CYBERSECURITY

Security Operations Center

Continuous security monitoring
of your company

Monitoring of IT resources

Security Operations Center (SOC) is a service for monitoring and analyzing IT security events to detect and prevent future cyber security incidents.
It uses the latest available technological solutions and properly defined processes. A qualified team working 24/7/365 continuously monitors your company's IT infrastructure and detects incidents from among security alerts on an ongoing basis. The service is a source of essential knowledge about the state of a company's IT security and enables it to protect against cyber threats.

The Security Operations Center service consists of the following components:

- **Security monitoring** and event investigation 24/7/365 according to predefined scenarios, elimination of false positives, categorization and prioritization of incidents (triage).
- **Incident response**, providing mitigation recommendations aimed at reducing or eliminating risks, conducting activities to handle the incident in accordance with the specified SLA.
- **Threat Intelligence** i.e. cyclical, proactive provision of information about possible new threats and attacks, managing them, and suggested security solutions.
- **SIEM** or Security Information and Event Management system is used for collecting, aggregating and correlating logs, on the basis of which alerts on possible security incidents are generated.
- **Professional Services** including a general security audit, mandatorily performed before the implementation of the SOC service.

Three SOC pillars

Technologies – the service is provided using Splunk or IBM QRadar - the best solutions available on the market.

Processes – compliant with recognized standards and best practices of ISO 27000, ITIL, NIST, ENISA.

People – a team of more than 30 IT engineers with numerous certifications and years of experience in the Cyber Security industry is responsible for handling incidents.

In 2021, 69% of companies in Poland recorded at least one security incident.

In 2021, there was a 50% increase in the number of weekly attacks on corporate networks.

Source: itwiz.pl

Benefits for Clients

Ensuring organization of 24-hour monitoring of infrastructure in terms of ICT security.

Access to the latest IT security solutions from the world's top manufacturers.

Responding to occurring IT security incidents immediately after their identification.

Access to reports showing the scale of cyber attacks on the organization and actions taken to counter them.

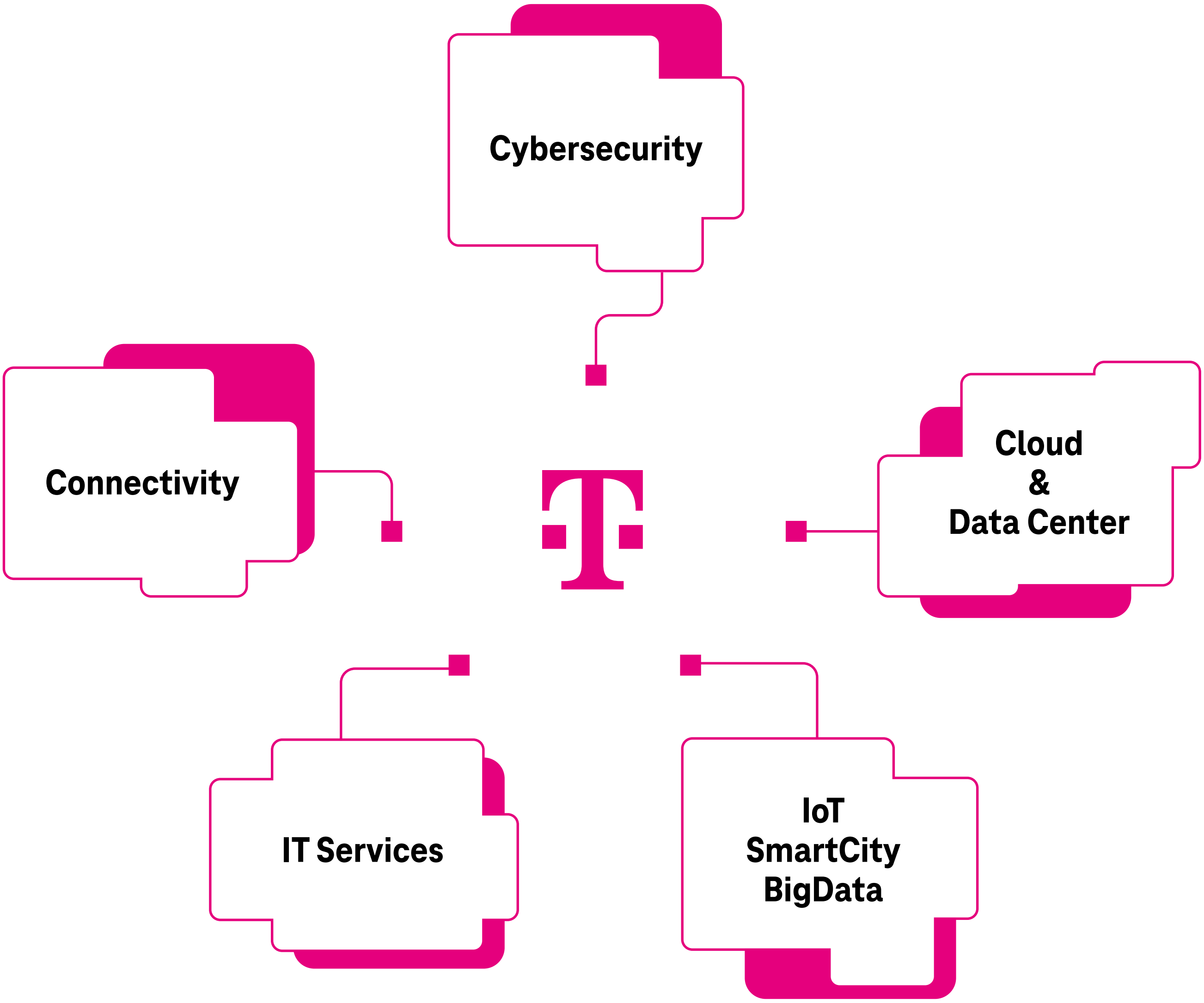
Fulfillment of requirements set forth in legal acts, norms and standards (e.g. Polish Regulation on Personal Data Protection, Act on the National Cyber Security System).

Why T-Mobile?

- Ensuring organization of 24-hour monitoring of infrastructure in terms of ICT security.
- T-Mobile Poland is one of the few SOC service providers on the Polish market.
- Free trials of the service are possible.
- Reference customers using the SOC service both in Poland and throughout Europe.
- T-Mobile's several years of experience in providing SOC services.
- A complete solution from T-Mobile - from technical design to implementation to management.
- The service is based on solutions from recognized global manufacturers: Splunk and QRadar (IBM).
- The service is provided solely on the basis of its own human and infrastructure resources.
- Ready-made, tried-and-true scenarios of how to proceed (the so-called play books), rather than dry rules in SIM.
- Guarantee of data security and information confidentiality.
- Offer tailored to customer requirements.
- Attractive prices - from as little as PLN 10 thousand net per month.

Comprehensive services

For large and medium-sized companies



Cybersecurity

Connectivity

Cloud
&
Data Center

IT Services

IoT
SmartCity
BigData

Material number: 1721818

POLSKA

OFICJALNY SPONSOR REPREZENTACJI

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

More information about services:
www.t-mobile.pl/biznes