



**Resilia**  
business resilience architects



# SECURITY OPERATIONS CENTER

SOC

Ongoing monitoring and analysis  
of the security of the organization



[www.resilia.pl/en](http://www.resilia.pl/en)



+48 22 243 39 37



43 Żurawia Street, Ap. 205, Warsaw



[kontakt@resilia.pl](mailto:kontakt@resilia.pl)



**Resilia**  
business resilience architects



Intensive digitization, a constantly changing IT threat landscape and increasingly sophisticated methods hacking attacks force companies to constantly raise the level of cybersecurity.



**Quickly detecting and effectively responding to security incidents is usually a major challenge for most organizations.**

Enterprises often aren't able to analyze all possible risks and skip important alerts in favor of the least important.

**Immediate action is of great importance for ensuring cybersecurity, effectively reducing the risks associated with attacks and mitigating the consequences resulting from them.**

**OF COMPANIES AROUND THE WORLD**

**55%**

**DON'T EFFECTIVELY STOP HACKING ATTACKS, ARE UNABLE TO IDENTIFY THEM, QUICKLY REMOVE THEM CAUSED VIOLATIONS AND LIMIT THEIR EFFECTS\***

\*According to the report of Cyfrowa Polska "Cybersecurity in Poland in 2021. Cyberattacks on end devices"



**Resilia**  
business resilience architects



**Rapid detection of cyber threats and immediate response is possible thanks to our**

**SECURITY OPERATIONS CENTER**

**SOC**

**REGARDLESS OF:**

- industry and sector of your operations
- number of employees
- already experienced cyber attacks or other security breaches
- having your cybersecurity team

**if you need to increase the cyber resilience of your organization, this service is just for you.**

**As part of our SOC Operations Center**

you receive support in detecting potential cybersecurity incidents **24/7/365** by our dedicated team of specialists responsible for constant monitoring of your IT and OT systems, threat analysis and incident response.



**Resilia**  
business resilience architects



## WHAT IS INCLUDED IN THE SOC SERVICE

- **Handling of events and notifications on a 24/7/365** basis in accordance with accepted procedures
- **Detection of cybersecurity events and incidents** based on selected data sources - we offer support in their selection, safe configuration and integration with basic SOC systems
- **Collecting, analyzing and correlating events** in networks and in the customer's systems along with the ongoing elimination of false alarms and improvement of the quality of detection in cooperation with the client
- **Monitoring security gaps** in architecture and configuration of hardware and software resources

Do you need more advanced possibilities, such as proactive threat hunting, application of complex detection systems and XDR response or structured security posture testing?

**Ask us for an additional service.**





**Resilia**  
business resilience architects



## WHY IS IT WORTH USING THE SOC SERVICE



You are receiving **dedicated support from a team of specialists** who monitor and, if necessary, react to cyber incidents



You can be sure that **your organization is protected against cyber threats** according to the latest level of knowledge



