PROJECT

Multi-tenant cybersecurity operations centre designed
as an open cloud service with machine learning elements

supporting document for V4

The SOC concept from a broader perspective, terminology and providers

Linked to work package KPB2 – Design of the SOCaaS service

Funded by the European Union
NextGenerationEU

RECOVERY AND RESILIENCE PLAN

GOVERNMENT OFFICE OF THE SLOVAK REPUBLIC

Contents

1. The SOC concept 3
1.1. Legislative background 3
1.2. Basic terminology 4
1.2.1. Preparation, planning and prevention 4
1.2.2. Monitoring, detection and response 5
1.2.3. Recovery, improvement and compliance 7
1.3. Requirements and components of a SOC 8
1.3.1. Basic types of models: 8
1.3.2. Staff tiers in a SOC 8
1.3.3. Performance metrics in a SOC 9
1.4. Advantages and disadvantages of a SOC 10
1.4.1. Advantages of a SOC 10
1.4.2. Disadvantages of a SOC 11
2. SOC vs. SOCaas 13
2.1. Functionalities and characteristics of SOCaaS 13
2.2. Differences between SOCaaS and a Co-Managed SOC 13
2.2.1. Advantages of the SOCaaS service 15
2.2.2. Disadvantages of the SOCaaS service 15
2.2.3. Differences between SOCaaS, MSSP and MDR 16
2.2.4. SOCaaS providers in Slovakia and worldwide 17
List of sources 18

1. THE SOC CONCEPT

In today's digital age, cybersecurity is an integral part of our lives and of business operations. With the growing number of cyber threats and vulnerabilities, it is becoming essential to build an effective security operations centre (SOC) capable of protecting organizations against these threats. With the advent of cloud technologies in IT infrastructure and services, cloud solutions provide us with an efficient and flexible framework for operating a SOC.

1.1. Legislative background

A fundamental step in building a SOC in the Slovak Republic is knowledge of the legislative requirements in the field of cybersecurity. For this reason, this section needs to summarize which legislative frameworks must be complied with and what impact the new NIS2 cybersecurity directive will have on the provision of SOC services.

Within the project, selected national, supranational and European plans and standards relating to cybersecurity were studied. All the information given in this paragraph is drawn from the NIS2 Directive.

On 14 December 2022, the European Parliament introduced the new NIS2 Directive, which deals with measures for a high common level of cybersecurity across the European Union (EU). The NIS2 Directive is an extension of the previous NIS1 Directive. In Article 6, in which the directive defines its terms, the term "managed security service provider" is particularly significant for this project. This term denotes a managed service provider that carries out or provides assistance for activities relating to cybersecurity risk management.

As with the NIS1 Directive, the NIS2 Directive also lays down measures aimed at achieving a high common level of cybersecurity across the entire EU, with a view to improving the functioning of the internal market. To this end, the directive defines obligations under which Member States are required to supplement the national cybersecurity strategies implemented in national legislation under the previous NIS1 Directive.

Parts of the directive relating to SOCaaS and other providers of security or managed services were selected, and we followed them during our work on this project.

1.2. Basic terminology

A security operations centre (SOC) is defined as an internal or external team of cybersecurity experts through which continuous monitoring of an organization's entire IT infrastructure is ensured. This monitoring is carried out in order to identify cybersecurity events in real time and to ensure that they are handled as quickly and efficiently as possible.

As part of the SOC's activities, the cybersecurity technologies used by the organization are selected, operated and maintained. At the same time, threat data is continuously analysed in order to identify opportunities to improve the organization's overall level of security.

The main advantage of operating a SOC or using SOC services provided by third parties is considered to be the unification and coordination of the organization's security tools, procedures and responses to security incidents. This approach improves preventive measures and security policies and achieves a faster, more effective and more cost-efficient response to emerging security threats. Operating a SOC also helps to increase customer trust and to simplify and strengthen the organization's compliance with industry, national and global personal data protection regulations.

1.2.1. Preparation, planning and prevention

Asset inventory

As part of the SOC's activities, an overview must be kept of all assets that need to be protected, regardless of whether they are located in the data centre or outside it (e.g. applications, databases, servers, cloud services, endpoints, etc.). At the same time, all tools used to protect these assets must also be recorded (e.g. firewalls, antivirus, anti-malware and anti-ransomware solutions, monitoring software, etc.). In many cases, specialized software solutions are used for asset discovery.

