Tip sheet

SET-UP AN AFFORDABLE SOC

IT systems are increasingly exposed to cybersecurity threats, potential incidents, and attacks that can lead to serious and costly consequences, such as system downtime or the loss of sensitive data. No institution or company can afford to overlook the protection of its information system, even when human or financial resources are limited.

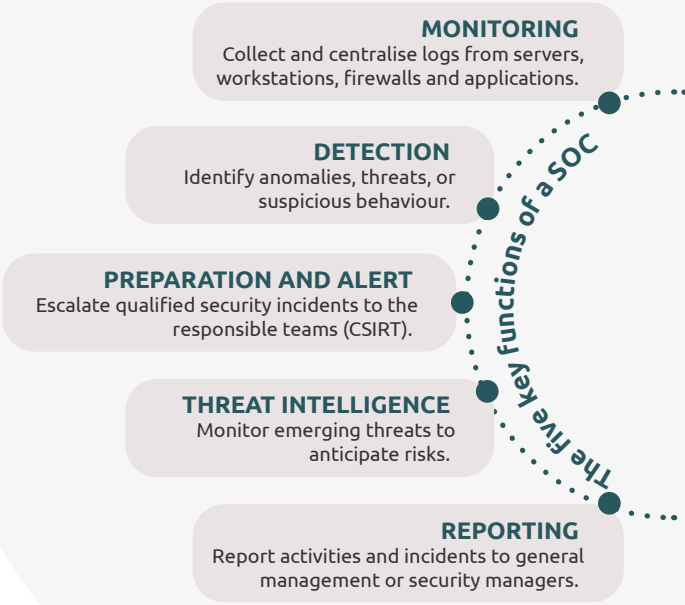
Monitoring your information system, detecting threats, and responding rapidly to incidents have become essential challenges.

What is a SOC?

The Security Operations Center (SOC) ensures continuous monitoring of the information system.

The SOC has several missions.

- It continuously monitors security events in real time.
- It detects suspicious behaviour, anomalies and malicious actions.
- It assesses alerts to determine their severity and impact.
- It informs and escalates them to the relevant entities (i.e. the Computer Security Incident Response Team - CSIRT) to handle the response.
- It contributes to the continuous improvement of the security posture (such as adjustment of detection rules, reports, indicators, etc.)



At the heart of the SOC: the SIEM

The Security Information and Event Management (SIEM) is one of the central elements of a SOC.

1 The SIEM collects, centralises, correlates and analyses logs from all components of the information system. It processes data from:

- network probes that analyse traffic and detect anomalies using an Intrusion Detection System (IDS);
- agents on workstations/servers that collect system and security logs;
- security equipment such as firewalls, proxies, antivirus software, VPNs, etc.
- Threat Intelligence sources that enhance detection with external indicators (IoCs).

2 The SIEM translates the collected data into operational information in order to:

- **monitor** information system's activity in real time;
- **detect** anomalies and security incidents;
- **automatically alert** analysts when suspicious behaviour is detected;
- **facilitate** investigation through log search and archiving;
- **produce** dashboards and reports for management and compliance purposes;
- **provide centralised visibility** of logs from any IT system.

Structuring an affordable SOC

The SOC is often described as the nerve centre of cybersecurity. Contrary to the image of a room filled with screens and analysts working 24/7, a SOC can be lightweight, distributed and cost-effective. To achieve this, a rigorous method, clear prioritisation and suitable open-source tools are essential. Such an affordable SOC thus established provides a level of operational security usually only available to large organisations.

Info !

Whether affordable or not, the success of a SOC depends on human commitment, rigorous processes and investment proportionate to the risks. A small team, clear processes and open-source tools are all you need to get started.

A motivated team of operators

Small team

One or more qualified individuals (computer engineer, chief information security officer (CISO), etc.)

