T Business

SECURITY OPERATIONS CENTER

Monitoring bezpieczeństwa



Connecting your world.

Cybersecurity

Monitorowanie zasobów IT

Security Operations Center (SOC) to usługa monitorowania oraz analizy zdarzeń bezpieczeństwa IT w celu wykrywania incydentów związanych z cyberbezpieczeństwem i zapobiegania im w przyszłości.

Wykorzystuje najnowsze dostępne rozwiązania technologiczne oraz właściwie określone procesy. Wykwalifikowany zespół pracujący w trybie 24/7/365 stale monitoruje infrastrukturę IT firmy i na bieżąco rozpoznaje incydenty spośród alertów bezpieczeństwa. Usługa ta jest źródłem niezbędnej wiedzy na temat stanu bezpieczeństwa IT w firmie oraz umożliwia chronienie jej przed cyberzagrożeniami.

Usługa Security Operations Center składa się z następujących elementów:

Monitorowanie bezpieczeństwa i badanie zdarzeń w trybie 24/7/365 według ustalonych scenariuszy, eliminowanie fałszywych alarmów (false positives), kategoryzacja i priorytetyzacja incydentów (triage).

Reakcja na incydent, przedstawienie zaleceń mitygacji, zmierzających do ograniczenia lub wyeliminowania zagrożeń, prowadzenie działań w celu postępowania z incydentem zgodnie z określonym SLA.

Threat Intelligence, czyli cykliczne, proaktywne dostarczanie informacji o możliwych nowych zagrożeniach i atakach, sposobach postępowania z nimi oraz sugerowanych rozwiązaniach zabezpieczających.

SIEM (Security Information and Event Management) to system, służący do zbierania, agregowania i korelowania logów, na bazie których generowane są alarmy dotyczące możliwych incydentów bezpieczeństwa.

Usługi profesjonalne, w tym ogólny audyt bezpieczeństwa, wykonywany obligatoryjnie przed wdrożeniem usługi SOC.



Trzy filary SOC

Technologie

Usługa świadczona jest z wykorzystaniem Splunk lub IBM QRadar – najlepszych rozwiązań dostępnych na rynku.

Procesy

Zgodne z uznanymi standardami i dobrymi praktykami ISO 27000, ITIL, NIST, ENISA.

Ludzie

Za obsługę incydentów odpowiada zespół ponad 30 inżynierów IT, posiadających liczne certyfikaty oraz wieloletnie doświadczenie w branży Cyber Security.



W 2024 r. **74% polskich firm** potwierdziło odnotowanie incydentów bezpieczeństwa.

Tylko **34,6% firm** w Polsce przyznaje, że monitoruje zagrożenia wynikające z cyberprzestępczości.

Raport VECTO „Cyberbezpieczeństwo w polskich firmach 2024".

Korzyści dla klienta

Zapewnienie organizacji całodobowego monitoringu infrastruktury pod kątem bezpieczeństwa teleinformatycznego.

Dostęp do raportów przedstawiających skalę cyberataków na organizację i podjętych działań, mających na celu przeciwdziałanie im.

Dostęp do najnowszych rozwiązań z zakresu bezpieczeństwa IT najlepszych światowych producentów.

Spełnienie wymagań wynikających z aktów prawnych, norm i standardów (np. Rozporządzenie o ochronie danych osobowych, ustawa o krajowym systemie cyberbezpieczeństwa).

