thein.security

SOC from Thein Security is a cloud-native service that guards your on-premise and hybrid environment 24/7/365 for a monthly fee.

With the increasing complexity of the IT environment and new trends, when we work from anywhere, new challenges arise for internal IT organizations to ensure the availability and security of individual services provided within the organization. Thein Security provides a modern way to protect against cyber threats.

❯ We will help you detect cyber threats, evaluate them and respond correctly

Our Security Operations Center service will help you reduce the time to detect security events and at the same time give you a guarantee in response to these events. Today, cyber-attackers offer enormous opportunities to attack corporate IT environments. Therefore, it is necessary to monitor the individual components of the IT infrastructure and respond in a timely manner.

IDENTITIES	E-MAILS	USERS	CLOUD PLATFORMS	SERVERS	DATABASES	INDIVIDUAL SERVICES

Thanks to its expertise, Thein Security offers you the opportunity to keep up with these advanced threats 24/7. We offer the service regardless of the size and complexity of your environment. We are able to cover or expand your internal security teams. We provide you with expertise in threat detection and evaluation.

❯ A hybrid environment? No problem!

Thanks to a cloud-native platform based on Microsoft technologies and components developed by us, we monitor the security of purely cloud and hybrid IT infrastructure. With minimal implementation costs and fast deployment.

Thein Security SOC High Level Architecture
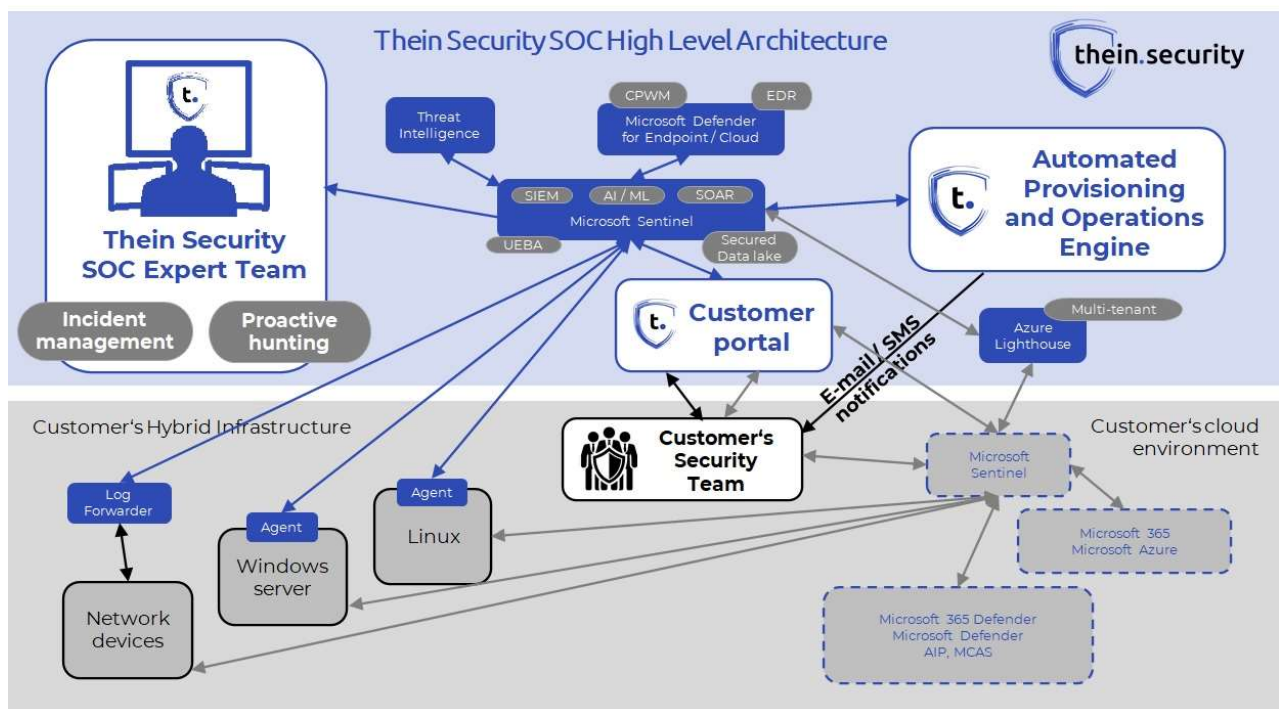
Why are we your ideal choice for cybersecurity?

Customer portal

The customer portal is a central place for transparent communication. You can see how many incidents we have resolved, you can change the settings of detection rules or report a security incident. You will see the status and time of the resolution in a clear report.

Deployment in a matter of days

Thanks to the use of cloud tools, we are able to connect you to SOC in a matter of hours, and for more complex environments in a matter of days. All you need is a reliable internet connection.

Utilize your existing Microsoft technologies

Have you already purchased a Microsoft 365 E3, E5, EMS or Business Premium license? We can make the most of them connected to SOC. The service is based on Microsoft technologies and also uses third-party tools. It is thus able to cover a wide range of hybrid environments while benefiting from the security tools and intelligence threats of the world's leading cyber security player.

Certified expert team

We search for and evaluate threats every day. Evaluating an incident severity is a breeze for us. And you can focus on the development of your business.

Detail information about the service

SOC activities

- Collection, processing and analysis of events
- Incident evaluation and processing
- Escalation and notification to the customer as needed
- Monthly report
- Quarterly evaluation
- Search for potential threats

Technological components

Microsoft Sentinel (SIEM & SOAR)
Microsoft Defender for Cloud
Microsoft Defender for Endpoint
Azure Lighthouse

Certification

PCI DSS 3.2.1 , ISO 27001:2013, SOC TSP, NIST SP, 800-53 R4, NIST SP 800 171 R2, UKO and UK NHS, Canada Federal PBMM, Azure CIS 1.1.0, HIPAA HITRUST, SWIFT CSP CSCF v2020, New Zeeland ISM Restricted, CMMC Level 3, Azure CIS 1.3.0

Compononents developed by our own

Log collecting Agents and Log forwarders
Customer portal
Automatic provisioning and operation

Compatibility

CLOUD: AWS, Google, Azure, M365, M365
NETWORK DEVICES: Fortinet, Cisco, CheckPoint, PaloAlto, and others
OPERATION SYSTEMS: Windows, Linux

The Security Operations Center ensures your safety

24 hours per day

7 days a week

365 days a year.

www.theinsecurity.eu

obchod.security@thein.eu

+420 226 531 832