ZAPYTANIE OFERTOWE
w postępowaniu prowadzonym
zgodnie z zasadą konkurencyjności

Zamówienie w ramach projektu pn *„Wdrożenie do firmy Paged Morąg SA. kompletnego cyberfizycznego systemu, umożliwiającego cyfryzację i robotyzację produkcji sklejki i wprowadzenie założeń przemysłu 4.0. na rzecz zwiększenia odporności do działania w warunkach kryzysowych”* współfinansowane z **KRAJOWEGO PLANU ODBUDOWY, A2.1.1 - Inwestycje wspierające robotyzację i cyfryzację w przedsiębiorstwach**

ZAMAWIAJĄCY:
Paged Morąg S. A.
14-300 Morąg, ul. Mazurska 1,
NIP 7411378488, REGON 510445569

ZAKŁAD PRODUKCJI SKLEJKI W PISZU

kody CPV:
72260000-5 - Usługi w zakresie oprogramowania
48000000-8 Pakiety oprogramowania i systemy informatyczne
72268000-1 Usługi dostawy oprogramowania

PRZEDMIOT ZAMÓWIENIA:
Przedmiotem zamówienia jest:

1) świadczenie usługi cyberbezpieczeństwa opartej o Security Operations Center (SOC) działającej w reżimie 24 H/7 dni w tygodniu wraz z audytami bezpieczeństwa i kampaniami phishisngowymi, szkoleniami dla personelu Zamawiającego i raportowaniem,
2) wdrożenie, uruchomienie i utrzymanie rozwiązania hybrydowego zawierającego w sobie systemy klasy SIEM (Security Information and Event Management), SOAR (Security Orchestration, Automation and Response),
3) wdrożenie, uruchomienie i utrzymanie rozwiązania XDR (Extended Detection and Response).
4) .

1. SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

a) Parametry świadczonej usługi

Z uwagi na fakt iż, Zamawiający dysponuje zdefiniowanym budżetem na zadanie określone zostały poniższe wymagania:

1. Parametry świadczenia usługi:
    a. Ilość korelacji w SIEM – bez ograniczeń,
    b. Ilość podłączonych źródeł danych – bez limitu,

c. Ilość przetwarzanych zdarzeń i incydentów w miesiącu - bez ograniczeń,
d. liczba playbooków - bez ograniczeń,
e. Ilość przetwarzanych danych w systemie SIEM – bez ograniczeń,
f. Ilość dostępnych w miesiącu godzin inżyniera – bez ograniczeń,
g. Ilość godzin dla usług III linii SOC w miesiącu – bez ograniczeń,

2. Zakres objęty usługą:
   a. Liczba endpointów odjętych usługą do uruchomienia XDR-a – 2250
   b. Liczba źródeł -166, w tym:
      i. Urządzenia brzegowe – 6
      ii. Serwery – 90
      iii. Urządzenia sieciowe – 50
      iv. Inne źródła - 20

a) Zakres / specyfikacja usługi SOC

- Monitorowanie poprzez agentów oprogramowania XDR:
  - Stacji roboczych z systemami MS Windows, Linux
  - Serwerów wirtualnych i fizycznych z systemami MS Windows Server i Linux
- Monitorowanie poprzez zbieranie logów:
  - Urządzeń sieciowych (UTM, routerów, Firewalli, przełączników)
  - Systemów aplikacyjnych (usługi pocztowej, usługi WWW, usługi AD, DHCP, DNS itp.)
  - Systemów bezpieczeństwa (systemów AV, DLP, NAC itp.)
- Zbieranie, agregacja, normalizacja i analiza niezbędnych dla świadczenia usługi monitorowania bezpieczeństwa danych, udostępnionych przez Zamawiającego.
- Identyfikację odchyleń od standardowego wzorca zachowań, na podstawie czego Wykonawca będzie dokonywał zgłoszeń do Zamawiającego (alertowania) wraz ze wskazaniem miejsca wystąpienia zdarzenia, określenia jak konkretne zdarzenie czy incydent może wpłynąć na Infrastrukturę Teleinformatyczną Zamawiającego.
- Identyfikację odchyleń od standardów pracy sieci i urządzeń, określonych dokumentami RFC (https://pl.wikipedia.org/wiki/Request_for_Comments).
- W zakresie monitoringu sieci wewnętrznej:
  - Monitorowanie wskazanych urządzeń w sieci, np. monitoring wielkości ruchu generowanego przez urządzenia i stacje robocze, działania skanujące oraz działania wskazujące na działania złośliwe;
  - Monitorowanie zagrożeń na podstawie danych o potencjalnych atakujących i intruzach z wykorzystaniem posiadanego urządzenia przez Klienta klasy IDS/IPS/NIDS;
  - Analiza dostępności (availability) wybranych kluczowych urządzeń.
- W zakresie monitoringu styku z sieciami publicznymi:
  - Monitorowanie ruchu przychodzącego z zewnątrz (źródło, cel, kto inicjował czy inicjował) w oparciu o dane z urządzeń brzegowych;
  - Monitorowanie ruchu wychodzącego na zewnątrz (źródło, cel, kto inicjował czy inicjował) w oparciu o dane z urządzeń brzegowych;
  - Monitorowanie i wykrywanie udostępnianych do sieci publicznej zasobów (otwarte porty, usługi, adresy i porty, wykrywanie zmian i dostępności);
  - Monitoring VPN (wykrywanie anomalii – wymagane logi systemów VPN).
  - Monitoring hostów (stacje robocze, serwery, etc.):
  - Monitorowanie dostępności urządzeń (w tym zgłaszanie braku dostępności oraz potencjalnej przyczyny – przy zapewnieniu logów z

urządzeń);
    - Monitoring kluczowych zdarzeń systemu operacyjnego hosta (wymagane jest ustalenie listy zdarzeń, które mają podlegać monitorowaniu oraz sposób zbierania zdarzeń z hostów);
- Ocena podatności na ataki
    - Monitoring podatności (stacje robocze, serwery, urządzenia sieciowe, oprogramowanie na wskazanych hostach w tym oprogramowanie narzędziowe):
    - Okresowe skany podatności wskazanych komponentów infrastruktury (autoryzowane i nie autoryzowane – wymagana konfiguracja po stronie urządzeń, oraz konfiguracja dostępów i przepuszczania ruchu sieciowego);
    - Okresowe skany inwentaryzacyjne oraz oceny podatności w wynikach skanów dla hostów końcowych (stacje robocze, serwery – wymaga instalacji agenta, konfiguracji urządzeń oraz konfiguracji dostępów i przepuszczania ruchu sieciowego).
- Analiza zachowań użytkowników
    - Oparta na badaniu działań użytkowników (UBA Verification) analiza zachowań użytkowników zapewnia możliwość upewnienia się, że osoby uzyskujące dostęp do zasobów organizacji są tym, za kogo się podają. Możliwości wykorzystywanego narzędzia pomagają identyfikować nieautoryzowane próby dostępu do sieci Klienta.
- Raportowanie:
    - Rodzaj zagrożeń
    - Incydenty oraz sposoby mitygacji wynikających z nich zagrożeń
    - Wykryte podatności i rekomendacje w zakresie ich usunięcia lub wprowadzone środki zaradcze, jeżeli podatności nie można wyeliminować
    - Wykryte zagrożenia w infrastrukturze zamawiającego
    - Znane podatności i zagrożenia pochodzące od producentów systemów, systemów bezpieczeństwa i jednostek CSIRT
    - Alerty spływające ze wszystkich opisanych systemów muszą być prezentowane w jednym centralnym dashboardzie.
    - Raportowanie w cyklach miesięcznych
- Monitorowanie DarkWeb:
    - Poszukiwanie i raportowanie wszystkich informacji związanych z Paged Morąg SA i jego Spółkami zależnymi i mających wpływ na jego bezpieczeństwo cybernetyczne.
    - Upublicznienia danych związanych z domeną klienta (adresy mailowe, nazwy użytkowników, hasła dostępowe, inne informacje związane z domeną),
    - Specyficznych informacji związanych z konkretnymi adresami mailowymi (adresami spoza domeny firmowej),
    - Informacji związanych z publicznymi adresami IP używanymi przez klienta,
    - Informacjami związanymi z konkretnymi użytkownikami po stronie klienta,
    - Zdarzeń związanych z upublicznianiem danych związanych z konkretnymi numerami telefonów.
    - Informacji o podobnych nazwach domen do domeny klienta (zakładanych m.ni. w celu przeprowadzenia akcji phishingowej lub wyłudzania danych, płatności).

