chmura krajowa

**Security Operations Centre** as a Service

**Krok wyżej,**
krok dalej

Bezpieczna Chmura

# **Security Operation Centre** (SOC)

W Chmurze Krajowej pracują eksperci ds. bezpieczeństwa z doświadczeniem w budowaniu i monitorowaniu zarówno środowisk chmurowych (Platforma OChK, Google Cloud oraz Microsoft Azure), jak również on-premise i hybrydowych, łączących różne technologie. W ramach oferowanych usług bezpieczeństwa nasi specjaliści mogą swoim ekspertyzą wesprzeć zespół klienta w zapewnieniu odpowiedniego poziomu bezpieczeństwa środowiska IT.

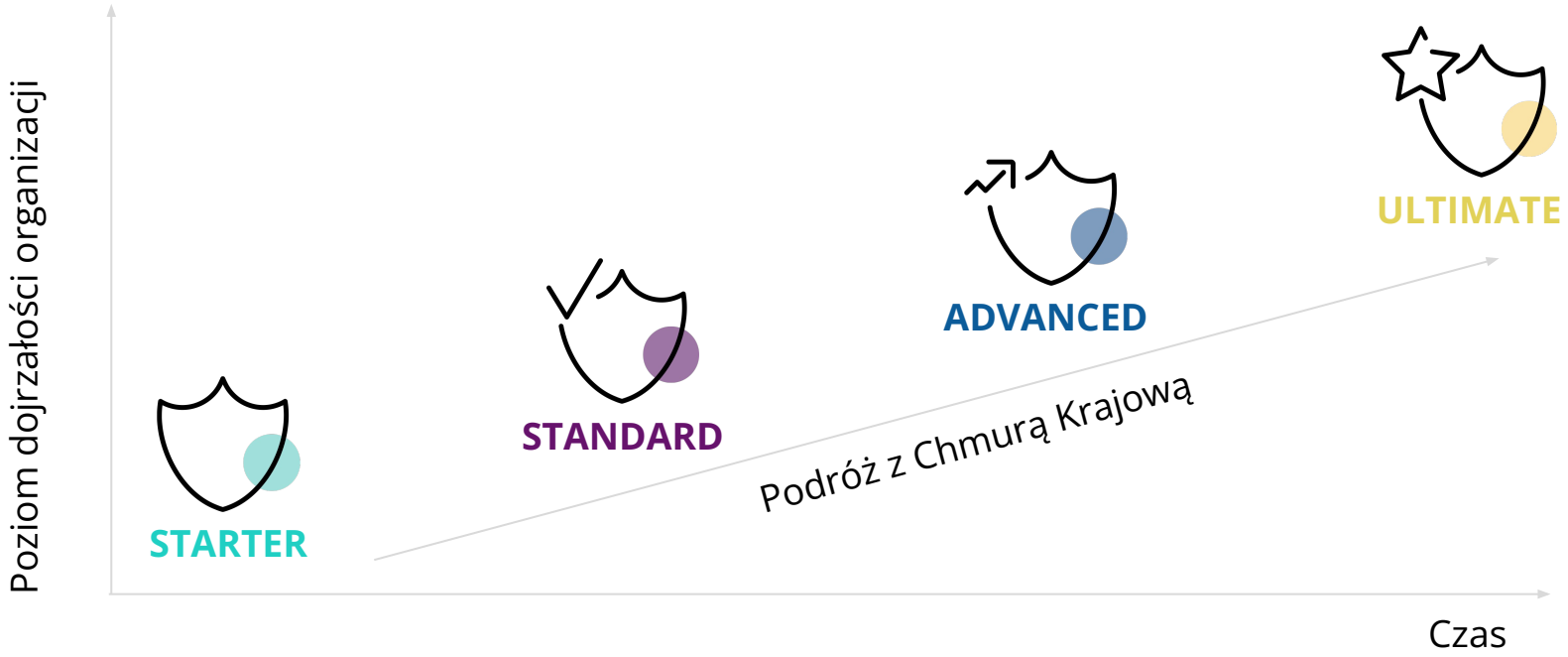
Naszą przewagą jest unikalne doświadczenie w obszarze zabezpieczania i monitorowania środowisk cloud computing, a także możliwość świadczenia usług w trybie 24/7.

