Załączniku nr 1 do umowy – Szczegółowy Opis Przedmiotu Zamówienia

I. Słownik:

Skrót lub Pojęcie	Opis
Best Effort	W ujęciu ogólnym najlepsze możliwe działanie w dążeniu do osiągnięcia celu. Stan realizacji usługi, w którym doszło do przekroczenia limitów SLA w związku ze zwiększonym zapotrzebowaniem na tę usługę. W przypadku przekroczenia limitów SLA, Usługodawca niezwłocznie informuje Klienta o zaistniałej sytuacji.
Cyberbezpieczeństwo	Adekwatny do potrzeb, stan ochrony systemów informatycznych, zapewniający możliwość wykrywania oraz reagowania na zdarzenia niepożądane oraz takie, które zostały określone w dokumentacji klienta dotyczącej systemu zarządzania bezpieczeństwem informacji.
Cyberprzestrzeń	Przestrzeń, w której występuje wymiana, gromadzenie i udostępnianie informacji za pośrednictwem komputerów oraz komunikacja między człowiekiem i komputerem.
SOC	Security Operations Center – centrum operacji bezpieczeństwa, którego zadaniem jest całodobowe monitorowanie, zapobieganie, wykrywanie, badanie i reagowanie na zagrożenia cybernetyczne.
Czas Reakcji	Zagwarantowany przez Usługodawcę okres czasu, od momentu wygenerowania alarmu przez system SIEM lub zgłoszenia incydentu przez Klienta do momentu potwierdzenia rozpoczęcia jego weryfikacji.
Czas rozwiązania	Zagwarantowany przez Usługodawcę okres czasu, od momentu potwierdzenia rozpoczęcia weryfikacji incydentu do momentu jego rozwiązania czyli przywrócenia prawidłowego funkcjonowania systemu lub usunięcia zagrożenia.
Dzień roboczy	Od poniedziałku do piątku od 08.00 – 18.00 z wyłączeniem dni ustawowo wolnych od pracy oraz dni wolnych u Klienta.
Praca ciągła	Praca w trybie 24/7/365 dni.
On-call	Dostępność konsultanta dyżurującego pod telefonem.
Punkt Końcowy	Oznacza instancję serwera w przypadku serwerów wirtualnych lub serwer fizyczny, stację roboczą objęte Usługą.
Incydent Bezpieczeństwa Informacji (Incydent)	Pojedyncze zdarzenie lub seria zdarzeń związanych z bezpieczeństwem informacji, które stwarzają

	prawdopodobieństwo zakłócenia działań biznesowych i/lub zagrażają bezpieczeństwu informacji.
AWS	Amazon Web Services - firma udostępniająca publicznie platformę chmurową oraz hostingowy serwis internetowy, będąca jednostką zależną firmy Amazon, udostępniająca usługi dostępne w sieci Web. Zlokalizowana w europejskiej przestrzeni gospodarczej.
Scenariusz Reakcji	Dokument opisujący wymagane czynności w przypadku wykrycia zdarzenia niepożądanego, składający się z:
	opisu możliwości technicznych wykrycia zdarzenia,
	warunków wywołania zdarzenia niepożądanego,
	opisu identyfikacji zdarzeń zależnych,
	instrukcji reakcji na zdarzenie,
	instrukcji uruchomienia działań korekcyjnych,
	instrukcji wykonywania działań informacyjnych,
	ogólnych i szczegółowych ścieżek eskalacyjnych.
Scenariusz użycia systemu bezpieczeństwa	Dokument opisujący zestaw zadań wymaganych do wykonania w ramach Pierwszej i Drugiej Linii Wsparcia, w skład którego wchodzi m.in.:
	skonfigurowanie jednego lub kilku źródeł zdarzeń;
	opisanie procesu normalizacji;
	przygotowanie Scenariuszy Reakcji w zakresie czynności wykonywanych przez Pierwszą Linię Wsparcia.
SLA	Zestaw wartości granicznych dla kluczowych wskaźników wydajności, dla których określona realizacja usługi jest wymagana w zakresie jakościowym.
System Informatyczny	System informatyczny to zbiór współpracujących ze sobą urządzeń, programów, procedur i narzędzi programowych, które wspólnie przetwarzają dane. Obejmuje sprzęt (komputery, serwery, sieci), oprogramowanie (systemy operacyjne, aplikacje), dane, a także ludzi (użytkowników, administratorów) i procedury, które służą do automatycznego przetwarzania informacji w określonym celu. Sprzęt komputerowy: Komputery, serwery, drukarki, skanery i sieci. Oprogramowanie: Systemy operacyjne, aplikacje, bazy danych i inne narzędzia programowe. Dane: Informacje przechowywane i przetwarzane w formie cyfrowej. Ludzie: Użytkownicy, administratorzy, programiści i osoby odpowiedzialne za system. Procedury: Zestaw reguł, algorytmów i protokołów, które określają sposób działania systemu.

