trecom

WHITE PAPER

Analiza Ryzyka W Kontekście NIS 2

Spis treści

Wprowadzenie do NIS 2

KONTEKST

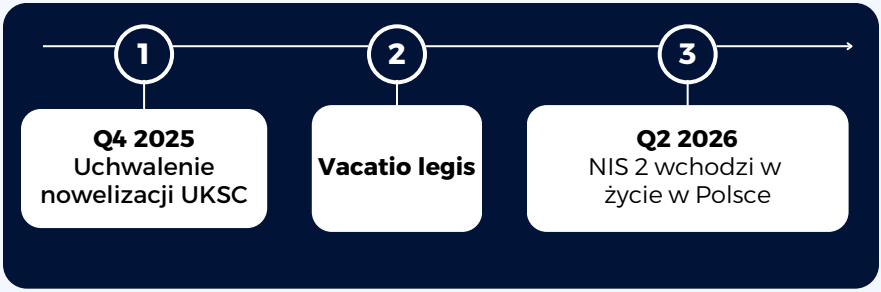
NIS 2 stanowi znaczący krok w poprawie ochrony i odporności przed cyberzagrożeniami organizacji w UE.

W Polsce dyrektywa NIS 2 będzie implementowana poprzez nowelizację ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Choć jeszcze nie wiadomo kiedy zostanie ona przyjęta, w projekcie został przewidziany jednomiesięczny okres vacatio legis.

Na realizację obowiązków wskazanych w ustawie podmioty kluczowe i ważne będą miały czas do Q2 2026 roku.

Wbrew pozorom nie jest to dużo czasu i w praktyce oznacza, że organizacje już dzisiaj powinny przystąpić do działań mających na celu przygotowanie się do wejścia w życie nowych przepisów.



WYMOGI NIS 2

NIS 2 definiuje elementy w ramach cyberbezpieczeństwa i ryzyka, co do których organizacje muszą opracować wewnętrzne procedury i polityki oraz wdrożyć narzędzia spełniające wymogi określone w dyrektywie.

KLUCZOWE WYMOGI NIS 2

Dyrektywa NIS 2 definiuje szereg wymogów i powinna zostać szczegółowo przeanalizowana przez ekspertów od IT, ryzyka i cyberbezpieczeństwa.

Nasi specjaliści, którzy mają już za sobą projekty wdrożeniowe z wymogów NIS 2, dzielą się swoją wiedzą i przygotowują serię white paper, która pozwoli organizacjom zrozumieć i wdrożyć wszystkie wymogi dyrektywy NIS 2. Na potrzeby tego projektu, zidentyfikowaliśmy wymogi w 10 kluczowych obszarach:

1. **Opracowanie i wdrożenie polityki bezpieczeństwa systemu informacyjnego i metodyki szacowania ryzyka**
2. **Opracowanie i wdrożenie procesu zarządzania incydentami i innych polityk tematycznych**
3. **Opracowanie i wdrożenie planów działania oraz polityk awaryjnych umożliwiających ciągłe i niezakłócone świadczenie usługi**
4. **Opracowanie i wdrożenie dokumentacji określającej bezpieczeństwo łańcucha dostaw produktów, usług i procesów, w tym polityk bezpieczeństwa stron trzecich**
5. **Zapewnienie bezpieczeństwa w procesie nabywania, rozwoju i utrzymania sieci i systemów**
6. **Wprowadzenie polityk i procedur służących ocenie skuteczności środków zarządzania ryzykiem**

7 **Zapewnienie podstawowych praktyk cyberhigieny między innymi poprzez szkolenia w zakresie cyberbezpieczeństwa**

8 **Wprowadzenie polityk i procedur stosowania kryptografii**

9 **Przygotowanie organizacji na zbieranie informacji o cyberzagrożeniach i podatnościach na incydenty**

10 **Monitorowanie bezpieczeństwa systemów teleinformatycznych w trybie ciągłym**

NA JAKIE PYTANIA ODPOWIADA WHITE PAPER?

White paper ma pomóc przygotować się organizacjom na wymogi NIS 2 dotyczące polityk analizy ryzyka. White paper jest częścią serii na temat NIS 2, którą będziemy kontynuować w kolejnych tygodniach.