**Korzyści**

- Zapewnienie odpowiedniego poziomu bezpieczeństwa IT w organizacji
- Identyfikacja ryzyka w obszarze zabezpieczeń środowiska IT
- Możliwość korzystania z usług monitoringu w trybie 24/7
- Zapewnienie zgodności regulacyjnej
- Dostęp do unikalnej wiedzy i doświadczenia w zakresie bezpieczeństwa środowisk chmurowych
- Liczne certyfikaty potwierdzające posiadane kompetencje

**Bezpieczna**
Chmura

# **Security Operation Centre** (SOC)
z Chmurą Krajową



# SOC: Wartość dodana dla organizacji

## STARTER

Identyfikacja słabości i podatności w infrastrukturze

Minimalizacja ryzyka poprzez detekcję i możliwie szybką reakcję na ataki:

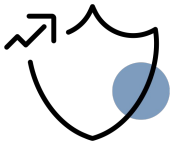
- Ransomware
- Phishing
- Ataki malware

## STANDARD

Wsparcie w obsłudze incydentów bezpieczeństwa

Zwiększenie widoczności działań pracowników oraz minimalizacja ich niepożądanych aktywności

Wsparcie w naprawianiu słabości i podatności w infrastrukturze



## ADVANCED

Niezależna ocena dojrzałości poziomu bezpieczeństwa w organizacji

Zwiększenie widoczności w aplikacjach oraz identyfikacja potencjalnie niebezpiecznych zachowań

## ULTIMATE

Wsparcie w realizacji wymagań compliance oraz w zarządzaniu ryzykiem

Wsparcie w przeprowadzaniu zmian w infrastrukturze klienta celem podniesienia poziomu bezpieczeństwa

# Security Operation Centre (SOC)

## STARTER

**ROZWIĄZANIE**

Microsoft Defender

**OCHRONA**

- Automatyczne reakcje na zdarzenia bezpieczeństwa
- Serwery Linux / Windows
- Urządzenia końcowe użytkownika

## STANDARD

**ROZWIĄZANIE**

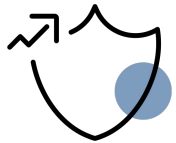
Microsoft Defender*

Microsoft Sentinel

**OCHRONA**

**STARTER +**

- Pakiety biurowe M365 / Google Workspace
- Sieć Cloud Native



## ADVANCED

**ROZWIĄZANIE**

Microsoft Defender*

Microsoft Sentinel

**OCHRONA**

**STANDARD +**

- Urządzenia sieciowe klienta on-prem (NGFW, F5)
- Aplikacje Custom klienta**

## ULTIMATE

**ROZWIĄZANIE**

**Na życzenie klienta Cloud Native / Hybrydowe**

**OCHRONA**

**ADVANCED +**

- rozwiązania spełniające potrzeby klienta

* Istnieje możliwość wykorzystania innego rozwiązania klasy EDR klienta
** Objęcie monitoringiem do 5 aplikacji klienta z założeniem stosowania określonego standardu logów z aplikacji

**Bezpieczna** Chmura

# **Security Operation Centre** (SOC)

## STARTER

**WDROŻENIE ROZWIĄZANIA**

**MONITORING ZESPOŁU OCHK W TRYBIE 24/7**

**IDENTYFIKACJA PODATNOŚCI** dla serwerów i urządzeń końcowych użytkowników

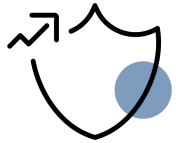
**Ochrona serwerów** (Windows/Linux) i **urządzeń końcowych użytkowników oraz zautomatyzowana reakcja na zagrożenia:**

- Zablokowanie zagrożonego konta użytkownika
- Wymuszenie potwierdzenia tożsamości zagrożonego użytkownika
- Izolacja sieciowa zagrożonego serwera / urządzenia końcowego
- Podstawowa analiza podejrzanych plików

## STANDARD

**Zakres STARTER +**

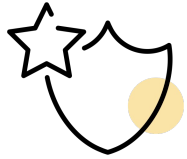
- Współpraca z zespołem IT klienta w zakresie **zarządzania podatnościami**
- **Identyfikacja zagrożeń dla bezpieczeństwa informacji** w pakietach biurowych M365 / Google Workspace
- **Identyfikacja zagrożeń dla usług sieciowych**
- Do **100 reguł identyfikujących** powyższe zagrożenia w infrastrukturze chmurowej i on-prem klienta oraz **zautomatyzowane działania mitygujące**



