SAFETECH INNOVATIONS SOC AS-A-SERVICE

Cybersecurity without compromise!

SAFETECH INNOVATIONS

Table of Contents

About the Service

Safetech Innovations SOC as-a-Service Cybersecurity without compromise!

Even though cybersecurity is considered a priority, many organizations face an acute skills shortage, which increases their exposure to an avalanche of cyber attacks.

Safetech Innovations' Security Operations Center outsourcing services (SOC as a Service) provide permanent monitoring and optimal incident management, contributing to the constant improvement of the security posture.

By leveraging the latest generation technology and Safetech expertise, organizations eliminate the costs and complexity of managing an internal SOC, benefiting from scalability and speed of response.

Cybersecurity, a critical priority in the modern economy

Organizations that do not prioritize cybersecurity become vulnerable and risk facing costly data breaches, business interruption, regulatory fines and penalties, reputation damage, loss of customer and partner trust, and high remediation costs. **IBM highlights in its "Cost of a Data Breach Report 2024" an average global cost of a data breach of $4.88 million, up 10% from the previous year.(*)**

As the modern economy transitions to the digital environment and online work models, cyber threats increasingly exceed traditional security approaches. Against the backdrop of an increasingly competitive business environment, the IT environment is diversifying and growing in complexity, with the expansion of cloud services, the adoption of remote work and the increase in the number of applications and devices used.

Cyber attackers are quickly adapting to this reality with the help of artificial intelligence technologies, threats becoming more sophisticated and more difficult to detect. In recent years, organizations have seen a significant increase in cyberattacks at all levels, but especially DDoS and Ransomware, most visible in the public space affecting critical industries such as public administration, healthcare and the financial sector.

(*) Source: https://www.ibm.com/reports/data-breach

According to data published in July 2024 by Checkpoint Research, organizations faced an average of 1636 cyberattacks per week in Q2 2024, a value 30% higher than in Q2 of the previous year. (*)

At the same time, compliance with regulations such as the EU NIS Directive 2 and DORA (Digital Operational Resilience Act) is putting increasing pressure on security teams, with increasingly stringent requirements for monitoring the digital environment and reporting incidents to authorities.

(*) Source: https://blog.checkpoint.com/research/check-point-research-reports-highest-increase-of-global-cyber-attacks-seen-in-last-two-years-a-30-increase-in-q2-2024-global-cyber-attacks/

Why is a Security Operations Center needed?

Security Operations Center (SOC) is essential for organizations that want to maintain a high level of cybersecurity and proactively defend against threats. It functions as a centralized unit where security analysts and state-of-the-art tools work together to monitor, detect, analyze, and respond to cybersecurity incidents across an organization's entire attack surface in real time. By using Security Information and Event Management (SIEM) systems, a SOC can aggregate and correlate log data from various sources, such as firewalls, intrusion detection systems (IDS), and endpoint detection and response (EDR) tools, providing complete visibility and anomaly detection.

SOC teams use advanced threat intelligence feeds to stay informed about the latest attack techniques, tactics, and procedures (TTPs). This integration supports real-time enrichment of alerts, increasing the accuracy of detections. Automated tools, including AI and machine learning algorithms, help analyze large amounts of traffic and event data to identify patterns that indicate sophisticated threats. These tools prioritize alerts by assigning a severity score and potential impact, reducing false positives and focusing analysts' efforts on high-priority incidents.

To strengthen incident response, SOCs deploy automated playbooks in combination with Security Orchestration, Automation, and Response (SOAR) platforms. These playbooks coordinate actions such as isolating compromised

endpoints, initiating malware scans, or blocking IP addresses, thereby accelerating response time and minimizing manual interventions.

For continuous improvement, SOCs frequently employ a vulnerability management process that includes regular scans, patch management, and threat hunting exercises.

This proactive approach ensures a hardened level of security that adapts to new attack surfaces, such as those created by the adoption of IoT or remote working.

Challenges of Operating an Internal SOC

High Costs:
Creating an internal SOC requires substantial upfront investments in specialized equipment, applications, and human resources. In addition, it takes a long time to become functional. All of these aspects end up destabilizing IT budgets, making the investment in a SOC economically unjustified.

