Security Operations Centre (SOC) Services

Service Definition Document

Sopra Steria

Contents

1 About Sopra Steria

1.1 Overview

About Sopra Steria

Sopra Steria, a major Tech player in Europe with 50,000 employees in nearly 30 countries, is recognised for its consulting, digital services and solutions. It helps its clients drive their digital transformation and obtain tangible and sustainable benefits. The Group provides end-to-end solutions to make large companies and organisations more competitive by combining in-depth knowledge of a wide range of business sectors and innovative technologies with a collaborative approach. Sopra Steria places people at the heart of everything it does and is committed to putting digital to work for its clients in order to build a positive future for all. In 2024, the Group generated revenues of €5.8 billion.

The world is how we shape it

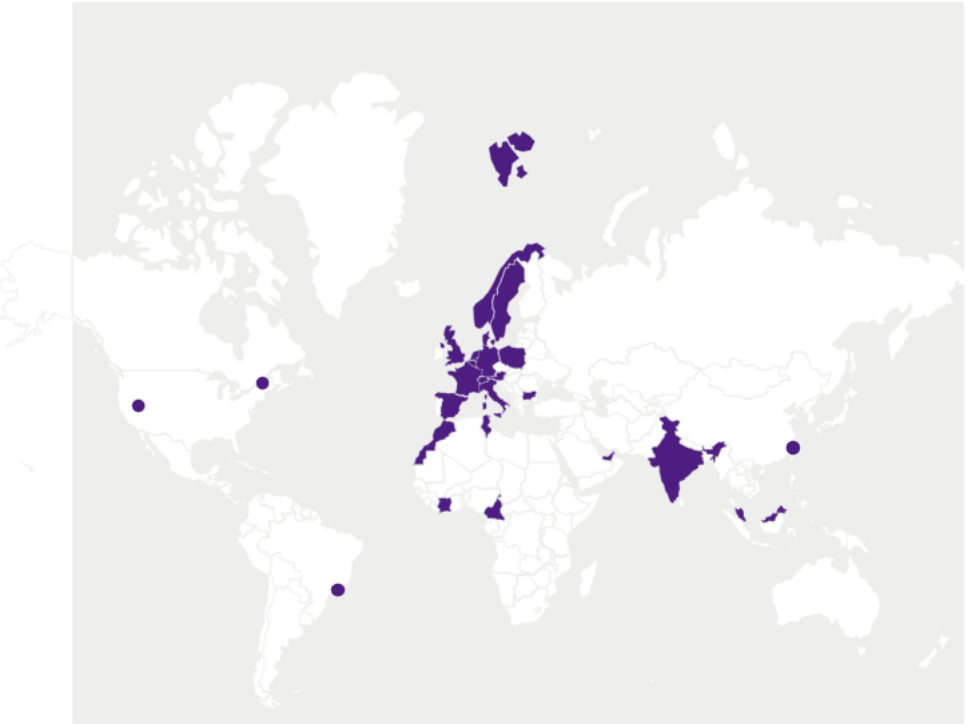
Sopra Steria (SOP) is listed on Euronext Paris (Compartment A) – ISIN: FR0000050809 For more information, visit us at www.soprasteria.com

50,000
employees

€5.8bn
2024 revenue

Top 5
European digital services companies

In nearly
30
countries



1.2 Our Cloud Capability

Sopra Steria Cloud Practice brings together leading digital, cloud and engineering expertise to accelerate transformation for our clients.

- Delivering comprehensive digital and cloud transformation, including strategic consulting, change management, large-scale migration, application modernisation, next-generation development and secure, optimised operations
- Integrating deep capability across applications, data, infrastructure, cloud platforms and security, supported by industrialised assets to enable solutions across Private, Public, Hybrid and Sovereign Cloud environments
- Using an end-to-end cloud delivery model that integrates business, engineering, security and operations, ensuring continuous innovation, strong governance, and measurable business value throughout the full cloud lifecycle.

1.3 Our Credentials

Capacity

More than 15,000 cloud experts in 30 countries (Vision, Ops, Design, Scale)

Market recognitions

- **Large account** (best category>$250m) **in the "Public Sector Industry Cloud Landscape"** (Forrester)
- **Leader "Cloud public in Europe" & " Next Gen Private & Hybrid Cloud"** (ISG)
- **Leader "Cloud Infra Brokerage"** (NelsonHall)
- **Best in Class "Azure" & "SAP" & "Service Now"** (PAC Radar)
- **Leader "Cloud Native Application" & "Application Transformation Services"** (Quadrant)
- **Major Contender "Cloud Services" & "Cloud Native Applications" & "Services on AWS Azure & CGP"** (Everest)