(a) Świadczenie usług w ramach I linii wsparcia w zakresie monitorowania i wykrywania incydentów (24x7x365):

- Ciągłe monitorowanie ruchu sieciowego i wykrywanie anomalii za pomocą zaawansowanych reguł korelacyjnych. Analiza logów z urządzeń sieciowych (zapory, rutery) oraz rozwiązań bezpieczeństwa (IDS/IPS).
- Zbieranie i analiza danych bezpieczeństwa z serwerów i komputerów użytkowników w celu identyfikowania złośliwego oprogramowania, anomalii behawioralnych oraz potencjalnych zagrożeń.
- Monitorowanie zmian w atrybutach plików, wykrywanie nieautoryzowanych modyfikacji, takich jak ataki typu ransomware
- Identyfikacja i reagowanie na zagrożenia w czasie rzeczywistym w sieciach oraz na urządzeniach końcowych.
- Wyodrębnianie prawdziwych incydentów od false positive na podstawie analizy logów i Threat Intelligence.
- Realizacja ustalonych procedur reagowania, w tym dokumentowanie i nadawanie priorytetów zdarzeniom oraz powiadamianie II linii wsparcia w przypadku istotnych / krytycznych incydentów
- Rejestracja zdarzeń w systemach obsługi incydentów

(b) Świadczenie usług w ramach II linii wsparcia (24x7x365):)

- Implementacja pułapek wewnątrz sieci w celu wykrywania wewnętrznych zagrożeń oraz zbierania informacji o atakujących.
- Analiza podatności na podstawie danych inwentaryzacyjnych oraz bieżących baz CVE w celu identyfikacji zagrożonych zasobów (w tym regularne skanowanie podatności – minimum 1x na kwartał).
- Audyt i monitorowanie konfiguracji systemów, aby upewnić się, że są zgodne z politykami bezpieczeństwa i standardami branżowymi.
- Symulowane kampanie phishingowe (raz na kwartał dla całej organizacji, raz na rok dla administratorów IT) i dwie kategorie warsztatów (on-site lub on-line dla IT i dla Kadry zarządzającej) podnoszące świadomość pracowników w zakresie zagrożeń cybernetycznych (raz na rok).
- Szczegółowa analiza zdarzeń oraz koordynacja działań w przypadku incydentów
- Dogłębna analiza zdarzeń i incydentów na podstawie danych z systemu SIEM oraz wywiadu o zagrożeniach
- Opracowanie scenariusza mitygacji zagrożenia wynikającego z incydentu oraz wsparcie pracowników zamawiającego przy realizacji przygotowanego scenariusza – usługa realizowana zdalnie.
- Przygotowanie scenariusza działań naprawczych mających na celu usunięcie skutków incydentu.
- Opracowanie wniosków z incydentu, mających na celu ograniczenie możliwości powtórzenia się danego typu incydentu w przyszłości.
- Proponowanie nowych scenariuszy bezpieczeństwa do wdrożenia (nowych zabezpieczeń i działań zabezpieczających systemy) oraz propozycje optymalizacji aktualnie działających scenariuszy mitygacji incydentów.
- Proponowanie zabezpieczenia systemu przed przyszłymi podobnymi incydentami, identyfikowanie przyczyn problemu oraz jego ew. autorów, zebranie dowodów i wreszcie ewentualne powiadomienie odpowiednich służb, o ile jest to wskazane lub wymagane.
- Automatyczne reagowanie poprzez moduł SOAR systemu SIEM i XDR na wykryte zagrożenia i anomalie w zakresie urządzeń sieciowych i serwerów (blokada ruchu, blokada użytkownika, przeniesienie użytkownika/komputera do innej grupy AD itp.).
- Tworzenie reguł SIEM
- Threat Intelligence i Threat Hunting. Proaktywne wyszukiwanie zagrożeń i analizowanie danych na temat specyficznych zagrożeń branżowych
- Tworzenie raportów i zestawień bezpieczeństwa
  - Na bieżąco z poważnych zdarzeń
  - Raz w miesiącu – dla kadry zarządzającej

- Świadczenie niewymienionych powyżej usług konsultingowych z zakresu bezpieczeństwa IT dla pracowników IT Zamawiającego w wymiarze 8h/miesiąc (w godzinach od 9 do 17 w dni robocze).
- Informatyka śledcza, po incydencie pogłębiona analiza, mająca na celu ustalenie przyczyny, zasięgu i wpływu zagrożenia.

b) Zakres / specyfikacja szkoleń i kampanii phishingowych

- Przeprowadzanie akcji Phisingowych połączonych ze szkoleniami z wykorzystaniem platformy e-learing (co najmniej 1 raz w roku).
- Przeprowadzenie badania deklaratywnego zachowania pracowników.
- Przygotowanie wiadomości e-mail łudząco przypominającej korespondencję Zamawiającego.
- Wykorzystanie domeny o nazwie zbliżonej do oficjalnej, publicznie wykorzystywanej domeny Zamawiającego.
- Przygotowanie serwisu WWW łudząco przypominającego serwis WWW Zamawiającego. Za pomocą tego serwisu będzie przeprowadzona próba wyłudzenia danych o charakterze poufnym (specyficzne dane firmowe np. dostępowe do systemów).
- Przygotowanie min. 6 szkoleń związanych z cyberbezpieczeństwem,
- Przygotowanie na żądanie zamawiającego treść wielojęzyczna — treści phishingowe i szkoleniowe (dostępne języki polski, niemiecki, angielski).

c) Wymagania w zakresie świadczenia usługi SOC

Wymaganie	Nazwa i Opis
SOC-1	wdrożenie, uruchomienie i utrzymanie systemu klasy SIEM i SOAR służącego do zbierania i korelacji logów z systemów Zamawiającego przy zachowaniu harmonogramu i bez limitu reguł korelacyjnych
SOC-2	podłączenie do systemu SIEM systemów i urządzeń Zamawiającego w ramach wdrożenia Wykonawca zobowiązany jest do przeprowadzenia audytu/ankietowania, które wskaże kluczowe z punktu widzenia cyberbezpieczeństwa systemy, które należy monitorować, audyt przeprowadzony wraz z Zamawiającym musi wskazać również, którym systemom przypisany zostanie wysoki, średni i niski priorytet w zakresie czasu podłączenia do systemu SIEM; zamawiający może wyrazić zgodę na odstąpienie od integracji systemów o niskim priorytecie pod warunkiem, że Wykonawca przedstawi argumenty na brak wpływu rozwiązania na bezpieczeństwo Zamawiającego
SOC-3	wykonanie playbooków dla wdrożonego systemu SOAR zapewniającego zabezpieczenie systemów. Wykonawca zobowiązany jest również do wskazania zmian i optymalizacji w konfiguracji wykorzystywanych urządzeń Zamawiającego typu UTM, WAF, XDR, AV i innych w celu wykorzystania pełnego potencjału tych rozwiązań w ramach SOC
SOC-4	Zamawiający zakłada, że w ciągu każdego roku trwania umowy do obsługi może zostać dołączonych kolejnych 20 systemów i/lub urządzeń
SOC-5	System SIEM i SOAR muszą przechowywać hasła do monitorowanych systemów, bez możliwości dostępu do nich (haseł) pracowników SOC.
SOC-6	świadczenie usługi pierwszej linii wsparcia SOC - L1, całodobowe 24/7/365, monitorowanie infrastruktury i systemów IT, korelacja zdarzeń, identyfikacja zdarzeń potencjalnie niebezpiecznych, wykrywanie i informowanie o incydentach z czasem reakcji 15 minut Wykonawca zapewnia Zamawiającemu: • przekazywanie informacji o potencjalnych incydentach wypracowanym kanałem

	komunikacji • dostęp do konsoli monitorowania SIEM i SOAR / hybrydy 24/7/365 w uzgodnionym zakresie • możliwość definiowania własnych reguł korelacyjnych SIEM • monitorowanie potencjalnych naruszeń bezpieczeństwa IT • przyjmowanie zgłoszeń o podejrzanych aktywnościach od personelu Zamawiającego • przeprowadzanie wstępnej analizy i eliminacji fałszywych alarmów • współpraca z II linią wsparcia SOC oraz z administratorami lokalnymi • przekazywanie uzgodnionych informacji o incydentach do CSIRT któremu zgodnie z dyrektywą NIC 2 będzie podlegał zamawiający i wypełnianie w imieniu Zamawiającego obowiązków wynikających z ustawy z dnia 10 czerwca 2016 r. *o działaniach antyterrorystycznych* w zakresie stopni alarmowych CRP i monitorowania systemów informatycznych oraz wsparcie Zamawiającego w wypełnianiu zaleceń wynikających z ustawy z dnia 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa* wraz z jej planowaną nowelizacją
SOC-7	świadczenie usługi drugiej linii wsparcia SOC - L2, całodobowe 24/7/365 Wykonawca zapewnia Zamawiającemu: • przygotowanie z administratorami lokalnymi Zamawiającego scenariuszy reakcji na incydenty wynikające z reguł korelacyjnych • przygotowanie z administratorami lokalnymi Zamawiającego planów postępowania z incydentami • analiza zdarzeń i obsługa incydentów, zebranie informacji niezbędnych do poprawnego obsłużenia incydentu, weryfikacja poprawności i kompletności dostarczonych danych źródłowych • wydanie zaleceń i opracowanie scenariusza mitygacji zagrożenia wynikającego z incydentu oraz wsparcie administratorów IT przy realizacji przygotowanego scenariusza • opracowanie wniosków z incydentu, mających na celu ograniczenie możliwości powtórzenia się danego typu incydentu w przyszłości • przygotowanie planu działania w celu ograniczenia strat związanych z incydentem, pozyskanie dodatkowych danych niezbędnych do obsługi incydentu (z I linii wsparcia, z logów systemowych, ze źródeł zewnętrznych – CSIRT, użytkowników i innych) • proponowanie nowych reguł korelacyjnych i scenariuszy SIEM i playbooków (zautomatyzowanych reakcji na incydenty) SOAR do wdrożenia w systemie SIEM/SOAR i propozycje optymalizacji aktualnie działających scenariuszy bezpieczeństwa • proponowanie rozszerzenia zakresu monitorowania o kolejne systemy teleinformatyczne Zamawiającego, przygotowywanie raportów dla Zamawiającego i jego dostawców • Wykonawca może w ramach usługi L2 uruchamiać okresowe testy podatności • Wykonawca może dokonywać niezautomatyzowanej analizy logów Zamawiającego w celu proaktywnego poszukiwania incydentów i zabezpieczenia materiałów po incydencie
SOC-8	świadczenie usługi trzeciej linii wsparcia SOC - L3, która obejmuje pomoc zdalną lub na miejscu w zakresie usunięcia skutków zaistniałego incydentu, rekomendacje w zakresie zachowania materiału dowodowego dla Zamawiającego wraz z pełną analizą powłamaniową, analizę złośliwego oprogramowania;
SOC-9	wykonanie audytów podatności zgodnie z poniższymi wymaganiami • wykonanie audytu i raportu podatności co 6 miesięcy w zakresie infrastruktury zewnętrznej Zamawiającego oraz co 12 miesięcy w zakresie infrastruktury wewnętrznej i stacji roboczych Zamawiającego - raporty muszą obejmować całą infrastrukturę serwerową, w tym wirtualną, kluczowe urządzenia i stacje robocze wykorzystywane przez

	użytkowników Zamawiającego (zakres infrastruktury kluczowej i kluczowych stacji roboczych zostanie ustalony w czasie wstępnego audytu) • wykrywanie podatności w systemach i infrastrukturze Zamawiającego wraz z przekazywaniem na bieżąco rekomendacji z podziałem na podatności wysokiego ryzyka – koniczne do usunięcia (niemożliwe jest ich monitorowanie i zabezpieczenie systemów), średniego ryzyka (włączone do stałego monitorowania, ale generujące ryzyka), podatności niskiego ryzyka – bezpieczne w przypadku monitorowania
SOC-10	Raportowanie: • każdorazowo przy wystąpieniu incydentu, który zwiera informacje o incydencie, wpływ na środowisko Zamawiającego, sposoby mitygacji, • miesięczny raport w zakresie wykonywanej usługi, który zawiera listę zaobserwowanych zdarzeń w podziale na kategorie zdarzeń typu (DDoS, ransomeware, phishing, brute force, itp.) oraz wykorzystane zabezpieczenia miesięczny raport zawierający informacje o stosunku zdarzeń false positive vs true positive z każdej reguły korelacyjnej wraz z rekomendacją ewentualnych zmian

d) Wymagania w zakresie wdrożenia, uruchomienia i utrzymania rozwiązania hybrydowego łączącego funkcjonalności systemów klasy SIEM (Security Information and Event Management) i SOAR (Security Orchestration, Automation and Response)