TREŚĆ WHITE PAPER

- Jak analizować i zarządzać ryzykiem z perspektywy procesowej?
- Jak identyfikować kluczowe zasoby i potencjalne zagrożenia oraz ryzyka?
- Jak narzędzia IT GRC pomagają w analizie i zarządzaniu ryzykiem?
- Jak podejść do strategii zarządzania ryzykiem?
- Z jakich programów do zarządzania ryzykiem warto korzystać?

O AUTORACH WHITE PAPER

Piotr Kępski
TrecomSEC
Analityk systemów bezpieczeństwa

Mirosław Maj
TrecomSEC
Dyrektor

Cyprian Gutkowski
TrecomSEC
Konsultant

Marcin Fronczak
TrecomSEC
Konsultant

Zapraszamy do lektury

Analiza i zarządzanie ryzykiem z perspektywy procesowej

IDENTYFIKACJA ZASOBÓW

Proces analizy i zarządzania ryzykiem powinniśmy zacząć od identyfikacji kluczowych aktywów, danych oraz informacji. Niezależnie od unikalnego zestawu wspomnianych elementów, do najważniejszych zasobów należą:

- **Topologia sieci**
- **Kluczowe procesy biznesowe**
- **Dane personalne**
- **Dane transakcyjne**
- **Dane klientów**
- **Dane technologiczne**
- **Informacje o elementach fizycznych (np. zakładach)**
- **Pozostałe**

Poza samą identyfikacją kluczowych aktywów należy zebrać uzupełniające dane.

1 DANE O WŁAŚCICIELACH ZASOBU

- Kto na co dzień odpowiada za dane aktywa?
- Jakie dostępy do aktywa ma wspomniana osoba?

2 **ZALEŻNOŚCI ZASOBU**

- Z jakim kluczowym procesem wiąże się zasób?
- Jakie kluczowe dane posiada zasób?

3 **KRYTYCZNOŚĆ AKTYWA**

- Jak bardzo krytyczny jest zasób? (należy przypisać skalę krytyczności do każdego zasobu)