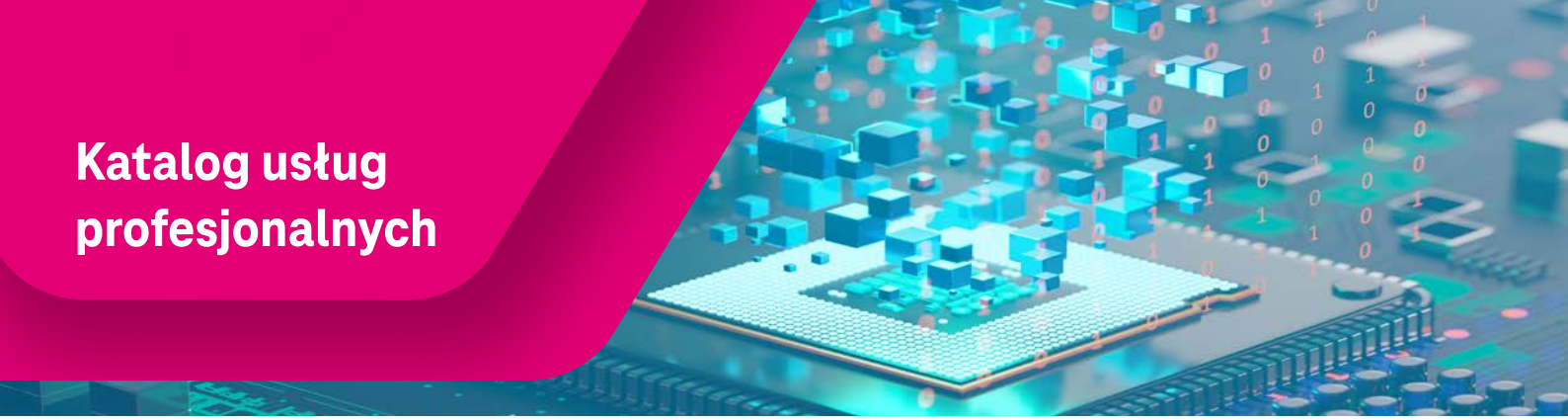
Reagowanie na pojawiające się incydenty bezpieczeństwa IT niezwłocznie po ich zidentyfikowaniu.



Dlaczego T-Mobile?

- Zapewnienie organizacji całodobowego monitoringu infrastruktury pod kątem bezpieczeństwa teleinformatycznego.
- T-Mobile Polska jest jednym z nielicznych dostawców usługi SOC na rynku polskim.
- Możliwe są bezpłatne testy usługi.
- Referencyjni klienci, korzystający z usługi SOC zarówno w Polsce, jak i w całej Europie.
- Kilkuletnie doświadczenie T-Mobile w dostarczaniu usług SOC.
- Kompleksowe rozwiązanie od T-Mobile – począwszy od projektu technicznego, poprzez wdrożenie aż po zarządzanie.
- Usługa oparta na rozwiązaniach uznanych światowych producentów: Splunk i QRadar (IBM).
- Usługa realizowana wyłącznie na bazie własnych zasobów ludzkich i infrastrukturalnych.
- Gotowe, sprawdzone scenariusze postępowania (tzw. play book).
- Gwarancja bezpieczeństwa danych i poufności informacji.
- Oferta dopasowana do wymagań klientów.
- Atrakcyjne ceny – już od 10 tys. zł netto miesięcznie.

Katalog usług profesjonalnych



Usługi profesjonalne – usługi doradczo-analityczne w obszarze bezpieczeństwa cybernetycznego świadczone przez ekspertów SOC. Usługi profesjonalne mogą być dostępne w ramach Usługi SOC (jako pula godzin w ramach abonamentu do wykorzystania w danym Cyklu Rozliczeniowym) lub realizowane jednorazowo na żądanie klienta i każdorazowo wyceniane.

Testy penetracyjne

Testy penetracyjne to kontrolowane ataki symulujące rzeczywiste działania cyberprzestępców. Podczas testów oraz w określonych ramach formalnych eksperci próbują zdobyć dostęp do systemów i aplikacji w firmie w celu identyfikacji słabych punktów infrastruktury IT, które mogą zostać wykorzystane do nieautoryzowanego dostępu, wycieku danych czy złośliwych działań.

Zakres

Analizy bezpieczeństwa aplikacji webowych i mobilnych prowadzone w modelu **greybox** oraz **blackbox**.

Testy infrastruktury sieciowej zarówno zewnętrznej, jak i wewnętrznej.

Weryfikacja konfiguracji zabezpieczeń systemów operacyjnych.

Raportowanie wykrytych podatności z zaleceniami naprawczymi.

Korzyści

Wczesne wykrywanie luk w zabezpieczeniach przed ich wykorzystaniem przez cyberprzestępców.

Szczegółowy raport z zaleceniami poprawy bezpieczeństwa, co pozwala na konkretne działania naprawcze.

Możliwość cyklicznego sprawdzania skuteczności wdrożonych zabezpieczeń.

Zwiększenie świadomości o potencjalnych zagrożeniach i lepsza ochrona przed przyszłymi atakami.

Threat Hunting

Threat hunting to aktywne poszukiwanie nieznanych zagrożeń w infrastrukturze IT, które mogłyby pozostać niewykryte przez standardowe narzędzia ochrony (np. antywirusowe). Specjaliści w tej dziedzinie prowadzą dogłębną analizę systemów, monitorują nietypowe działania i zachowania w sieci, identyfikując zagrożenia w ich wczesnych fazach. Do tego celu wykorzystywane są logi systemowe i sieciowe, dane z punktów końcowych (EDR, XDR), bazy IoC (Indicators of Compromise), dane forensyczne czy dane z SOC.