Key partners

NumSpot, Google Cloud, Oracle Cloud, IBM Cloud, Scaleway, vmware, aws, Microsoft Azure, Visa, OVHcloud, redhat, OUTSCALE

Main market recognitions

2nd in IT Services in France and 10th in EMEA*

Cybersecurity	Digital	AI	IT for Green	Cloud
• **Leader "Cyber resiliency services"** (NelsonHall) • **Leader "cybersecurity" in France & Germany** (ISG) • **Top 5 "cybersecurity" in France** (Markess)	• **Leader "Application Transformation Services"** (Quadrant) • **Leader "Digital Banking"** (NelsonHall) • **Leader "Digital Banking Services"** (ISG) • **Major Contender "Digital twin Services"** (Everest) • **Innovator "Digital Manufacturing"** (NelsonHall)	• **Leader AI Services & Gen AI** (PAC Innovation Radar) • **Leader AI Services** (Quadrant) • **Leader "Intelligence Process Automation"** (Quadrant) • **Major player "European Professional Services for Data-Drive"** (IDC) • **Major contenders "AI services" & "Intelligent Process Automation services"** (Everest)	• **Leader "ESG for Banking Services"** (NelsonHall) • **Best in class "consulting and digital services for sustainable development"** (PAC Innovation Radar) • **Major Contender "NetZero Consulting Services"** (Everest)	• **Large account (best category>$250m) in the "Public Sector Industry Cloud Landscape"** (Forrester) • **Leader "Cloud Infra Brokerage"** (NelsonHall) • **Best in Class "Azure" & "SAP" & "Service Now"** (PAC Radar) • **Leader "Cloud Native Application" & "Application Transformation Services"** (Quadrant) • **Leader "Cloud public in Europe" & " Next Gen Private & Hybrid Cloud"** (ISG) • **Major Contender "Cloud Services" &"Cloud Native Applications" & "Services on AWS Azure & CGP"** (Everest)

PAC, IDC, ISG, Quadrant, PEAK MATRIX, NelsonHall, FORRESTER, exægis

* Source PAC 2024

2 Service Overview

2.1 Service Description

Sopra Steria's Security Operation Centre (SOC) Services is a proactive and reactive defence mechanism, providing continuous monitoring, incident response, threat intelligence analysis and support for compliance and regulatory requirements. Its critical role is to protect your organisations' digital assets and data, to minimise the impact of cyber threats and incidents.

Many organisations rely heavily on cloud security tools to protect their cloud infrastructure and data. However, these tools often fall short when it comes to providing comprehensive threat detection. This limitation leaves organisations vulnerable to sophisticated attacks that can go undetected. Without integrating a SOC, the visibility and context needed to effectively identify and respond to these complex threats across both traditional and cloud environments are lacking. This poses a significant problem as organisations face an increased risk of potential breaches and data loss.

Data breaches carry some of the costliest fines for organisations. Reports have demonstrated that security analytics is a core component to significantly reduce the cost of a data breach, taking the savings into the millions. Implementation of a SOC underpinned with a streamlined and defined security incident response process is reported to reduce the cost of a breach by around 10%.

By adopting our SOC services, we can swiftly detect potential high-impact attacks across an organisation's entire landscape, providing reassurance during audits or assessments conducted by prospective clients or stakeholders.

2.2 Features

- **Holistic risk and threat view:** Obtain a unified view of risk and threats across your entire enterprise, including private and public clouds
- **Threat Landscape awareness:** Shared intelligence across organisations allows for a comprehensive view of indicators of compromise identified through collective understanding of the threat landscape
- **Proactive threat identification:** Identify and address threats before they escalate into incidents
- **Access to specialist skill sets:** Specially trained, certified and experienced professionals that deliver SOC Operational and Engineering Services.

2.3 Benefits

- **Comprehensive security assurance:** Gain end-to-end business security confidence and meet essential security audit requirements by continuously monitoring and assessing security controls. This ensures adherence to industry standards and regulations, mitigating the risk of penalties and legal consequences
- **Monitor and analyse security events:** Enabling prompt incident response and minimising the impact of potential incidents
- **Increased Operational Efficiency:** By centralising and automating security monitoring and response activities we improve incident coordination and enhance our ability to detect, respond to and mitigate security threats efficiently
- **Substantiated Threats:** Alongside alerts, we provide evidence of threats. This information supports incident investigations, ensuring accurate analysis and facilitating informed decision-making
- **Cost savings:** Reduce the expense of security monitoring by consuming Managed Detection and Response services whilst expanding security coverage.