Incident response planning

The SOC is responsible for drawing up the organization's cyber incident response plan. This plan must define the specific activities, tasks and responsibilities of the parties involved, as well as the metrics by which the success of the incident response carried out will be evaluated.

Routine maintenance and preparation

In order to maximize the effectiveness of security tools and measures, preventive maintenance is regularly carried out in the SOC. This includes applying software patches and updates, as well as continuously adjusting firewalls, whitelists, blacklists, security policies and procedures for monitoring, classifying and handling security incidents. As part of these activities, system backups are also created, or input is provided for the design and implementation of backup policies and procedures that ensure business continuity in the event of a cyber incident, including a ransomware attack or a data leak.

Regular testing

Vulnerability assessments are regularly carried out in the SOC. These assessments serve to identify weaknesses in individual assets and to evaluate their resilience to possible cyber threats, including estimates of financial and reputational losses. These activities also include penetration tests, which simulate real attacks on the organization's systems. The results of

these tests are then used to adjust or streamline applications, security policies, best practices and incident response plans.

Staying up to date

The SOC ensures continuous tracking of the latest trends in security technologies and solutions, as well as the acquisition of up-to-date information on cyber threats. This information is drawn from a variety of sources – including social media, specialist security portals, community forums and environments such as the dark web – and is used in decision-making and in updating security measures.

1.2.2. Monitoring, detection and response

Monitoring, detection and response

The SOC ensures continuous oversight of the entire extended IT infrastructure – applications, servers, system software, computing devices, cloud workloads and network infrastructure – 24 hours a day, 7 days a week, 365 days a year. Monitoring is focused on detecting signs of known exploits and any suspicious activity.

SIEM (Security Information and Event Management) and SOAR (Security Orchestration, Automation and Response) technologies are used for this purpose.

Use of SIEM

SIEM systems are deployed in SOCs so that the data generated by firewalls, network devices, intrusion detection systems and other devices can be analysed. These systems provide collection, filtering, detection, classification and investigation of threats. At the same time, they can be used to implement preventive measures and to predict future threats.

Modern SIEM solutions are equipped with artificial intelligence, thanks to which processes can be automated and streamlined. By learning from data, these systems continuously improve at identifying suspicious activity.

Interconnection of SIEM and SOAR

SIEM systems are often integrated with SOAR platforms because their capabilities complement each other. In large SOCs, these technologies are used in parallel in order to optimize operations.

SOAR platforms aggregate, correlate and analyse alerts in a similar way to SIEM, while additionally providing threat intelligence integration and enabling the automation of incident investigation and response processes. These activities are carried out on the basis of predefined procedural manuals (so-called playbooks).

Functions of SOAR systems

The following activities are carried out using SOAR technologies:

- **Collection of alert data** from all system components.
- **Incident investigation**, assessment and forensic analysis.

- **Automation of response procedures** according to predefined scenarios, ensuring a rapid and consistent response.
- **Automatic implementation of measures** in response to detected threats, where these measures can be triggered automatically or manually by a SOC staff member.

Manual response of the security team

If an incident is assessed by SOC staff as genuine, it is responded to with the aim of minimizing damage. Commonly performed measures include:

- Investigating the causes of the incident and identifying technical or procedural deficiencies (e.g. weak passwords, ineffective policies).
- Shutting down or isolating compromised endpoints.
- Redirecting or blocking network traffic from compromised segments.
- Suspending applications or processes suspected of being compromised.
- Removing malicious or infected files.
- Running antivirus or anti-malware tools.