Difficult access to expertise:
Operating an internal SOC requires specialized personnel, with a level of expertise difficult to find on the local market.

The need for scalability:
Equally important is the scalability of such a security operations center, which must have the ability to dynamically adapt to the requirements of the organization or the evolution of the IT infrastructure, the volume of data and the threats. Scalability limits frequently appear when systems or applications reach their maximum parameters, which requires their replacement with more efficient solutions, or when the SOC team reaches its maximum working capacity, which requires the hiring, training and operationalization of new specialists.

What is the alternative?

To overcome these challenges, more and more companies are opting for the solution of outsourcing – partially or completely – their security operations to a SOC service provider.

This eliminates the problems of initial investment, recruiting qualified personnel, keeping operating costs under control and complying with compliance requirements.

6 signs that you need SOC as a Service

Increased frequency of security incidents in critical sectors.
Organizations operating in sectors such as health, finance, energy and critical infrastructure are frequent targets of cyber attacks and are required by law (NIS2, DORA, PCI DSS) to have robust and updated security systems.

Limited budget.
The organization cannot (anymore) cover the costs associated with creating/operating an internal SOC (staff, infrastructure, software, maintenance). Access to advanced cybersecurity technologies is limited.

Lack of qualified personnel.
Difficulty in finding, continuously training and retaining employees with advanced cybersecurity skills. Existing staff is overwhelmed by workload, unable to provide 24/7 monitoring of networks and systems.

Time pressure.
The internal SOC cannot ensure a real-time response, increasing the response time to incidents. A delayed response can lead to significant losses, in some situations, even closing the business.

Regulatory pressure
The organization cannot keep up with the constant legislative changes imposed by cybersecurity regulations. Cumbersome reporting and incident traceability, required to comply with these regulations, cause waste of resources or unplanned costs due to non-compliance with regulations.

Difficult scalability.
The internal SOC does not cope with business expansion. The increase in the number of employees, the number of locations and the complexity of the IT infrastructure means a higher volume of security events, an increase in the attack surface and the number of potential threats.

SAFETECH INNOVATIONS

SOC as a Service (SOCaaS) – benefits and opportunities

Organizations that opt for SOC as a Service outsource their security operations center functions to an external provider. SOCaaS offers the same capabilities as an internal SOC, but without the investments in technical infrastructure and specialized personnel.

- **Cost predictability.**
  By outsourcing the SOC, the initial investments and operating costs of an internal SOC are eliminated. Advanced SOC services can be accessed without major costs, on a subscription basis.

- **Access to highly qualified experts.**
  Beneficiaries have access to a larger, better-trained, better-organized team of cybersecurity specialists hired by the provider. Thus, they no longer waste resources recruiting, retaining/ motivating all the personnel needed in an internal SOC.

- **Continuous monitoring and reduced incident response time.**
  An outsourced SOC monitors the organization's networks and systems in real time 24/7/365, quickly detecting threats. The response time is reduced and the impact on the organization (risk of operational/financial losses) is minimal.

- **Scalability.**
  An outsourced SOC is sized to serve a large number of clients simultaneously and has a reserve for peaks in activity. Unlike an internal SOC, it adapts quickly to changing requirements. The beneficiary can scale security services without additional investments.

- **Access to advanced technologies.**
  Outsourced SOC providers use advanced technologies for threat detection and response. Thus, the organization benefits from these complex solutions without purchasing, implementing or maintaining them.

- **Regulatory compliance.**
  Outsourced SOC service providers are ready to help organizations comply with cybersecurity regulations, such as GDPR, NIS2 or PCI DSS, avoiding sanctions and protecting the company's reputation.

- **Focus on the organization's core business.**
  SOCaaS services free up resources for the organization's core activities and allow it to focus on its strategic objectives, knowing that its security is managed by professionals.