Zakres

- Analiza powłamaniowa i poincydentalna.
- Analizy związane z naruszeniem polityk bezpieczeństwa.
- Sprawdzenie zasadności podejrzeń o nielojalność pracowniczą.
- Identyfikacja tożsamości osób na podstawie informacji sieciowych.
- Zabezpieczanie danych zgodnie z zasadami informatyki śledczej do dalszej analizy.
- Zgodny z prawem monitoring pracowników, z poszanowaniem ich prywatności.
- Specjalistyczne ekspertyzy i opinie.
- Udział w zabezpieczaniu danych.
- Odzyskiwanie i wyszukiwanie informacji.
- Wyodrębnianie wskazanych danych.
- Analiza treści rozmów z komunikatorów.
- Analizy porównawcze.
- Analiza zgodności SIWZ z wykonaniem zamówienia.
- Konwersja danych z programów, baz danych lub nośników.
- Analiza urządzeń mobilnych – analiza malware pod kątem złośliwego oprogramowania.

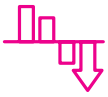
Korzyści



Wczesne wykrywanie zagrożeń, które mogą nie być zidentyfikowane przez automatyczne systemy zabezpieczeń.



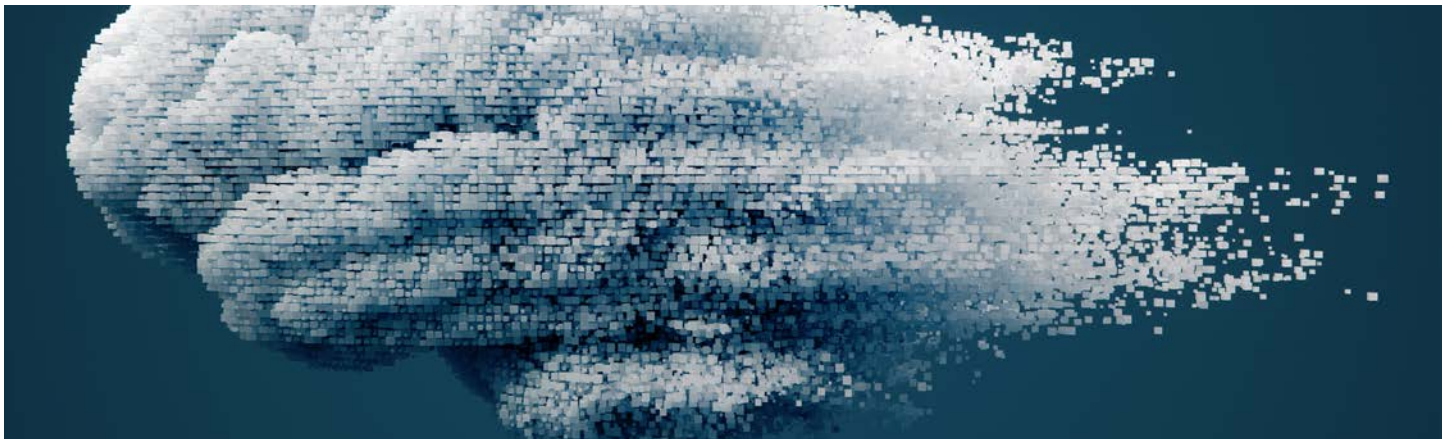
Zwiększenie szans na wykrycie ukrytych lub trudnych do zauważenia ataków.



Minimalizacja ryzyka długoterminowego uszkodzenia systemów, wycieku danych czy utraty reputacji firmy.



Zwiększenie poziomu świadomości zagrożeń w organizacji oraz poprawa ogólnej odporności na cyberataki.



Analiza Malware

Analiza Malware polega na badaniu podejrzanych plików, skryptów lub programów w celu zrozumienia jego działania, pochodzenia, metody ataku i możliwych konsekwencji. Analiza ta obejmuje także określenie, jak Malware może rozprzestrzeniać się w sieci oraz jak najlepiej go usunąć, aby zapobiec dalszym infekcjom.

Korzyści

Dokładna identyfikacja i eliminowanie złośliwego oprogramowania, minimalizujące dalsze uszkodzenia.

