

Penetration Testing

Service Definition Document

Sopra Steria



Contents

- 1 About Sopra Steria 2
 - 1.1 Overview 2
 - 1.2 Our Cloud Capability 3
 - 1.3 Our Credentials 4
- 2 Service Overview 5
 - 2.1 Service Description 5
 - 2.2 Features 5
 - 2.3 Benefits 5
 - 2.4 Our Approach 5
 - 2.5 Inputs 10
 - 2.6 Outputs and Deliverables 10
 - 2.7 Certifications and Skills 10
 - 2.8 Case Study 11
- 3 Pricing 11
- 4 Next Steps 11
 - 4.1 Contact 11
 - 4.2 More Information 11

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





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)			
							

* Source PAC 2024

2 Service Overview

2.1 Service Description

Penetration Testing services provide the most effective way to accurately determine the risk that threats pose to an organisation. This is determined by simulating the activities of a threat actor, using the same tools and techniques that they would employ to identify and exploit vulnerabilities within the organisation's systems. The Sopra Steria Penetration Testing team can work with you to establish your needs and tailor a penetration testing activity. This will provide the answers you need, adding value to your organisation. Our goal is to provide a written report that details our findings and good practice recommendations for mitigation.

2.2 Features

- Network Vulnerability Assessment
- Network Penetration Testing
- Web Application Penetration Testing
- Mobile Application Penetration Testing
- Wireless Penetration Testing
- Simulated Phishing Campaign
- Tailored Testing or consultancy services creating a bespoke testing solution
- Onsite and Remote Testing capability.

2.3 Benefits

- Understand technical vulnerabilities of a system
- Capture and assess risk to target system
- Provide information and good practice to remediate findings
- Capture and understand security posture
- Programme of testing techniques can provide continual visibility of security posture.

2.4 Our Approach

Sopra Steria do not have a 'one size fits all' approach to security testing. We have found that close collaboration and consultation with customers and key stakeholders are key to an engagement. Our approach results in actionable information for the business, and successful delivery of all the customer's objectives.

After gaining a clear understanding of the customer's requirements, and agreeing the scope of the engagement, Sopra Steria will prepare a proposal summarising what is known about the target to be tested and provide a clear plan for achieving the objectives. Our proposal will detail the agreed targets, the required outcomes and deliverables, any pre-requisites which need to be achieved before testing can take place, any necessary resources, and the associated costs.

Once all parties have agreed the delivery plan, and a signed copy of the proposal has been returned to Sopra Steria, consultants will be assigned to the engagement and a schedule for delivery will be agreed.

Throughout the period of testing, Sopra Steria consultants will liaise closely with the customer's stakeholders as necessary to minimise and address any challenges that arise, alerting the customer to any identified high risk issues that could require immediate attention.

Network Vulnerability Assessment

In contrast to penetration testing; which involves focussing on one or two key weaknesses and attempting to leverage them to gain additional access; a network vulnerability assessment is very much a 'one shot' engagement, where the aim is to report all of the potential vulnerabilities within a system or network which can be identified by automated means.

Because of the automated nature of the engagement, there is little opportunity for variances within the methodology, therefore a vulnerability assessment will generally contain the following activities (although this is dependent on the exact tooling used to a degree):

Mapping the attack surface

Accurately mapping the in-scope target networks and systems is key to understanding potential vulnerabilities and their impact. Identifying and categorising 'live' (i.e. responding) hosts, determining what services they expose, and fingerprinting operating systems and installed software versions, allows the vulnerability assessment tools to target the checks and tests to be performed, rather than simply running every test possible.

Identifying potential vulnerabilities

Automated vulnerability scanning tools will then rapidly appraise the target systems, identifying potential security misconfigurations, missing patches, or vulnerable services, which could allow an attacker to gain a foothold within a target system.

Verifying identified vulnerabilities

Where time constraints and network access allow, Sopra Steria consultants will use the same tools and techniques as a malicious threat actor to verify any identified vulnerabilities and remove false positives. In this way we can be sure that we are presenting only actionable intelligence within the report. This is in stark contrast to some of our competitors who consider the job 'done' when they simply deliver the output from the automated tools with no further effort put into reviewing the results for accuracy. If the Customer requires a more thorough exploration of any identified vulnerabilities Sopra Steria can provide a separate proposal for delivering a thorough penetration test of the network or affected systems.

Network Penetration Testing

Penetration testing is a cyclical process, involving a methodical approach to vulnerability identification and exploitation. Unlike a Vulnerability Assessment; where the aim is to report all potential vulnerabilities within a system or network; penetration testing involves focussing on identified weaknesses and then attempting to leverage them to gain additional access where appropriate. Where such access is obtained, or a vulnerability reveals additional information about the target, the process begins again.

