



Cybersecurity

**T Business**  
**SECURITY**  
**OPERATIONS**  
**CENTER**  
MONITORING  
BEZPIECZEŃSTWA



# 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** to system Security Information and Event Management, 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** proc. 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 najnowszych rozwiązań z zakresu bezpieczeństwa IT najlepszych światowych producentów.



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



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



Spełnienie wymagań wynikających z aktów prawnych, norm i standardów (np. Rozporządzenie o Ochronie Danych Osobowych, ustawa o krajowym systemie cyberbezpieczeństwa).

## 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.

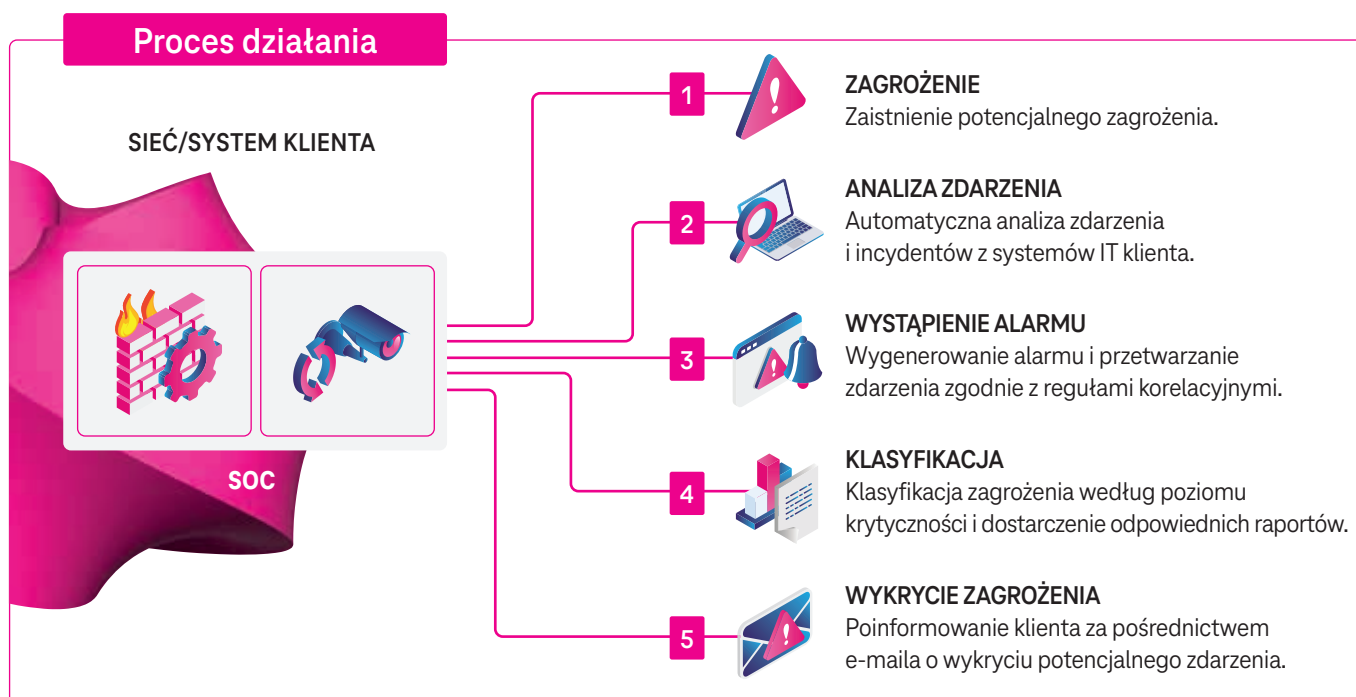
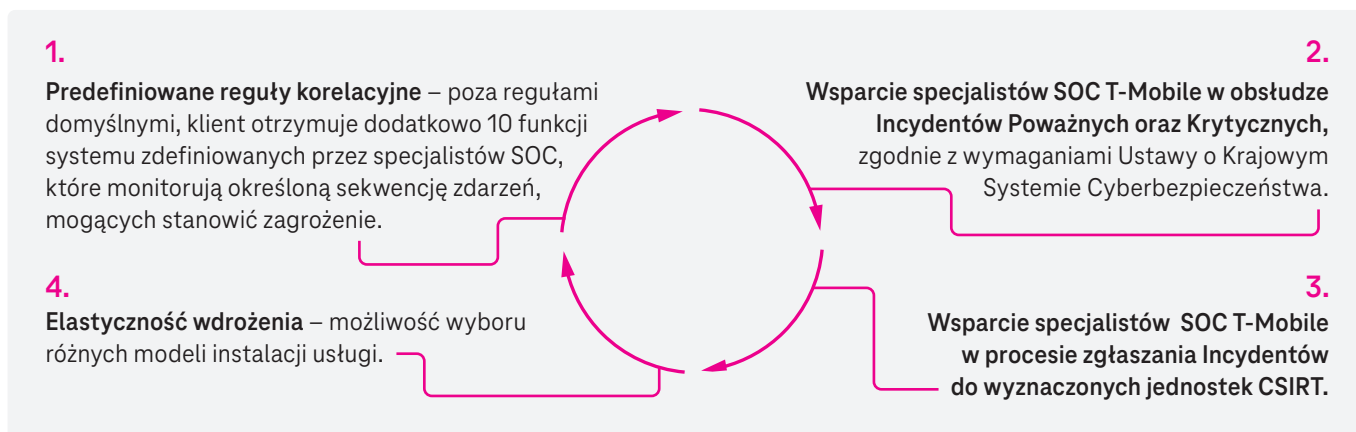
## NOWOŚĆ!

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.
- **Automatyczne generowanie alarmów**  
Na podstawie predefiniowanych reguł korelacyjnych system natychmiast generuje alarmy o wykrytych zagrożeniach.
- **Raporty tygodniowe**  
Automatycznie generowane i wysyłane osobom upoważnionym statystyki na podstawie zebranych danych w zakresie usługi.
- **Identyfikacja zagrożeń i incydentów**  
System klasyfikuje zagrożenia według poziomu krytyczności i dostarcza odpowiednie raporty, pomagając w efektywnym zarządzaniu incydentami.
- **Powiadomienia o nowych incydentach**  
Klient jest na bieżąco informowany o wszelkich nowych zagrożeniach i incydentach.
- **Konfiguracja i utrzymanie**  
System jest konfigurowany i utrzymywany przez ekspertów T-Mobile Polska, zapewniając najwyższy poziom wsparcia i aktualizacji.

### DLACZEGO SOC LITE?



# KOMPLEKSOWE USŁUGI

DLA DUŻYCH I ŚREDNICH FIRM



Mobile

Cybersecurity

Modern  
Workplace

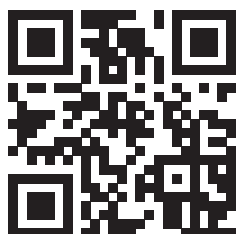
Smart City  
IoT

Data Center  
&  
Cloud

Next Generation  
Connectivity

ERP

Dowiedz się więcej



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

Więcej informacji o usługach: [www.biznes.t-mobile.pl](http://www.biznes.t-mobile.pl)