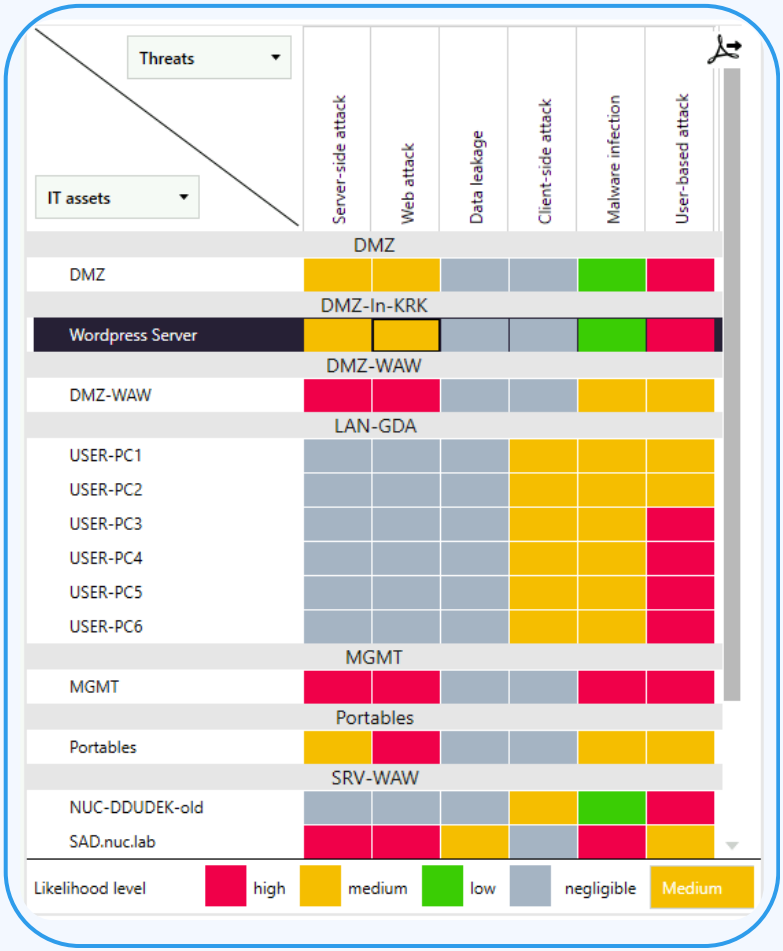
IDENTYFIKACJA POTENCJALNYCH RYZYK

Po identyfikacji zasobów, które są narażone na potencjalne ryzyka przechodzimy do przydzielenia samych zagrożeń. Najczęściej mowa o:

- **Cyberatakach**
- **Ryzykach na warstwie fizycznej**
- **Technicznych niedoskonałościach**
- **Ryzykach wewnątrz organizacji**
- **Pozostałych ryzykach**

Organizacje powinny przypisywać indywidualne ryzyka do aktywów. Dodatkowo powinno się szacować ilościowo prawdopodobieństwo wystąpienia konkretnego ryzyka.

PRZYKŁAD ANALIZY RYZYKA W NARZĘDZIU IT GRC



ANALIZA RYZYKA W ROZWIĄZANIU SECUREVISIO

PRZYGOTOWANIE STRATEGII ODPOWIEDZI NA RYZYKO

W celu przygotowania strategii odpowiedzi na ryzyko należy ustalić priorytety dla konkretnych zasobów. Priorytetyzacja umożliwi efektywną ochronę przed najpoważniejszymi ryzykami.

Dla każdego ryzyka należy obliczyć indywidualne wskaźniki ryzyka (ang. risk score), które będą podstawą w priorytetyzacji. Narzędzia do analizy i zarządzania ryzykiem mogą brać pod uwagę wartość zagrożonego zasobu, prawdopodobieństwo wystąpienia danego ryzyka czy obecny stopień zabezpieczenia aktywa.

Po dogłębnym ustaleniu poziomu ryzyka dla kluczowych aktywów należy przygotować strategię reakcji na ryzyko. Reakcje mogą zakładać wdrożenie konkretnych inicjatyw ograniczenia poziomu ryzyka, ale również samo uznanie ryzyka i ciągły monitoring ryzyka w celu reakcji w przypadku zwiększenia poziomu ryzyka.

Analiza ryzyka powinna zmieniać się w zależności od otaczającego podmiot świata, zarówno w warstwie technicznej, legislacyjnej, ale również występujących w otoczeniu zagrożeń. Analiza ryzyka powinna więc opierać się o feedy z CTI i działów compliance lub prawnego.

Identyfikacja kluczowych zasobów

ZASOBY

Pomocne w przygotowaniu bazy zasobów mogą okazać się bazy CMDB, które umożliwiają identyfikację zasobów i ich zależności. Definiowanie aktywów i w kolejnym kroku ich roli powinno nastąpić na podstawie wspólnej dyskusji w ramach organizacji. Do najważniejszych elementów należą:

- **Elementy fizyczne (np. serwery)**
- **Warstwa programowa**
- **Zasoby informacyjne**
- **Infrastruktura fizyczna organizacji**
- **Usługi i procesy biznesowe (np. krytyczne procesy, usługi prawne, usługi online)**
- **Zasoby ludzkie**

DODATKOWE DANE O ZASOBACH

Poza samymi technicznymi danymi (jak np. adres IP czy wersja kluczowych oprogramowań i systemów) należy zebrać pozostałe dane, które dają lepszy kontekst, w tym:

- **Powiązane kluczowe procesy biznesowe**
- **Informacje o użytkownikach końcowych**
- **Powiązane technologie i systemy**
- **Krytyczność**
- **Zastosowane mechanizmy ochrony**
- **Osoby odpowiedzialne za zarządzanie zasobem (“właściciele zasobów”)**
- **Wymagania funkcjonalne**
- **Zasoby informacyjne**

KLUCZOWE ELEMENTY

Wśród wymienionych wcześniej elementów kluczowe jest zidentyfikowanie właścicieli zasobów. To właśnie właściciele powinni w pierwszej kolejności odpowiadać za bezpieczeństwo wybranych zasobów.

