



SCI

CYBERSECURITY



About us

SCI is a **multinational company** specialized in information technology and **cybersecurity** services, formed by a team of **professionals** with extensive experience.

Our portfolio consists of more than **16 years of experience** which enable us to meet all needs regarding prevention, contingency and persistence, as well as customized training.

Audits, analysis and solutions in sectors such as industrial, financial, pharmaceutical, chemical, public administration and services speak for us.

Our main goal is the rethink of how to **tackle** current and future threats, bring the term security closer to companies without interfering with their **professional activities**.



BASIC PILLARS OF SCI RISK APPROACH STRATEGY



SECURITY

A secure company should focus on **protecting** the most risk-sensitive resources which are critical to its **performance** and **image**.



SURVEILLANCE

To establish a general awareness of permanent risk across the **organization**. To **develop** some behaviour patterns that could **predict** risky situations.



RESILIENCE

To have the **ability** to contain the damages **quickly** and mobilize the necessary resources in order to **minimize** impacts.



TRAINING

Inadequate **training** of internal employees or collaborators on various types of **profiles** may cause that all applied efforts both **technical** and **human** would come to nothing.



PERSISTENCE

The **security** of your assets, today protected, within a few months, weeks, even days may no longer be so. Classical audits are no longer sufficient. An audit without **persistence** has an expiration date with an increasingly shorter length. New **attack methods** and threats that emerge every day make that the automated solutions **provided** by other companies do not allow facing up to this dynamics on equal terms. **SCI** customizes persistence by **analysing** each individual case and emphasizing the **human factor** as essential point.



WHO CAN BENEFIT FROM OUR SERVICES ?

Large, medium and small organizations from all areas and sectors that want to improve and **protect** their business continuity, protect their customers and suppliers' reputation as well as their own.

Those organizations that want to take **proactive** measures to identify which of their assets are most vulnerable, to understand why they can be **compromised** and use this **information** to **improve** their processes when making decisions.

PROJECT METHODOLOGY

SCI has its own and exclusive **methodologies** (R&D) for implementing **solutions**, in **compliance** with **quality standards** that guarantee the proper **development** of a comprehensive security project at all stages, as well as its **sustainability** in the future.

This sustainability is based on risk **identification** and rating, taking into account the specific **typology** and conditions of each business or scope of action, **planning** accordingly all its development. Everything will be much more effective if it is conceived and designed considering the activity or **business** in particular and not using it simply as the same regular pattern for all situations*.



WWT

We Work Together

*Nowadays most companies in the same sector base their methodology on the result of information extracted through fully automated tools, of which a consultant may have neither made a correct interpretation and assessment, nor taken into consideration the real needs of the audited company, by simply processing massive data.



SOLUTIONS AND SERVICES

SOLUTIONS



Solutions and services that enable your company to meet all needs in terms of **security, integrity, prevention, correction, contingency and persistence.**

- Penetration testing (pentest)
- Black box audit (external)
- Red Team / Blue Team
- Web application audit
- Security incidents response
- Computer forensics
- Data loss prevention audit (DLP)
- WIFI, RDIF, VoIP, Satellite audit
- APT analysis (persistent threats)
- APPS and source code audit
- BYOD,MDM audit and policies
- Security policies audit
- OSINT Social engineering
- SSL/TLS audit (certificates)
- Stress test audit, DoS test
- IDS,IPS,FW,VPN and WAF layers audit
- Identity Management analysis (IAM)
- Cloud services and SaaS analysis
- Visibility analysis
- Analysis of false positives and negatives
- Active Directory, GPO, analysis
- LSSI, GDPR, PCI-DSS compliance

TECHNOLOGY



Comprehensive **consulting** of physical **security** tools.

- Internal security
- Perimeter security

SOFTWARE



Integration and **implementation** of specific logical **security software.**

- Anti-malware software
- Monitoring software
- Alert software
- Control software

TRAINING



Customized **training** and risk awareness adapted to the **expertise** of each profile among the users who work for the **company.**

SCI OVER THE WORLD

BARCELONA • MADRID • CANARY ISLANDS • MEXICO CDMX • LISBON