Zrozumienie technik i metod użytych przez cyberprzestępców, co pozwala na lepszą ochronę w przyszłości.

Zwiększenie zdolności firmy do reagowania na tego rodzaju incydenty i szybkie przywracanie normalnej działalności po infekcji.

Prewencja przed przyszłymi atakami poprzez opracowanie skutecznych środków ochrony.

Zakres

Analiza statyczna podejrzanych plików.

Analiza dynamiczna podejrzanych plików.

Analiza behawioralna.

Określenie źródła, zasięgu i funkcjonalności złośliwego kodu.

Rekomendacje dotyczące usunięcia zagrożenia i zapobiegania przyszłym incydentom.



Skanowanie podatności

Skanowanie podatności to proces automatycznego lub ręcznego przeszukiwania infrastruktury IT w celu identyfikacji wszelkich potencjalnych luk w zabezpieczeniach, które mogłyby zostać wykorzystane przez cyberprzestępców. Może obejmować systemy operacyjne, aplikacje, urządzenia sieciowe, bazy danych itp.

Korzyści

Regularne wykrywanie nowych podatności, zanim zostaną one wykorzystane przez atakujących.

Łatwiejsze zarządzanie bezpieczeństwem poprzez szybsze identyfikowanie elementów wymagających aktualizacji lub poprawek.

Zmniejszenie ryzyka cyberataków, co przekłada się na większe bezpieczeństwo danych.

Zwiększenie efektywności działań prewencyjnych i minimalizowanie potencjalnych strat.

Zakres

Skanowanie sieciowe.

Skanowanie aplikacyjne.

Skanowanie systemów operacyjnych i baz danych.

Skanowanie oprogramowania i usług.

Rekomendacje i plan naprawczy.

Klasyfikacja zagrożeń według standardów CVE i CVSS.

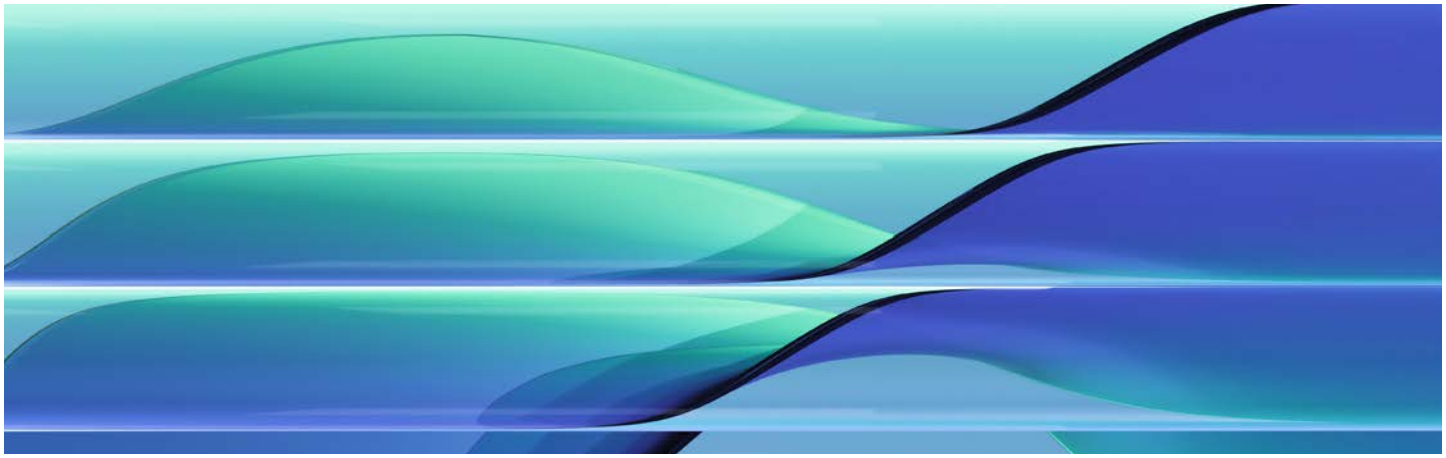
Regularne raportowanie i rekomendacje aktualizacyjne.



Threat Intelligence

Threat Intelligence to proces zbierania i analizowania informacji na temat aktualnych zagrożeń w cyberprzestrzeni, które mogą dotyczyć firmy. Podsawowym źródłem informacji są dane wewnętrzne organizacji, tj. logi z SIEM, IDS, EDR czy ogólnodostępne źródła informacji o zagrożeniach (OSINT).