Ponadto drugim ważnym czynnikiem jest ustalenie roli aktywa w ramach organizacji. Chodzi o odpowiedź na kluczowe pytania, w tym:

- **Gdzie przechowywane są aktywa?**
- **Jakie procesy i aktywa w firmie uzależnione są od prawidłowego działania aktywa?**
- **Jak potencjalne zakłócenia (np. na warstwie technologicznej czy ludzkiej) wpływają na aktywa?**

Organizacje powinny również klasyfikować aktywa na poziomie wpływu na działalność - np. 1) niski wpływ, 2) średni wpływ i 3) wysoki wpływ

Niezwykle ważnym zagadnieniem jest klasyfikacja zasobów informacyjnych. Zasoby informacyjne obejmują m.in. dane zawarte w różnego rodzaju plikach czy bazach danych. Klasyfikacja informacji opiera się na poziomie wrażliwości, krytyczności i dostępności.

W przypadku samych danych mówimy między innymi o publicznych rejestrach, danych z systemów krytycznych, wewnętrznych narzędzi, czy kodach źródłowych.

Organizacje powinny zidentyfikować kluczowe zasoby informacyjne powiązane z zasobami i dbać o poufność, dostępność, autentyczność i integralność danych.

Identyfikacja potencjalnych ryzyk i narzędzia klasy IT GRC

IDENTYFIKACJA RYZYK

Po zidentyfikowaniu zasobów i ich zależności przechodzimy do samego przypisania potencjalnych ryzyk, w tym m.in. potencjalnych:

- **Ataków sieciowych**
- **Ryzyk związanych z dostawcami**
- **Klęsk żywiołowych**
- **Awarii systemowych**
- **Błędów ludzkich**
- **Ryzyk wewnątrz organizacji**
- **Pozostałych ryzyk**

Ryzyka należy kategoryzować na podstawie ich wagi i potencjalnego wpływu na organizację.

NARZĘDZIA KLASY IT GRC

Narzędzia klasy IT GRC mogą okazać się pomocne w identyfikacji i szacowaniu ryzyk. Wspomniane narzędzia identyfikują profil ryzyk poszczególnych zasobów i same przypisują indywidualne poziomy ryzyk. Każde indywidualne ryzyko jest liczone na podstawie wybranej formuły dostawcy narzędzi IT GRC - tak przykładowo może wyglądać formuła do szacowania ryzyka.

Poziom ryzyka = krytyczność wybranego zasobu x prawdopodobieństwa przełamania zabezpieczeń

Wynik osiągnięty w narzędziach IT GRC pozwala zakwalifikować je do odpowiedniej grupy ryzyk spośród wspomnianych trzech poziomów.

SZACOWANIE RYZYKA W IT GRC

Proces wyznaczania prawdopodobieństwa wystąpienia zagrożenia może wyglądać w następujący sposób:

- **Określenie zagrożeń, na jaki narażony jest zasób oraz z jakich kierunków (stref bezpieczeństwa) mogą pochodzić zagrożenia**
- **Ustalenie, jakie zabezpieczenia lokalne posiada zasób oraz jakie zabezpieczenia sieciowe mają urządzenia na trasie pomiędzy źródłami zagrożeń a zasobem**
- **Sprawdzenie, czy występują szczególne warunki zmieniające listę zagrożeń lub poziom prawdopodobieństwa wystąpienia określonego zagrożenia**

KRYTYCZNOŚĆ ZASOBU

Krytyczność zasobu dla organizacji może być wyznaczana na podstawie listy warunków zdefiniowanych w formie macierzy. Wynik uzyskany przy spełnieniu określonych warunków umożliwia osiągnięcie określonej wartości parametru ważności dla organizacji (np. wysoki, średni czy niski).

Szacowanie krytyczności zasobu powinno odbywać się poprzez analizę konsekwencji naruszenia bezpieczeństwa danych, wagi powiązanych procesów biznesowych oraz ogólnej roli zasobu w ramach organizacji.