Whilst, broadly speaking, the path of a penetration test will vary depending on the nature of the targets and the vulnerabilities that are identified, there are some common activities which will be undertaken:

Mapping the attack surface

Accurately mapping the in-scope target networks and systems is key to understanding potential vulnerabilities and their impact. Identifying and categorising 'live' (i.e. responding) hosts, determining what services they expose, and fingerprinting operating systems and installed software versions, allows the consultants to create a detail-rich list of targets which may offer a route into the network.

Identifying potential vulnerabilities

Automated vulnerability scanning tools are used to rapidly appraise the target systems, identifying potential security misconfigurations, missing patches, or vulnerable services, which could allow Sopra Steria Penetration Testing Consultants to gain a foothold within a target system. Manual testing of exposed services is also used to enumerate sensitive information about the target systems and users such as valid hostnames and usernames, exact software versions, password policies, domain groups and group membership, all of which will be useful in latter stages of the engagement.

Verifying and exploiting vulnerabilities

Using the same tools and techniques as a malicious threat actor, Sopra Steria Penetration Testing Consultants will explore and verify any identified vulnerabilities, where appropriate vulnerabilities will be exploited to gain further access to the network or target systems. Custom exploit code may be developed or publicly accessible exploits used to help assess a specific vulnerability.

Escalating privileges

Successful exploitation of a vulnerability may only provide an attacker with low-privileged access, limiting the damage that they can do or the data that they can access. Their aim will be to gain the highest level of privilege possible to enable them complete control over - and access to – the network, its systems, and its data.

Sopra Steria Penetration Testing Consultants will try to gain privileged access within the target systems or network following exploitation of a vulnerability. This could involve re-using poorly secured authentication tokens, exploiting

trust relationships between a compromised device and other in-scope targets, moving laterally to less secure connected assets, or creating chains of exploits to leverage multiple vulnerabilities in sequence.

Web Application Penetration Testing

Penetration testing is a cyclical process, involving a methodical approach to vulnerability identification and exploitation. Penetration testing involves focussing on key weaknesses and attempting to leverage them to gain additional access. Where such access is obtained, or a vulnerability reveals additional information about the target, the process begins again.

Whilst, broadly speaking, the path of a web application penetration test will vary depending on the nature of the targets and the vulnerabilities that are identified, and tends to be broader in nature than that of a network penetration test, there are some common areas of application security upon which all tests will focus:

Application hosting platform and technologies

A minimal attack surface, and well maintained applications and application servers, are key defences against web application attacks. The application server will be assessed to ensure that only those protocols required for hosting of the application are exposed, and that all exposed services are configured securely and in accordance with established good practice. Where possible, the Operating System's likely version and patch level will be assessed.

Requests to, and responses from, the application server will be checked to ensure that they implement modern security controls designed to protect application users and data.

Data exposure

Sopra Steria Penetration Testing Consultants will look at the methods being used to protect data being transmitted between the application server and the user's browser. Where deployed, the TLS configuration will be reviewed to ensure that the chosen protocols and ciphers are robust and sufficient to protect user data. TLS certificates will be examined to ensure that they are correctly formatted and provide the necessary assurance for end users.

Content exposed by the application or its server (for example web pages, directory listings, server banners, error messages) will be reviewed to ensure that it does not provide an attacker with information about the application or its hosting environment which could assist them in targeting their attacks against the platform.

Access controls and authentication

The application will be tested from an unauthenticated perspective to ensure that an anonymous attacker cannot bypass or otherwise subvert the authentication mechanism. Attempts will be made to enumerate valid user names, and to conduct brute force attacks against the login functionality. Authenticated testing will also be conducted; consultants will look at elements including session management and storage, password rules and quality, and password recovery functions.

Authenticated testing will also be conducted from multiple user accounts. Our Penetration Testing Consultants will ensure that application enforced segregation of data or functionality (for example according to a user's role, or to some business unit restriction) cannot be bypassed. Our Consultants will attempt to bypass restrictions on user permissions, and to gain access to administrative functions with 'standard' user accounts.

User input validation

Scripting and injection vulnerabilities are often amongst the most serious encountered during web application security testing. Scripting vulnerabilities such as Cross-Site Scripting (XSS) or Cross-Site Request Forgery (CSRF) could allow an attacker to cause malicious script to run within a user's web browser – the effect of this could be the theft of sensitive data, defacement of the application, or unauthorised access to the user's session. An injection vulnerability could be used to run commands on the underlying web server, bypass authentication controls, or access sensitive data, and will often lead to a complete compromise of the application.

Mobile Application Penetration Testing

Penetration testing is a cyclical process, involving a methodical approach to vulnerability identification and exploitation. For mobile applications, the aim of testing is to identify any weaknesses within the application and its hosting infrastructure, and then to leverage those weaknesses in an attempt to gain additional access to data and systems. Where such access is obtained, or a vulnerability reveals additional information about the target, the process begins again.