## ADVANCED

**Zakres STANDARD +**

- **Threat Intelligence** - informowanie klienta o nowych zagrożeniach adekwatnych do infrastruktury i technologii klienta
- **Identyfikacja zagrożeń** dla aplikacji custom klienta
- **Identyfikacja zagrożeń dla usług sieciowych** Cloud Native oraz rozwiązań sieciowych NGFW / F5 z infrastruktury on-prem klienta
- Do **250 reguł identyfikujących** powyższe zagrożenia w infrastrukturze chmurowej i on-premise klienta oraz **zautomatyzowane działania mitygujące**



## ULTIMATE

**Zakres ADVANCED +**

- Szczegółowa analiza zdarzeń bezpieczeństwa i analiza śledcza
- **Threat hunting** - aktywny monitoring zagrożeń w infrastrukturze klienta przez zespół SOC
- Wsparcie w zarządzaniu ryzykiem technologicznym
- **Hardening** - Identyfikacja możliwych usprawnień konfiguracji bezpieczeństwa w infrastrukturze klienta
- **Elastyczna ilość reguł identyfikujących** powyższe zagrożenia w infrastrukturze chmurowej klienta oraz **zautomatyzowane działania mitygujące**

# **Security Operation Centre** (SOC)

| | STARTER | STANDARD | ADVANCED | ULTIMATE |
|---|---|---|---|---|
| WARIANTY | Do 100 / 250 / 500 komponentów objętych monitoringiem (serwery + urządzenia końcowe użytkowników) | Do 250 / 500 / 1000 komponentów objętych monitoringiem (serwery + urządzenia końcowe użytkowników + pakiety biurowe + usługi sieciowe cloud native) | Do 500 / 1000 / 1500 komponentów objętych monitoringiem (serwery + urządzenia końcowe użytkowników + pakiety biurowe + usługi sieciowe cloud native + urządzenia sieciowe on-prem klienta + aplikacje custom klienta) | Wycena indywidualna |

**Bezpieczna**
Chmura

# Microsoft 365 Defender

## Ochrona użytkowników końcowych

Skanowanie stacji końcowych w poszukiwaniu złośliwych plików ale także podatności oraz reakcja na nie.

Microsoft 365 Defender automatycznie blokuje wykryte zagrożenia i zbiera wszystkie informacje niezbędne do przeprowadzenia szybkiej analizy takie jak:

- przyczyna, rodzaj wykrytego zdarzenia (malware, ransomware itp. ),
- powiązane procesy,
- połączenia internetowe,
- działania użytkownika. Obejmuje to także jeden z najczęstszych przyczyn incydentów czyli phishing .

## Security Recommendations

Dzięki regularnemu skanowaniu defender jest wstanie wykryć i wygenerować raport z możliwości zwiększenia bezpieczeństwa stacji końcowej takie jak:

- aktualizacja aplikacji do najbezpieczniejszych wersji,
- włączenie lub wyłączenie konkretnych funkcji systemu
- zmianę konfiguracji polityk i innych ustawień.

## Threat Hunting ( pakiet ultimate )

Istnieją zagrożenia których z definicji nie wykryje żaden skan czy reguła, są to tak zwane “zero day” czyli zagrożenia i metody ataków które zostały odkryte bardzo niedawno, o których wiedzą jedynie osoby, które to odkryły.
Dzięki funkcji Advanced Hunting w Defender architekci OChK są w stanie sprawnie przeprowadzać ręczne przeszukiwanie logów stacji końcowych w celu wykrycia podejrzanych zdarzeń w systemach mogących wskazywać na użycie zero day.

# Azure Sentinel

## Security Information and Event Management / Security Orchestration, Automation and Response

Rozwiązanie klasy **SIEM** oraz **SOAR** stworzone przez firmę Microsoft. Usługa Microsoft Sentinel zapewnia **inteligentną analizę zabezpieczeń** i **analizę zagrożeń** w całej organizacji, zapewniając rozwiązanie do generowania alertów, wykrywania zagrożeń oraz aktywnego polowania i reagowania na potencjalne zagrożenia. Dzięki usłudze Microsoft Sentinel uzyskasz jedno rozwiązanie do **wykrywania ataków**, widoczności zagrożeń, proaktywnego wyszukiwania zagrożeń oraz reagowania na zagrożenia.

