Today. Tomorrow. Together.

+46 40 59 24 00
information@itm8.com
itm8.se

SECURITY OPERATIONS CENTER

Detect intrusions into your business 24/7, every day of the year

Threats to your IT infrastructure do not follow working hours. Hire itm8 to get a SOC that prevents and detects intrusions 24/7, every day of the year. By automatically collecting and correlating information from your various systems using artificial intelligence, we ensure that threats are identified faster.

The service is based on Azure Sentinel and Defender XDR, which are market-leading tools from Microsoft. This, combined with itm8's security specialists in everything from data centers, endpoints, identity and networks, makes itm8 a complete service provider in cybersecurity.

itm8's SOC service gives you the best of both reactive and proactive security. With access to our experienced CSIRT team and 24/7 incident management, you can rest assured that we are always ready to respond quickly to an incident. Our simple pricing model includes unlimited log sources, so you can focus on your business without worrying about unexpected costs.

In addition to quickly handling incidents, we also work proactively to strengthen your security efforts. Through tailored security recommendations, Security Awareness Trainings, and realistic attack simulations, we ensure that your organization is always one step ahead.

Swedish staff 24/7

Have threats automatically graded and investigated by itm8 staff. Get automatic or manual response to incidents.

CSIRT with cutting-edge skills

In the event of major incidents, the SOC convenes a CSIRT team led by an Incident Manager. The team consists of relevant area specialists.

Proactivity

With regular monitoring of Threat Intelligence and Threat Hunting, threats are averted before they arise. itm8 educates your users and challenges your resilience against cyber threats.

Simple pricing model

Customer pays a fixed cost and a price per user. However, Customer can choose to connect an unlimited number of log sources to MS Sentinel.

Cooperation

Direct communication with itm8's analysts and regular monthly meetings where security recommendations are discussed.

Log Sources

itm8 SOC consults with the customer on which log sources are relevant and value-creating for their business.

+46 40 59 24 00
information@itm8.com
itm8.se

SECURITY OPERATIONS CENTER

Reactive security

24/7 Incident & Response

itm8 SOC monitors, analyses and acts on all alerts that occur in Azure Sentinel 24/7 to identify potential security threats and incidents. Threats are prevented by isolating devices, changing passwords and disabling user accounts and features. Actions taken according to the agreed Incident Response Plan (IRP) are communicated to the customer and followed up in connection with operational meetings.

Access to itm8 CSIRT

If an incident is deemed critical, such as a major breach, itm8 has a Cyber Security Incident Response Team (CSIRT) managed and coordinated by the Incident Manager (IM). The team is staffed by itm8 area specialists and is assembled based on the affected parts of the customer's environment.

Unlimited number of log sources

itm8's SOC service offers continuous, advanced monitoring, not only of endpoint detection and authentication events, but also of network activities, system logs, and application logs. Our customers are allowed to connect unlimited log sources to the service at no additional cost.

SECURITY OPERATIONS CENTER

Proactive security

+46 40 59 24 00
information@itm8.com
itm8.se

Monthly reports

Comprehensive reports are compiled monthly that not only highlight suggested recommendations but also provide an overview of any security incidents. These reports serve as a tool for reflection and learning, enabling continuous improvements to the security posture. The service's proactive strategies include leveraging Microsoft's Secure Score, which provides a quantitative measure of an organization's security posture.

Monthly operational meetings

Every month, operational meetings are arranged together with the Client to methodically review the monthly report. The operational meeting delves into the relevant security incidents in the report and presents tactical and strategic recommendations with the aim of strengthening the Client's security position. During these meetings, we highlight the measures that we believe are essential for the Client to implement. The aim is to proactively raise the level of security in the Client's operational environment.

Threat Hunting and Threat Intelligence

itm8 works proactively with Threat Hunting and continuously searches for vulnerabilities, anomalous behavior or known attack patterns in customer environments, leading to the introduction of custom detection rules for preventive purposes. Furthermore, Threat Intelligence is also used to stay one step ahead of new threats and adapt to Microsoft best practices to ensure the robustness of the customer's cybersecurity defenses.