Safetech Innovations SOC as a Service

The SOC as a Service services offered by Safetech Innovations are provided by the Safetech Computer Emergency Response Team (STI CERT®). They have a granular structure, which allows organizations to opt for only the services they need, and include:

- **Onboarding and integration services.**
- **Asset discovery, vulnerability assessment, security testing.**
- **Monitoring, detection and investigation.**
- **24/7, 365 days a year threat response.**
- **Reporting and support for regulatory compliance.**
- **Governance, Risk and Compliance (GRC).**

Technologies and platforms used by STI CERT

The STI CERT team has expertise in using advanced cybersecurity technologies specific to SOC centers, such as SIEM, NDR, EDR, NGFW (Next-Generation Firewall), XDR, etc.
Safetech's strategy emphasizes using as many existing data sources as possible in the client's network, including cybersecurity tools and integrating them into a single console. In the case of a reduced security infrastructure of the beneficiary, Safetech recommends and implements additional solutions to increase the efficiency and accuracy of SOC services, which can be purchased as investments or provided as-a-Service.

Based on over 9 years of experience in providing SOC services, Safetech Innovations recommends implementing, at least, a minimal architecture consisting of:

- **Firewall:** protects the lines of connection with the outside of the organization's network and allows the application of policies and access restrictions,
- **Endpoint Detection and Response (EDR):** protects the most exposed entry points into the organization's network,
- **Multi-technology platform based on eXtended Detection and Response (XDR) technology:** Integrates EDR tools as well as other sources of alerts and logs into a single monitoring panel at the SOC level.

Safetech Innovations also provides organizations with Vulnerability Management, Risk Management and Operational Technology Security security tools.

Technology platforms included in Safetech SOC as a Service bundles

Annual subscription packages	Essential	Advanced	Elevate
Endpoint Detection & Response			
· Endpoint Protection (EPP)	√	√	√
· Endpoint Detection and Response (EDR)	√	√	√
· Sandbox	–	√	√
· Deception	–	–	√
· Mobile Threat Detection (MTD)	+	+	+
eXtended Detection & Response			
· EDR integration based on out-of-the box connectors (customer existing EDR)	√	√	√
· Next Generation Security Information and Event Management (NextGen SIEM)	√	√	√
· Intrusion Detection System (IDS)	√	√	√
· Case Management	√	√	√
· Network Detection and Response (NDR)	–	√	√
· User and Entity Behavior Analytics (UEBA)	–	√	√
· Automated Response	–	–	√
Vulnerability Management			
· Web/Network Vulnerability assessment (VA)	–	√	√
Risk Management			
· Asset inventory and business processes maping	–	√	√
· Security risk analysis and Management of Security Indicators	–	–	√
Operational Technology Security			
· OT Threat Detection	+	+	+
· OT Risk Management	+	+	+

Legend:
√ included – not included + optional

Services included in Safetech SOC as a Service bundles

Annual subscription packages	Essential	Advanced	Elevate
Startup Services			
· Onboarding Services	√	√	√
· Integration Services	√	√	√
Planning & Prevention			
· Asset Discovery	√	√	√
· Monthly External Vulnerability Assessment	–	√	√
· Monthly Internal Vulnerability Assessment	–	–	√
· Security Testing (*)	+	+	Up to 2 activities/year
Monitoring, Detection & Investigation			
· 24/7 Continuous Monitoring	√	√	√
· Threat Detection & Investigation	√	√	√
· Root Cause Analysis	–	√	√
· Advanced Threat Hunting	–	–	Up to 2 activities/year
· External Internet Asset Monitoring	+	+	√
Response			
· Recommended Remediation Actions	√	√	√
· Contain / Shutdown Host (**)	–	√	√
· Coordination of Remediation Actions for Major and Critical Incidents	–	Up to 24 hours/year	Up to 40 hours/year
· Custom Playbooks	–	up to 5	up to 10
Service Governance			
· Monthly Reports	√	√	√
· Quarterly Assessment / Lessons Learned	–	√	√
· Audit / Regulatory Compliance Support	+	+	Up to 2 interventions/year
Add-on Services			
· Governance, Risk & Compliance (GRC) Activities (***)	+	+	+

Notes:
(*) Security testing: penetration testing, code review, social engineering, Red Teaming
(**) If these actions are possible on the platforms managed by Safetech and based on the procedures agreed with the client.
(***) Governance, risk and compliance activities: development/review/update of standards/policies/procedures, risk analysis, business impact analysis, business continuity and disaster recovery plans, compliance audit.