- Zbieranie danych w wymiarze chmurowym - z urządzeń, aktywności użytkowników, aplikacji i infrastruktury - zarówno z Azure, on-premise jak i innych providerów;
- Wykrywanie wcześniej nieodkrytych zagrożeń dzięki Microsoft analytics oraz threat intelligence;
- Badanie zagrożeń za pomocą sztucznej inteligencji i polowanie na podejrzaną aktywność w dużej skali;
- Szybka reakcja dzięki orkiestracji i automatyzacji typowych działań.

Azure Sentinel zawiera również funkcjonalność SOAR - orkiestracji zabezpieczeń i automatycznej odpowiedzi. Funkcja SOAR platformy Microsoft Sentinel jest **w pełni konfigurowalna** i umożliwia zespołom ds. Bezpieczeństwa pisanie elementów tzw. playbook, które mogą (w razie potrzeby) **zautomatyzować** całą odpowiedź na zdarzenie związane z bezpieczeństwem.

# SOC: Monitoring i Reakcja

## Monitoring

Usługa polega na monitorowaniu bezpieczeństwa zasobów IT klienta w trybie 24/7/365 przez zespół SOC OChK. Usługa będzie realizowana z wykorzystaniem rozwiązania Microsoft Sentinel i świadczona zgodnie z uzgodnionymi z klientem scenariuszami bezpieczeństwa.

**Monitorowanie:**

- Ciągła weryfikacja zdarzeń przesyłanych ze źródeł do systemu SIEM z wykorzystaniem zaimplementowanych reguł bezpieczeństwa,
- Weryfikacja występujących alarmów przez Operatora SOC zgodnie z kryteriami zdefiniowanymi w **scenariuszu bezpieczeństwa** w celu wykluczenia fałszywych alarmów,
- dostrajanie reguł generujących alarmy,

**Reagowanie na wykryte zdarzenia** bezpieczeństwa (w podstawowym wariancie usługi; wariant rozszerzony znajduje się w opisie usługi rozszerzonej reakcji na incydent):

- zebranie informacji i analiza zdarzenia (w zależności od dostępności danych),
- realizacja instrukcji reagowania ustalonej w **scenariuszu bezpieczeństwa** dla danego typu zdarzenia,
- przekazanie zebranych informacji i opisu dotychczas podjętych kroków do klienta wraz z rekomendacjami w zakresie dalszej mitygacji incydentu,
- eskalacja wykrytych zdarzeń bezpieczeństwa w przypadku braku reakcji ze strony Klienta, zgodnie z ustalonymi **ścieżkami eskalacyjnymi** i kryteriami określonymi w **scenariuszach bezpieczeństwa**,
- pomoc w obsłudze incydentów zgłaszanych przez klienta,
- współpraca z klientem w celu usunięcia skutków incydentu.

# SOC: Monitoring i Reakcja

## Raportowanie

- W ramach realizacji usługi, SOC dostarcza generowane cyklicznie lub na życzenie Klienta raporty,
- Forma i zakres raportów zostanie ustalona z klientem. Możliwe jest także planowanie cyklicznych spotkań z klientem w celu oceny i tuningu usługi SOC.

## Rozszerzona reakcja na Incydent

Usługa polega na **rozbudowie scenariuszy bezpieczeństwa** realizowanych w podstawowej usłudze Monitorowania o zaplanowane oraz zdefiniowane wspólnie z klientem plany reakcji na zaistniałe zdarzenia niepożądane lub incydent bezpieczeństwa. Plany te mają formę playbooków, czyli predefiniowanego zbioru akcji ułożonych w drzewo decyzyjne, które tworzą reakcję na zaistniałą sytuację.

Zaletą usługi SOC  jest znaczne skrócenie czasu reakcji na wykryte zdarzenie, co w przypadku niektórych typów ataków (ransomware) może mieć kluczowy wpływ na konsekwencje incydentu dla klienta. Zastosowanie zdefiniowanych na etapie wdrożenia oraz ciągle tune'owanych w trakcie trwania usługi drzew decyzyjnych minimalizuje zaangażowanie personelu klienta w proces obsługi powtarzalnych zdarzeń o niskim poziomie krytyczności. Każdy z playbooków jest dostosowany do konkretnych typów zagrożeń. Reakcje mogą zostać zdefiniowane w taki sposób, aby wchodziły w interakcję oraz wprowadzały zmiany w systemach.