Wymaganie	Opis
SISO-1	wdrożone systemy klasy SIEM i SOAR muszą być produktami komercyjnym, oferowanymi na rynku wraz ze wsparciem producenta rozwiązania; wyklucza się rozwiązania pozbawione wsparcia producenta
SISO-2	Wykonawca jest zobowiązany dostarczyć/posiadać wszystkie niezbędne licencje do uruchomienia systemów SIEM i SOAR pozwalające na świadczenie usług na systemach, na czas trwania umowy; w przypadku systemów instalowanych
SISO-3	system SIEM i SOAR muszą umożliwić autoryzację użytkowników oraz precyzyjne nadawanie uprawnień dla administratorów i użytkowników oraz zapewniać pełną ich rozliczalność minimum w zakresie login/logoff, zmiana konfiguracji systemu, wykonane akcje; Zamawiający oczekuje minimum dostępu read-only dla systemu
SISO-4	system klasy SIEM musi pozwolić na zbieranie logów z systemów Zamawiającego, w szczególności pozwolić na zbieranie informacji z końcówek i systemów klasy XDR, a w szczególności Cynet360 oraz z urządzeń UTM; system klasy SOAR musi umieć wykonywać akcje na końcówkach z wykorzystaniem wymienionych wyżej systemów XDR oraz urządzeniach typu UTM
SISO-5	system SIEM musi posiadać zaimplementowane mechanizmy automatycznej kontroli własnego stanu oraz alarmowania w przypadku wykrytych nieprawidłowości (ang. healthcheck)
SISO-6	system SIEM musi umożliwiać uwierzytelnienie oraz szyfrowanie połączenia między wszystkimi komponentami systemu
SISO-7	system SIEM musi umożliwiać budowanie profili aktywności użytkowników oraz zasobów IT poprzez integrację z AD i pobieranie danych odnośnie użytkowników i zasobów i korelowanie ich ze zdarzeniami wykrytymi w infrastrukturze Zamawiającego

SISO-8	Wykonawca musi dostosowywać na bieżąco reguły korelacyjne do zmieniającego się środowiska Zamawiającego tak, aby maksymalizować wykrywanie incydentów i minimalizować fałszywe alarmy
SISO-9	system SOAR musi zapewniać możliwości orkiestracji i automatyzacji bezpieczeństwa oraz odpowiedzi na incydenty
SISO-10	Wykonawca musi dostosowywać na bieżąco playbooki do zmieniającego się środowiska Zamawiającego tak, aby maksymalizować automatyczną reakcję na incydenty
SISO-11	aktywności użytkowników systemu SOAR musi być śledzona i logowana na potrzeby ewentualnej analizy

a) Wymagania w zakresie szkoleń

Wymaganie	Opis
EDU-1	Pakiet szkoleniowy w którego skład wchodzą 5 szkoleń oraz moduły treningowe dostępne dla każdego pracownika w formie kursu online do samodzielnego przerobienia
EDU -2	Poziom zdawalności testu zostanie ustawiony po konsultacjach z zamawiającym
EDU -3	Zakres raportu końcowego z przeprowadzonych szkoleń: • Podsumowanie Szkolenia ▪ Tytuł i cel szkolenia: Krótki opis szkolenia, jego głównych celów i oczekiwanych korzyści dla uczestników. ▪ Data i czas trwania: Informacje, kiedy szkolenie zostało zainicjowane i zakończone. ▪ Format szkolenia: Opis platformy e-learningowej i narzędzi wykorzystanych do przeprowadzenia szkolenia. • Uczestnictwo ▪ Liczba zaproszonych uczestników: Ile osób zostało zaproszonych do udziału w szkoleniu. ▪ Liczba uczestniczących osób: Ile osób faktycznie wzięło udział w szkoleniu. ▪ Frekwencja: Procent uczestników, którzy faktycznie wzięli udział w szkoleniu w stosunku do liczby zaproszonych. • Wyniki Szkolenia ▪ Oceny końcowe: Jak uczestnicy poradzili sobie z końcowymi testami lub ocenami. • Zaangażowanie Uczestników ▪ Feedback uczestników: Zbieranie i analiza opinii uczestników na temat użyteczności szkolenia, jakości materiałów i ogólnej satysfakcji. • Ocena Efektywności Szkolenia ▪ Analiza osiągniętych celów szkoleniowych: Ocena, czy i w jakim stopniu osiągnięto cele szkoleniowe.

	▪ Rekomendacje dla przyszłych szkoleń: Sugestie dotyczące zmian w treści, formacie lub dostarczaniu materiału szkoleniowego, na podstawie analizy danych i feedbacku. • Działania Poprawkowe i Kontynuacja Edukacji ▪ Zaplanowane działania poprawkowe: Działania zaplanowane w odpowiedzi na wykryte luki w wiedzy lub umiejętnościach. ▪ Zaplanowane kolejne kroki szkoleniowe: Informacje o przyszłych szkoleniach lub kursach uzupełniających. • Podsumowanie i Wnioski ▪ Ogólne wnioski: Podsumowanie kluczowych wniosków z przeprowadzonego szkolenia. Zalecenia strategiczne: Zalecenia na poziomie organizacyjnym dotyczące dalszego rozwoju programów szkoleniowych z cyberbezpieczeństwa.
EDU -4	• Zakres podstawowy szkoleń: • Podstawowe pojęcia odnośnie bezpieczeństwa informacji, cyberbezpieczeństwa • Zagrożenia związane z cyfrową działalnością gminy ▪ Rodzaje zagrożeń w cyberprzestrzeni ▪ Rodzaje zabezpieczeń, rodzaje działań zabezpieczających ▪ Podstawy bezpiecznego zachowania w cyberprzestrzeni • Rozpoznawanie zagrożeń i im przeciwdziałanie • Bezpieczne hasła – jakie, jak je przechowywać • Bezpieczne poruszanie się w cyfrowym świecie – media społecznościowe, email, strony www, sklepy internetowe ▪ Zasady bezpiecznej pracy w cyfrowym świecie • Nośniki zewnętrzne • Komunikatory i media społecznościowe • Poczta elektroniczna ▪ Zarządzanie zdarzeniami i incydentami bezpieczeństwa • Wdrożenie i utrzymanie systemu zarządzania bezpieczeństwem informacji ▪ Źródła wymagań i zaleceń - norma ISO 27001 ▪ Role i odpowiedzialności. ▪ Klasyfikacja informacji. ▪ Analiza ryzyka bezpieczeństwa informacji. ▪ Zarządzanie ryzykiem bezpieczeństwa informacji. ▪ Zabezpieczenia techniczne i organizacyjne. ▪ Struktura dokumentacji systemu zarządzania. ▪ Szkolenia pracowników. ▪ Utrzymanie systemu zarządzania • Zagrożenia jakie można spotkać w Internecie, • Metodyka skutecznego oceniania wiarygodności otrzymanej wiadomości mailowej, • najczęściej spotykane zagrożenia związane z korzystaniem z serwisów społecznościowych, • Czym jest ransomware i jak się przed nim bronić.

b) Wymagania w zakresie kampanii phisihingowych

Wymaganie	Opis
PH-1	Do przeprowadzenia kampanii phisingowych wykorzystane muszą być komercyjne platformy lub oprogramowanie komercyjne służące do tworzenia tego typu platform