**You are minimizing the costs** of maintaining your SOC team and purchasing advanced tools and technologies



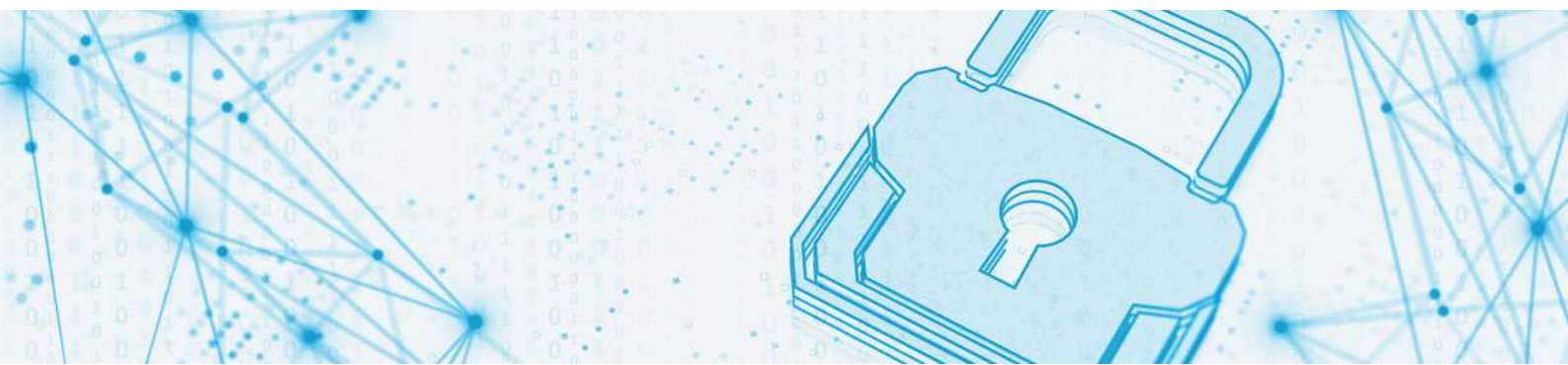
**You are avoiding downtime** caused by security breaches and reduce related costs



**You are saving time** that you can spend on developing the company's core business



You can be sure that **you act in accordance with legal regulations**



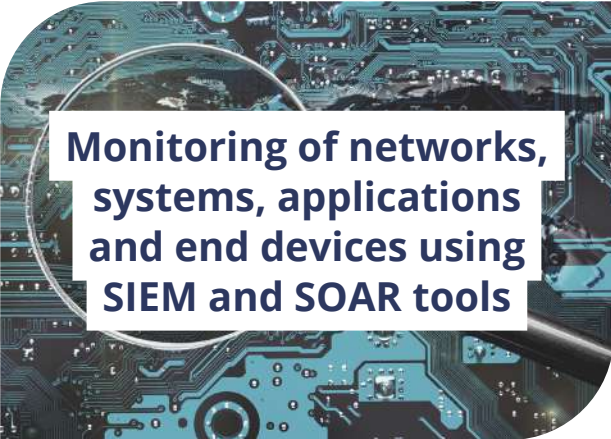


**Resilia**  
business resilience architects



Security Operations Center is a comprehensive service consisting of ongoing monitoring, analysis and quick response to cybersecurity incidents.