Do wybranych czynników wpływających na finalny wynik należą:

- **Poufność danych powiązanych z zasobem**
- **Sposób użytkowania danych**
- **Powiązanie z krytycznym procesem biznesowym**
- **Ryzyko reputacyjne**
- **Pozostałe**

KLASYFIKACJA KRYTYCZNOŚCI AKTYWA W NARZĘDZIU IT GRC

Consequences / IT asset importance	Acquisition of computer / mobile device via Botnet / APT	Classified information leakage	Disturbance of important organization process	Legal consequences	Reputation losses and / or distribution of malicious content via web
❄ Private User Data +					
Critical ×			☑		
High ×		☑		☑	
Medium ×					☑
Low ×	☑				
❄ Company Data +					
Critical ×			☑		
High ×		☑		☑	
Medium ×					☑
Low ×	☑				
Intellectual property / własność intelektualna +					
High ×		☑	☑		
Medium ×	☑			☑	☑
Confidential company data / Poufne dane firmowe +					
High ×		☑	☑		
Medium ×	☑			☑	☑
Confidential customer data / Poufna dane klientów +					
High ×		☑	☑		
Medium ×	☑			☑	☑
Cardholder data / Dane kart kredytowych/bankowych +					
High ×		☑	☑		
Medium ×	☑			☑	☑

ANALIZA RYZYKA W ROZWIĄZANIU SECUREVISIO

Strategie zarządzania ryzykiem

WPROWADZENIE

Po zdefiniowaniu poziomu ryzyka dla konkretnych zasobów i stworzeniu matrycy ryzyka przechodzimy do wybrania samej strategii reakcji. Wyróżniamy 4 strategie reakcji:

- **Akceptacja ryzyka (i aktywne śledzenie ryzyka)**
- **Ograniczenie ryzyka poprzez identyfikację i wdrożenie dodatkowych środków umożliwiających ograniczenie ryzyka**
- **Zapobieganie ryzyku, czyli zmiana procesowa lub zasobowa, która umożliwia niemal pełne wyeliminowanie ryzyka**
- **Transfer ryzyka**

OGRANICZENIE RYZYKA

Ograniczenie ryzyka ma za zadanie ograniczenie powierzchni ataków, czyli zabezpieczenie elementów w organizacji, które mogą być wykorzystane w celu naruszenia zasad bezpieczeństwa.

TRANSFER RYZYKA

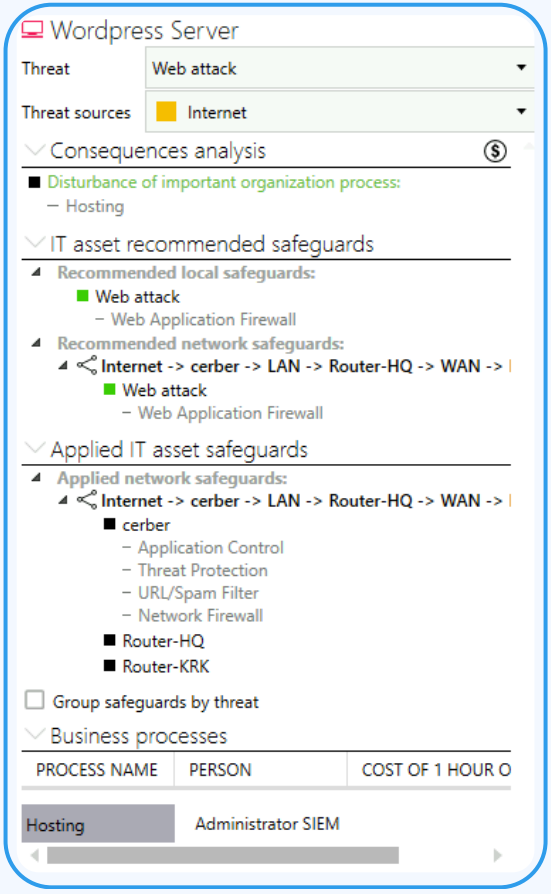
Warto również przeanalizować transfer ryzyka na różnego rodzaju dostawców usług zewnętrznych, w tym między innymi ubezpieczycieli.