Whilst, broadly speaking, the path of a mobile application penetration test will vary depending on the nature of the targets and the vulnerabilities that are identified, there are some common activities which will be undertaken:

Mapping the attack surface

Accurately mapping the application's user interface, together with any external systems it integrates with, is key to understanding potential attack vectors and possible risks to the application and environment. Identifying and categorising the features and functionality, together with the web services they call, allows the consultants to create a detail-rich list of targets to test that may offer potential for exploitation.

Identifying potential vulnerabilities

Using mostly manual methods, supplemented by automated tools where appropriate, the mobile application is tested for vulnerabilities in areas such as authentication and authorisation, user input validation, encryption of data at rest and in transit together with separation of data and functionality between different accounts and roles. Checks are made for common application vulnerabilities such as SQL injection and logic flaws, as well as reviewing the endpoints for potential security misconfigurations, missing patches, or vulnerable services that could allow Sopra Steria Penetration Testing Consultants to gain a foothold within the target system.

The application programming interface (API) the application interfaces with, hosted by the web services running on the end-points servers, are assessed for injection and functional flaws together with the authentication and encryption methods it employs.

Verifying and exploiting vulnerabilities

Using the same tools and techniques as a malicious threat actor, Sopra Steria Penetration Testing Consultants will explore and verify any identified vulnerabilities. Where appropriate, vulnerabilities will be exploited to gain further access to the application, data or target systems. Custom exploit code may be developed or publicly accessible exploits used to help assess a specific vulnerability.

Escalating privileges

Successful exploitation of a vulnerability may provide an attacker with unauthenticated access to a user's account and data, or more seriously, access to all other users' accounts and data. Additionally, should flaws be identified within the remote web-services or their end-point servers, the attacker may gain a foothold within the infrastructure itself, allowing them to progress further into the corporate environment, its hosts and data.

Sopra Steria Penetration Testing Consultants will try to gain privileged access within the target application and network, attempt to move laterally within the application and supporting hosts. This could involve re-using poorly secured authentication tokens, exploiting missing patches on end-point servers or finding a remote code execution vulnerability with the web-services used by the mobile application.

Wireless Penetration Testing

Penetration testing is a cyclical process, involving a methodical approach to vulnerability identification and exploitation. Penetration testing involves focussing on weaknesses and attempting to leverage them to gain additional access where appropriate. Where such access is obtained, or a vulnerability reveals additional information about the target, the process begins again.

The path of a wireless penetration test will vary depending on the nature of the targets and the vulnerabilities that are identified, however, there are some common areas of application security upon which all tests will focus:

Protection against unauthorised access

Sopra Steria Penetration Testing Consultants will attempt to gain 'unauthorised' access to the target wireless networks. Consultants will assess the authentication mechanisms in place (for example whether the network use a static pre-shared key or requires presentation of a valid certificate) and attempt to either bypass them or leverage any weak configuration discovered. Where pre-shared keys are used, our Consultants will assess their complexity, and seek to understand what processes are in place for managing/changing them. Captive portals, such as those typically used to provide authentication in hotels or on organisations' 'Guest' networks, will be assessed to ascertain whether they adequately protect the networks from unauthorised access.

Network isolation and protection

Sopra Steria Penetration Testing Consultants will look for the presence of other networks connected to, or accessible from the in-scope wireless network. This stage helps to ensure, for example, that 'Guest' and BYOD networks are not connected directly to business critical networks or those which might contain or process sensitive data. It also allows our Consultants to identify the corporate networks' exposure in the event that an unauthorised client is connected to corporate wireless networks.

This is an essential test if an organisation maintains PCI-DSS accreditation to ensure that wireless networks do not facilitate access to the Cardholder Data Environment (CDE).

Client isolation and protection

Sopra Steria Penetration Testing Consultants will review the measures in place to segregate wireless clients once they are connected to the network, and to protect clients from attacks launched against them by other connected clients. This is particularly important in 'Guest' or BYOD networks where the clients themselves may not be subject to the same strict security controls and patching regimes as corporate end-user devices.

Unauthorised ('rogue') wireless access points

Sopra Steria Penetration Testing Consultants will review the wireless access points which are broadcasting within the organisation's location during the time of the assessment. The list of access points will be reviewed with the customer to identify any which are either a) simply unauthorised within the location (for example a personal access point on a mobile device, or an unauthorised incoming Internet connection being broadcast wirelessly), or b) which are unauthorised and are pretending to be a legitimate corporately deployed wireless access point.

Where necessary, our Consultants will attempt to triangulate the position of any identified wireless point in coordination with the customer's technical team.

Sopra Steria Penetration Testing Consultants will also deploy their own rogue access point during the course of the test and check that corporate assets, which are often pre-configured to automatically connect to corporately deployed wireless networks, cannot be forced to connect to the rogue access point in preference to the authorised ones.