PH-2	Koszty subskrypcji platformy phisingowej pokrywa wykonawca
PH-3	Każda z kampanii phisingowych zostanie uzgodniona z zamawiającym w zakresie typów maili i ich formy.
PH-4	Raporty bieżące dotyczące kampanii phishingowej powinny zawierać: • Statystyki kampanii w tym: ▪ Ilość wysłanych maili, ▪ Ilość dostarczonych maili, ▪ Ilość skompromitowanych kont pocztowych, • Informacje o użytkownikach, w tym: ▪ Określenie poziomu ryzyka użytkownika dla organizacji, ▪ Status realizacji kampanii przez użytkownika, ▪ Status realizacji szkoleń przez użytkownika,
PH-5	Planowanie Kampanii • Realistyczne Symulacje Ataków Phishingowych • Scenariusze dostosowane do Zamawiajacego: Symulacje powinny odwzorowywać ataki, na które Zamawiający może być rzeczywiście narażony, np. fałszywe faktury, podrobione pisma urzędowe, próby wyłudzenia informacji o kontrachentach. • Zaawansowana personalizacja kampanii: Możliwość dostosowywania treści phishingowych do różnych działów Zamawiajacego, np. różne kampanie dla działu finansowego, kadr z uwzględnieniem języka specyficznego dla danego obszaru.
PH-6	Śledzenie Postępów i Raportowanie • Zaawansowane narzędzia raportowe: Platforma powinna oferować szczegółowe raporty dotyczące wyników kampanii phishingowych i postępów w szkoleniach, z opcją dostosowania do wymagań urzędu. • Wizualizacja danych: Dashboardy i infografiki prezentujące kluczowe metryki, które pomagają w zrozumieniu skuteczności kampanii i szkoleń.
PH-7	Bezpieczeństwo i Prywatność • Szyfrowanie danych wrażliwych: Pełne szyfrowanie danych osobowych i innych wrażliwych informacji zarówno podczas transmisji, jak i w spoczynku. • Zgodność z RODO i lokalnymi przepisami o ochronie danych: Zapewnienie, że wszystkie operacje na danych są zgodne z obowiązującymi przepisami o ochronie danych osobowych.
PH-8	Zarządzanie Kampaniami • Automatyzacja procesów: Narzędzia do automatyzacji uruchamiania i zarządzania kampaniami phishingowymi, minimalizujące potrzebę interwencji manualnej. • Interaktywny feedback: Możliwość zgłaszania przez użytkowników podejrzanych wiadomości, co może być wykorzystane do poprawy przyszłych kampanii.
PH-9	Wsparcie Techniczne i Szkoleniowe • Dostępność wsparcia technicznego: Łatwy dostęp do wsparcia technicznego w razie wystąpienia problemów z platformą. • Materiały pomocnicze dla administratorów: Kompleksowe przewodniki i materiały szkoleniowe, wspierające zarządzanie

	platformą.
PH - 10	Raport końcowy z zakończenia kampanii phishingowej powinien zawierać: • Podsumowanie Kampanii ▪ Opis kampanii: Krótkie streszczenie celów kampanii, zastosowanych technik phishingowych, i grupy docelowej. ▪ Okres przeprowadzenia kampanii: Data rozpoczęcia i zakończenia kampanii. • Statystyki Ogólne ▪ Liczba wysłanych wiadomości: Ile e-maili phishingowych zostało wysłanych w ramach kampanii. ▪ Procent otwartych e-maili: Jaki procent odbiorców otworzył e-mail. ▪ Procent kliknięć w linki: Jaki procent osób kliknął w linki zawarte w e-mailach phishingowych. ▪ Liczba wprowadzonych danych: Ile osób podało swoje dane na fałszywej stronie. • Analiza Zachowań Użytkowników ▪ Typowe błędy: Jakie błędy najczęściej popełniali pracownicy, np. ignorowanie oznak ostrzegawczych. ▪ Wzorce odpowiedzi: Czy istnieją konkretne wzorce w odpowiedziach różnych grup pracowników lub działów. ▪ Porównanie z innymi kampaniami: Jak kampania wypada na tle danych statystycznych z innych kampanii pod względem efektywności i zachowań pracowników. ▪ Szczegółowe Wyniki dla Różnych Grup Docelowych • Wyniki według działów: Szczegółowa analiza reakcji różnych działów lub grup zawodowych na kampanię. • Wyniki według lokalizacji: Jeśli urząd ma więcej niż jedną lokalizację, analiza, jak reakcje różniły się między lokalizacjami. • Rekomendacje i Ścieżki Naprawcze ▪ Obszary wymagające poprawy: Wskazanie, które obszary wiedzy lub świadomości wymagają dodatkowych działań edukacyjnych. ▪ Zaproponowane działania szkoleniowe: Propozycje konkretnych szkoleń lub warsztatów, które mogłyby zwiększyć świadomość i umiejętności pracowników. ▪ Plan poprawek: Krótkoterminowe i długoterminowe działania, które urząd powinien podjąć, aby poprawić bezpieczeństwo informacyjne. • Feedback od Uczestników

c) Wymagania w zakresie systemu XDR

Wymaganie	Opis
XDR-1	***Prewencja i detekcja zagrożeń:*** • System ma umożliwiać pracę w 2 trybach: ▪ Tryb Detekcji – wykrywanie zagrożeń, informowanie o nich, jednak bez automatycznych remediacji;

	▪ Tryb Prewencji – wykrywanie zagrożeń oraz wykonywanie automatycznych remediacji, akcji które powstrzymują zagrożenie; • System ma umożliwiać pracę autonomiczną tj. agent bez kontaktu z konsolą zarządzającą ma wykonuje wszystkie akcje detekcji i prewencji według parametrów lokalnych (pobranych w ostatniej sesji z konsolą); • System ma obsługiwać systemy operacyjne: ▪ MS Windows – klienckie i serwerowe; ▪ Linux – systemy 64 bitowe; ▪ MacOS; • System ma monitorować i wizualizować zagrożenia cybernetyczne w czasie rzeczywistym zarówno na fizycznych jak i wirtualnych komputerach użytkowników końcowych oraz serwerach. • System ma zapewnić ochronę przed złośliwym oprogramowaniem na podstawie sygnatur, analizy zachowania aplikacji w czasie rzeczywistym oraz przy wykorzystaniu statycznych mechanizmów uczenia maszynowego • System ma identyfikować złośliwe oprogramowanie w danych znajdujących się w spoczynku poprzez możliwość konfiguracji profili skanowania AV • System ma wykorzystywać metadane (IOC) dostarczone przez producenta rozwiązania do analizy i wykrywania zagrożeń • System ma wykorzystywać serwisy reputacyjne do analizy online reputacji plików • System ma wykorzystywać metadane (IOC) dostarczone przez dział SOC do analizy i wykrywania zagrożeń, pozwala wykonywać poszukiwania zagrożeń w oparciu o takie parametry jak Sha256, MD5 itp. • System ma umożliwiać wykrywanie zdarzeń dotyczących bezpieczeństwa, pochodzących przynajmniej z niżej wymienionych obszarów w infrastrukturze informatycznej: ▪ ruchu sieciowego ▪ urządzeń końcowych (stacje robocze oraz serwery) ▪ zachowanie plików na urządzeniach końcowych ▪ Zachowanie użytkowników na urządzeniach końcowych • System ma posiadać mechanizmy ograniczające generowanie fałszywych alarmów z wykorzystaniem co najmniej poniższych metod ▪ Automatycznej weryfikacji wskaźników wykrytych zagrożeń w odniesieniu do wbudowanej bazy znanych zagrożeń, która jest na bieżąco uaktualniana za pośrednictwem dostępnego w chmurze producenta zestawu narzędzi, ▪ Meta-skanowanie antywirusowe, wykorzystujące wszystkie silniki dostępne w bazie VirusTotal. ▪ Wzorce schematów działania malware oraz bazy przykładowych kodów źródłowych (ang. Post Ex Sources) ▪ Manualne oznaczanie poziomu ważności wykrytego zagrożenia na podstawie analizy przez zespół SOC. • System ma wykrywać nietypowe zachowania urządzeń, użytkowników oraz plików w sieci. • System ma zbierać wskaźniki kompromitacji (IOC) i zachowania z obszaru stacji końcowych, zachowania użytkowników, połączeń sieciowych oraz aktywności w systemie plików. • System ma posiadać funkcjonalność samodzielnego „uczenia się” zachowań typowych w organizacji poprzez zbieranie i ustalenie wskaźników dotyczących zachowania monitorowanych elementów w lokalnej oraz rozległej sieci komputerowej. • System ma profilować typowe zachowania i odstępstwa od nich • Umożliwia stworzenie tzw. „białych listy” (ang. White list) znanych i zaufanych plików, zachowań na każdym monitorowanym urządzeniu w celu obniżenia poziomu fałszywych alarmów i poprawy wydajności działania całego rozwiązania. • System ma posiadać funkcjonalność szczegółowego skanowania zachowania

	konkretnego wykonywalnego pliku na chronionej stacji poprzez automatyczny sandbox lub poprzez analizę pliku przez dział SyOps producenta systemu XDR • System ma posiadać funkcjonalność nadzoru pamięci zewnętrznych USB w zakresie: ▪ Rozpoznania i blokowania urządzeń pamięci zewnętrznej USB ▪ Tworzenia dopuszczonych w organizacji urządzeń USB (tzw. White List), które będą monitorowane i dopuszczone do użytkowania • S System ma skanowanować urządzenia USB modułem AV w przypadku podłączenia urządzenia do portu USB.
XDR-2	***mylenia atakującego*** • System XDR ma posiadać wbudowany mechanizm pułapek (ang. Decoys) wspomagający wczesne wykrywanie nieznanych ataków oraz źródeł zagrożeń a także aktywności szpiegowskiej w infrastrukturze informatycznej w oparciu o obiekty: ▪ Hostów (fałszywe usługi sieciowe, serwery i stacje końcowe) ▪ Użytkowników ▪ Plików • System ma posiadać wbudowany mechanizm pułapki przeciw zagrożeniu klasy Ramsomware, poprzez budowanie odpowiednio zdefiniowanych katalogów i plików, które pozwalają wychwycić działanie procesu ramsomware.
XDR-3	***reakcji i remediacja*** • System ma posiadać możliwość wykonania manualnych i automatycznych działań naprawczych (ang. Remediation), niwelujących skutki ataków oraz zapobiegających podobnym zdarzeniom w przyszłości. • System ma posiadać wykrywanie w czasie rzeczywistym i automatyczne blokowanie na chronionych stacjach końcowych i serwerach poprzez analizę behawioralną m.in. zagrożeń typu: ▪ Ransomware ▪ Memory Injection • System ma posiadać możliwość automatycznego zabicia (ang. kill) procesu, jeśli wykryje metodę ataku typu Memory Injection, Ramsomware itp. • System ma posiadać powiadamia o wykryciu zagrożenia na stacji końcowej poprzez wyświetlony komunikat, w panelu zarządzania (na konsoli zarządzającej) oraz drogą mailową na wskazaną skrzynkę pocztową i ma możliwość wysyłania logów do zewnętrznego systemu SIEM. • System ma posiadać możliwość wykonania predefiniowanych akcji naprawczych (ang. Remediation) bezpośrednio na chronionych komputerach i serwerach, polegających na możliwości utworzenia reguł, które umożliwią usuwanie w sposób automatyczny każdego kolejnego zagrożenia o podobnym charakterze, z możliwością indywidualnego dostosowania sposobu reakcji systemu. • System umożliwiać podjęcie automatycznej lub ręcznej akcji na poniższych obiektach: ▪ Plik (usuń plik, poddaj plik kwarantannie, zabij powiązany proces) ▪ Host (zrestartuj hosta, wyłącz hosta, wyłącz wszystkie karty sieciowe, izoluj – zablokuj komunikację sieciową poza komunikacją związaną z działaniem Systemu, uruchom komendę) ▪ Użytkownik (zablokuj użytkownika) ▪ Sieci (blokuj ruch) • System ma umożliwiać tworzenie złożonych remediacji (Playbook) w oparciu o predefinowane proste remediacje, jak również przez tworzone własne skrypty remediacyjne. • Playbooki powinny zawierać możliwość wykonywania akcji równolegle tj. kilka akcji jednocześnie lub szeregowo tj. następna akcja wykonuje się po zakończeniu poprzedniej. • Dodatkowe remediacje (playbooki) można dopisywać do istniejących