Organizacje ubezpieczeniowe zgadzają się przyjąć na siebie ryzyko i zrekompensować szkody spowodowane konkretnym ryzykiem.

W przypadku współpracy z ubezpieczycielami należy podejść indywidualnie do ryzyka, gdyż część niestandardowych ryzyk nie będzie podlegała możliwości ubezpieczenia lub może być nieopłacalna.

Po określeniu ryzyk, systemy IT GRC wspierają zespoły bezpieczeństwa w automatycznym zdefiniowaniu środków (np. narzędzi z zakresu cyberbezpieczeństwa), które umożliwią ograniczenie konsekwencji ryzyk

PRZYKŁAD REKOMENDACJI OGRANICZENIA RYZYKA W NARZĘDZIACH IT GRC

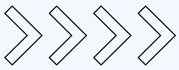


ANALIZA RYZYKA W ROZWIĄZANIU SECUREVISIO

ŚRODKI OGRANICZAJĄCE RYZYKO

Po identyfikacji konieczności ograniczenia ryzyka organizacje powinny wdrożyć odpowiednie procesy i narzędzia. W zależności od konkretnych przypadków możemy mówić m.in. o:

- **Regularnej instalacji aktualizacji**
- **Inwestycji w konkretne narzędzia**
- **Wykorzystaniu uwierzytelniania wieloskładnikowego**
- **Przeprowadzaniu regularnych szkoleń pracowników**
- **Aktualizacji planu reagowania na incydenty**
- **Ograniczeniu i kontroli dostępu do systemów**
- **Poprawie skuteczności planu ciągłości działania**
- **Poprawie skuteczności funkcji bezpieczeństwa sprzętowego**
- **Zabezpieczeniu kont, w tym kont uprzywilejowanych**
- **Pozostałych zmianach**



Dodatkowo, ważnym elementem w kwantyfikacji ryzyka mogą być symulacje ataków na systemy, które umożliwią walidację założeń organizacji w zakresie ryzyk

Najlepsze praktyki do zarządzania ryzykiem - checklista

- IDENTYFIKACJA AKTYWÓW I RYZYK, KTÓRYM PODLEGA ORGANIZACJA
- OPRACOWANIE STRATEGII I POLITYK W RAMACH CYBERBEZPIECZEŃSTWA
- OPRACOWANIE INDYWIDUALNYCH STRATEGII ZAPOBIEGAJĄCYCH WYSTĄPIENIU SYTUACJI WYSOKIEGO RYZYKA
- MONITOROWANIE RYZYKA I TESTOWANIE WDROŻONYCH ŚRODKÓW DO ANALIZY I MINIMALIZACJI RYZYKA
- REGULARNE ANALIZOWANIE OTOCZENIA REGULACYJNEGO POD KĄTEM WSZELKICH AKTUALIZACJI

Przykładowe programy do zarządzania ryzykiem

PROGRAMY DO ZARZĄDZANIA RYZYKIEM

Istnieje wiele programów definiujących najlepsze praktyki umożliwiające zarządzanie ryzykiem. Na dole przygotowaliśmy krótkie założenia najważniejszych programów:

1 NIST

NIST opiera się na następujących elementach:

- Kategoryzowanie systemów i danych
- Selekcja środków umożliwiających ograniczenie ryzyk
- Wdrożenie środków umożliwiających ograniczenie ryzyk
- Ocena wdrożonych środków
- Monitorowanie środków i ryzyk

2 FAIR

Podejście FAIR skoncentrowane jest na ilościowej analizie ryzyka czyli działaniu w oparciu o określone parametry wpływające na ryzyko. Do przykładowych czynników, które wpływają na parametr ilościowy należą częstotliwość wystąpienia zdarzeń powiązanych z zagrożeniem czy prawdopodobieństwo wystąpienia zagrożenia.

3 ISO 31000

ISO3100 zakłada zarządzanie ryzykiem jako podstawowy element wszystkich procesów realizowanych w ramach organizacji stając się fundamentem podejmowania kluczowych decyzji.

4 OCTAVE

OCTAVE opiera się na identyfikacji kluczowych aktywów informacyjnych oraz potencjalnych zagrożeń i podatności dla zidentyfikowanych aktywów.