Celem jest **dostarczenie aktualnych i trafnych danych o zagrożeniach**, które pozwalają na lepsze przygotowanie organizacji.



Korzyści

Proaktywne zarządzanie bezpieczeństwem dzięki bieżącej wiedzy na temat globalnych i lokalnych zagrożeń.

Możliwość lepszego dopasowania zabezpieczeń do specyficznych zagrożeń, które mogą dotyczyć określonej branży lub firmy.

Ułatwienie podejmowania decyzji o wprowadzeniu odpowiednich środków ochrony.

Zwiększenie skuteczności działań ochronnych i zmniejszenie ryzyka ataków.

Zakres

Zbieranie danych z wewnętrznych **(SIEM, EDR)** i zewnętrznych źródeł **(OSINT, bazy IOC)**.

Analiza technik, taktyk i procedur **(TTP)** zgodnie z **MITRE ATT&CK**.

Tworzenie i udostępnianie feedów **IOC**, raportów zagrożeń i rekomendacji.

Analiza śledcza (Forensic)

Analiza śledcza (Forensic) to proces dochodzenia i analizy incydentów związanych z bezpieczeństwem IT. Polega na zbieraniu dowodów, identyfikowaniu źródła ataku oraz metod użytych przez cyberprzestępców, zabezpieczeniu dowodów oraz określeniu zakresu i skutków ataku. Dodatkowo pomaga w przygotowywaniu raportów niezbędnych do działań prawnych.

Korzyści

Umożliwienie szybkiego określenia przyczyny i zakresu incydentu, co pozwala na skuteczne reakcje i naprawę szkód.

Pomoc w identyfikacji i zapobieganiu podobnym incydentom w przyszłości.

Wsparcie w dochodzeniach prawnych oraz procesach odzyskiwania danych i ochrony reputacji firmy.

Lepsze zrozumienie sposobów atakowania i implementacja bardziej efektywnych zabezpieczeń w przyszłości.

Zakres

- Analiza powłamaniowa i poincydentalna.
- Analizy związane z naruszeniem polityk bezpieczeństwa.
- Sprawdzenie zasadności podejrzeń o nielojalność pracowniczą.
- Identyfikacja tożsamości osób na podstawie informacji sieciowych.
- Zabezpieczanie danych do dalszej analizy zgodnie z zasadami informatyki śledczej.
- Zgodny z prawem monitoring pracowników z poszanowaniem ich prywatności.
- Specjalistyczne ekspertyzy i opinie.
- Udział w zabezpieczaniu danych.
- Odzyskiwanie i wyszukiwanie informacji.
- Wyodrębnianie wskazanych danych.
- Analiza treści rozmów z komunikatorów.
- Analizy porównawcze.
- Analiza zgodności SIWZ z wykonaniem zamówienia.
- Konwersja danych z programów, baz danych lub nośników.
- Analiza urządzeń mobilnych – analiza malware pod kątem złośliwego oprogramowania.



Nowość!

Poznaj **SOC Lite** – usługę, która automatycznie identyfikuje i klasyfikuje zagrożenia, a następnie przekazuje informacje o incydentach do upoważnionych osób.



Funkcje usługi

Monitorowanie w czasie rzeczywistym
System umożliwia automatyczną analizę zagrożeń w czasie rzeczywistym, zapewniając szybkie informowanie o incydentach.

Identyfikacja zagrożeń i incydentów
System klasyfikuje zagrożenia według poziomu krytyczności i dostarcza odpowiednie raporty, pomagając w efektywnym zarządzaniu incydentami.

Automatyczne generowanie alarmów
Na podstawie predefiniowanych reguł korelacyjnych system natychmiast generuje alarmy o wykrytych zagrożeniach.

Powiadomienia o nowych incydentach
Klient jest na bieżąco informowany o wszelkich nowych zagrożeniach i incydentach.

Raporty tygodniowe
Automatycznie generowane i wysyłane osobom upoważnionym statystyki na podstawie zebranych danych w zakresie usługi.

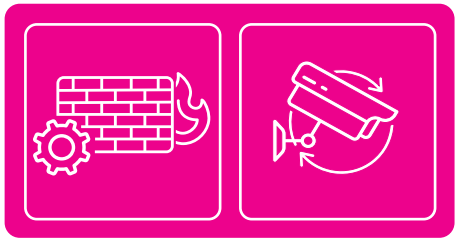
Konfiguracja i utrzymanie
System jest konfigurowany i utrzymywany przez ekspertów T-Mobile Polska, co zapewnia najwyższy poziom wsparcia i aktualizacji.