	automatycznie przypisanych przez system i będą one wykonane dodatkowo po nich jako dodatkowa remediacja • Rozwiązanie ma posiada możliwość wysyłania nieznanych plików wykonywalnych do analizy w środowisku Sandbox oraz w przypadku konieczności dokładniejszej analizy do CyOps producenta oprogramowania XDR.
XDR - 4	**raportowania** • System koreluje różne elementy aktywności na hoście w celu oceny poziomu zagrożenia w postaci liczbowej odrębnie dla każdego hosta, pliku, użytkownika oraz zewnętrznych adresów IP. Wskaźnik ryzyka wyliczany jest w systemie na podstawie : ▪ wskaźniki kompromitacji (IOC) ▪ zachowania w zakresie połączeń sieciowych ▪ aktywności procesów ▪ aktywności użytkownika ▪ aktywności w ramach systemu plików • System XDR umożliwia generowanie raportów na podstawie zebranych danych, takich jak np.: ▪ Alerty otwarte i zamknięte ▪ Szczegółowe raporty związane z wykrytym ryzykiem ▪ Trendy alertów, pokazujące podatne elementy w sieci w funkcji czasu ▪ Najczęstsze typy alertów • Możliwe do wygenerowania z Systemu raporty powinny zawierać informacje o poziomie ryzyka związanego z danym obiektem. • Rozwiązanie umożliwia generowanie raportów w postaci plików csv, excel lub pdf
XDR - 5	**badania poincydentalne oraz wyszukiwanie zagrożeń** • System ma posiadać możliwość przeprowadzania szczegółowych analiz po włamaniowych. Wspiera działania takie jak przeszukiwanie drzew procesów biorących udział w incydencie. Wspiera wyszukiwanie w organizacji plików biorących udział w incydencie np. poprzez wynik funkcji skrótu MD5. • System ma posiadać możliwość wysłania podejrzanych plików do wykonania w sandbox producenta lub w infrastrukturze lokalnej. • System ma posiadać możliwość wysłania podejrzanych plików do SOC producenta w trybie 24/7 celem analizy, oceny ryzyka oraz zalecanych działań naprawczych. • System ma umożliwiać badanie zdarzeń dotyczących bezpieczeństwa, pochodzących przynajmniej z niżej wymienionych obszarów w infrastruktury informatycznej: ▪ ruchu sieciowego, ▪ urządzeń końcowych (stacje robocze oraz serwery), ▪ zachowanie plików na urządzeniach końcowych, ▪ zachowanie użytkowników. • System ma zbierać wskaźniki kompromitacji (IOC) i zachowania z obszaru stacji końcowych, zachowania użytkowników, połączeń sieciowych oraz aktywności w systemie plików. • System w zakresie wsparcia analiz po włamaniowych i prowadzenia dochodzeń (and. Forensics) ma umożliwiać przeszukiwanie IOC w powiązaniu z poniższymi obiektami: ▪ Pliki, ▪ Hosty, ▪ Użytkownicy, ▪ Połączenia sieciowe (zarówno w oparciu o adresy domenowe jak i adresy IP), • Rozwiązanie w obszarze wsparcia zaawansowanych analiz i przeszukiwania danych ma umożliwiać złożone przeszukiwanie zdarzeń dotyczących obiektów

	plikowych, hostów, połączeń sieciowych poprzez tworzenie złożonych filtrów opartych na regułach takich jak: ▪ Rozpoczyna się od ▪ Kończy się na ▪ Zawiera ▪ iNie Zawiera ▪ Jest równy ▪ Nie równa się ▪ większy niż ▪ mniejszy niż ▪ równy ▪ mniej niż ▪ więcej niż ▪ równe ▪ Od data ▪ Do data ▪ Dnia (określony dzień) • System ma posiadać na podstawie złożonych wyszukań tworzenie alertów, nadawać im odpowiednie priorytety i oraz przypisywać do nich działania remediacyjne. • Dane telemetryczne, metadane zbierane przez agentów muszą być przechowywane przez okres co najmniej 90 dni a informacje o alertach, zdarzeniach wykrytych przez system dostępne są bez ograniczeń czasowych • System ma posiadać narzędzie do analizy zbieranych ze stacji logów z systemów Windows oraz informacji o działaniach na plikach i umożliwia ich analizę. • W ramach działań forensic system ma prezentować powiązane obiekty do aktualnie wybranego w postaci przynajmniej uproszczonej (zminimalizowanej) linii czasowej z listą informacji dystynktywnych dla danego typu obiektu. • System ma zapewniać informacje o domenach, do których były zapytania z monitorowanych hostów. • System ma generować automatycznie listę domen z którymi występowała komunikacja, która zawiera poniższe informacje: ▪ Nazwa Internetowa domeny ▪ Poziom ryzyka związany z domeną ▪ Klasyfikacja domeny (biała lista, brak klasyfikacji) ▪ Data i czas, kiedy po raz pierwszy wystąpiła komunikacja z domeną ▪ Data i czas, kiedy po raz ostatni wystąpiła komunikacja z domeną ▪ Liczba hostów komunikujących się z daną domeną ▪ Liczba adresów IP rozwiązywanych pod daną domeną ▪ Liczba lokalnych adresów IP łączących się z daną domeną ▪ Liczba użytkowników łączących się z daną domeną ▪ Dla listy inwentaryzacyjnej połączeń monitorowane są m.in. pola: ▪ Nazwy hostów związanych z ruchem sieciowym ▪ Poziom ryzyka związany z danym połączeniem ▪ Lokalny adres IP związany z ruchem sieciowym ▪ Lokalny port źródłowy ▪ Docelowe IP związane z ruchem sieciowym ▪ Port docelowy związany z ruchem sieciowym ▪ Data i czas, kiedy po raz pierwszy dany ruch sieciowy był widoczny ▪ Data o czas, kiedy po raz ostatni dany ruch sieciowy był widoczny
XDR - 6	***interfejs użytkownika/administratora*** • System ma zapewnić dostęp do panelu operatorskiego przez zwykłą przeglądarkę (GUI webowe). • System ma posiadać Wyświetla dodatkowe informacje związane z alertami, m.in.: opis zdarzenia, zalecenia dotyczące usunięcia przyczyn alertu oraz wszystkie

	powiązane ze zdarzeniem obiekty (hosty, użytkowników, pliki i adresy IP). • System ma posiadać panel informacyjny, w którym są wyświetlane informacje o statusie podatności monitorowanych urządzeń końcowego, alertach, skanowaniach i przeprowadzonych analizach. • System ma na konsoli operatorskiej wyświetlanie wygenerowanych przez system aktywnych alertów oraz status skompromitowania poszczególnych urządzeń końcowych. • System ma wyświetlać informacje potrzebne podczas analizy dokonywanej po incydentach w zakresie informacji o plikach, użytkownikach, stacjach i ruchu sieciowym. • System ma wyświetlać informacje o wykonanych akcjach naprawczych. • System ma wskazywać listę chronionych hostów z informacją o aktualnym stanie ich ochrony. Przypisuje poziom ryzyka hostom wyrażony w postaci liczbowej na podstawie powiązanych z danym hostem zdarzeniami/anomaliami. • System ma zapewniać ogólny widok z poziomu panelu konsoli do zarządzania (ang. dashboard), pokazujący aktualny pogląd sytuacyjny, zawierający przynajmniej liczbę otwartych alertów w podziale na monitorowane obszary takie jak: pliki, użytkownicy, stacje i komunikacja sieciowa. • System ma umożliwiać aby wykryte alerty były dodatkowo opisywane kolorem wskazującym na ich ważność za pomocą zróżnicowania kolorystycznego, przy czym alerty krytyczne są wyświetlane zgodnie z branżowymi standardami na czerwono, a alerty o średnim poziomie krytyczności w kolorze pomarańczowo/żółtym. Zdarzenia o niższym poziomie są wyświetlane w odcieniach zieleni lub niebieskiego. • System ma posiadać widok prezentujący ilość alertów na wykresie czasowym, zawierającym liczbę alertów wygenerowanych w poszczególnych dniach w podziale na monitorowane obszary w tym na: hosty, pliki, użytkowników oraz ruch sieciowy. • Dostępne w systemie widoki powinny pozwalać zarządzać alertami i posiadać listy alertów w podziale na: otwarte, zamknięte, oznaczone do ignorowania przez operatora systemu. • Rozwiązanie z interfejsu administratora ma umożliwiać automatyczne tworzenie na urządzeniach końcowych fałszywych obiektów, tzw. pułapek (ang. Decoy), których zadaniem jest wprowadzanie atakujących w błąd. Zestaw pułapek jest automatycznie generowany z poziomu serwera centralnego i nie wymaga manualnego przygotowania na hostach. Włączanie i wyłączanie funkcjonalności Decoy jest dostępne z poziomu konsoli administratora systemu. • System ma posiadać możliwość gradacji poziomu dostępu do konsoli administracyjnej w sposób granularny wraz z możliwością tworzenia własnych poziomów dostępu. • Rozwiązanie ma posiadać możliwość tworzenia WhiteList i wykluczeń odnośnie reguł korelacyjnych (alertów) dla poniższych wszystkich wykrywanych zagrożeń a między innymi dla: ▪ Skanowanie portów ▪ Zatruwanie tablic ARP ▪ Atak typu Pass the Hash ▪ Wykrycie Mimikatz ▪ Wykrycie Powershell Empire ▪ Zdarzenia administracyjne związane z VSS ▪ Tunelowanie DNS ▪ Tunelowanie ICMP ▪ Atak Brute Force ▪ Wykrycie narzędzi Hackerskich ▪ Wykrycie narzędzi do zdalnego dostępu ▪ lWykrycie Trojana ▪ Wykrycie tunelowania Http