5 TARA

TARA proponuje identyfikację obecnych ryzyk oraz ustalenie bazowych poziomów ryzyka.

W kolejnym kroku program zakłada identyfikację potencjalnych ścieżek materializacji zagrożenia.

Ostatnim elementem jest określenie stopnia narażenia na ryzyko i dostosowanie strategii bezpieczeństwa.

Jak Trecom pomaga spełnić wymogi NIS 2?

NASZE USŁUGI

Trecom pomaga organizacjom w spełnieniu wymogów dyrektywy NIS 2, wykorzystując najlepsze standardy branżowe oraz oferując zarówno ekspertyzę techniczną, jak również wsparcie w implementacji gotowych rozwiązań.

MIROSŁAW MAJ (DYREKTOR TRECOMSEC)

TRECOMSEC

- Trecom świadczy kompleksowe usługi audytu luki zgodności organizacji z wymogami NIS2 oraz DORA
- Zapewniamy również usługi wspierające budowanie zespołów od cyberbezpieczeństwa, wprowadzania procedur zachodzących w SOC czy modelowania zagrożeń

MICHAŁ KACZMAREK (MENADŻER SOC)

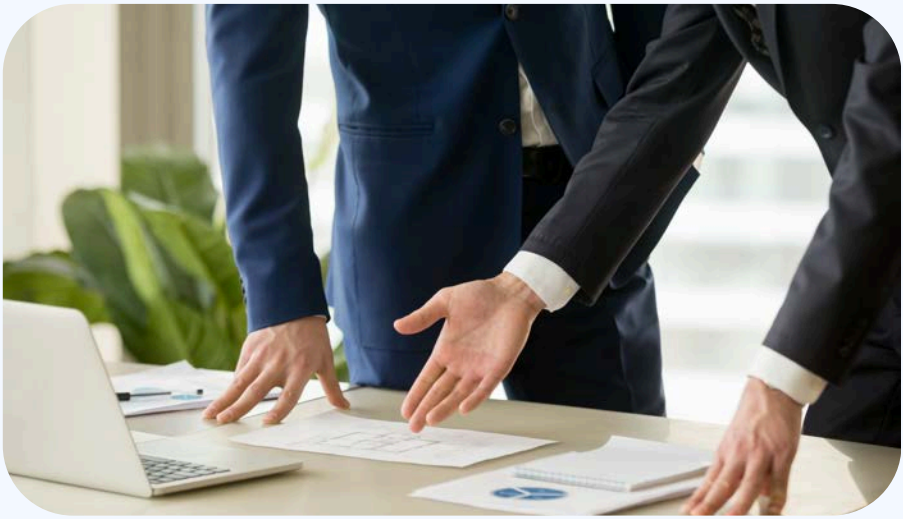
TRECOM SOC

- Trecom SOC oferuje kompleksowe zarządzanie incydentami (m.in wykrywanie, ocenę wpływu, eskalację i rozwiązanie)
- Oferujemy również szeroki zakres dodatkowych usług, w tym analizę ryzyka, CTI czy analizę malware
- Nasza usługa SOC jest zgodna z SIM3 oraz posiada status trusted introducer

NASZE ROZWIĄZANIA

Oferujemy szeroki zakres rozwiązań technologicznych wspierających spełnienie wybranych wymogów w zakresie NIS 2:

- Rozwiązania klasy SIEM, SOAR i UEBA
- Rozwiązania do zarządzania ryzykiem i podatnościami
- Rozwiązania klasy XDR czy EDR
- Firewall
- Rozwiązania klasy IAM
- Bazy CMDB
- Rozwiązania do ochrony sieci i środowiska chmurowego
- Rozwiązania do ochrony aplikacji
- i wiele innych



Przygotujemy Twoją organizację na NIS 2

BEZPŁATNE KONSULTACJE NIS 2

Wszystkich zainteresowanych NIS 2 zapraszamy na darmowe konsultacje, podczas których będziemy mogli porozmawiać o tym, jak spełnić wymogi NIS 2 w konkretnych przypadkach.