2.4 Our Approach

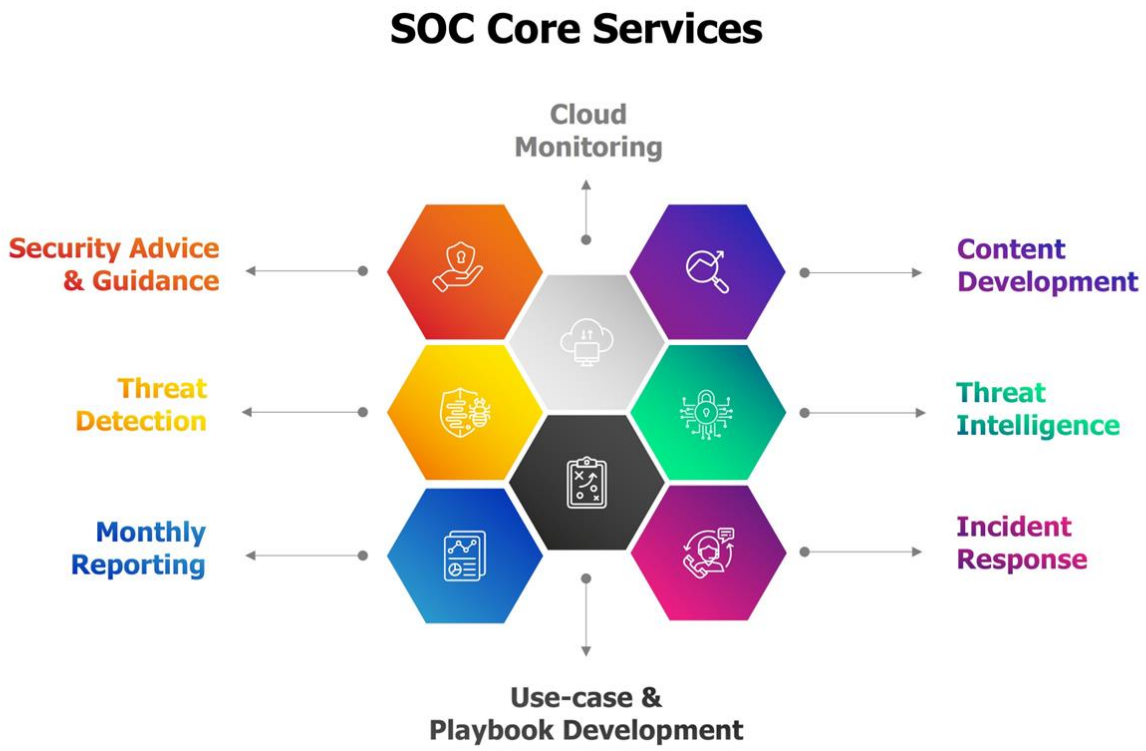


Figure 1: Our Cyber Security Operations Centre (SOC) comprises various interconnected elements such as monitoring tools, threat intelligence, incident response protocols, and skilled personnel working collaboratively to detect, analyse, and mitigate cyber threats in real time.

Threat Detection
Threat Detection is provided as part of our core offering; our Security Incident and Event Management (SIEM) Solution provides continuous Threat Detection. Cyber attackers are becoming increasingly sophisticated and are constantly developing new tactics, techniques and procedures to compromise systems and networks. To allow us to monitor the service scope, we work with clients to design their Threat Detection solution, to identify and integrate security-relevant log sources into the SIEM and to develop custom use cases that may be required to support client requirements. By integrating these into our SIEM tooling, we will monitor for and detect client specific security events and identify potential threats.

The advantage of Threat Detection being in place for our clients is we can stay ahead of the latest threats, ensuring that systems and data are monitored at all times, as well as aligning log sources and alarms to defined standards.

Monitoring and detection is provided through the implementation of our SIEM Solution, a market leading cloud-based Software-as-a-Service (SaaS) offering that provides SIEM and Security Orchestration, Automation and Response (SOAR) capabilities.

Alternatively, the SOC is also able to offer an on-premises SIEM solution should a client require due to security classifications.

Both options are highly scalable and offer a range of features:

- They have been selected due to their industry leading scalability and key security features, including real-time threat detection
- Integrated SOAR capability, improved systems integration with a wider source of data feeds, integrated playbook automation for faster detection and containment response
- Improved analyst interface, boosting productivity and efficiencies and ease of integration with a variety of other supplemental security tools and technologies which results in improved operational efficiency, faster incident response times, and better security outcomes for clients.

