reset hasła odbywa się automatycznie. Operator musi zostać powiadomiony o konieczności podjęcia decyzji za pośrednictwem np. Microsoft Teams, Cisco Webex lub drogą mailową. Użytkownik, którego hasło zostało zresetowane, musi otrzymać powiadomienie o tym fakcie drogą mailową.
- 3.2 **10 pkt** - uruchomienie w ramach dostarczonej licencji do wdrażanego Systemu modułu raportowania o podatnościach systemu operacyjnego oraz zainstalowanych aplikacji na systemach Windows i Linux, a także tworzenie inwentaryzacji zainstalowanych aplikacji i dodatków do przeglądarek. Dopuszcza się rozwiązanie, w którym inwentaryzacja ta będzie wykonywana ad-hoc na żądanie przy wykorzystaniu dedykowanych skryptów (np. Python), a wynik będzie prezentowany w konsoli Systemu.
- 3.3 **5 pkt** – zwiększenie okresu przechowywania szczegółowych danych telemetrycznych z wszystkich zabezpieczonych agentem systemów do 365 dni zgodnie z punktem 2.18.
- 3.4 **Maksymalnie 10 pkt** – Rozbudowa modułu ITDR opisanego w punkcie 2.41: jeśli System będzie umożliwiał realizację poszczególnych funkcji z wykorzystaniem pojedynczego agenta, zasady punktacji dla poszczególnych funkcji zostały opisane poniżej:
- 1) **4 pkt** - Bieżąca weryfikacja konfiguracji środowiska Active Directory pod kątem bezpieczeństwa wraz z rekomendacją zmiany konfiguracji;
  - 2) **1 pkt** - Wykrywanie kont użytkowników posługujących się takim samym hasłem wraz z opcją automatycznego resetu hasła;
  - 3) **1 pkt** - Wykrywanie kont użytkowników posługujących się hasłem, które zostało ujawnione w publicznym wycieku poprzez integrację

z serwisem haveibeenpwned.com lub podobnym wraz z opcją automatycznego resetu hasła.

4) **2 pkt** - Wykrywanie ataków na protokół Kerberos (Golden Ticket, Pass The Hash, Kerberoasting) i LDAP;

5) **2 pkt** - Możliwość blokowania prób logowania po RDP do wskazanych serwerów z komputerów bez zainstalowanego agenta;

4. Usługi świadczenia wsparcia Wykonawcy.

4.1 Usługi wsparcia Wykonawcy będą świadczone w języku polskim.

4.2 Wykonawca udostępni Zamawiającemu elektroniczny kanał zgłaszania zdarzeń, umożliwiający zdalne zgłaszanie i monitorowanie awarii krytycznych oraz awarii niekrytycznych Systemu. Zgłoszenia będą wykonywane przez Administratorów centralnych lub koordynatorów merytorycznych Umowy. Platforma nie może zawierać żadnych ograniczeń, co do liczby dokonywanych zgłoszeń. Informacja o statusach zgłoszeń tj. utworzeniu nowego zgłoszenia/aktualizacji/zamknięcia musi być wysyłana na adresy e-mail Administratorów centralnych oraz koordynatorów merytorycznych Umowy.

4.3 Zgłoszenia mogą być przekazywane w trybie 365 dni w roku, przez 7 dni w tygodniu, 24 godziny na dobę, również w dni wolne od pracy.

4.4 Przewiduje się następujący czas usuwania awarii:

Opis	Potwierdzenie przyjęcia zgłoszenia	Rozwiązanie problemu od momentu zgłoszenia
Awaria krytyczna	1 godz.	24 godz.
Awaria niekrytyczna	4 godz.	5 dni roboczych

**Awaria krytyczna:**

- 1) utrata funkcji monitorowania i wykrywania zagrożeń;
- 2) brak możliwości reagowania na incydenty;
- 3) brak możliwości korzystania z konsoli Systemu;
- 4) w przypadku nieprawidłowego działania agentów na minimum 30% stacji roboczych danej jednostki organizacyjnej zgodnie z punktem 2.10 uniemożliwiające prawidłowe ich funkcjonowanie lub minimum 10% wszystkich stacji roboczych;
- 5) w przypadku nieprawidłowego działania agentów na minimum 5% serwerów danej jednostki organizacyjnej zgodnie z punktem 2.10 uniemożliwiające prawidłowe ich funkcjonowanie lub minimum 1% wszystkich serwerów.

**Awaria niekrytyczna:**

wada skutkująca nieprawidłowym działaniem Systemu powodująca ograniczenie korzystania z Systemu, nie powodująca skutków opisanych dla Awarii Krytycznej.

- 4.5 Wykonawca zapewni Zamawiającemu wsparcie w zakresie instalacji i aktualizacji komponentów Systemu przez okres obowiązywania Umowy.

### **III. Zadanie fakultatywne**

Wykonawca będzie świadczył usługi płatne konsultingowe dla Administratorów centralnych Systemu w liczbie maksymalnie 1000 godzin w okresie od dnia podpisania ostatecznego Protokołu Odbioru Wdrożenia Systemu do końca okresu obowiązywania Umowy. Usługa będzie obejmować między innymi obszary monitorowania, analizy i reagowania na incydenty. Zgłoszenie będzie rozliczane za każdą rozpoczętą godzinę konsultacji telefonicznej lub w formie wideo spotkania. Konsultacja będzie potwierdzana w formie obustronnie podpisanej notatki, która będzie podstawą do rozliczenia godzin konsultacji i wystawienia faktury przez Wykonawcę. Faktury będą wystawiane w okresach trzymiesięcznych na ZILP.

### **IV. W ramach prawa opcji Wykonawca dostarczy licencje wraz ze wsparciem Producenta i Wykonawcy.**

1. W ramach prawa opcji jednostki organizacyjne PGL LP, wskazane w Załączniku do Umowy będą miały możliwość zakupienia dodatkowych licencji Systemu, na zasadach opisanych w Umowie, ważnych do końca trwania umowy, do maksymalnej ilości:
  - 1.1. 10 000 szt. licencji dla roboczych z systemem Microsoft Windows;
  - 1.2. 1100 szt. licencji dla serwerów z systemem Microsoft Windows Server/Linux;
  - 1.3. 100 szt. licencji dla stacji roboczych z systemem Linux.
2. Wykonawca zapewni możliwość zakupienia licencji w ramach „prawa opcji” wraz ze wsparciem Producenta i wsparciem Wykonawcy do końca okresu obowiązywania Umowy zgodnie z poniższymi zasadami:
  - 2.1 licencje mogą być zamawiane przez jednostki organizacyjne PGL LP w okresie od odbioru końcowego Zadania ZN-4, jednak nie później niż na 12 miesięcy przed zakończeniem okresu obowiązywania Umowy;
  - 2.2 Wykonawca zobowiązuje się dostarczyć licencje wraz z potwierdzeniem wykupienia wsparcia Producenta w terminie nie dłuższym niż 5 dni roboczych od dnia zlecenia zakupu i zostać uwidocznione na koncie klienta u Producenta Systemu;
  - 2.3 Wsparcie Wykonawcy dla dostarczonych licencji będzie świadczone w okresie równym wsparciu Producenta.