Dlaczego SOC Lite?

1. **Predefiniowane reguły korelacyjne** – poza regułami domyślnymi, klient otrzymuje dodatkowo 10 funkcji systemu zdefiniowanych przez specjalistów SOC, które monitorują określoną sekwencję zdarzeń, mogących stanowić zagrożenie.
2. **Wsparcie specjalistów SOC T-Mobile w obsłudze incydentów Poważnych oraz Krytycznych**, zgodnie z wymaganiami Ustawy o krajowym systemie cyberbezpieczeństwa.
3. **Wsparcie specjalistów SOC T-Mobile w procesie zgłaszania Incydentów do wyznaczonych jednostek CSIRT.**
4. **Elastyczność wdrożenia** – możliwość wyboru różnych modeli instalacji usługi.

Proces działania

Sieć/system klienta



SOC

1. **Zagrożenie**

Zaistnienie potencjalnego zagrożenia.

2. **Analiza zdarzenia**

Automatyczna analiza zdarzenia i incydentów z systemów IT klienta.

3. **Wystąpienie alarmu**

Wygenerowanie alarmu i przetwarzanie zdarzenia zgodnie z regułami korelacyjnymi.

4. **Klasyfikacja**

Klasyfikacja zagrożenia według poziomu krytyczności i dostarczenie odpowiednich raportów.

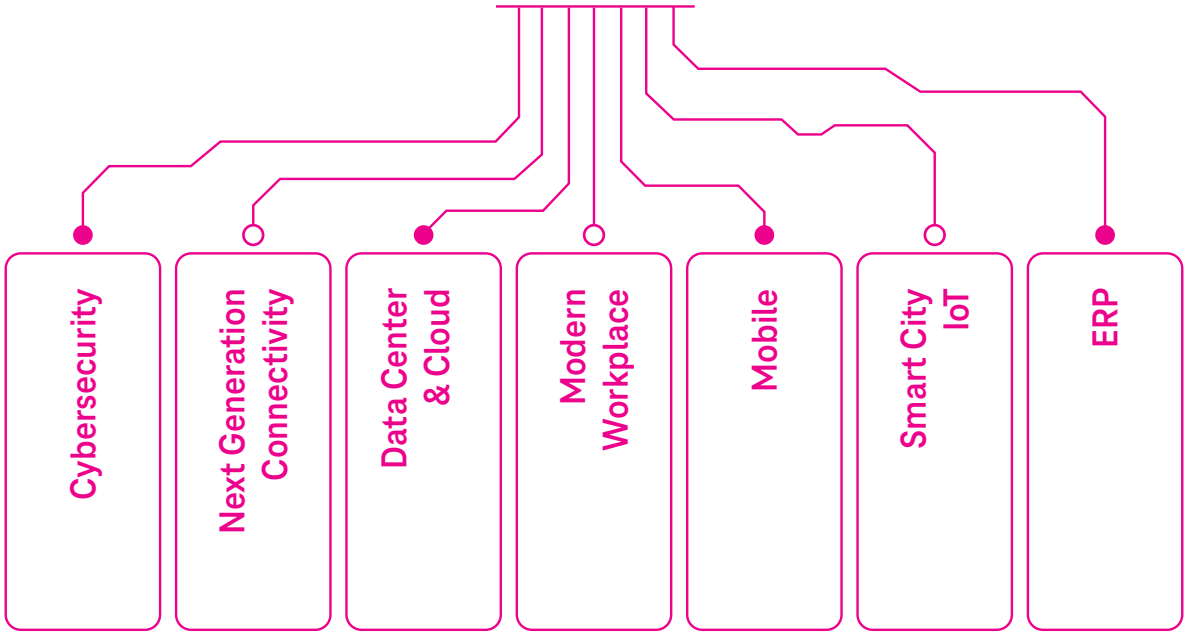
5. **Wykrycie zagrożenia**

Poinformowanie klienta za pośrednictwem e-maila o wykryciu potencjalnego zdarzenia.



BUSINESS

KOMPLEKSOWE USŁUGI DLA DUŻYCH I ŚREDNICH FIRM



T-Mobile Polska S.A.
ul. Marynarska 12
02–674 Warszawa

Więcej informacji o usługach:
www.biznes.t-mobile.pl

Numer jobu: 1425 4857