IDS/IPS/NIDS	IDS (Intrusion Detection System) Funkcja: Wykrywa potencjalne zagrożenia i ataki na sieć. Działanie: Analizuje ruch sieciowy i porównuje go z znanymi wzorcami ataków (sygnatury) lub szuka nietypowych zachowań. Pasożyty: Informuje o wykrytych zagrożeniach, ale nie blokuje ich. IPS (Intrusion Prevention System) Funkcja: Wykrywa i blokuje ataki w czasie rzeczywistym. Działanie: Obejmuje funkcje IDS, ale dodatkowo reaguje na wykryte zagrożenia, np. blokując połączenie, usuwając szkodliwe pliki lub zmieniając ustawienia sieci. Działanie: Może być implementowane w sieci (NIPS) lub na hostach (HIPS), a nawet jako rozwiązanie hybrydowe. NIDS (Network Intrusion Detection System) Funkcja: Monitoruje ruch sieciowy na poziomie sieci, wykrywając ataki na całej infrastrukturze. Działanie: Analizuje dane z sieci i wykrywa nieprawidłowe zachowania, takie jak próbę włamania, atak typu DoS/DDoS, czy złośliwe oprogramowanie. Zalety: Nie obciąża serwerów, na których jest zainstalowany, i może wykrywać ataki z zewnątrz.
Dyrektywa NIS2	Dyrektywa Parlamentu Europejskiego i Rady Unii Europejskiej 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148

II. Zakres usług:

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

1. Parametry świadczenia usługi:
    a. Ilość korelacji wytwarzanych w SIEM – bez ograniczeń,
    b. Tworzenie kolejnych korelacji – bez opłat,
    c. Ilość podłączonych źródeł danych do systemu SIEM – bez limitu,
    d. Ilość przetwarzanych zdarzeń i incydentów bezpieczeństwa w miesiącu - bez ograniczeń,

e. Liczba scenariuszy działania – bez ograniczeń,
f. Ilość przetwarzanych danych w systemie SIEM – bez ograniczeń,
g. Ilość dostępnych w miesiącu godzin inżyniera wsparcia technicznego – 8 h,
h. Ilość godzin dla usług III linii SOC rozliczanych w roku– 160,

2. Zakres objęty usługą:

   a. Liczba endpointów odjętych usługą – 300
   b. Liczba osób objętych szkoleniem – 300
   c. Liczba osób objętych kampanią phishingową – 300,

3. 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 Zamawiającym 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.

(c) Świadczenie usług w ramach III linii wsparcia (24x7x365):

Zadania III linii SOC koncentrują się na najbardziej zaawansowanych i skomplikowanych zadaniach, odgrywa ona kluczową rolę w przygotowaniu zaleceń dla klienta i wyjaśnienia pochodzenia incydentu.

