The world is how we shape it

Cybersecurity

Penetration Testing Services

A risk based approach

Sopra Steria follows a Risk Based Approach that reveals business risks and not just technical vulnerabilities. Our security experts understand the business process and deliver valuable results based on real scenarios. Different risk rating methodologies (CVSS, OWASP) are used based on company specific factors.

The different penetration tests scenarios

- **Internal testing:** to simulate the damage a disgruntled employee could do on your systems.
- **External testing:** to simulate an outside hacker attacking your public facing infrastructure.
- **White box testing:** the tester has been provided with some information regarding the target network before starting work.
- **Black Box / Blind testing:** the tester has been provided with very limited data or none before the test procedure takes place.
- **Double blind testing:** the company's blue team is unaware of the attack and its response capabilities are tested.

Traditional Pen Test	Risk-based Pen test
Focus is on technical vulnerabilities	Focus is on business risks
Severity levels are based on technical parameters	Severity levels are based on business risks
Risk levels in report are assigned post facto	Risk levels in report reflect the levels assigned prior to testing
Test cases are build based on testing methodologies	Tests cases additionally build on risk scenarios
Usually, the report is directed to the IT and Security teams	The report is also directed to the business process owners and heads of departments
Understanding the regulatory environment is good	Understanding the regulatory environment is mandatory
Requires technical know-how	Requires both technical and business process know-how

Methodologies

- OWASP (Testing Guide, Risk Rating, Top 10, ASVS)
- CVSS
- CWE/SANS TOP 25 Most Dangerous Software Errors
- Penetration Open Source Security Testing Methodology Manual (OSSTMM)
- Testing Execution Standard (PTES)

Penetration Testing

Sopra Steria takes the time to understand your business needs and think like a real attacker. This allows us to gain a **holistic business overview**, as well as a **technical** point of view. We will first identify the weakest link that may cause a severe impact to the organization, and then escalate to gain privileged access to information or systems.
Our services are based on a hybrid approach composed of **automated** and **manual tests**. Tests will be conducted in a controlled and **safe manner**. For successful exploited vulnerabilities, our penetration testing experts will attempt further actions to increase their presence and gain elevated privileges.

Web Applications
Web services and APIs that may be used to store and access critical business information are assessed with the goal to identify and exploit vulnerabilities and gain access to sensitive data.
Mobile Applications
Access to your mobile applications to identify and exploit vulnerabilities related to mobile computing environments.
Network & Infrastructure
Assessment of your internal or external infrastructure and the ability to withstand attacks. Our penetration experts will attempt to break into your infrastructure by exploiting vulnerabilities, as well as end-user security policies.
Wireless Networks
Wireless penetration testing includes identifying and exploiting vulnerabilities in the access points that may result further access to the company's internal network.

Vulnerability Management

Vulnerability Assessments is a good starting point for organizations who are aware their security posture needs improvement.
Issues are categorized based on criticality. **We will first identify the most serious vulnerabilities** and recommend mitigation actions.
Minimization or decrease of business cyber risks depends on many factors such as technical and business impact and the likelihood of an event.
As an added value, Sopra Steria security experts will **analyze** and **consult** your organization on current **vulnerabilities** and recommend **solutions** to decrease your risks.

Social Engineering

Evaluation of your employees' preparedness to identify and respond to Social Engineering attacks. Sopra Steria uses real-world use-cases and scenarios (e.g. advance reconnaissance, phishing, vphishing, etc.) to launch effective social engineering campaigns.

- Email Phishing with Website Mirroring
- Email Phishing with Attachments
- Email Phishing with Hyperlinks
- Email Phishing with File Download
- USB Drop
- Voice Phishing (Vishing)
- Staff Impersonation & Physical Security Controls

SERVICE-SIDE EXPLOITATION

Remote code execution

Buffer overflow

Code Injection

Web Application exploitation (XSS, SQLi, XXE, CSRF, LFI, RFI, and more)

NETWORK MANIPULATION & EXPLOITATION

VLAN Hopping attacks

Man-In-The-Middle attacks

Routing attacks

IDENTITY & AUTHENTIFICATION WEAKNESS EXPLOITATION

Default usernames and passwords

Weak and guessable user credentials

PRIVILEGE ESCALATION

Race conditions

Kernel attacks

Local exploit of high-privilieged programs or services

Red Teaming

Red Teaming is a full-scope, multi-layered attack simulation designed to measure how well your People, Processes and Technology controls, withstand an attack from a real-life adversary.