	▪ Alerty związane wykorzystaniem NetBIOS (np. atak LLMNR) • System ma umożliwiać wyświetlanie w konsoli operatorskiej także tych alertów, które zostały przejrzane i zostały zamknięte przez operatora systemu. • System ma umożliwiać wyeksportowanie m.in. w formacie Excel (*.xlsx) Listy alertów. • System ma posiadać widoki dostarczające informacje z zakresu Vulnerability Management tj.: ▪ Listę zainstalowanych poprawek Windows ▪ Lista nie autoryzowanych Aplikacji ▪ Walidacja wersji wybranych Applikacji ▪ Walidacja wersji Agenta Systemu • System ma posiadać możliwość anonimizacji nazwy Hosta i nazwy użytkownika dla danych wysyłanych do SOC • System jest licencjonowany jako subskrypcja na liczbę chronionych urządzeń/systemów końcowych bez rozróżnienia na typ chronionego hosta (serwer, stacja końcowa) oraz system operacyjny (Windows, Linux, MacOS)
XDR - 7	***instalacji i wdrażania Systemu oraz współpracy z innymi systemami*** • Instalacja agenta wymaga jedynie uprawnień na poziomie lokalnego administratora stacji końcowej. • Agent na hoście ma działać z uprawnieniami „LocalSystem” w celu minimalizacji ew. konfliktów z innymi systemami zainstalowanymi na tym samym systemie operacyjnym w obszarach takich jak sterowniki, itp. • System ma umożliwiać dystrybucję agentów służących do ochrony stacji końcowych za pomocą następujących mechanizmów: ▪ Wbudowane mechanizmy Active Directory i użycie pliku .msi ▪ Poprzez użycie dowolnego systemu do instalacji grupowej umożliwiającego dystrybucję i instalacje poprzez użycie plików .msi ▪ Użycie narzędzia producenta oprogramowania do instalacji w oparciu o listy adresów IP i uprawnienia lokalnego administratora ▪ Ręczne poprzez pliki .msi • System ma umożliwiać wysyłanie syslogiem lub poprzez integrację API informacji do narzędzi klasy SIEM. • System ma umożliwiać integrację z zewnętrznymi systemami i narzędziami za pośrednictwem pełnego REST API. • System ma umożliwiać zdalną w pełni automatyczną deinstalację agenta monitorującego stacje końcowe.

d) Wymagania w zakresie systemu SIEM/SOAR

Wymaganie	Opis
SIEM-1	System ma być oparty o nowoczesną nierelacyjną bazę danych typu noSQL"
SIEM-2	System ma pracować w oparciu o architekturę Linux.
SIEM-3	System ma posiadać możliwość centralnego zbierania i zarządzania logami

SIEM-4	System ma działać w trybie zbliżonym do rzeczywistego
SIEM-5	System ma umożliwiać funkcjonowanie bez dostępu do sieci Internet, analiza następuje wówczas tylko w oparciu o logi wewnętrzne
SIEM-6	System ma zapewniać efektywną obsługę co najmniej 4000 EPS lub 80 GB danych dziennie
SIEM-7	System ma zapewniać retencję danych w okresie minimum 365 dni (retencja danych zależna jest od posiadanych przez klienta zasobów na których jest instalowany system zbierania logów).
SIEM-8	Oferowana licencja nie może ograniczać ilości zarejestrowanych lub jednoczesnych użytkowników systemu.
SIEM-9	System ma umożliwiać rozbudowę bez potrzeby wyłączania lub restartu środowiska.
SIEM-10	System ma zapewniać pełen audyt aktywności jego użytkowników, w tym: udanych/nieudanych logowań, pełną historię operacji, realizowanych zapytań, zmian uprawnień.
SIEM-11	System ma pozwalać na tworzenie parserów z poziomu GUI
SIEM-12	System ma umożliwiać predykcję danych w oparciu o dowolne dane historyczne zgromadzone w systemie.
SIEM-13	System ma zapewniać wizualizację danych w postaci oryginalnych logów, list, wykresów i diagramów.
SIEM-14	Wizualizacja danych ma być możliwa dla wartości tekstowych jak i liczbowych przekazywanych w logach.
SIEM-15	System ma umożliwiać eksport danych o Zdarzeniach i Incydentach do formatu CSV i HTML m.in. w celu analizy wyników działania reguł korelacyjnych.
SIEM-16	System ma zapewniać parsowanie spływających do niego wiadomości w formatach: • Syslog, • Flat file, • Event log, • WMI, • XML, • JSON, • JDBC/ODBC • CSV,
SIEM-17	System ma 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.

SIEM-18	System do przyjmowania zdarzeń ma wykorzystywać zarówno mechanizmy agentowe jak i bezagentowe.
SIEM-19	System ma umożliwiać definiowanie parserów dla niestandardowych formatów logów w oparciu o składnię wyrażeń regularnych oraz formatów wymiany danych dla wszystkich obsługiwanych formatów.
SIEM-20	Interfejs ma umożliwiać parsowanie warunkowe na podstawie dopasowania wartości pól. Po dopasowaniu wzorca dalsze parsowanie jest konfigurowalne w celu wyboru optymalnej metody parsowania, np.: REGEX, JSON, XML oraz umożliwia zastosowanie innego parsera.
SIEM-21	System ma posiadać predefiniowany zestaw parserów zdarzeń.
SIEM-22	System ma wspierać geolokalizację zdarzeń na bazie adresów IP.
SIEM-23	System ma umożliwiać przeszukiwanie Danych Wejściowych z uwzględnieniem filtracji po sparsowanych polach.
SIEM-24	Proces parsowania ma umożliwiać wzbogacanie treści obieranych Wiadomości poprzez matematyczne operacje wykonywane na innych polach.
SIEM-25	Proces parsowania ma umożliwiać anonimizację Danych Wejściowych celem ukrycia fragmentów informacji, których składowanie nie jest konieczne lub narusza wewnętrzny procedury bezpieczeństwa.
SIEM-26	System ma pozwalać na rozpoznanie formatów czasu i daty oraz normalizowanie ich do jednego wspólnego formatu.
SIEM-27	Incydent, który powstał w wyniku korelacji, ma dać się wyszukiwać korzystając ze standardowego dostępnego w systemie mechanizmu wyszukiwania. System umożliwia budowanie na jego podstawie kolejnych reguł korelacyjnych lub generowania alarmów.
SIEM-28	System ma posiadać funkcjonalność korelacji danych w czasie rzeczywistym.
SIEM-29	System ma umożliwiać tworzenie nowych reguł korelacyjnych oraz modyfikowanie istniejących.
SIEM-30	System ma umożliwiać tworzenie własnych reguł korelacyjnych na bazie reguł odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie: • Wykrycia dowolnej treści w logach, • Wykrycia wystąpienia wartości pola na wybranej liście, • Wykrycia niewystępowania wartości pola na wybranej liście, • Wykrycia zmiany jednego z kilku pól, • Wykrycia zdarzeń występujących z zadaną częstotliwością, • Wykrycia zdarzeń, których liczba zmienia się w wskazany sposób względem czasu poprzedniego, • Wykrycia zaniku Wiadomości,

	• Wykrycia nowej wartości pola w zadanym okresie czasu, • Wykrycia incydentu będącego pochodną zdarzeń występujących w określonej kolejności
SIEM-31	System ma pozwalać na określenie okna czasowego oraz warunków dla zdarzeń, które mają zostać poddane regułom korelacyjnym.
SIEM-32	System ma pozwalać na realizację zapytań obejmujących całą historię gromadzonych w nim danych
SIEM-33	Rozwiązanie ma posiadać funkcjonalność wysyłania powiadomień o Incydentach do innych systemów bądź zdefiniowanych użytkowników (powiadamianie email, opcjonalnie SMS, czat).
SIEM-34	System ma umożliwiać testowanie reguł korelacyjnych i alertów na etapie ich tworzenia.
SIEM-35	Tworzone incydenty będące wynikiem pracy reguł bezpieczeństwa mają posiadać przypisany poziom istotności. Jest możliwość modyfikacji poziomu istotności dla każdej reguły.
SIEM-36	Oferowana licencja nie może ograniczać ilości urządzeń będących źródłem logów.
SIEM-37	System ma umożliwiać czasowe przyjęcie zwiększonej ilości danych o minimum 30% bez potrzeby zwiększania zasobów sprzętowych lub licencyjnych.

e) Parametry świadczenia usług – czasy maksymalne

Zadanie	**Czas reakcji / podjęcia**	**Czas realizacji**
SOC L1, całodobowe 24/7/365, podjęcie działań związanych z incydentem, rozwiązanie incydentu polegające na zatrzymaniu zagrożenia lub przekazanie do SOC L2	15 minut	2h
SOC - L2, 24/7/365, podjęcie działań związanych z incydentem i rozwiązanie incydentu w czasie reakcji	1h	8h
SOC L2 SOAR 24/7/365, zautomatyzowane podjęcie incydentu i aplikacja rozwiązania zatrzymującego zagrożenie w czasie realizacji	15 min	1h
SOC L3, podjęcie działań związanych z incydentem i rozwiązanie incydentu w czasie realizacji	8h	40h

2. WARUNKI UDZIAŁU W POSTĘPOWANIU

O udzielenie zamówienia mogą ubiegać się wykonawcy, którzy spełniają warunki udziału w postępowaniu w zakresie:

1) sytuacji ekonomicznej lub finansowej,

2) zdolności technicznej lub zawodowej.