Tools for monitoring, forensic analysis and incident response

Various tools are used in practice for monitoring, collecting and analysing network traffic:

- **Sigma –** It is used as a format for sharing detection rules for malicious behaviour within security teams. It was created as an open-source standard that allows the same detection rules to be used across different SIEM platforms (e.g. Splunk, Azure Sentinel), logging systems (Graylog) and databases (MySQL).
- **YARA –** is a rule-based framework designed to identify and classify malware samples. Using both textual and binary patterns, descriptions of malware families and other digital artefacts, including hexadecimal strings, are created.
- **Velociraptor –** An open-source platform developed by DFIR (Digital Forensics and Incident Response) specialists for endpoint monitoring, digital evidence hunting and incident response. Velociraptor is used for:
  - Reconstructing attacker activities.
  - Searching for evidence of advanced threats.
  - Detecting malware and non-standard network activity.
  - Monitoring suspicious user activity (e.g. copying to USB).
  - Detecting leaks of sensitive data outside the organization.
  - Long-term data collection for threat hunting and retrospective analyses.
- **QRadar –** is a comprehensive tool from IBM that interconnects SIEM, SOAR and EDR/XDR/MDR solutions and provides a centralized user interface. It uses artificial intelligence to streamline incident analysis, thereby contributing to greater efficiency of SOC analysts.
- **Wazuh –** is an open-source solution for security monitoring and threat detection. Agents are used to collect data from various sources (e.g. logs, events), which is subsequently analysed by a central manager. Wazuh provides extended capabilities for detection, alert generation and incident response, thereby supporting the organization's cybersecurity.

1.2.3. Recovery, improvement and compliance

Recovery and remediation

Once the incident has been contained, the threat is removed by SOC staff and steps are then taken to restore the affected resources to their original pre-incident state. These steps include, for example, wiping, restoring and reconnecting disks, end-user devices and other endpoints, restoring network traffic and restarting applications and processes. In cases such as a data leak or a ransomware attack, recovery may also be achieved by switching to backup systems and changing passwords or authentication credentials.

Post-incident analysis and improvement

In order to prevent the incident from recurring, all new information obtained during its handling is used to remediate the identified vulnerabilities, update processes and policies, select more suitable cybersecurity tools or adjust the incident response plan. At the strategic level, the SOC team may seek to identify trends or new directions in the evolution of cyber threats that could affect the organization's security profile in the future.

Compliance management

Ensuring compliance with legislative and regulatory requirements is one of the core tasks of a SOC. It is ensured that all applications, systems, security tools and processes meet the requirements arising from applicable data protection regulations, such as GDPR, PSD2 and other regulations in force in the country where the SOC is operated.

In the territory of the Slovak Republic, compliance with the requirements of Act No. 69/2018 Coll. on Cybersecurity and on amendments to certain acts is ensured. In particular, §18 (Identification criteria of the operated service) and §19 (Obligations of the operator of an essential service) are complied with.

Following a cyber incident, it is ensured that all affected parties – users, regulatory authorities, law enforcement authorities and other stakeholders – are informed in accordance with the relevant provisions, e.g. §24 of Act No. 69/2018 Coll. At the same time, all relevant data on the incident are retained for the purposes of forensic evidence and audit.

Requirements according to NIST – Incident Handling Guide

The National Institute of Standards and Technology of the United States of America (NIST) has issued the publication "NIST Special Publication 800-61 Rev. 2", also known as the "Computer Security Incident Handling Guide". This guide provides detailed recommendations and methodologies for organizations in the field of cyber incident management.

The document defines standard procedures for:

- identifying and classifying incidents,
- reporting, analysing and handling them,
- securing records and forensic documentation.

The guide also includes recommendations for creating and implementing incident response plans (Incident Response Plans), which help organizations respond quickly to threats and mitigate their impact on infrastructure, operations and reputation.

1.3. Requirements and components of a SOC

Types of SOC models

In addition to the standard SOC, there are also other types of centres and services through which the protection of organizations' networks and digital infrastructure is ensured. These centres may have common or overlapping features and functions, and it is not strictly defined what scope each centre must cover. In practice, the scope of each SOC model is tailored to the specific needs of the organization.

1.3.1. Basic types of models:

Internal SOC (Internal SOC) – It is established by the enterprise itself. The staff are employed directly by the organization and form an internal cybersecurity team. The SOC is owned and operated by the enterprise.

External SOC (External SOC, SOCaaS) – It is provided by an external supplier as a service. Operation is carried out, for example, in the form of Managed Security Services (MSS). It can be implemented as a cloud solution.

Global or command SOC (Global / Command SOC) – It acts as a central authority coordinating the activities of several smaller SOCs within an organization or region.

Co-managed SOC (Co-Managed SOC) – Operation is carried out in cooperation between the organization's internal IT team and an external SOC service supplier. Responsibilities and activities are divided between both parties.