Testing for the presence of any rogue access points is a crucial part of any PCI-DSS assessment; unauthorised access points connected to a Cardholder Data Environment network could be used to provide insecure and unauthorised access to PCI data.

Optional site survey

Sopra Steria Penetration Testing Consultants can conduct a wireless survey of the customer's premises to determine to what extent the signal broadcast by wireless access points extends beyond the physical boundaries of the location.

Optional end user device assessment

Our Consultants will take a 'standard' end user device, such as a laptop, which is in use by the business and assess the security of its presentation on the wireless network. Using techniques typically employed during a network penetration test, our Consultants will test the end user device remotely across the wireless network to identify any vulnerabilities that could be leveraged by an attacker sharing the same network as the device. This will allow the business to have confidence that the devices are secure from attacks directed against them whilst connected to public wireless networks, such as those found in hotels and coffee shops.

Simulated Phishing Campaign

Achieving a high success rate (where success is measured by numbers of users who succumb to the lure) in phishing campaigns requires a certain degree of collaboration with the customer and the project's stakeholders. Often only a limited number of individuals from the customer are involved so that chances of awareness that the exercise is imminent, is minimised.

Phishing campaigns vary depending on the reasons behind the exercise, however, there are some common activities which will be undertaken:

Baiting the hook

A compelling theme is crucial for a successful campaign. Sopra Steria Penetration Testing Consultants will liaise with the customer to create a theme for the campaign that aims to attract most readers to the corresponding website. Themes may offer employees benefits or vouchers if they sign-up (people love free stuff), or may tie-in with upcoming product releases or events that may capture the reader's attention.

Our Consultants will purchase a suitable domain name tailored to match the campaign theme, and will then design, build and host a website containing a small number of fields for the unsuspecting visitor to complete and submit.

Swim selection

The customer may be asked to provide Sopra Steria with a list of names and email addresses to use, or the Consultants will perform an OSINT gathering exercise - utilising the power of search engines and other tools to scour the internet

for names and email addresses associated with the customer's organisation, for example, those found in LinkedIn profiles.

Some customers are happy for all users discovered to be included, to make the campaign as realistic as possible, whereas others like to vet the list first, possibly removing any very senior members of staff (who, interestingly enough, can often be the first to click on links in an email).

Casting

Prior to launching the campaign, our consultants will work with the customer to ensure that the phishing email does in fact make it through to their desktop, adjusting the contents so that it is not identified as SPAM or malicious by any security systems currently in place. Occasionally it is necessary for the Sopra Steria source email address to be whitelisted by such systems to help ensure it will reach the target audience.

The email will then be sent to all recipients at the agreed time. The phishing platform used for the engagement provides real-time information so that activity can be monitored, including logging the location of the user opening the email. The campaign may be enabled for a few hours, or in some cases a few days in order to achieve the largest number of participants possible. Our consultants maintain close contact with the customer and can shut the campaign down instantly if necessary.

2.5 Inputs

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

- A conversation about the security requirements for the testing; the questions to answer
- Technical details of the target solution
- Provision of agreed dependencies to enable testing.

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

2.6 Outputs and Deliverables

A selection of the outputs and deliverables generated from the service is detailed below:

- The primary deliverable will be a report written by the lead consultant for the engagement. The report will include a narrative summary of the engagement's findings, drawing out high level themes along with providing any strategic recommendations for improvements. This section will also call out any particularly critical or sensitive findings from the report.

The report will also provide detailed information on each of the issues identified during testing, provide technical information describing how they were leveraged, and include screenshots or other supporting evidence to help illustrate the issue and aid understanding. Alongside each specific finding we will provide recommended mitigations, and also links to additional references.

- During testing execution the delivery team will notify the client of any High/Critical findings immediately.

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:

- CREST
- Cyber Scheme Team Member
- Cyber Scheme Team Leader
- GIAC Cloud Penetration Testing.

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

2.8 Case Study

Client: Government Department, November 2023.

The challenge: The solution was due to go live to the public and the penetration testing executed was not acceptable to the accreditor and a more in depth assessment was required. This was to be captured, scoped and executed in a short period of time to enable the solution to go live.

What we delivered: Sopra Steria's Penetration Testing Consultants captured the security requirements and crafted a scope that meant several consultants were deployed simultaneously across the country in order to execute an activity that covered all areas of concern for the solution owners and accreditors.

Outcome:

- Testing was completed and the report issues, contextualised on the deployment of the particular solution
- Identified risks were understood and then mitigated or accepted
- The solution went live to the public on the expected date.

3 Pricing

Please refer to the Pricing Document for this Service.

4 Next Steps

4.1 Contact

Please contact ukpt@soprasteria.com if you would like to know more about this service.

Please contact us if you would like to know more about 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](#).