1. Zamawiający, wymaga wykazania spełniania warunku udziału w postępowaniu dotyczącego sytuacji ekonomicznej lub finansowej. Wykonawca składający ofertę musi wykazać, że jest ubezpieczony od odpowiedzialności cywilnej w zakresie prowadzonej działalności związanej z przedmiotem zamówienia na sumę gwarancyjną nie mniejszą niż 1 000 000,00 zł (jeden milion złotych),
2. Zamawiający, wymaga wykazania spełniania warunku udziału w postępowaniu dotyczącego zdolności technicznej lub zawodowej. Wykonawca składający ofertę musi wykazać, że:
    a. posiada doświadczenie w postaci wykonania (a w przypadku świadczeń powtarzających się lub ciągłych również wykonywania) w okresie ostatnich trzech lat, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, co najmniej 4 zamówień na świadczenie usług cyberbezpieczeństwa w oparciu o systemy SIEM, SOAR i XDR w organizacji posiadającej minimum 400 użytkowników lub minimum 400 stacji roboczych, w tym:
        i. co najmniej 1 (jednego) polegającego na świadczeniu usług cyberbezpieczeństwa w oparciu o systemy SIEM, SOAR i XDR w organizacji posiadającej minimum 1000 użytkowników lub minimum 1000 stacji roboczych,
    b. dysponuje osobami zdolnymi do wykonania zamówienia, tj. minimum 12-osobowym zespołem analityków bezpieczeństwa, w tym:
        i. 3 osoby posiadające certyfikaty inżynierskie producenta oferowanego systemu SIEM i SOAR
        ii. 3 osoby posiadające certyfikaty inżynierskie producenta oferowanego systemu XDR
        iii. 1 osoby posiadające specjalistyczną wiedzę w zakresie cyberbezpieczeństwa potwierdzoną certyfikacją Certified Ethical Hacker - CEH lub równoważnym,
        iv. 1 osoby posiadające specjalistyczną wiedzę w zakresie cyberbezpieczeństwa potwierdzoną certyfikacją Certified Incident Handling Engineer – CIHE lub Certified Information Security Manager - CISM lub Certified Information Systems Security Professional – CISSP.

        Zamawiający dopuszcza posiadanie równoważnych certyfikatów, innych niż wskazane przez Zamawiającego. Przez certyfikat równoważny Zamawiający rozumie certyfikat, który jest analogiczny co do zakresu z przykładowymi certyfikatami wskazanymi z nazwy, co jest rozumiane jako analogiczna dziedzina merytoryczna, której dotyczy certyfikat, analogiczny stopień poziomu kompetencji, analogiczny poziom doświadczenia zawodowego wymaganego do otrzymania danego certyfikatu. Certyfikat musi być potwierdzony egzaminem.

    c. posiada aktualny certyfikat ISO 27001 wydany przez jednostkę uprawnioną i poświadczający wdrożenie systemu zarządzania bezpieczeństwem informacji i obejmujący swym zakresem usługi SOC.
    d. posiada status GOLD partnerstwa twórcy systemu XDR potwierdzony certyfikatem producenta.

O udzielenie zamówienia mogą ubiegać się wykonawcy, którzy nie są powiązani osobowo lub kapitałowo z Zamawiającym. Przez powiązania kapitałowe lub osobowe rozumie się wzajemne powiązania między Beneficjentem lub osobami upoważnionymi do zaciągania zobowiązań w imieniu Beneficjenta lub osobami wykonującymi w imieniu Beneficjenta czynności związanych z przygotowaniem i przeprowadzeniem procedury wyboru wykonawcy a wykonawcą, polegające w szczególności na:

- uczestniczenie w spółce jako wspólnik spółki cywilnej lub spółki osobowej;
- posiadanie co najmniej 10% udziałów lub akcji (o ile niższy próg nie wynika z przepisów prawa);
- pełnienie funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika;
- pozostawanie w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa lub powinowactwa w linii bocznej do drugiego stopnia, lub związanie z tytułu przysposobienia, opieki lub kurateli albo pozostawanie we wspólnym pożyciu z wykonawcą, jego zastępcą prawnym lub członkami organów zarządzających lub organów nadzorczych wykonawców ubiegających się o udzielenie zamówienia;
- pozostawanie z wykonawcą w takim stosunku prawnym lub faktycznym, że istnieje uzasadniona wątpliwość co do ich bezstronności lub niezależności w związku z postępowaniem o udzielenie zamówienia.

3. KRYTERIA OCENY OFERTY I WAGI PROCENTOWE

1. Zamawiający ustala następujące kryteria oceny ofert:
   (a) Kryterium „łączna cena” - C - znaczenie - 50%.
   (b) Kryterium „dojrzałość technologiczna XDR” - X – znaczenie - 25%
   (c) Kryterium „dojrzałość technologiczna SIEM i SOAR” - S znaczenie - 25%

4. OPIS SPOSOBU PRZYZNAWANIA PUNKTACJI ZA SPEŁNIENIE DANEGO KRYTERIUM OCENY OFERTY.

Ocena ofert będzie dokonywana według następujących zasad:

(a) Kryterium „łączna cena” - wskaźnik C - wg poniższego wzoru:

C =najniższa łączna cena spośród nieodrzuconych ofert (obejmująca zamówienie podstawowe i opcję) x 50/cena badanej oferty

(b) Kryterium „dojrzałość technologiczna XDR” – wskaźnik X - wg poniższych zasad:

Zamawiający w zakresie rozwiązania XDR oceniając dojrzałość technologiczną oprze się na raporcie „2024 MITRE ATT&CK Evaluations: Enterprise”. Zamawiający przyzna ofercie punkty za rozwiązanie XDR w zależności od miejsca które oferowane rozwiązania zajęło w raporcie w kategorii:

- Protection Rate
- Prevention Rate.

Do oceny będzie brana średnia wartość osiągnięta w obu kategoriach.

Miejsce 1-4 – 25 pkt.

Miejsce 5-8- 10 pkt.

Miejsce 9 i poniżej – 0 pkt.

Zamawiający nie będzie przyznawał punktów częściowych. Oznacza to, że Wykonawca w ramach tego kryterium może otrzymać odpowiednio 0, 10 albo 25 punktów.

(c) Kryterium „dojrzałość technologiczna SIEM i SOAR” – wskaźnik X - wg poniższych zasad:

Zamawiający przyzna 25 punktów za rozwiązanie zawierające systemy SIEM i SOAR w jednym rozwiązaniu hybrydowym jednocześnie rozwiązanie hybrydowe SIEM i SOAR musi być komercyjne i mieć ugruntowaną pozycję rynkową, przez ugruntowaną pozycję rynkową rozumie się oferowanie rozwiązania w co najmniej 5 krajach UE.

Zamawiający nie będzie przyznawał punktów częściowych. Oznacza to, że Wykonawca w ramach tego kryterium może otrzymać odpowiednio 0 albo 25 punktów.

Sposób oceny ofert:

ocena ofert zostanie przeprowadzona w oparciu o przedstawione powyżej kryteria,

o wyborze oferty zadecyduje największa liczba uzyskanych punktów, tj. Lp= C+X+S+I. Ilość pkt. równa się ilości %.

Lp = liczba punktów uzyskanych przez ofertę.

5. **MIEJSCE ORAZ TERMIN SKŁADANIA OFERT**
   Oferty prosimy składać do 24 lutego 2025 r na adresy:

   tomasz.wisniewski@paged.pl
   tomasz.oldakowski@paged.pl
   krzysztof.mykowski@paged.pl

6. **INFORMACJA O MOŻLIWOŚCI SKŁADANIA OFERT CZĘŚCIOWYCH**
   Zamawiający nie dopuszcza możliwości składania ofert częściowych.
7. **INFORMACJĘ O PLANOWANYCH ZAMÓWIENIACH UZUPEŁNIAJĄCYCH**
   Zamawiający nie planuje zamówień uzupełniających.
8. **TERMIN REALIZACJI UMOWY**
   Okres realizacji usługi maksymalnie 12 miesięcy.
9. **ISTOTNE POSTANOWIENIA UMOWY I WARUNKI ZMIANY ISTOTNYCH POSTANOWIEŃ UMOWY**

Zamawiający wymaga, aby Wykonawca, którego oferta zostanie uznana za najkorzystniejszą, zawarł umowę zgodnie z treścią zapytania. Wykonawca ma prawo zaproponować wzór umowy stosowany w praktyce handlowej. Zamawiający dopuszcza wypłatę zaliczki na poczet realizacji zamówienia w kwocie uzgodnionej z Wykonawcą nie wyższą niż 50% ceny ujawnionej przez Wykonawcę w ofercie.

Podstawą rozliczeń między stronami będą faktury.

Z zastrzeżeniem innych kar umownych, za niewykonanie lub nienależyte wykonanie zobowiązań wynikających z niniejszej Umowy, Usługodawca zapłaci Usługobiorcy kary umowne za niedochowanie parametrów realizacji Usługi (SLA) wskazanych w Umowie dotyczących Czasu Podjęcia Działania i/lub Czasu Realizacji:

a. w zakresie pierwszej Linii wsparcia i incydentu krytycznego/wysokiego – 100 zł za każdy przypadek;

b. w zakresie drugiej Linii wsparcia i incydentu krytycznego/wysokiego – 200 zł za każdy przypadek;
c. w zakresie trzeciej Linii wsparcia: 500 zł za każdy przypadek;
d. w pozostałych przypadkach: 100 zł – za każdy przypadek,

10. WARUNKI EWENTUALNEGO ODSTĄPIENIA OD ZAWARCIA UMOWY

W przypadku gdy zaoferowana cena przekracza kwotę środków przeznaczonych przez Zamawiającego na realizację zamówienia, Zamawiający może unieważnić postępowanie i odstąpić od podpisania umowy.