Security Awareness Training

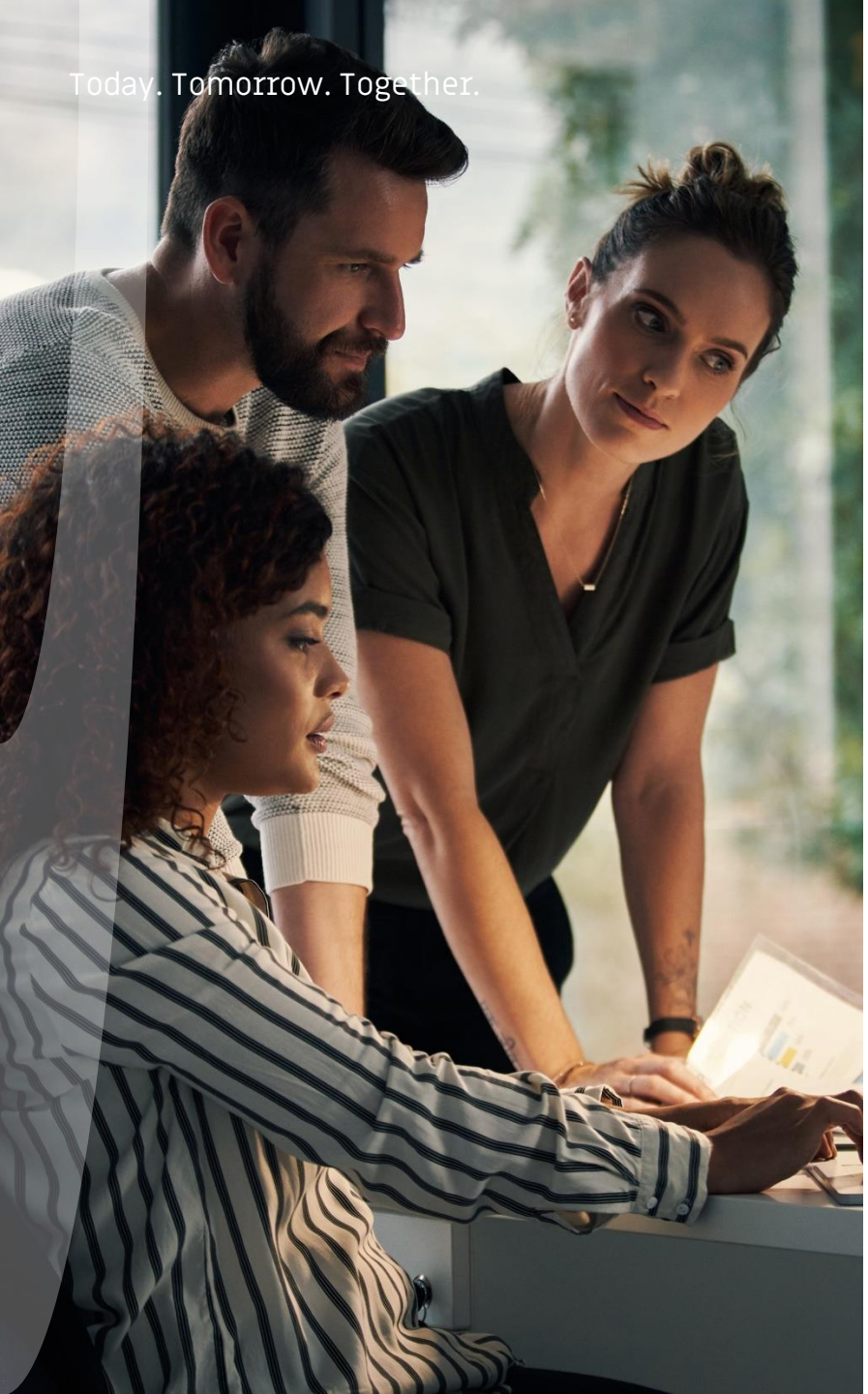
As part of the service, Security Awareness exercises are conducted regularly. These exercises are training sessions that aim to increase the awareness and knowledge of the Customer's employees about cybersecurity. itm8 uses the features of Microsoft Defender for Office 365 to conduct these trainings, which include training sessions in various areas.

Incident Response Plan (IRP)

itm8's IRP is based on a well-proven template structure that is adapted for each individual Customer through the collaboration and includes recommendations, defined mandates and a structured communication plan. A clear RACI matrix is implemented to clarify roles and responsibilities, ensuring that itm8 can act quickly and effectively and inform or escalate correctly in the event of incidents.

Attack simulations

To ensure that the Customer’s organization is well prepared for real-world cyber threats, regular attack simulation exercises are conducted. These exercises are designed to test and evaluate the Customer’s security systems and the Customer’s employees’ ability to identify and respond to intrusion attempts. The simulations include a range of scenarios, from phishing attempts to more sophisticated targeted attacks, and are tailored to reflect the latest threat actor tactics.



+46 40 59 24 00
information@itm8.com
itm8.se

SECURITY OPERATIONS CENTER

Cooperation & integrity

Communication & cooperation

The fundamental aspect of the service is the commitment to seamless and continuous collaboration with our Customers. Fast, accurate and clear communication is the success factor for a good collaboration. To comply with this, several communication channels are established within the collaboration.

For real-time collaboration, document sharing and rapid updates, we establish a shared Teams channel where the Customer and the SOC analysts communicate directly with each other.

When an action has been taken on an account or a user, we have the option of using an automatic SMS notification system. Whether it is a response to a potential threat or a routine security measure, the Customer will receive an immediate SMS notification that keeps the Customer informed and involved in every step of the security process.

Information management & integrity

itm8 SOC use the Customer's instance of Azure Sentinel, ensuring that all data, including sensitive personal data, resides in the Customer's own environment. This approach not only improves data privacy and compliance with data protection regulations, but also enables seamless integration with the Customer's existing security infrastructure.

The monthly security reports provided are carefully encrypted and classified to ensure the highest level of data protection and confidentiality. These reports are then securely stored in the Microsoft Teams environment for easy and secure access by authorized resources.

Access management follows the principle of using the least privilege possible to deliver the service. This means that permissions are strictly controlled and assigned only for necessary tasks.