MSSP – Managed Security Service Provider – This is a service provider with many features in common with SOCs. A more detailed specification is given in Section 4.3.1.

MDR – Managed Detection and Response – It focuses on detection and active response to threats. Incidents are analysed, false alarms are eliminated and genuine threats are handled on behalf of the client.

1.3.2. Staff tiers in a SOC

In a SOC, work tasks are assigned according to SOC analyst tiers. The tiers are determined by the expertise and responsibilities required for each tier. A SOC usually has four tiers:

Tier 1 – Alert analyst

- monitors incoming alerts.
- if they find that the alert is a true positive:
  - takes basic measures to mitigate the impact of the threat.
  - or, if necessary, escalates the handling of the threat to a Tier 2 staff member.
- if they find that the incident is a false positive:
  - updates the incident detection system that generated the alert.

- if they are unable to resolve the incident, escalates the threat to a Tier 2 staff member.

Tier 2 – Incident responder (Incident Responder)

- investigates incidents in depth.
- proposes how the problem should be resolved,
- recommends remediation (action),

Tier 3 – Threat hunter (Threat hunter)

- is an expert in networks, endpoints, threats, threat intelligence and malware reverse engineering.
- traces malware processes in order to determine its impact and how it can be removed (including preventive measures).
- is deeply involved in hunting for potential threats and implementing threat detection tools.
- proactively hunts for cyber threats that are present in the network but have not yet been detected.

SOC manager (SOC Manager)

- manages all resources in the SOC.
- serves as the point of contact for organizations and customers.
- implements standardized operating procedures (Standard Operating Procedures, SOPs) for the incident handling process, which guide analysts through triage and response procedures.

Security teams in cybersecurity

Colour-coded teams are used for the division of tasks and simulations:

- **Red team (Red Team)** – Simulates an attacker. Weaknesses in defences are identified.
- **Blue team (Blue Team)** – Responds to incidents and ensures defence mechanisms.
- **Purple team (Purple Team)** – Integrates the activities of the red and blue teams. It focuses on collaboration.
- **Yellow team (Yellow Team)** – Consists of security architects and security system developers.
- **Green team (Green Team)** – Improves the code created by the yellow team based on the outputs of the blue team.
- **Orange team (Orange Team)** - Uses insights from red team analysis to raise developers' awareness.

The activities of these teams, primarily the red and blue teams, are used in the SOC to detect and eliminate vulnerabilities.

1.3.3. Performance metrics in a SOC

Various KPIs – Key Performance Indicators – are used to evaluate the efficiency of SOC operations. The following metrics are commonly tracked:

- **Dwell time (Dwell Time) –** The period during which a threat actor had access to the network before being detected and neutralized.
- **Mean time to detect (MTTD – Mean Time to Detect) –** The time required to identify a genuine incident.
- **Mean time to respond (MTTR – Mean Time to Respond) –** The time required to stop and eliminate an incident.
- **Mean time to contain (MTTC – Mean Time to Contain) –** The time required to contain an incident before damage spreads.
- **Time to control (Time to Control)** – The time required to stop the spread of malware in the network.

1.4. Advantages and disadvantages of a SOC

There are many reasons why a security operations centre (SOC) should be implemented, either as an internal or as an external solution. Cybersecurity is an area that all modern enterprises must address, because as an organization grows, so does the likelihood that it will become the target of a cyber attack.

This section summarizes the main advantages and disadvantages of deploying a SOC. The information was compiled on the basis of sources .

1.4.1. Advantages of a SOC

Continuous monitoring

Thanks to continuous monitoring and analysis of activities across the entire network infrastructure, cybersecurity incidents can be identified in time and responded to immediately. This feature is considered one of the most essential, since time is a decisive factor in an effective response to a security incident.

Rapid incident response

When an incident occurs, a rapid response by SOC analysts is ensured. Once an alert is received, the incident is investigated, the threat contained and the consequences of the incident minimized. In this way, the downtime of systems and services is reduced.

Proactive threat detection

By monitoring network activity and system logs, anomalies and potential threats are sought out before they break out. Based on these findings, preventive measures are taken to prevent incidents and damage.

Threat intelligence integration

SOC analysts are given access to up-to-date information on emerging types of attacks and the techniques used by attackers. Thanks to this information, it is possible to stay ahead of potential threats.

