Information Security, Managed Services, Vulnerability Management

Service Definition Document

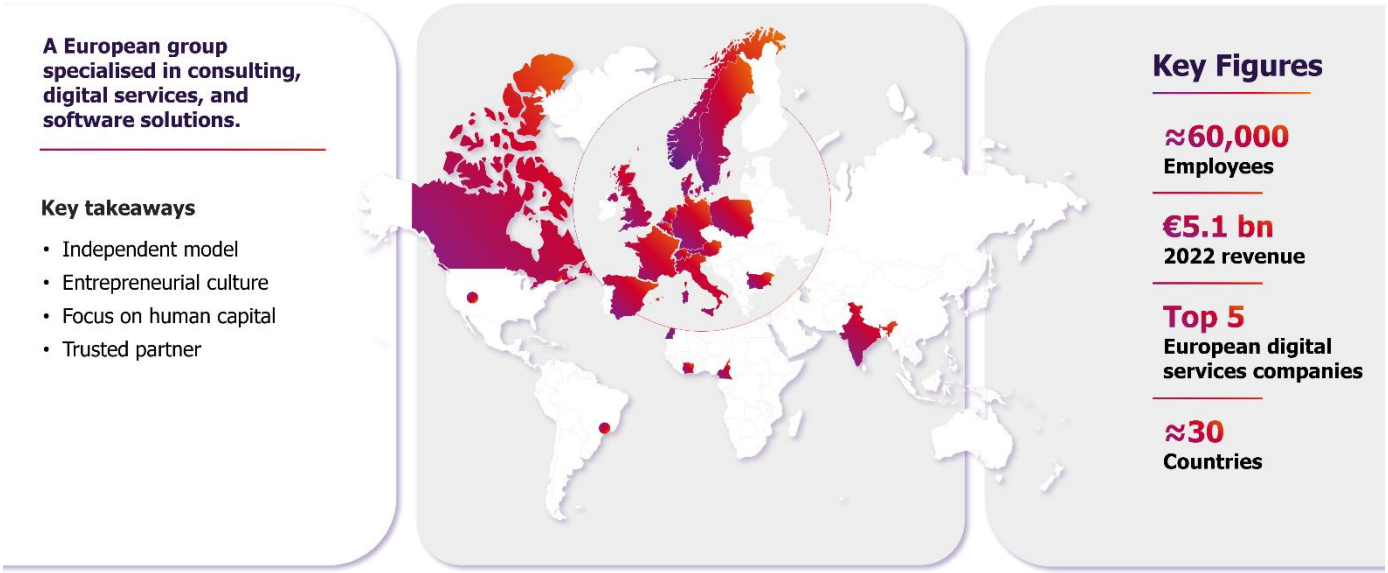
Sopra Steria

Contents

1 About Sopra Steria

1.1 Overview

Sopra Steria is a European tech leader recognised for consulting, digital services, and software development, helping our clients drive digital transformation to obtain tangible and sustainable benefits. We provide end-to-end solutions to make organisations more competitive by combining in-depth knowledge of a wide range of business sectors and innovative technologies with a fully collaborative approach. Sopra Steria places people at the heart of everything we do and is committed to making the most of digital technology to build a positive future for our clients. Our reach is illustrated below:

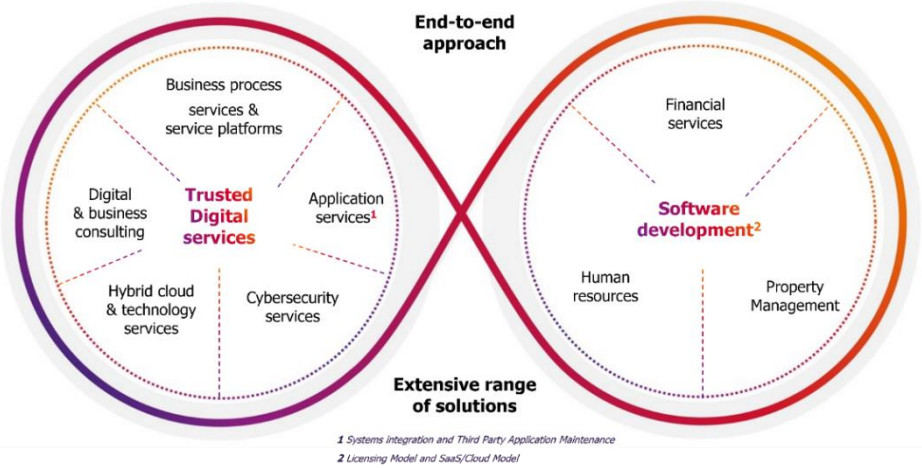


Making a difference is central to what we do and how we support our clients, and in turn, citizens. We reshape public services, making them more efficient to deliver and more accessible for the people that need them, across central and local government, devolved governments, and the wider public sector.