Cloud Monitoring
A vital component of our Core SOC offering is the ability to integrate Cloud Services. With the increasing adoption of cloud services and applications and data being placed in the cloud, the threat landscape scope and complexity increases the potential risk of compromise. Many monitoring tools are provided by various cloud vendors but not integrated to provide a holistic oversight of potential threats.

Sopra Steria can integrate a customer's cloud-based solution into our SOC's Threat Detection managed Service and incident response capability. The goal of integrating Cloud-based solutions into our SOC is to correlate security incidents across a number of applications and cloud-based services to enable faster and more effective incident response and to provide end-to-end visibility of security threats across an organisation. By integrating Cloud-based services into our Managed SOC we are able to collect security related data from a variety of Cloud-based sources, including infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS).

Figure 2 Ingesting cloud security alerts enables the consolidation and comprehensive analysis of potential threats across cloud environments, enhancing situational awareness and response effectiveness.

Content Development
Ongoing SIEM management requires continual development of rule configuration and tuning to enable visibility of suspicious or potentially malicious actions or events. Rules and tuning form the basis for effectively identifying, detecting, and responding to security incidents. The SOC achieves this by aligning our rule development capability against the industry recognised MITRE ATT&CK framework. MITRE ATT&CK is a globally accessible knowledge base of adversary tactics, techniques and procedures based on real-world observations. The development of our security rules, in line with MITRE ATT&CK, involves mapping the techniques used by attackers to the controls and assets that are critical to our clients. This mapping process allows us to develop detection rules that specifically focus where strong mitigations cannot be applied or where critical assets/data are held and enables the identification of any key sources of event data and informs steps to be taken to address any potential monitoring gaps. Aligning to MITRE ATT&CK is a continuous process, maintaining our awareness and constantly adapting our security playbooks to accommodate the ever-changing Threat Landscape.

Threat Intelligence
Sopra Steria's SOC utilises a variety of open-source threat information collateral, vendor notifications, Indications of Compromise (IOC) and community Threat Intelligence platforms, white papers and news articles. This is used to enhance anomaly detection during the triage process, identify, document and implement new use cases, improve our detection coverage within a client's environment, and respond rapidly to security events.

Incident Response and Containment support
SOC services play a key role in the security Incident Management process. The SOC core service encompasses the detection, triage, analysis and verification, including escalation through integration with our clients' Incident Management process. We offer two service tiers to align with the specific needs of our clients for "Response" component of the Core Service.

Our SOC team's expertise and experience in handling Security Incidents is critical to minimising the impact of the incident and ensuring a quick and effective response.

- **Detection** - Ingestion of data across a client's estate into our Monitoring Solution will be actively correlated against a comprehensive database of rules developed in line with the client's risk posture and compliant

with industry best practice. As alerts are triggered, our monitoring solution will prioritise the severity based upon pre-configured, contextualised rules, which are subject to continual improvement and tuning

- **Reaction** - Our analysts will analyse and triage alerts, to determine their validity and respond accordingly. This may include the collection and analysis of available client data and any other supporting threat intelligence. Our SOC analysts will assess the severity and impact of the alert
- **Response** - Depending on the incident severity and the playbook instructions, the SOC will determine how best to escalate to our clients, sharing relevant information and evidence with them, including the findings of the SOC's analysis and support them to contain a security incident once identified quickly and effectively. Response time is calculated from the time an Alert is triggered through to an ITSM ticket being raised/scalation as per defined processes
- **Lessons Learnt** – Post security incident we will work with clients to understand root cause and identify improvements and recommendations in security posture or process to mitigate potential future risk and improve response process feeding any findings back into the content development process for enhanced visibility.

Monthly Reporting
A critical component of the service we provide is to offer insights into the state of our clients' security posture and the effectiveness of our security operations. Our monthly reporting provides information on security incidents that have occurred, including details on the type of incident, how it was detected and resolved.

Our monthly reporting also includes key security metrics, such as the number of incidents detected, the volume of security alerts to demonstrate the effectiveness and quality of the service through the measurement of key performance indicators and service level agreements.

Reports cover details on pro-active tuning activities, false positive reductions in monitoring, details on trending, alerts, triaged security events and where necessary any lessons learnt as well as detailed assessment recommendations which will be provided to allow clients to make data driven decisions.

Use Case and Playbook Development
We develop playbooks which are an essential component within the service. A key component of incident response, playbooks provide analysts with clear instructions on incident response procedures in a way that aligns with clients' own incident management processes. Playbooks ensure security events are triaged efficiently and effectively. We work closely with clients to ensure that playbooks reflect their individual incident management processes.