- Zaawansowana Analiza Zagrożeń
- Głęboka analiza danych: Trzecia linia SOC powinna specjalizować się w zaawansowanej analizie danych zebranych przez systemy monitorowania. Obejmuje to korzystanie z zaawansowanych narzędzi do analizy behawioralnej i heurystycznej, które pomagają identyfikować subtelne i złożone zagrożenia.
- Forensic cyfrowy: W przypadku incydentów trzecia linia odpowiedzialna jest za przeprowadzenie dogłębnej analizy incydentu (forensic, aby zrozumieć źródło, metodę ataku oraz zakres wpływu zagrożenia na systemy.
- Reagowanie na Incydenty
- Rozwój i implementacja środków zaradczych: Opracowywanie skomplikowanych strategii reagowania na incydenty, które mogą obejmować izolację zainfekowanych systemów, eliminację zagrożeń oraz przywracanie operacji.
- Automatyzacja reakcji: Tworzenie i wdrażanie automatycznych skryptów lub procedur, które umożliwiają szybkie reagowanie na podobne incydenty w przyszłości.
- Rozwój i Implementacja Polityk Bezpieczeństwa
- Opracowywanie polityk i procedur: Trzecia linia SOC bierze aktywny udział w tworzeniu i aktualizacji polityk bezpieczeństwa, które odpowiadają wymogom NIS2 i najlepszym praktykom branżowym.
- Zgodność i audyty: Przeprowadzanie regularnych przeglądów bezpieczeństwa, aby zapewnić zgodność z obowiązującym prawem (np. dyrektywą NIS2) i innymi standardami. Współpraca z klientem w zakresie kontaktu z zewnętrznymi audytorami i inspektorami.
- Szkolenia i Rozwój Umiejętności
- Szkolenia dla innych linii wsparcia: Przeprowadzanie zaawansowanych szkoleń dla personelu pierwszej i drugiej linii SOC, podnosząc ich umiejętności w zakresie wykrywania i reagowania na incydenty.
- Zarządzanie Kryzysowe
- Planowanie i testowanie ciągłości działania: Opracowywanie kompleksowych planów ciągłości działania i regularne przeprowadzanie testów tych planów, aby zapewnić gotowość firmy na różne scenariusze cyberataków.
- Koordynacja działań kryzysowych: Współpraca z klientem w celu koordynacji działań podczas poważnych incydentów bezpieczeństwa.
- Przygotowanie raportu poincydentalnego dla Klienta celem przekazania do odpowiedniego organu.

4. 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.

- Przygotowanie serwisu WWW 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).

III. Wymagania szczegółowe:

1. 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 po włamaniową, 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 – konieczne 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

2. 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	Systemy 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 do 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 oraz z urządzeń UTM; system klasy SOAR musi umieć wykonywać akcje na końcówkach z wykorzystaniem 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

3. 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 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 instytucji 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 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. Zakres szkoleń dla kadry kierowniczej dodatkowo obejmuje: 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 Zarządzanie zdarzeniami i incydentami bezpieczeństwa

4. Wymagania w zakresie kampanii phishingowej

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. Zaproponowanie działań szkoleniowych: Propozycje konkretnych szkoleń lub warsztatów, które mogłyby zwiększyć świadomość i umiejętności pracowników. Plan poprawek: Krótkoterminowe i długoterminowe działania, które instytucja powinna podjąć, aby poprawić bezpieczeństwo informacyjne. Feedback od Uczestników

5. 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 730 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 anonimizację Danych Wejściowych celem ukrycia fragmentów informacji, których składowanie nie jest konieczne lub narusza wewnętrzny procedury bezpieczeństwa.
SIEM-25	System ma pozwalać na rozpoznanie formatów czasu i daty oraz normalizowanie ich do jednego wspólnego formatu.
SIEM-26	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-27	System ma posiadać funkcjonalność korelacji danych w czasie rzeczywistym.

SIEM-28	System ma umożliwiać tworzenie nowych reguł korelacyjnych oraz modyfikowanie istniejących.
SIEM-29	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-30	System ma pozwalać na określenie okna czasowego oraz warunków dla zdarzeń, które mają zostać poddane regułom korelacyjnym.
SIEM-31	System ma pozwalać na realizację zapytań obejmujących całą historię gromadzonych w nim danych
SIEM-32	Rozwiązanie ma posiadać funkcjonalność wysyłania powiadomień o Incydentach do innych systemów bądź zdefiniowanych użytkowników (powiadamianie email, chat).
SIEM-33	System ma umożliwiać testowanie reguł korelacyjnych i alertów na etapie ich tworzenia.
SIEM-34	Tworzone incydenty będące wynikiem pracy reguł bezpieczeństwa mają posiadać przypisany poziom istotności. Jest możliwość modyfikacji poziomu istotności dla każdej reguły.
SIEM-35	Oferowana licencja nie może ograniczać ilości urządzeń będących źródłem logów.
SIEM-36	System ma umożliwiać czasowe przyjęcie zwiększonej ilości danych o minimum 30% bez potrzeby zwiększania zasobów sprzętowych lub licencyjnych.

