RFC 2350

thein.security

Thein Security s.r.o.
Pikrtova 1737 / 1a
140 00 Praha 4 – Nusle

e-mail: info.security@thein.eu

Společnost vedená
u Městského soudu v Praze
oddíl C, značka 109813
IČO: 27415546
DIČ: CZ 27415546

1. DOCUMENT INFORMATION

This document contains a description of SOC Thein in accordance with RFC 2350. It provides basic information about SOC Thein, its channels of communication, and its roles and responsibilities.

1.1. DATE OF LAST UPDATE

February 13th, 2025

1.2. DISTRIBUTION LIST FOR NOTIFICATIONS

N/A

1.3. LOCATIONS WHERE THIS DOCUMENT MAY BE FOUND

On the company web page theinsecurity.eu, About us, section “Credentials”

2. CONTACT INFORMATION

2.1. NAME OF THE TEAM

SOC Thein

2.2. ADDRESS

Thein Security
1a, Pikrtova 1737, Nusle, 140 00 Prague 4, Czech Republic

2.3. TIME ZONE

CET/CEST

2.4. TELEPHONE NUMBER

+420 296 182 014

2.5. ELECTRONIC MAIL ADDRESS

csirt@socthein.eu

2.6. OTHER TELECOMMUNICATION

N/A

2.7. PUBLIC KEYS AND ENCRYPTION INFORMATION

We do not offer a public key for encryption, please contact us for other ways of secure communication and information sharing. In case of an incident, secure encrypted communication will be established.

2.8. TEAM MEMBERS

The manager of SOC Thein is Patrik Budz.
The team includes around 10 staff members.

2.9. OTHER INFORMATION

N/A

3. CHARTER

3.1. MISSION STATEMENT

The mission of our SOC is to protect the organization's information systems and critical assets by providing proactive and reactive cybersecurity services. We aim to monitor, detect, respond to, and recover from security incidents with the highest level of professionalism and efficiency. Our team is committed to enhancing organizational resilience through continuous improvement, collaboration, and knowledge-sharing to mitigate cyber threats and ensure the availability, confidentiality, and integrity of our systems.

3.2. CONSTITUENCY

The SOC provides cybersecurity monitoring, detection, and incident response services to multiple customers across diverse industries under a Security Operations Center as a Service (SOCaaS) model. The scope of our responsibility varies based on individual customer agreements and includes monitoring and protecting systems, networks, and applications specified in each service contract.
Our team serves as a trusted partner to enhance the security posture of our customers by safeguarding their critical assets against cyber threats, ensuring confidentiality, integrity, and availability within the agreed-upon boundaries. The SOC does not take responsibility for systems or assets outside the contracted scope of work.

3.3. SPONSORSHIP AND/OR AFFILIATION

SOC Thein is a department within Thein Security s.r.o.

3.4. AUTHORITY

In case of security incidents, SOC Thein cooperates with representatives of its constituency. It is the responsibility of SOC Thein to provide customers with service.

4. POLICIES

4.1. TYPES OF INCIDENTS AND LEVEL OF SUPPORT

SOC Thein addresses all kinds of security incidents which occur, or threaten to occur, within its constituency.
Incidents are prioritized according to contract status/type and therefore the service level agreed with the affected constituent.

4.2. COOPERATION, INTERACTION AND DISCLOSURE OF INFORMATION

SOC Thein cooperates with relevant public authorities and regulatory bodies. SOC Thein cooperates at a national level with other entities.
SOC Thein follows industry best practices, including anonymization and data minimization when sharing data with public authorities or other teams.

4.3. COMMUNICATION AND AUTHENTICATION

For regular electronic communication (not containing sensitive information) SOC Thein might use conventional methods like unencrypted e-mail.
For secure communication telephone or end-to-end encrypted messaging will be used.

5. SERVICES

SOC Thein is a Security Operations Center (SOC).

5.1. SECURITY INFORMATION EVENT MANAGEMENT

5.1.1. MONITORING AND DETECTION

- Log and sensor management
- Detection use case management
- Contextual data management

5.1.2. EVENT ANALYSIS AND EVALUATION AND ORCHESTRATION

- Correlation
- Orchestration and automation
- Qualification

5.2. SECURITY INCIDENT MANAGEMENT

SOC Thein coordinates incident prevention, handling and response within its constituency.

5.2.1. INCIDENT TRIAGE

- Determine whether an event is incident or not
- Determine whether severity of incident is relevant
- Assessing and prioritizing the incident
- Determine the involved applications and customers

5.2.2. INCIDENT COORDINATION

- Ask involved customers to investigate and take appropriate mitigation steps
- Notify other customers if appropriate
- Facilitate contact with other parties that can help resolve the incident

5.2.3. INCIDENT RESOLUTION

Advise the customer security teams on appropriate actions. Follow up on the progress of the concerned customer security teams

- Request status reports
- Report back to the customer

SOC Thein collects statistics about incidents within its constituency.

5.3. VULNERABILITY MANAGEMENT

- Vulnerability response
- Vulnerability detection/scanning
- Management of vulnerability tools

5.4. EMAIL ABUSE

- Manage and evaluate reported emails
- Cooperate on blocking malicious domains
- Provide recommendations on email filtering

5.5. PROACTIVE ACTIVITIES

SOC Thein collects statistics about incidents within its constituency.

- Enhance security awareness within the constituency
- Monitor emerging technology trends
- Share relevant knowledge with the constituency

6. INCIDENT REPORTING

There are no local forms available yet. When sending incident reports via e-mail, please follow these rules:

- A report must contain:
  - first name and last name of the reporter
  - telephone number
  - e-mail address
  - name of reporting organization
  - IP address and type of incident
  - approximate time when the incident started
  - time, when the incident was detected
  - relevant description of the problem

7. DISCLAMER

While every precaution will be taken in the preparation of information, notifications and alerts, SOC Thein assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within. This document is subject to change without prior notice, and SOC Thein reserves the right to update its policies and procedures as necessary.