## THE SCOPE OF THE SOC SERVICE



**Monitoring of networks, systems, applications and end devices using SIEM and SOAR tools**



**Analyzing events**



**Eliminating false positives**



**Incident detection**



**Incident response**



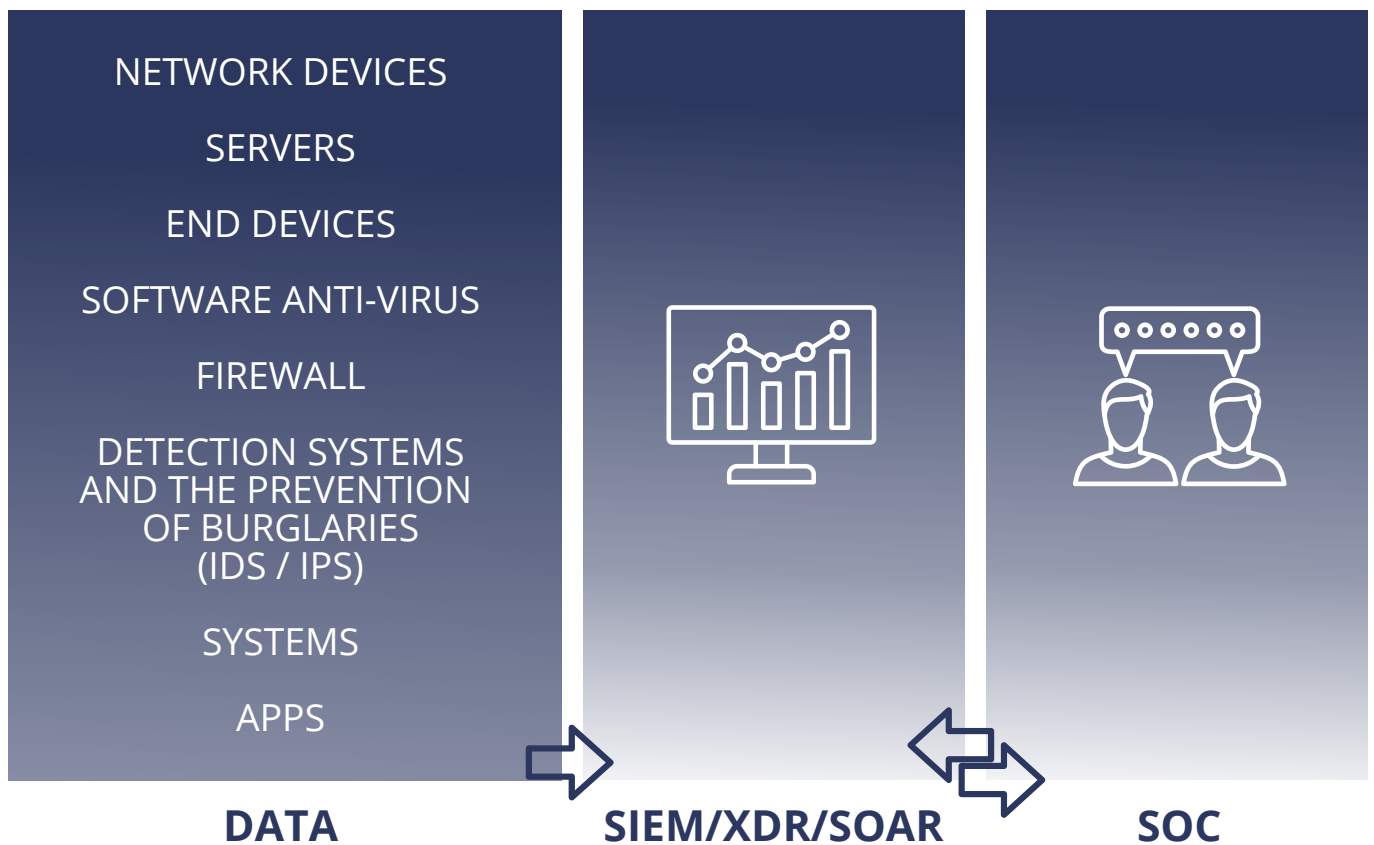
**Managing vulnerabilities**



**Resilia**  
business resilience architects



**Operations Center SOC collects and analyzes the indicated data using SIEM (Security Information and Event Management) and SOAR (Security Orchestration, Automation and Response) systems.**



The key element of the SOC service is **the knowledge and expert practice of our team**, which allows for the effective detection of cyber incidents and efficient response to threats.

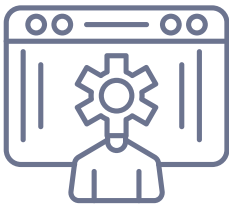




**Resilia**  
business resilience architects



**We will detect threats before they affect your organization!**



Our team of specialists combines extensive experience in cybersecurity management and building resilience to security incidents with advanced technologies enabling the implementation of the SOC service at the highest level.



Our skills are confirmed by international certificates such as CISSP, CISA, CISM, CEH, OSCP, OSWP, FCNSP, CBCP, ABCP, Lead Auditor ISO 22301, ISO 27001, ISO 20000, ISO 31000 Risk Manager PECB.

Our clients include enterprises, public institutions and large international corporations. We always provide services taking into account the individual needs, possibilities and expectations of the client.





**Resilia**  
business resilience architects



**IF YOU HAVE ANY QUESTIONS**

**CONTACT US!**

**[kontakt@resilia.pl](mailto:kontakt@resilia.pl)**

**+48 22 243 39 37**



43 Żurawia Street, Ap. 205, Warsaw



[www.resilia.pl/en](http://www.resilia.pl/en)