Centralized security management

The SOC acts as the main hub for managing the organization's security policy. It provides a centralized overview of the level of security, simplified management of security measures, enforcement of internal policies and compliance with regulatory requirements.

At the same time, it enables:

- effective real-time incident response,
- consolidation of security data from various sources,
- coordination between analysts, IT administrators and responsible staff.

Tailored security solutions

The solutions provided by the SOC are tailored to the specific needs of the organization. Tools, processes and technologies are selected in line with the security challenges and strategic objectives of the enterprise.

A personalized SOC enables:

- alignment of security with business objectives,
- ensuring compliance with legislation and standards,
- protection of sensitive data and prevention of unauthorized access.

Cost-effectiveness

Although establishing a SOC represents an initial investment, the long-term benefits, such as a reduction in the occurrence of incidents and their impact, can significantly outweigh the costs. Preventing incidents makes it possible to avoid financial losses and reputational damage.

1.4.2. Disadvantages of a SOC

Large volume of data

With the increasing number of alerts, advanced analytical systems and qualified staff are required to evaluate and triage them correctly. Under a high workload, there is a risk of misclassification or of serious incidents being overlooked. This underlines the need for automation and a sufficiently large team of experts.

Cost

Building and maintaining a SOC requires considerable financial resources and time. In view of the dynamic evolution of threats, it is necessary to ensure:

- regular system updates,
- continuous staff training,
- expert capacity in in-depth security analysis.

For these reasons, many organizations prefer outsourcing SOC functions through SOCaaS-type services.

Shortage of staff capacity

Cybersecurity is a field that demands expertise. Finding and retaining qualified staff is a significant challenge, especially for internal solutions. Many experts prefer to work for SOC service providers, where professional support, knowledge sharing and a more attractive professional environment are usually provided.

2. SOC VS. SOCAAS

The main difference between an internal SOC and SOCaaS (Security Operations Center as a Service) lies in their management and ownership.

An internal SOC is established, owned and operated by the organization for which it is intended. Cybersecurity experts who ensure the operation of the centre are employed within the enterprise.

By contrast, SOCaaS, i.e. an external SOC provided as a service, is delivered by an external supplier that provides either the entire SOC or only its components as a service. In this section, the information was drawn from sources.

2.1. Functionalities and characteristics of SOCaaS

SOCaaS is a cloud-based cybersecurity model provided on a subscription basis. It is designed as a managed threat detection and response service, covering the functions and capacities typical of a full-fledged SOC. This model serves to fill gaps in organizations' existing security teams.

Like internal centres, SOCaaS also provides:

- continuous monitoring,
- threat detection,
- prevention and attack surface analysis,
- monitoring of the network, endpoints, databases and cloud infrastructure,
- use of SIEM systems, firewalls and threat intelligence tools.

2.2. Differences between SOCaaS and a Co-Managed SOC

Co-managed SOC (Co-managed SOC)

In the co-managed SOC model, the organization is provided with security staff from an external supplier (including Tier 1–3 analysts and a SOC manager), who work together with the customer's internal IT team. The equipment and infrastructure for network monitoring are owned by the customer; the supplier provides only the expertise.

Activities in this model usually include:

- threat monitoring and detection,
- incident investigation,
- possibly also compliance and the proposal of corrective measures.

However, the provision of complete incident handling is not guaranteed – it depends on the specific service provider.

Advantages of a co-managed SOC:

- Cost savings – the organization does not have to employ its own security team.

Disadvantages of a co-managed SOC:

- Integration complexity – cooperation between two teams (internal and external) requires a high degree of coordination.

- Dependence on the supplier – in the event of its failure, cybersecurity may be compromised.

This model is particularly suitable for small and medium-sized enterprises that do not have sufficient internal resources to build a full-fledged security team.

SOCaaS – A fully outsourced model

SOCaaS is a model in which the security operations centre is operated in the cloud and provided as a service. The service is usually provided on a subscription basis, without the need to build internal infrastructure or employ specialists.

The SOCaaS service includes:

- remote monitoring and incident response,
- provision of expertise without the need to retain it in-house,
- cost savings through a scalable model.

