Security Operations Center (SOC)

Cyber security pioneers since 2010,
we have a team of experts with decades of experience.
The speed of detection and response is a crucial parameter of cyber defense for us.

Every risk comes with a price

How much will the loss of reputation cost you? Would you be able to estimate the reputational risk your company would face if a cyberattack succeeded and you could have prevented it?

24/7/365 protection

Cyberattacks are everywhere, you can no longer ignore them. It is important that your business, organization, and sensitive information be protected. You investment in technology, establish processes, and hire experts. Do you know how much it will cost you in a year, three or five years? Are you getting the most out of these investments?

We have an expert team

Do you need cyber security experts? How do you get them, pay for them, and ultimately keep them? Do you know if the technologies you purchased are being used properly? Are you sure you know what you need to protect and how? In your organization, what is the most critical risk? Is your security team only reacting to attacks and struggling to cope with them, or are you taking a proactive approach?

> ***„We can provide our clients with time and experts."***
>
> Irena Hýsková,
> CEO

thein.security
Security Operations Center

Thanks to the Security Operations Center (SOC), we can resolve an increasing number of security incidents. We find and process the most important ones as a matter of priority.

Using machine learning and intelligent playbooks, we solve recurring problems automatically.

A proactive approach to critical vulnerabilities is used, information is gathered from multiple independent sources is used, and the Internet is monitored.

We use advanced tools to detect hidden anomalies and attempts to steal sensitive information using artificial intelligence (AI).

Retention of historical data is not a problem, we will find possible attacks even several years back.

We work according to MITRE ATT&CK international standards and we comply with all the requirements given by the Cybersecurity Act and the GDPR.

We can quickly and efficiently combine cyber security in any hybrid environment, whether you have application data in clouds, our own data centers or directly on local servers.

Security incident monitoring

The SOC monitors security incidents 24/7/365, checks, prioritizes and correlates data based on standardized methodologies and defined rules, and at the same time proactively reacts to events based on client requirements, based on which specific security controls are developed.

Customers can access detailed reports through our customer portal, which can be customized according to their needs.

Proactive detection and response

The Security Operations Center (SOC) monitors both the customer's local infrastructure as well as the cloud environments. Communication systems, applications, user behavior, and ongoing security incidents are monitored by analysts.

Logs and Event Analysis provides customers with access to security events via a graphical web interface. For example, it allows you to run both your own queries and views as well as prepared "best practices" as needed. When the customer consents, reactive measures can be automatically taken to prevent a cyberattack. An audited record of all SOC analyst activity is included in the activity.

Audit record and activity monitoring

For each operator activity, we make an audited record of all SOC operator and analyst activity. Activities can be viewed and audited if necessary.

Correlation rules and anomaly detection

The MITRE ATT&CK methodology, identification of weak points, and long-term traffic analysis will be used by our experts to define a basic secure communication model that we will further enhance. Thanks to this model, we can very quickly detect even skillfully hidden anomalies and latent attacks and zero-day vulnerabilities. The technology used enables our experts to access over 300 advanced detection rules, automated playbooks, and other information sources that speed up and improve cyberattack detection.

www.theinsecurity.eu