6. 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

IV. Parametry SLA

Poziom świadczenia usług (SLA) monitorowania i reakcji na cyberzagrożenia (MDR)

1. Usługa monitorowania bezpieczeństwa jest świadczona przez SOC z następującymi minimalnymi poziomami SLA dla działań zespołu SOC.

1. Pierwsza Linia Wsparcia

a. czasy dla pierwszych 75 Incydentów każdego dnia, pozostałe zadania realizowane w trybie „Best Effort”:

Priorytet incydentu	Czas od wykrycia do	
	Podjęcia działania	Realizacji
Krytyczny	15 min	2 h
Wysoki	60 min	3 h
Średni	90 min	6 h
Niski	2 h	12 h
Informacyjny	4 h	24 h

b. dostępność usługi w trybie 24/7/365.

2. Druga Linia Wsparcia

a. czasy dla pierwszych Incydentów każdego dnia, jednak nie więcej niż 10, pozostałe zadania realizowane w trybie „Best Effort”:

Priorytet incydentu	Czas od wykrycia do	
	Podjęcia działania	Realizacji
Krytyczny	30 min	24 h
Wysoki	60 min	24 h
Średni	2 h	2 dni
Niski	4 h	4 dni
Informacyjny	8 h	7 dni

b. dostępność usługi w dni robocze pomiędzy godzinami 8:00 a 18:00. Dodatkowo dla incydentów o priorytecie Wysokim - w trybie „on-call” w dni robocze w godzinach 00:00 do 8:00 i 18:00 do 24:00, w pozostałe dni w trybie „on-call” w godzinach 00:00 do 23:59.

3. Trzecia Linia Wsparcia/Linia wsparcia producenta systemów użytych w usłudze MDR

a. czasy dla pierwszych Incydentów, jednak nie więcej niż 10, pozostałe zadania realizowane w trybie „Best Effort”:

	<table><tr><th rowspan="2">Priorytet incydentu</th><th colspan="2">Czas od wykrycia do</th></tr><tr><th>Podjęcia działania</th><th>Realizacji</th></tr><tr><td>Krytyczny</td><td>2 h</td><td>7 dni</td></tr><tr><td>Wysoki</td><td>4 h</td><td>7 dni</td></tr></table> Gdzie poziom incydentu zdefiniowany jest następująco:
2.	a. Poziom KRYTYCZNY: ▪ Jest stosowany w przypadku wystąpienia na wskazanych zasobach lub zasobie mogącym przetwarzać lub przechowywać rekordy danych objętych definicją rozporządzenia RODO. ▪ Jest stosowany w przypadku wystąpienia na wskazanych zasobach lub zasobie mogącym przetwarzać lub przechowywać rekordy danych objętych definicją tajemnicy przedsiębiorstwa. ▪ Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczą o wystąpieniu co najmniej jednego wskaźnika: ▪ Zestawienie zwrotnego kanału komunikacji z serwera dowodzenia i kontroli złośliwego oprogramowania (C&C) aktywnie wykorzystywanego (więcej niż 1kb/min). ▪ Przełamanie zabezpieczeń aplikacji oraz ujawnienie nieznanych lub nieautoryzowanych procesów lub wątków aplikacyjnych lub systemowych. ▪ Nieautoryzowane dysponowanie uprawnieniami administracyjnymi. ▪ Zidentyfikowane oraz potwierdzone naruszenie integralności plików konfiguracyjnych, binariów lub skryptów aplikacji i/lub systemu operacyjnego. ▪ Nieuprawniony dostęp i wykorzystanie uprawnień mogące pozwolić na ustanowienie tylnej furtki, podsłuchiwanie transmisji lub wykorzystanie podatności. ▪ Ujawnienie wycieku danych z chronionego obszaru z wykorzystaniem protokołów mailowych, przesłanie na dyski webowe lub danych z wykorzystaniem nieautoryzowanych nośników przenośnych; ▪ Nieuprawniony dostęp i wykorzystanie uprawnień mogące pozwolić na utworzenie tylnej furtki, podsłuchu transmisji lub wykorzystania podatności; ▪ Ujawnienie nieautoryzowanego kodu służącego jako oprogramowanie administracyjne (tzw. adminware) lub ofensywnych technik przełamywania zabezpieczeń (tzw. grayware); ▪ Celowany atak na personel klienta z wykorzystaniem systemów komputerowych mający na celu wyłudzenie danych umożliwiających autoryzację w środowisku chronionym; ▪ Wykrycie przez system antywirusowy oprogramowania złośliwego na zasobie realizującym funkcje systemu informacyjnego.
3.	b. Poziom WYSOKI: Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczą o wystąpieniu co najmniej jednego wskaźnika: ▪ Zestawienie zwrotnego kanału komunikacji z serwera dowodzenia i kontroli złośliwego oprogramowania (C&C) aktywnie wykorzystywanego (więcej niż 1kb/min). ▪ Przełamanie zabezpieczeń aplikacji oraz ujawnienie nieznanych lub nieautoryzowanych procesów lub wątków aplikacyjnych lub systemowych. ▪ Nieautoryzowane dysponowanie uprawnieniami administracyjnymi. ▪ Zidentyfikowane oraz potwierdzone naruszenie integralności plików konfiguracyjnych, binariów lub skryptów aplikacji i/lub systemu operacyjnego. ▪ Nieuprawniony dostęp i wykorzystanie uprawnień mogące pozwolić na ustanowienie tylnej furtki, podsłuchiwanie transmisji lub wykorzystanie podatności.