SOCaaS functionalities:

A technology stack is provided that includes the tools and processes of the SOC, as is a team of experts (analysts and managers).

The following are implemented:

- monitoring and alerting mechanisms,
- escalation matrices,
- automation of response and analytics,
- remote oversight of security operations.

After onboarding and system integration, continuous oversight and communication with the customer's organization are ensured. The organization has the option to:

- monitor its infrastructure,
- perform security tests,
- obtain recommendations for improving its level of security.

Scope of the SOCaaS service

It is not stipulated which functions SOCaaS must unconditionally include – therefore the offering varies by provider. Some suppliers provide only passive monitoring and reporting, leaving incident remediation to the customer.

Responsibility for security does not lie exclusively with the service provider. The organization must comply with internal security policies and measures created in cooperation with the SOC analysts, in line with legislative frameworks.

2.2.1. Advantages of the SOCaaS service

The SOCaaS (Security Operations Center as a Service) service provides advantages comparable to those described for an internal SOC, while also addressing several disadvantages identified in the implementation of an internal SOC. This section presents the advantages that are unique to SOCaaS.

Cost-effectiveness

The SOCaaS service is provided on a subscription basis. Organizations thus no longer need to invest in infrastructure, licences and the recruitment of internal staff. In this way, initial capital expenditure is minimized and operating costs are optimized.

Access to experts

Given the global shortage of qualified cybersecurity specialists, it is difficult for many organizations to build an internal team of analysts. Using the SOCaaS service ensures access to experts without the need to employ them directly.

Automated security processes

A high degree of automation and the integration of artificial intelligence enable efficient triage and evaluation of alerts. Repetitive tasks are processed automatically, which increases the efficiency of incident response and allows analysts to focus on critical tasks.

2.2.2. Disadvantages of the SOCaaS service

Despite the numerous advantages, the use of external SOC services presents certain challenges that may not arise with an internal SOC.

Adapting to a new process

Implementing the SOCaaS service requires the reorganization of internal processes and the acceptance of new security protocols. Complexity may arise when determining the compatibility of the provider's technology stack with the specifics of the organization's IT environment. Employees need to adopt new policies and the provider's analysts need to understand the client's infrastructure. Introducing the service requires a planned ramp-up period.

Regulatory requirements

Not all SOCaaS providers cover the obligations related to legislative compliance, such as GDPR, HIPAA, ISO 27001 or the Slovak Act No. 69/2018 Coll. Compliance needs to be verified individually.

Information sharing

For the service to be performed effectively, the provider must be given access to the internal infrastructure and sensitive data. This involves a risk of misuse or leakage of information, because the provider's staff may monitor employee activity and have access to confidential information.

2.2.3. Differences between SOCaaS, MSSP and MDR

MSSP – Managed Security Service Provider

An MSSP is an external security service provider whose role is to supplement or replace the organization's internal security team. In addition to monitoring and managing security devices, an MSSP also focuses on the design and implementation of security policies.

Although the technologies and services are similar to those of a SOC, the difference lies in the lower degree of incident analysis. An MSSP acts rather as a strategic partner for designing the security framework, with incidents handled in less depth than in a SOC.

MDR – Managed Detection and Response

MDR is a service specialized in detection and response. Compared to an MSSP, it concentrates on actively detecting and handling incidents on behalf of the organization.

MDR combines technologies and analysts and makes use of a high degree of automation. It focuses on complex incidents, while network configuration and routine administration remain the responsibility of the organization.

A disadvantage of MDR is that it covers only the area of detection and response – other areas of cybersecurity require a dedicated team.

Characteristic	MSSP	MDR	SOCaaS
Primary focus	Prevention, monitoring, policy design	Detection, response, incident analysis	Comprehensive protection and incident response
Service level	Monitoring and configuration	Advanced response and forensic analysis	All phases – from detection to recovery
Human resources	External analysts	External analysts with specialization	External team for monitoring and support
Technological demands	Low to medium	Medium to high	High – automation, AI, cloud platforms
Need for an internal team	Optional (can be fully replaced)	Requires a complementary team	Basic IT team required

Who SOCaaS is suitable for

The SOCaaS service is particularly suitable for small and medium-sized enterprises with limited resources. Investments in cybersecurity tend to be demanding for these enterprises, and SOCaaS offers an affordable option for professional protection without the need to build their own team and infrastructure.