1.2 Our Cloud Capability

Our Cloud Centre of Excellence and cloud-enabled Practices serve clients across the public sector, delivered by a global team of cloud practioners, with certified resources in AWS, Microsoft Azure, Google Cloud, and Oracle Cloud.

Sopra Steria offers a comprehensive end-to-end offering, comprising trusted digital services and software development:



1.3 Our Credentials

Cybersecurity

Leader "Cyber resiliency services" (NelsonHall)

Cloud

Large account (best category>$250m) in the "Public Sector Industry Cloud Landscape" (Forrester)

Leader "Cloud public in Europe" (ISG)

Leader "Cloud Native Application" & "Application Transformation Services" (Quadrant)

IA

Leader "Intelligence Process Automation" (Quadrant)

Major player "European Professional Services for Data-Drive" (IDC)

Major contenders "AI services" & "Intelligent Process Automation services" (Everest)

Digital twins

Industrial metaverse

Partnership with Nvidia & SkyReal

Major Contender "Digital twin Services" (Everest)

IT for Green

Best in class "consulting and digital services for sustainable development" (PAC Innovation Radar)

Major Contender "NetZero Consulting Services" (Everest)

PAC IDC ISG Quadrant

Everest Group PEAK MATRIX NelsonHall FORRESTER

2 Service Overview

2.1 Service Description

Managed Security Service(s) are essential for organisations to protect their assets, maintain operational resilience, and safeguard customer trust. By leveraging specialised expertise, advanced technologies, and proactive security assurance measures, cybersecurity services can help organisations stay ahead of cyber threats and minimise the risk of cyber security incidents and data breaches.

Vulnerability management is the ongoing, regular process of identifying, assessing, reporting, managing and remediating cyber vulnerabilities across endpoints, workloads, and systems. Our security team will leverage a vulnerability management tool to detect vulnerabilities and utilise robust processes to assess, prioritise and co-ordinate their remediation.

2.2 Features

- Scope Discovery, classification & Contextualisation
- Defined Roles and Responsibilities
- Tooling – Solution design and implementation
- Scan scheduling & Execution
- Remediation Prioritisation and Co-Ordination
- Reporting
- Assurance Re-Scan

2.3 Benefits

- Continuous visibility of security posture of target solution
- Ownership of resolution prioritisation and co-ordination
- Provides a level of interaction that allows management to understand issues and the remediation action plan and status

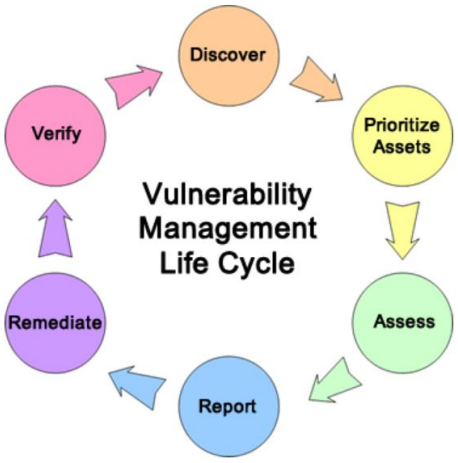
2.4 Our Approach

Our Vulnerability Management service resides in the Managed Security Services Pillar within the Cyber Security Centre of Excellence at Sopra Steria. We have a team of skilled security professionals who are dedicated to delivering an effective and efficient service. To ensure we stay ahead of evolving cyber threats and technologies, our team undergoes continuous training and certifications. This ongoing investment in their skills and knowledge enables us to provide you with the highest level of support and expertise.

Our Vulnerability Management services described are provided remotely within the UK and on-premise as required. All our staff are security cleared professionals, operating from different locations within the UK, allowing us access to a wider pool of talent and expertise allowing us to scale up or down quickly as needs change whilst providing our clients with greater flexibility to respond to changing security requirements. In addition, we can deliver service on-premise from our FSC location to allow us to operate in environments up to SECRET.