Why choose Safetech SOCaaS? Key differentiators

- **Extensive coverage of security risks.** The STI-CERT team offers a full range of cybersecurity services and access to advanced security tools and Threat Intelligence services. The large client portfolio allows the team to gain a deep understanding of the latest techniques and cyber threats and apply customized solutions.

- **Certified services at the highest level.** The STI CERT center is accredited by Trusted Introducer, NICP (NATO Industry Cyber Partnership), ISO 9001 and 14001, ISO/IEC 20001 and 27001, as well as OHSAS 18001.

- **Access to a large team of experienced specialists.** STI CERT team members hold multiple personal certifications, including, among others, SANS, MICROSOFT, (ISC)², ISACA, CREST, EC-Council. They work in 3 shifts to ensure uninterrupted coverage.

- **9 years of experience in handling a large volume of events/alerts/incidents and advanced analysis capabilities.**
  On average, STI CERT receives 100 billion events per month, analyzes 15,000 security alerts and handles 200 security incidents. STI CERT serves clients from diverse industries, including finance and banking, utilities, healthcare, technology, retail, distribution, consulting, gaming.

- **Insurance policy** with specific clauses for cyber event risks, with coverage for all STI CERT services.

- **Competitive pricing, predictable costs and financial stability.**
  STI CERT services allow companies to eliminate the problem of the budget required to develop an internal SOC and the costs associated with its operation. Organizations can take advantage of three SOC outsourcing service packages, which can be customized according to the needs and resources of each client.

- **Safetech Innovations** was included in the prestigious Top 250 MSSPs 2024, conducted by CyberRisk Alliance, which recognizes the 250 best performing managed security service providers globally. Safetech Innovations is the first ranked MSSP company from Romania included in the top, occupying position 153.

Quality and performance of STI CERT services

STI CERT guarantees continuous quality improvement and focus on the needs and requirements of each client, applying the following measures:

1. **Monthly governance meetings**
Information is provided on the number/type of alerts investigated, alerts per monitored solution, the percentage of alerts that generated incidents, the categories and criticality of incidents. The level of coverage by security solutions of the systems in the client's infrastructure and the percentage of systems not covered by security solutions are calculated.

2. **Detailed report for each high and critical severity incident**
STI CERT creates incident reports that contain an executive summary, technical description, root cause analysis, conclusions and recommendations.

3. **Monthly improvement of alert accuracy**
STI CERT proposes monthly measures to improve the accuracy of alerts within the monitored solutions and validates them with customers. The agreed measures are subsequently implemented.

4. **Internal quality assurance process**, carried out by the level 3 (expert) team
This continuously evaluates the response to incidents, adapting methods/procedures to customer requirements and the evolution of threats. The process includes weekly meetings to improve the quality of investigations and internal technical and human capabilities.

5. **Emailed bulletins with information about recent threats and vulnerabilities**
Information about specific vulnerabilities, including affected software versions and exploitation methods, allows Safetech customers' IT teams to properly prioritize their activities and apply security updates/ patches before vulnerabilities are exploited.

Conclusion

The SOC as a Service model offers organizations a proactive and scalable way to protect the entire IT infrastructure without major investments in internal resources.

The SOC as a Service services offered by Safetech Innovations are a complex package built of people, processes and technology. It guarantees a high level of security, through the synergy between certified specialists, well-defined and validated processes/methodologies and advanced technologies, at a competitive price. This approach ensures complete protection, adapted to the complex needs of modern organizations.

SAFETECH INNOVATIONS

APPLIED CYBER INTELLIGENCE

SAFETECH INNOVATIONS S.A.

12-14 Frunzei Street, Floors 1-3, District 2,
021533 Bucharest, Romania

+40 21 3160565
sales@safetech.ro
www.safetech.ro