Preparation

Before engaging in any activity it is essential to assess the company's current needs and scope of the actions that will be undertaken. Limitations such as duration, the legal boundaries and prohibited actions must be determined.

Execution

Execution consists of:

- Reconnaissance
- Exploitation
- Privilege Escalation
- Lateral Movements
- Establishing Persistence
- Command and Control (C&C)
- Operational Impact.

Analysis and Reporting

All findings will be documented in a final report based on scoring from international security standards presenting the business risk.
The identified vulnerabilities will be evaluated. Tailor-made recommendations and remediation actions will be proposed.
They will be prioritized according to the associated risk.

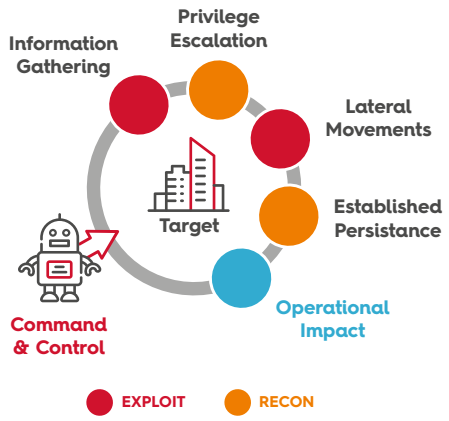
The final report will be discussed with the Organizations' Security Team. The report will include a comprehensive executive summary of the executed Red Teaming actions.
All detailed results with respective evidence and proof of concept will be included.

Lessons Learned

Red teaming is offensively oriented, but it is also a great tool to improve overall security posture, both technical and organizational.
A workshop with all necessary representatives will be organized at the end of the engagement.

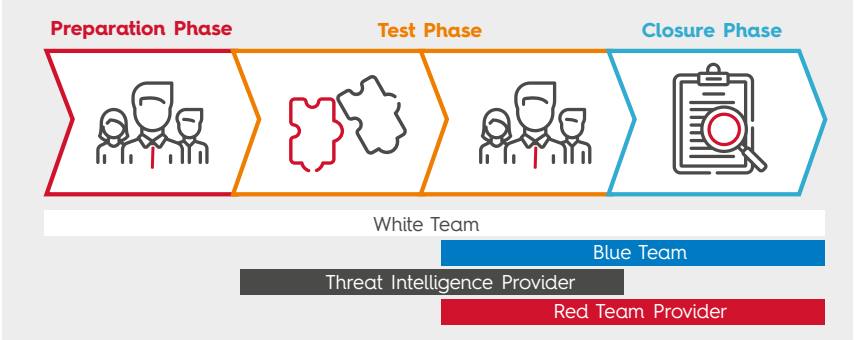
The workshop's main objective is to:

- Present all actions performed by the red team.
- Describe actions undetected by blue team.
- Find what detection mechanisms and procedures failed and why.
- Create lessons learned and improvement actions.



Sopra Steria as a TIBER Provider

Sopra Steria using a combination of all mentioned services and extensive knowledge from large scale IT projects offers Threat Intelligent and Red Teaming Services as described on TIBER-BE with the highest international security standards.



Sopra Steria

Sopra Steria, a European leader in digital transformation, provides one of the most comprehensive portfolios of end to end service offerings on the market: Consulting, Systems Integration, Software Development, Infrastructure Management and Business Process Services. Sopra Steria is trusted by leading private and public-sector organisations to deliver successful transformation programmes that address their most complex and critical business challenges. Combining high quality and performance services, added-value and innovation, Sopra Steria enables its clients to make the best use of digital technology.
With 45,000 employees in more than 25 countries, Sopra Steria generated revenue of €4.1 billion in 2018.

Sopra Steria
15-23 Avenue Arnaud Fraiteurlaan
1050 Brussels - Belgium
T. +32 (0)2 566 66 66
contact-benelux@soprasteria.com
www.soprasteria.com

sopra steria