Our Security services are part of Sopra's UK ISO 27001 certification and adheres to Cyber Essentials Plus. Our staff and service are also on a continued journey to maintain alignment with the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)

Vulnerability management is an ongoing cyclical process of detection, assessment, remediation, and reassessment. It differs from Vulnerability Assessment which is a one-time evaluation of a host or network.



Scope Discovery, classification & Contextualisation

The Sopra Vulnerability Management Team will initially agree a high-level scope of the service with the client. This will typically take the form of understanding all environments within the scope of the vulnerability management service, including Cloud, on premise and hybrid environments together with their respective network address ranges.

Sopra Vulnerability Management Consultants shall seek to understand and document key and critical systems, Network access points, systems with external interfaces (Public IP Addresses) and any other data to aid in contextualisation and prioritisation.

An initial discovery scan of the agreed environments scope will be carried out to both verify and reconcile the accuracy of any asset database and to establish a base line of scanning scope to inform the future vulnerability scan scope.

Discovery scanning shall also form part of the regular scanning lifecycle to capture any changes in the scanning scope, positive or negative, to be reconciled against expected changes and aid in the detection of any rogue devices which may have appeared since the last scan cycle.

All activities will observe and be compliant with any locally mandated rules of operation, such as change management.

Defined Roles and Responsibilities

During service establishment the Security / Vulnerability Manager shall establish and maintain a document of key members of the team, both client, supplier and third party as required, together with their agreed responsibilities.

These may include, but not be limited to;

- Client Security Representative
- Security / Vulnerability Manager
- Security Engineering & Threat Management
- Service Management
- Environments Management
- Change Management
- Asset Management
- Technical Resources
    - Cloud
    - Server
    - Middleware & Database
    - End use devices
    - Networks
    - Applications
- Third Parties

This data shall be used to inform a detailed process and RACI matrix and aid in effective and timely remediation to any detected vulnerabilities and their effective contextualisation and priority.

Tooling – Solution design and implementation
Upon initial engagement, the Sopra's Vulnerability Management Team will immediately carry out a review of the existing IT environments and systems and document these in full. This will include any pre-existing vulnerability management tooling, should it exist. The resultant architecture and configuration data shall then be maintained throughout the life of the contract.

Any pre-existing vulnerability management tooling shall be assessed against the target scan scope to ensure suitability and compatibility and its configuration also reviewed against vendor best practice with any identified areas of improvement presented to the client for consideration ahead of implementation.

In the case where there is no pre-existing tooling to support the vulnerability management service, Sopra's Security Architects will design and solution a suitable technology solution, subject to agreement with the client's design authority. Our Security Engineering team will then implement, configure, and test the solution, working with respective technical support teams, such as Networks, to enable defined communications channels and server and end user device teams should any agent deployment be required.

Once fully tested and accepted, operational responsibility will then pass the Security/Vulnerability manager for ongoing management, scan scheduling and maintenance.

Scan scheduling & Execution

The Security/Vulnerability manager shall work to establish a robust scan schedule which enables the completion of discovery and vulnerability scanning to support organisations in delivering vulnerability management aligned to one or more of the following strategies:

- *Change Based*: In settings that employ high volume, rapid levels of change we would look to integrate the scanning schedule to form part of the deployment pipeline and assurance cycle of change. Thereby avoiding the unexpected introduction of unknown vulnerability and risk resulting from such changes.
- *Hygiene Based:* All software vendors are constantly monitoring their products and releasing security fixes to discovered vulnerabilities and flaws. Malicious threat actors are continually finding new and innovative means to compromise systems often utilising newly discovered vulnerabilities. New vulnerabilities are discovered every day, so even if no changes are deployed to client systems, they could become vulnerable overnight. Regular hygiene based scanning ensures organisations are made aware when their systems become vulnerable to new vulnerabilities. Scanning frequency would be agreed with the client in line with their defined risk appetite, but typically a monthly cycle would be recommended.
- *Compliance Based:* Clients may be subject to strict legal requirements, standards, or regulation (such as PCI-DSS, Cyber Essentials etc.) and in order to remain compliant with such standards, evidence of regular and effective vulnerability management is essential. The Sopra Steria Vulnerability Management Team work with clients to deliver an effective management regime and continuous compliance assurance.

The final documented schedule for scanning would be agreed with the client and managed and maintained by the Security/Vulnerability manager throughout the life cycle of the contractual agreement. Execution of scanning will operate in line with client processes for change as required.