# SOC: Automatyczna reakcja

Playbooki reakcji będą realizowane z wykorzystaniem systemu **SOAR**, w zależności od ustaleń zdefiniowanych w scenariuszu bezpieczeństwa:

- w sposób automatyczny,
- w sposób półautomatyczny, który każdorazowo wymaga akceptacji wykonania zdefiniowanej akcji przez:
  - pracownika SOC,
  - zdefiniowaną osobę po stronie klienta np.:
    - pracownika działu bezpieczeństwa,
    - pracownika działu zarządzania infrastrukturą IT,
- poprzez ręczne wywołanie przygotowanych wcześniej akcji w postaci skryptów lub wywołań programu przez operatora pierwszej lub analityka drugiej linii SOC (w zależności od krytyczności podejmowanej akcji).

**Wykorzystanie systemu SOAR zapewnia pełną rozliczalność** wykonywanych akcji poprzez rozbudowany system audytowy. Obsługa każdego incydentu lub innego zdarzenia niepożądanego zakończona będzie automatycznie wygenerowanym raportem zawierającym listę wykonanych czynności wraz z ich wynikami.

**Raport może być dostarczany do klienta lub dostępny w konsoli SOAR** dla wskazanych przez niego pracowników posiadających konta w systemie. Realizowanymi czynnościami mogą być m. in. operacje zablokowania użytkownika w domenie, izolacji zainfekowanego hosta, zebrania atrybutów obiektów w domenie, itp.

# Wspierające usługi cybersecurity

## Zarządzanie podatnościami

**Usługa polega na koordynowaniu procesu zarządzania podatnościami w infrastrukturze klienta przez zespół SOC OChK**. W zakres usługi wchodzą następujące elementy:

Utrzymywanie bazy zasobów zawierającej informacje o:

- właścicielach biznesowych oraz technicznych
- wersjach systemów operacyjnych
- aplikacjach serwerowych i klienckich
- obszarze sieciowym, w którym znajduje się dany asset
- ścieżce eskalacyjne dla procesu weryfikacji wykonania zaleceń mitygacyjnych.

Określanie klasy assetów ze względu na istotność dla organizacji oraz jakie konsekwencje poniesie za sobą kompromitacja systemu oraz do jakich systemów, połączonych z potencjalnie skompromitowanym system, atakujący mógłby próbować uzyskać dostęp lub próbować je atakować.

Wycena ryzyka zostanie również adekwatnie podniesiona lub obniżona ze względu na możliwe przepływy sieciowe pomiędzy analizowanym systemem, a systemami o wyższej lub niższej wartości.

# Wspierające usługi cybersecurity

**Identyfikowanie podatności następuje na podstawie:**

1. Skanów wykonywanych w infrastrukturze klienta
2. Informacji o znanych podatnościach w technologiach wykorzystywanych u klienta pozyskanych w procesach **Threat Intelligence**.

Znalezione podatności są oceniane przez pryzmat zasobu, na którym zostały wykryte oraz łatwości przeprowadzenia ataku z ich wykorzystaniem w infrastrukturze klienta. W następstwie wykrycia i oceny zidentyfikowanych podatności przygotowywane są raporty agregujące uzyskane w procesie informacje.

Elementem procesu raportowania jest **automatyczne tworzenie zadań dla właścicieli technicznych systemów** (zgłoszeń w systemie ticketowym), informujących o konieczności usunięcia podatności poprzez instalację aktualizacji lub zastosowanie innej mitygacji (jeśli istnieje).

W zakres usługi wchodzi **zarządzanie odstępstwami**, polegające na rejestrowaniu podatności, których załatanie jest niemożliwe z przyczyn technicznych lub biznesowych (brak wprowadzenia takiego procesu będzie skutkował spadkiem efektywności programu zarządzania podatnościami), **weryfikacja wykonywania zaleceń wraz z eskalacją** (w przypadku stwierdzenia braku zaadresowania zgłoszonych podatności) oraz utrzymywanie bieżącej listy zasobów oczekujących na wykonanie akcji naprawczych.

Cykl zarządzania podatnościami będzie realizowany zgodnie z harmonogramem skanów oraz patchowania obowiązującym u klienta.

# Wspierające usługi cybersecurity

## Forensic

Usługa głębokiej analizy śledczej systemów klienta, realizowana na życzenie z wykorzystaniem posiadanych przez SOC OChK narzędzi. Uruchomienie usługi polega na **zdefiniowaniu zakresu technologicznego,** a także opracowaniu i przetestowaniu planów oraz procedur, które będą realizowane w przypadku wystąpienia incydentu wymagającego podjęcie działań  z zakresu informatyki śledczej.

