SOC AS A SERVICE

Protect your IT and OT environments with the assurance that your infrastructure is monitored by a team of certified experts 24 hours a day, 7 days a week, all year round.

Our specialized cybersecurity center void SOC monitors, analyzes, and responds to incidents in real time - so that attacks, intrusions, or attempts to exploit your systems are stopped before they cause damage.

WHY VOID SOC?

Cyber attacks are faster, more sophisticated, and more frequent than ever before. Successful defense requires technologies, processes, and people who can respond immediately. Our **SOC as a service** combines all these elements into a single security ecosystem:

- 24/7 monitoring of your infrastructure
- expert analysis and coordination in the event of incidents
- early detection and response to threats
- support for system recovery and prevention of repeated attacks

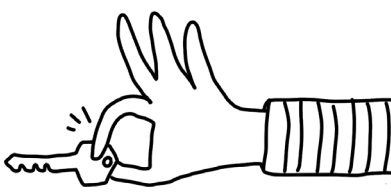
HOW DOES SOC AS A SERVICE WORK?

Continuous monitoring of your security

Devices located in your network collect security-related data (logs, events, network communication) and transmit it via an encrypted channel to the void SOC technology cluster. Our systems normalize, enrich, and analyze this data in real time so that we can identify suspicious activity immediately after it occurs.

Incident detection and verification

Using advanced analytical tools and the experience of our specialists, we can detect even hidden or long-term attacks.
Each incident is verified by our security analyst - false positives are eliminated and you receive only relevant and accurately evaluated information.

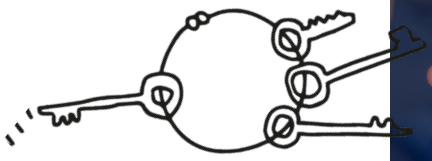


Quick response and expert support

When a real incident is confirmed, our experts:
• immediately inform your IT team according to the agreed communication matrix,
• provide accurate recommendations for resolution,
• help isolate, mitigate, and eliminate the impact of the attack.
In critical situations, we take on a coordinating role - we manage the response across teams, ensure communication, and oversee system recovery.

Recovery and prevention

After an incident, we help you recover data, audit vulnerabilities, and implement measures to prevent the same type of attack from happening again.
The goal is not just to respond, but to strengthen your organization's overall resilience to future threats.



WHERE DO WE OPERATE?

As a SOC, we provide services from two geographically independent and securely separated locations:

• Bratislava (EU) - for clients within the European Union,
• Istanbul (Turkey) - for clients outside the EU.

Each center has its own technological infrastructure in a PCI DSS-certified data center and, for the EU location, NATO certification for processing classified information up to the "Secret" level.

At the same time, we guarantee that EU client data never leaves the European Union. Our data centers are resistant to natural disasters and outages, with the overall void SOC solution achieving a guaranteed availability of 99.8%.

THE PEOPLE BEHIND THE PROTECTION OF YOUR DATA

The SOC as a service is backed by a team of more than 100 experts within the Soitron Group, who provide security services in seven European countries.
The SOC in Bratislava itself employs more than 15 specialized analysts and operators who hold renowned certifications such as:

• CEH Master / CEH
• CHFI - Computer Hacking Forensic Investigator
• CySA+ - Cybersecurity Analyst
• CISSP - Certified Information Systems Security Professional
• CCIE - Cisco Certified Internetwork Expert
• MCSE - Microsoft Certified Systems Engineer
• Security clearances from the National Security Authority of the Slovak Republic/Czech Republic - Level II (Confidential)

Our experts combine practical experience from real incidents with state-of-the-art technologies to keep your organization one step ahead of attackers.

SOC FOR INDUSTRIAL NETWORKS (OT)

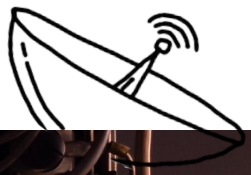
Cybersecurity is no longer just about IT. At void SOC, we therefore provide specialized services for OT and industrial environments, where system failure poses not only a financial risk but also an operational risk. In cooperation with Cisco Cyber Vision solutions such as Claroty, Nozomi, Armis, and Gerycortex, we are able to monitor and protect production technologies, SCADA systems, and other operational networks.
At the same time, we are developing our own SOCulus_OT platform, supported by the European Cybersecurity Competence Center as part of the Digital Europe program.
Its goal is to bring a locally developed solution for threat detection in industrial networks, optimized for the needs of Slovak and Czech manufacturing companies.