Remediation Management

The Sopra Security/Vulnerability Manager will work with technical resource teams, Service management and third parties to raise, track, monitor and assure effective and timely remediation. Findings are rated from Critical to informational and together with the criticality of system will be used to inform risk level of the issue, which will then determine the response priority and actions to be taken.

Where recommended time scales cannot be met, the Security/Vulnerability Manager will work with technical teams and the client to agree an appropriate risk-based approach and time scale.

2.5 Inputs

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

- Solution Design – HLD and LLD
- Authority to liaise with teams that own the infrastructure and applications.

- Ability to escalate issues as required to resolve findings as quickly as possible.
- Authority to execute scans as required.

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 & Deliverables

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

- Executive Summary
- Status update of active remediation activity – Compliance view (RAG)
- New detections by criticality
- Vulnerability Trending analysis
- Details of new and emerging threats and Zero Days
- Top 10 Vulnerabilities by criticality (volume) (Unique & Detected)
- Top 10 Vulnerabilities by System (Volume) (Unique & Detected)
- Overall compliance score
- Actions log and status update.

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

2.7 Certifications & Skills

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

- ISO27001
- NIST CSF
- Cyber Essentials Plus

Plus, Individuals holding

- CISSP
- CISM
- CISA
- CRISC

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

2.8 Case Study

Introduction:
We provide a comprehensive Vulnerability Management service, which is a critical aspect of cybersecurity, helping organisations identify and remediate security weaknesses before they can be exploited by attackers.

Client / Challenge:
In 2022, Our client a pan European, manufacture of defence and space products, had several challenges in their vulnerability management process, which came to the forefront during the Log4J vulnerability, exposing thousands of systems to be potentially exploited by attackers. The main challenges our client faced were:

1. Lack of Visibility: Our client struggled to gain a comprehensive visibility into their vast network environment, making it difficult to prioritise and address vulnerabilities effectively.
2. Manual Processes: Manual vulnerability assessments and patch management processes were time consuming, resource intensive, and prone to human error, hindering timely remediation efforts.

3. Compliance Requirements: Regulatory compliance mandates required to maintain a robust vulnerability management program to protect sensitive data and adhere to industry standards.

With their a vast network infrastructure and a diverse range of IT assets across Europe, they recognised the importance of proactively identifying and addressing vulnerabilities to safeguard their sensitive data and maintain market value and trust.

Objectives:
To support our client in overcoming these challenges and enhancing the security posture and mitigate potential risks our Cyber Security experts in Vulnerability Management, using our structured process and procedures the following activities were conducted:

1. Assessment and Planning: Conduct a thorough assessment of the clients existing vulnerability management processes and requirements, followed by strategic planning for the implementation of the vulnerability management tool across the several technologies.
2. Configuration and Deployment: Configured according to the client's specific needs and requirements, the vulnerability management tool ensuring automated authenticated vulnerability scans across the entire network infrastructure.
3. Reporting and Metrics: Creation of detailed reporting and dashboards with metrics, which is critical component as it allows to assessment and effectiveness of the vulnerability management processes and controls.

Outcomes:
Our Vulnerability Management Consultants using market leading tools were able to enhance the security posture and mitigate potential risks, addressed security challenges and streamlined the vulnerability management processes, offering the following key features and capabilities:

1. Automated Scanning: Performed automated authenticated vulnerability scans across the entire network infrastructure, identifying potential security weaknesses and misconfigurations.
2. Reporting and Analytics: Our detailed reporting and dashboards offered a comprehensive reporting and analytics capability, providing actionable insights into vulnerability trends, compliance status, and remediation progress.
3. Risk Prioritisation: Our analysis of the vulnerability scan results provided a risk-based prioritisation of vulnerabilities, allowing our client to focus and plan remediation efforts on critical assets and high-risk vulnerabilities.
4. Processes: We implemented a new patch management process and streamlined the vulnerability remediation workflows using the client's ticketing platform.

Conclusion:
The deployment of our comprehensive Vulnerability Management service enabled our client to achieve greater visibility, efficiency, and effectiveness in identifying and addressing security vulnerabilities.
Our client enhanced their security posture, mitigated potential risks, and demonstrated their commitment to safeguarding sensitive data and maintaining regulatory compliance in an increasingly challenging threat landscape.

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: soprasteria-gcloud@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.