Proponowane zakres usługi to:

1. Proces **zebrania wstępnych dowodów** powiązanych z incydentem, mający na celu klasyfikację incydentu oraz wybór odpowiednich procesów technicznych w celu zebrania pełnego materiału dowodowego
2. **Koordynacja z pracownikami klienta zabezpieczenia i/lub zajęcia (jeżeli będzie to konieczne) sprzętu elektronicznego**, który może być dowodem w sprawie związanej z incydentem bezpieczeństwa. W szczególnych przypadkach pomoc klienta w przekazaniu zebranych materiałów organom śledczym.
3. **Zebranie pełnego materiału dowodowego** ze wszystkich systemów powiązanych z danym incydentem (z uwzględnieniem uzyskanych zgód na adekwatnym poziomie):
    a. **Analiza** zabezpieczonych kopii obrazów dyskowych.
    b. **Zebranie artefaktów** z badanych systemów.
    c. **Dostarczenie raportu** zawierającego dokładną dokumentację przeprowadzonych czynności wraz z ich wynikami.

# Wspierające usługi cybersecurity

## Threat Hunting i Threat Intelligence

**Usługa polega na ciągłym, aktywnym przeglądaniu zdarzeń zbieranych przez SIEM, flowów, konfiguracji usług oraz systemów wdrożonych u klienta i innych źródeł informacji o infrastrukturze w celu identyfikacji nowych zagrożeń, nie zdefiniowanych w scenariuszach bezpieczeństwa.**

W zakres usługi wchodzi manualne przeszukiwanie przez analityka źródeł informacji dostępnych z systemów, które opiera się na założeniu, że doszło do naruszenia bezpieczeństwa (badanie hipotez o wystąpieniu zagrożenia lub sytuacji niepożądanych w infrastrukturze klienta).

Proponowana metodologia działań **Threat Hunting** polega na:

1. Postawieniu **hipotezy**.
2. **Analizy wybranych źródeł** danych oraz, gdy zajdzie konieczność, uruchomieniu ad-hoc dodatkowych narzędzi w porozumieniu z działem bezpieczeństwa oraz działem IT
3. **Wykrycie, opisanie nowych wzorców zachowań infrastruktury** oraz, jeżeli zostaną zidentyfikowane, TTP
4. **Zintegrowanie pozyskanych informacji** w systemach detekcji (definiowanie nowych reguł w SIEM)
5. **Walidacja modyfikacji** wprowadzonych w systemach detekcji (testy zaimplementowanych reguł)

# Wspierające usługi cybersecurity

**W zakres usługi wchodzi Threat Intelligence w następującym zakresie:**

1. **Monitorowanie publicznie dostępnych źródeł informacji** w celu identyfikacji potencjalnych zagrożeń dla Infrastruktury klienta, takich jak: kampanie malware, grupy APT, podatności zero-day i inne
2. **Analiza i przekazanie informacji** dopasowanej do specyfiki rynku, na którym działa klient
3. **Analiza potencjalnej skuteczności historycznych ataków** na podobne organizacje
4. **Kolekcja, korelacja oraz przygotowywanie i dostarczanie IoC** dostosowanych do wykorzystywanych technologii

Efektem realizowanych w ramach usługi czynności są raporty opisujące zidentyfikowane zagrożenia lub słabości wraz z rekomendacjami w zakresie hardeningu, propozycjami nowych scenariuszy monitorowania itp. Raporty będą dostarczane przez SOC na kilku poziomach decyzyjnych:

1. **Poziom strategiczny:** kwartalne raporty dla decydentów dotyczące bieżących ryzyk cyberbezpieczeństwa i prawdopodobieństwa ich materializacji
2. **Poziom operacyjny:** raport miesięczny (w przypadku wystąpienia znacznych zagrożeń oraz zidentyfikowania ich źródeł dostarczany niezwłocznie po ich zidentyfikowaniu) z rekomendacją, jakie dostępne środki zaradcze należy zastosować
3. **Poziom taktyczny:** precyzyjne wytyczne dotyczące wdrożenia rekomendacji określanych na wyższych poziomach raportowania np. hardening GPO, rekonfiguracja kernela, ustawień Tomcat wraz z pomocą konsultanta w ich wdrażaniu