	▪ Ujawnienie wycieku danych z chronionego obszaru z wykorzystaniem protokołów mailowych, przesłanie na dyski webowe lub danych z wykorzystaniem nieautoryzowanych nośników przenośnych; ▪ Nieuprawniony dostęp i wykorzystanie uprawnień mogące pozwolić na utworzenie tylnej furtki, podsłuchu transmisji lub wykorzystania podatności; ▪ Ujawnienie nieautoryzowanego kodu służącego jako oprogramowanie administracyjne (tzw. adminware) lub ofensywnych technik przełamywania zabezpieczeń (tzw. grayware); ▪ Celowany atak na personel klienta z wykorzystaniem systemów komputerowych mający na celu wyłudzenie danych umożliwiających autoryzację w środowisku chronionym; ▪ Wykrycie przez system antywirusowy oprogramowania złośliwego na zasobie realizującym funkcje systemu informacyjnego.
4.	c. Poziom ŚREDNI: Zebrane dowody w systemach realizujących monitoring bezpieczeństwa zaświadczą o wystąpieniu co najmniej jednego wskaźnika: ▪ Ujawnienie nieznanego przez VirusTotal lub przez inne bazy reputacyjne oprogramowania mającego złośliwe funkcje pozwalające operatorowi na uruchomienie nieautoryzowanych skryptów lub kodu. ▪ Ujawnienie podatności systemów lub infrastruktury mających wartość CVSS powyżej 7. ▪ Przełamanie zabezpieczeń aplikacji oraz ujawnienie nieznanych lub nieautoryzowanych procesów lub wątków aplikacyjnych lub systemowych w strefie chronionej. ▪ Wykrycie przez system antywirusowy oprogramowania złośliwego na zasobie realizującym funkcje systemu informacyjnego.
5.	d. Poziom NISKI: Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczą o wystąpieniu co najmniej jednego wskaźnika na systemie chronionym. ▪ Częściowo personalizowany atak na personel klienta z wykorzystaniem systemów komputerowych mający na celu wyłudzenie danych umożliwiających autoryzację w środowisku chronionym. ▪ Wszystkie przypadki wystąpienia na chronionych systemach komputerowych złośliwego oprogramowania, które jest rozpoznawane przez system antywirusowy, ale nie zostało zatrzymane przez inny system bezpieczeństwa. ▪ Wszystkie potwierdzone przypadki z naruszenia poufności, dostępności lub integralności wykryte przez systemy bezpieczeństwa dla których użytkownik wyklucza świadome działanie.
6.	e. Poziom INFORMACYJNY: ▪ Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu zdefiniowanego zdarzenia bezpieczeństwa opisanego scenariuszem reakcji, ale udało się potwierdzić, że wywołanie zdarzenia było efektem realizacji autoryzowanych czynności służbowych z pominięciem ustalonych procedur bezpieczeństwa.