Oferty prosimy składać wraz z wypełnionymi załącznikami:

FORMULARZ OFERTY

Pełna nazwa i adres Wykonawcy_____

_____

NIP / REGON / KRS _____

_____

OFERTA

W odpowiedzi na ogłoszenie o w postępowaniu prowadzonym zgodnie z zasadą konkurencyjności składamy ofertę na wykonanie zamówienia w zakresie i na warunkach określonych w zapytaniu ofertowym na:

1) świadczenie usługi cyberbezpieczeństwa opartej o Security Operations Center (SOC) działającej w reżimie 24 H/7 dni w tygodniu wraz z audytami bezpieczeństwa i kampaniami phishisngowymi, szkoleniami dla personelu Zamawiającego i raportowaniem,

2) wdrożenie, uruchomienie i utrzymanie rozwiązania hybrydowego zawierającego w sobie systemy klasy SIEM (Security Information and Event Management), SOAR (Security Orchestration, Automation and Response),

3) wdrożenie, uruchomienie i utrzymanie rozwiązania XDR (Extended Detection and Response).

za cenę obejmującą:

Lp.	Zadanie	Cena netto (w zł)
1	wdrożenie, uruchomienie i utrzymanie systemu klasy SIEM/SOAR zgodnie ze specyfikacją opisaną w dokumentacji przy zachowaniu harmonogramu i bez limitu reguł korelacyjnych oraz z liczbą playbooków wynikającą z oferty i akcji z nich wynikające	_____ zł
2	wdrożenie, uruchomienie i utrzymanie systemu klasy XDR zgodnie ze specyfikacją opisaną w dokumentacji przy zachowaniu harmonogramu dla 2250 endpointów	_____ zł
3	Uruchomienie i świadczenie usługi SOC - zgodnie ze specyfikacją opisaną w dokumentacji	_____ zł
4	świadczenie usługi trzeciej linii wsparcia SOC - L3 zgodnie z ofertą i specyfikacją opisaną w dokumentacji – bez limitu godzin, oferowana cena zawiera wszystkie niezbędne koszty związane z przygotowaniem raportu poincydentalnego	_____ zł
5	wykonywanie szkoleń dla pracowników i administratorów zgodnie ze specyfikacją opisaną w dokumentacji dla 1500 użytkowników	_____ zł

6	wykonywanie kampanii phishingowych dla pracowników i administratorów zgodnie ze specyfikacją opisaną w dokumentacji dla 1500 użytkowników	_____ zł
7	**Cena netto zamówienia (na 12 miesięcy)** **(suma poz. 1-9)**	_____ zł

1) **oświadczając, iż oferowany system SIEM i SOAR jest rozwiązaniem hybrydowym (All in one) i nie wymaga integracji.**
   ☐ tak
   ☐ nie

2) **oświadczając, iż oferowany system XDR występuje w raporcie 2024 MITRE ATT&CK Evaluations: Enterprise. W zakresie:**
   - **Protection** umieszczony jest na miejscu _____
     (proszę podać producenta, nazwę produktu, wersję, uzyskany wynik w kategorii)
   - **Protection** umieszczony jest na miejscu _____
     (proszę podać producenta, nazwę produktu, wersję, uzyskany wynik w kategorii)

3) **oświadczając, iż oferowany system XDR zawiera moduł pułapek (deception) zgodnie z zapisami swz:**
4) ☐ tak
5) ☐ nie, wymagane jest zintegrowanie rozwiązania trzeciego, cena oferowana za rozwiązanie XDR zawiera również niezbędną liczbę licencji rozwiązania deception dla 1500 użytkowników wraz z integracją z narzędziem XDR w taki sposób aby prezentacja zdarzeń następowała na jednej konsoli.

6) **deklarując miejsce instalacji systemu (proszę zaznaczyć właściwe),**
   ☐ na zasobach Wykonawcy lub w bezpiecznej chmurze opłaconej przez Wykonawcę,
   ☐ na zasobach Zamawiającego

7) **oferując:**
   - **SIEM/SOAR** _____
     (proszę podać producenta, nazwę produktu, wersję)

6) w terminie i na warunkach płatności – zgodnie z zapisami swz

2. *****W celu wykazania spełniania warunków udziału w postępowaniu, powołujemy się na zasoby poniższych podmiotów:
   - *nazwa (firma) podmiotu*:_____
   w zakresie_____,
   - *nazwa (firma) podmiotu*:_____
   w zakresie_____.

3. *Zamierzamy powierzyć podwykonawcom wykonanie następujących części zamówienia (wpisać jakiej części zamówienia dotyczy podwykonawstwo i nazwę podwykonawcy, jeśli jest już znany):
_____
_____

4. **Oświadczam/y, że:**

1) wykonamy zamówienie zgodnie z SWZ wraz z załącznikami do SWZ,
2) zapoznaliśmy się z dokumentami zamówienia i przyjmujemy je bez zastrzeżeń,
3) czynności określone przez Zamawiającego w zakresie świadczenia usługi SOC będą realizowane przez pracowników wykonawcy.

4) w razie wyboru naszej oferty jako najkorzystniejszej, zobowiązujemy się do zawarcia umowy we wskazanym terminie i miejscu, na warunkach przedstawionych przez Zamawiającego w załączonej do swz umowy,
5) do oferty zostały załączone następujące dokumenty:
   a) oświadczenie w zakresie przesłanek i okoliczności wskazanych w art. 5k ust. 1 Rozporządzenia (UE) 833/2014 zmienionego Rozporządzeniem (UE) 2022/576 dotyczące środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie
   b) (o ile dotyczy) pełnomocnictwa do reprezentowania wykonawców występujących wspólnie,
   c) (o ile dotyczy) pełnomocnictwa do reprezentowania wykonawcy, jeżeli w imieniu wykonawcy działa osoba, której umocowanie do jego reprezentowania nie wynika z dokumentów rejestrowych (KRS, CEDiG)
   d) (o ile dotyczy) zobowiązanie podmiotu udostępniającego zasoby do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji danego zamówienia lub inny podmiotowy środek dowodowy potwierdzający, że wykonawca realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów,
   e) certyfikat ISO 27001 lub równoważny,
   f) Certyfikat producenta narzędzia XDR,
   g) Zestawienie wykonanych usług,
   h) Kopia polisy ubezpieczeniowej,
   i) Zestawienie zespołu realizującego usługę SOC,
   j) Skany wymaganych certyfikatów,

5. Oświadczam(y), że nie jestem(eśmy) powiązani z Zamawiającym osobowo lub kapitałowo.
6. Uprawniony do kontaktów z Zamawiającym jest (wpisać osobę, jej adres e-mail i nr tel., precyzyjne wskazanie adresu e-mail jest konieczne w celu zapewnienia komunikacji z Zamawiającym):_____
   _____
7. Podstawa reprezentowania wykonawcy (podać rodzaj i nr dokumentu):_____

Podpis kwalifikowanym podpisem elektronicznym
osoby (osób) upoważnionej (upoważnionych) do reprezentowania Wykonawcy/ów

**niepotrzebne skreślić

ZAMAWIAJĄCY:

Paged Morąg S.A.
ul. Mazurska 1
14-300 Morąg, Polska
NIP: 7411378488
KRS: 0000010478
REGON: 510445569

WYKAZ OSÓB

Świadczenie usługi zabezpieczenia przed cyberincydentami (SOC)

Pełna nazwa i adres Wykonawcy_____

_____

NIP / REGON / KRS _____

_____

Ja/my niżej podpisani:
(imię, nazwisko, stanowisko/podstawa do reprezentacji)

działając w imieniu i na rzecz:

(pełna nazwa Wykonawcy/Wykonawców w przypadku wykonawców wspólnie ubiegających się o udzielenie zamówienia)

ubiegając się o udzielenie powyższego zamówienia poniżej przedstawiamy wykaz osób, które będą uczestniczyć w realizacji zamówienia (min. 12 osób)**:**

Imię i nazwisko	**Rodzaj i zakres uprawnień (w tym rodzaj posiadanego certyfikatu)**

…… ….. ……
(miejscowość, data) (podpis)

WYKAZ ZREALIZOWANYCH USŁUG

W ZAKRESIE NIEZBĘDNYM DO WYKAZANIA WARUNKU DOTYCZĄCEGO ZDOLNOŚCI TECHNICZNYCH LUB ZAWODOWYCH

Świadczenie usługi zabezpieczenia przed cyberincydentami (SOC)

Pełna nazwa i adres Wykonawcy_____

_____

NIP / REGON / KRS _____

_____

Oświadczam/y, że wykonaliśmy w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie wykonał, co najmniej:

1) 3 (trzech) zamówień na świadczeniu usług cyberbezpieczeństwa w oparciu o systemy SIEM, SOAR i XDR w organizacji posiadającej minimum 400 użytkowników lub minimum 400 stacji roboczych.
2) 1 (jednego) polegającego na świadczeniu usług cyberbezpieczeństwa w oparciu o systemy SIEM, SOAR i XDR w organizacji posiadającej minimum 1000 użytkowników lub minimum 1000 stacji roboczych,

Lp.	Odbiorca usługi	Przedmiot zamówienia	Okres świadczenia usługi*
1.			
2.			
3.			
4.			

* należy wskazać okres od-do

załączam dowody określające czy te usługi zostały wykonane lub są wykonywane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty sporządzone przez podmiot, na rzecz którego usługi zostały wykonane, a w przypadku świadczeń powtarzających się lub ciągłych są wykonywane, w przypadku świadczeń powtarzających się lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające ich należyte wykonywanie powinny być wystawione w okresie ostatnich 3 miesięcy.

…… ….. ……
(miejscowość, data) (podpis)