A dynamic of continuous improvement

Clear processes

- **Define roles** (who monitors, who analyses, who decides and who acts?)
- **Document procedures** (playbooks) for typical incidents (phishing, ransomware, account compromise, etc.)
- **Test responsiveness** (through regular exercises)
- **Gradually increase capabilities** (depending on the size and maturity of the organisation)

Appropriate tools

Free open-source tools

MONITORING

OpenSearch, to centralise logs and detect anomalies.
Open Search collects, correlates, and visualises logs from all systems; it forms the backbone of the SOC for monitoring and detection.

DETECTION

Suricata and **Zeek**, to identify threats to the network and workstations.
Suricata detects and prevents network intrusions (IDS/IPS); Zeek identifies unusual or malicious behaviour.

PREPARATION AND ALERT

Flowintel or **DFIR-RIS**, to manage cases ans respond to incidents.
Flowintel or DFIR-RIS enable analysts to track investigations and collaborate with one another.

THREAT INTELLIGENCE

MISP, to enrich detection with threat intelligence.
MISP shares indicators of compromise (IoC) and threat intelligence.

REPORTING

OpenSearch Dashboards, to view the recorded data.
OpenSearch Dashboards enable the creation of clear and dynamic dashboards.

Did you know?

The open-source OpenSearch tool can be used as a SIEM.

Setting up a SOC is not a luxury of large companies or organisations

Prerequisites and points to consider

Even if the open-source tools can reduce costs, setting-up a SOC is not something that can be improvised. Certain conditions should be met to ensure its effectiveness.

- **Sufficient human resources**: trained personnel in log analysis and incident management are essential.
- **Time**: monitoring, maintenance and response require consistent attention.
- **An initial budget**: investments are needed for infrastructure (servers, storage, network) and skills development.
- **A clear governance**: responsibilities and decision-making processes in the case of an incident must be clearly defined.
- **A realistic deployment strategy**: start small, prioritise critical systems, and expand gradually following a structured plan.

Beware of common pitfalls!

- Trying to monitor everything from the outset.
- Underestimating the daily analysis workload.
- Neglecting analyst training and the maintenance of detection rules.

Even a 'low-cost' SOC remains a structural project that must be planned for the long-term and supported by a minimum level of human and financial resources.

Best practices on low budgets

1. **Automate** repetitive tasks (such as alerts, correlation, reporting).
2. **Focus** on your critical assets before expanding the scope.
3. **Build** on the open-source community for detection models and threat intelligence.
4. **Document** each incident to improve processes.
5. **Train and raise awareness** among your network users, security begins with them.

Tip!

A consistent open-source architecture provides a complete, high-performance, low-cost detection and correlation chain. These challenges must be addressed with appropriate solutions, including robust monitoring mechanisms, training on best practices, investment in user-friendly analysis tools, enhanced data security methods, and a comprehensive business continuity plan.

DISCOVER (OR REDISCOVER) IN THE SAME SERIES...

- 'Carefully select a password'
- 'Spam & phishing messages'
- 'From a cyberattack to data acquisition'
- 'Social engineering attacks'
- 'Back up your data safely'
- 'Best practices for email hygiene'

READ AND APPROVED BY HEX

Service offer

Restena designed and implemented a complete SOC based on open-source tools and led by cybersecurity experts as part of the European 'Enhancing Cybersecurity Services for the Luxembourgish Research and Education community' - LuCySe4RE project that intends to improve protection against the cybersecurity risks faced by the Luxembourg research and education community. The SOC will be added to the Restena's service portfolio in 2026 and provided to the education and research community in Luxembourg. The latter will then benefit from continuous monitoring of its information system, centralised incident detection and response, and support from specialists at a controlled cost.

For more information on this service, please visit www.restena.lu

Co-funded by the European Union

This tip sheet is one of the awareness-raising activities set up as part of the European LuCySe4RE project that has received funding from the European Union's Digital Europe programme (DIGITAL) under grant agreement No. 101127864.

restena
réseau · sécurité · .lu