2.2.4. SOCaaS providers in Slovakia and worldwide

Global SOCaaS providers

- **Arctic Wolf Networks** – Provides SOCaaS as well as MSP services, cyber insurance solutions and supplementary SOC services.
- **Rapid7** – Focuses on MDR, penetration testing, and training in vulnerability management, detection and automation.
- **Alert Logic** – Provides SOCaaS, MSP services and both free and paid training.

Other major providers include **Secureworks, Qualysec, Trustwave and Blackpoint Cyber.**

Slovak SOCaaS providers

- **ESET** – Offers MDR services and related security services for the corporate sector.
- **Slovak Telekom –** Offers two service levels: SOCaaS Light (incident notification) and SOCaaS Plus (immediate response).
- **Soitron –** Operates Soitron Security Sensor and provides SOC services, analytics, consultancy and the podcast Lokál hosť.
- **Aliter Technologies –** Provides SOCaaS; further information is available on request.
- **Binary Confidence –** Offers 24/7 monitoring and incident handling.
- **TÜV SÜD Slovakia –** Focused on critical infrastructure sectors under Act 69/2018 Coll., it offers three service variants: BASIC, STANDARD, PREMIUM.

LIST OF SOURCES

[1] EUR-Lex, “CELEX_32022L2555_SK_TXT”, Accessed: Oct. 21, 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:32022L2555&qid=1697886701099
[2] Národný bezpečnostný úrad, “Strategia_kybernetickej_bezpecnosti_2021”, Accessed: Apr. 27, 2024. [Online]. Available: https://www.nbu.gov.sk/612-sk/narodna-strategia-a-akcny-plan-kybernetickej-bezpecnosti/
[3] IBM, “What is Security Operations Center (SOC)? | IBM.” Accessed: Nov. 26, 2023. [Online]. Available: https://www.ibm.com/topics/security-operations-center
[4] Cisco, “Cisco Certified CyberOps Associate - Cisco.” Accessed: Dec. 03, 2023. [Online]. Available: https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/cyberops-associate.html
[5] Clearnetwork, “What is a Managed SOC? Benefits and Variants -.” Accessed: Apr. 25, 2024. [Online]. Available: https://www.clearnetwork.com/what-is-managed-soc-benefits-and-variants/
[6] IBM, “What is Security Operations Center (SOC)? | IBM.” Accessed: Feb. 21, 2024. [Online]. Available: https://www.ibm.com/topics/security-operations-center
[7] GitHub, “GitHub - SigmaHQ/sigma: Main Sigma Rule Repository.” Accessed: Feb. 21, 2024. [Online]. Available: https://github.com/SigmaHQ/sigma?tab=readme-ov-file#readme
[8] Picus Security, “What Is a YARA Rule?” Accessed: Feb. 21, 2024. [Online]. Available: https://www.picussecurity.com/resource/glossary/what-is-a-yara-rule
[9] Rapid7, “Velociraptor Overview :: Velociraptor - Digging deeper!” Accessed: Feb. 21, 2024. [Online]. Available: https://docs.velociraptor.app/docs/overview/
[10] Wazuh, “Wazuh - Open Source XDR. Open Source SIEM.” Accessed: Apr. 12, 2024. [Online]. Available: https://wazuh.com/
[11] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, “Computer Security Incident Handling Guide,” Aug. 2012, doi: 10.6028/NIST.SP.800-61R2.
[12] The National Institute of Standards and Technology (NIST), “SP 800-61 Rev. 2, Computer Security Incident Handling Guide | CSRC.” Accessed: Apr. 24, 2024. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/61/r2/final
[13] Cisco, “Course: 2023_CyberOps.” Accessed: Feb. 21, 2024. [Online]. Available: https://lms.netacad.com/course/view.php?id=2141844
[14] Coursera, “Red Team vs. Blue Team in Cybersecurity | Coursera.” Accessed: Mar. 10, 2024. [Online]. Available: https://www.coursera.org/articles/red-team-vs-blue-team
[15] Tata Communications, “MSSP vs SOC: Unraveling Key Differences for Enterprises.” Accessed: Mar. 08, 2024. [Online]. Available: https://www.tatacommunications.com/knowledge-base/mssp-vs-soc/