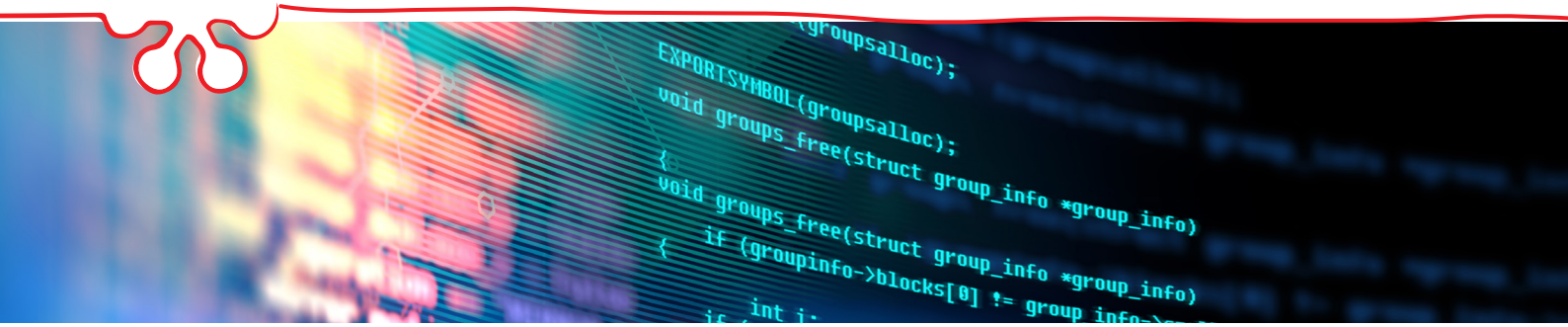
CISCO CYBER VISION AS A CENTRAL MONITORING TOOL

Cisco Cyber Vision deployed within your infrastructure is specifically designed for industrial organizations and critical infrastructure. It provides protection for OT environments, reduces the risk of attacks, prevents the spread of threats, ensures secure remote access, and extends IT security into industrial networks.

Cisco Cyber Vision provides:

- Real visibility into OT assets, their automatic inventory, monitoring of vulnerabilities, communication patterns, and anomalies. It detects malicious traffic and alerts on vulnerabilities.
- Network segmentation for secure separation of OT environments, Zero Trust remote access – secure access for teams and vendors with a least-privilege policy (MFA, SSO, time-based restrictions).
- Utilization of sensors built into network devices – without the need for separate appliances, by enabling the feature on Cisco switches and routers.
- Flexible deployment in brownfield environments through support for Docker and hardware sensors.
- Detailed visibility even at the lowest levels of the Purdue model.

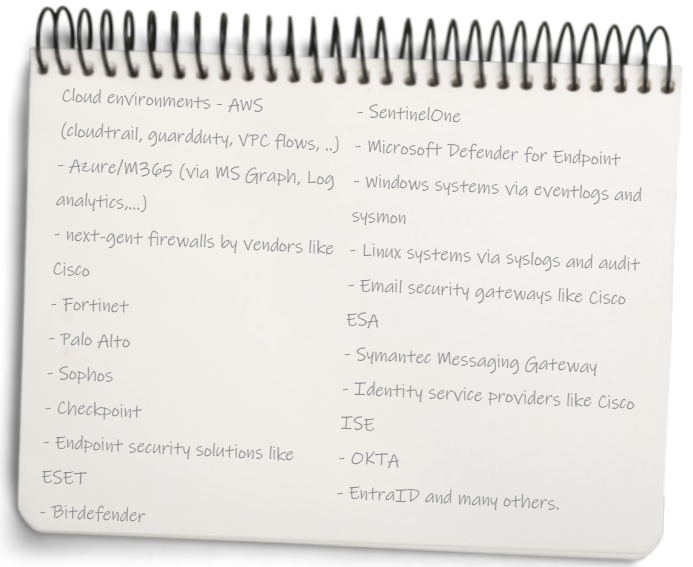




SUPPORTED TECHNOLOGIES AND DATA SOURCES

At void SOC, we process a wide range of security data from IT and cloud environments, including:

Thanks to flexible connectors, we can also integrate your own or less standard systems - without platform or manufacturer restrictions.



KEY BENEFITS OF VOID SOC

24/7 protection
continuous monitoring of all systems, devices, and networks

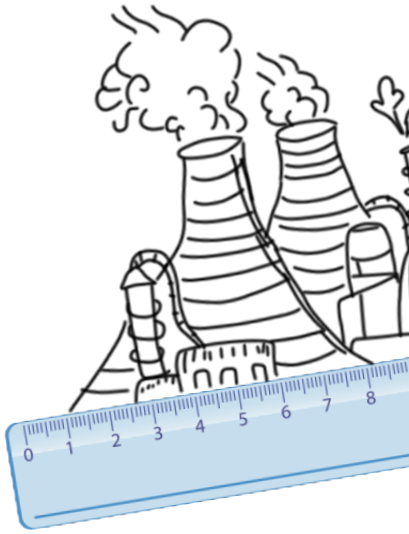
Secure data centers in the EU and outside the
separate environments, no data sharing

Rapid detection and response
we reduce the time from detection to resolution (MTTD/MTTR)

IT & OT
Full support for IT and OT infrastructures

Experienced certified experts
we are your remote security team

Service availability
High service availability (SLA 99.8%)



SOITRON, member of SOITRON Group

Soitron is a Central European integrator operating in the IT market since 1991. The company's philosophy is to constantly move forward, and that is why it is a leader in implementing unique technologies and innovative solutions. It offers its clients products and services in the field of network and communication solutions, cybersecurity, data centres, IT outsourcing, IT support and advisory. Its product portfolio includes smart police car solutions – Mosy and cybersecurity services – void SOC (Security Operations Center).
Soitron is a part of the Soitron Group and employs more than 850 international experts. The group brings together professional teams in Slovakia, the Czech Republic, Romania, Turkey, Bulgaria, Poland, and the UK.