A security use-case is a documented description of a specific security scenario that a SOC is expected to address. Use-cases include the threat sources, attack vectors, detection and response strategies, the tools and technologies needed to effectively detect and respond to incidents. Our SOC's security uses cases are aligned to MITRE ATT&CK and we develop supporting incident management playbooks to ensure we respond to threats effectively and integrate into our clients' processes.

We apply a standardised set of security use cases and playbooks for each client. If there are bespoke monitoring requirements, we also develop client-specific use cases and playbooks, to meet their needs.

Figure 3: MITRE ATT&CK and threat intelligence are vital for our service as they offer standardised strategies and current insights into how cyber attackers operate, empowering us to better identify, understand, and counter new and evolving cyber threats.

Security advice and guidance

We provide critical advice and guidance to our clients once an incident has been identified to help them quickly and effectively respond to the incident. Throughout the incident, our SOC team will provide regular updates and status reports to key stakeholders as agreed to keep them informed of the situation and provide guidance on next steps.

We will work with our client to develop a threat model, working through assets to be on boarding and identifying business critical components which will allow us to tailor our service accordingly. Through monthly reporting, we continuously work with clients to help them interpret the data and make continued recommendations and improvements.

2.5 Inputs

We would anticipate the following inputs from you as part of this service:

- Engagement into design phase
- Asset information and services including system criticality
- Custom business use cases
- Incident management process
- Contextualisation on environments/services.

This is a high-level list and is not exhaustive. If you cannot provide all of these inputs, then we can discuss altering our approach to accommodate your situation.

2.6 Outputs and Deliverables

Some of the outputs and deliverables generated from the service are identified below:

- Through the collection of security-related data from various sources, such as Cloud Services, firewalls, servers and endpoints we provide Threat Detection as a core offering. The objective of threat detection is to detect anomalies to identify potential threat actors and respond to incidents before they cause significant harm to client businesses across blended environments from on-premises to public/private cloud environments
- To continuously assess an organisation's security landscape and implement improvements to enhance protection against future threats by alignment against industry best practice such as the MITRE ATT&CK

framework (Adversarial Tactics, Techniques, and Common Knowledge) and NIST (National Institute of Standards and Technology) Cyber Security Framework
- Integrate clients' Hybrid Cloud-based solution into our SOC's Threat Detection and Incident Response capability
- Our SOC seamlessly integrates with clients' incident processes, playing a key role in the detection, response, containment and recovery of cyber incidents.

This is a high-level list and is not exhaustive.

2.7 Certifications and Skills

Some of our certifications and skills related to this service are identified below:

- ISO27001
- NIST CSF
- Cyber Essentials Plus
- Incident Response handling
- CompTIA Security+
- Blue Team Level 1
- CISM.

This is a high-level list and is not exhaustive.

2.8 Case Study

The challenge: In 2023, the Sopra Steria SOC team was engaged by a client to deliver SOC services, however, upon initial engagement with the client, it was identified that their existing SIEM solution would need meet the requirements laid out in their longer-term strategy.

What we delivered: We worked with client to help define their specific requirements, accounting for their business and regulatory needs and the current and planned architecture of their environment. We then successfully implemented and ran a SIEM solution and managed security service that met with the defined requirements despite a high volume of technical debt across a diverse landscape within a highly regulated environment.

Our approach to this challenge was to support our client in developing a robust solution to deliver against their strategy and regulatory requirements which was achieved by the implementation of the SOC Service underpinned by SIEM technology.

Since implementation of the initial service, we have supported our client to continually mature and improve the SOC service to ensure continued effective risk mitigation in an ever-changing threat landscape. We achieved this irrespective of a significant volume of high velocity changes to their complex environment which has continually evolved. As the environment evolved, we continued to develop the services that we provided along with the underpinning tools and technologies to enable us to continue providing a high-quality Managed Detection and Response service and to support the on-going partnership with our client in line with market trends and industry best practice.

Working in partnership with our client, we deliver the service using the Microsoft Sentinel solution.

Outcome:

- Our service and enhancements provided enabled our client to conform with regulation requirements and help them achieve cyber essentials plus and keep step with all emerging threats and assure them of their level of preparedness' and effectiveness of enacted security controls, both physical and logical.
- A successful partnership underpinned in trust, respect and highly effective Cyber Security.

3 Pricing

Please refer to the Pricing Document for this Service.

4 Next Steps

4.1 Contact

Please contact us if you would like to know more about this service or any of our listings on G-Cloud.

Email: sector-support@soprasteria.com

As all of our G-Cloud enquiries initially come into a single contact, please remember to tell us:

- Your name, your organisation name and contact details
- Which service you are enquiring about
- A brief summary of your requirements or problem statements that you would like support to address.

4.2 More Information

More information about our services and capabilities can be found on our website here.