Inside

INTELLIGENCE & SECURITY INVESTIGATIONS

InsideCyberSecurity

www.inside.agency • info@inside.agency

Your new choice for risk management

ABOUT US

INSIDE gathers information, at a national and international level, that is useful to companies for risk management, in compliance with regulations, professional ethics and corporate governance standards. The information is used to assess the economic, financial and reputational risks of organisations and individuals with whom the company may establish business relations.

This series of information allows **strategies and techniques to be prepared to counteract the dangers** inherent in various market sectors (pharmaceuticals, automobiles, insurance, finance, government...), which can affect small businesses as well as larger companies.

Reports can also be prepared on **politically exposed persons** (PEPs), who hold or have previously held public office, and are therefore more exposed to the risk of committing certain crimes, such as corruption, bribery or money laundering.

INSIDE **helps organisations to know their business partners**, guiding their activity towards more informed decisions, through a range of services that ensure regulatory compliance and fulfilment of legal and auditing requirements (regulations of the Foreign Corrupt Practices Act - FCPA, the UK Bribery Act, Anti-Money Laundering – AML controls, the USA PARTRIOT Act and Countering the Financing of Terrorism – CFT controls); the research conducted - which can cover all market sectors and any organisation, regardless of its size - provides a thorough check on potential business relations, highlighting any risks of corruption arising from a geopolitical analysis of the case.

The reports provide all information on a company and its directors, activities, history, administration, conflicts of interest, financial liabilities, legal and judicial affairs (compliance risk), and reputational risk. They also include verification of statements by the administrators, compliance with anti-money laundering (AML) rules, anti-corruption controls, FCPA and UKBA rules, sanctions against Iran, and International and US due diligence procedures.

INSIDE reports are generally recommended for verification of financial crimes, but are not limited to this: the research by INSIDE provides **a valid solution in situations of geopolitical risk** (high-risk countries) regarding a transaction or an individual involved in it, for supply chain and due diligence checks, before major investments such as mergers or acquisitions, and for **an integrated compliance programme**.

INSIDE conducts the investigations itself, thereby maintaining a high level of quality and efficiency, with access to a large number of **operators located across five continents and speaking over 60 international languages**; it also uses native speaker professionals, who can grasp language nuances that are often incomprehensible to those outside of a particular culture. The information and “open source” data collected is abundant and of high quality, as the various sources used are constantly updated with foreign official information.

INSIDE's Cyber Security Division is aimed at combating computer crime and provides assistance not only in support of law enforcement activities but also to companies.

Attention to **Information Security** is increasing rapidly, since it is impossible to think of managing business activities today without the help of computer systems, which are now essential tools in the production processes of companies.

It is therefore important to find professional help for defence against computer attacks that could seriously threaten your most important asset: **your know-how**.

INSIDE's Cyber Security Division can detect the **level of vulnerability** of your systems and perform a careful diagnostic analysis to identify the appropriate steps for ensuring the safety of your information property.

The main objective of the INSIDE Cyber Security Division, with its experience acquired in the industry, its high quality and safety standards, and the support of its highly qualified technical staff, is to analyse and strengthen the **security of your company's IT infrastructure**, for which it has developed a series of specific services.

After each activity, the INSIDE Cyber Security Division issues a report containing details of all the operations carried out and providing all the necessary solutions for the total security of your company.

Services

The services offered by the INSIDE Cyber Security Division are designed to achieve the following objectives:

VULNERABILITY ASSESSMENT AND MITIGATION
- Assessment of the strength of the security system in use
- Identification of known vulnerabilities
- Implementation of countermeasures

PENETRATION TEST
- Assessment of the strength of the security system in use
- Identification of the weaknesses of the platform through a simulated attack

WEB APPLICATION PENETRATION TESTING
- Identification of vulnerabilities in web applications
- Resolution of the problems detected

THREAT DETECTION & ANALYSIS
- Identification and analysis of hostile hardware or software devices

ETHICAL HACKING
- Identification of the exposure risk of the computer system to hostile technological and/or human events

CODE REVIEW
- Detection of vulnerabilities in the source code

SECURITY EVALUATION
- Assessment of the security level of hardware and software applications, processes and platforms

IT RISK MANAGEMENT
- Identification of risks from corporate IT investments
- Defining strategies to govern them

SECURITY AUDIT
- Accurate identification of vulnerabilities in the computer system
- Increasing the capacity for assessment of the risks it contains

HIGH LEVEL SECURITY CONSULTING
- Provision of advice on computer security issues

The following section of this document describes the methods used and the characteristics of the activity carried out, together with the procedures followed regarding the delivery of the final report to the Client.

1. AREA OF INTERVENTION

The intervention requested will focus on the technology structure used by the Client, namely:
- the computer system
- internal and external infrastructure
- networks
- hardware/software devices
- web applications used by the Client

2. METHODOLOGY

The INSIDE Cyber Security Division has a group of experts specialised in the field, with a series of internationally accredited certifications.

Image 1. Main international standards

More specifically, it carries out its professional activity in the strictest compliance with the following standards:

- ISO/IEC 19011:2003 – Guidelines for quality and/or environmental management
- ISO/IEC 20000-1:2005 – Service management – Part 1: Specification
- ISO/IEC 27002:2005 – Code of practice for information security management
- ISO/IEC27004:2009 – Information security management – Measurement
- ISO/IEC 27005:2008 – Information security risk management
- BS25999-2:2007 – Business continuity management – Specification
- COBIT v4.1 – Control Objectives for Information and related Technologies
- OSSTMM v3 – Open Source Security Testing Methodology Manual
- OWASP Testing Guide v3 – Open Web application Security Project Testing Guide
- CC v3.1 – Common Criteria
- CEM v3.1 – Common Methodology for Information Technology Security Evaluation
- ITIL v3 – Information Technology Infrastructure Library
- PCI-DSS v2.0 – Payment Card Industry Data Security Standard
- Basilea2 – International Convergence of Capital Measurement and Capital Standards
- SOX of 2002 – Public Company Accounting Reform and Investor Protection Act
- Legislative Decree 231/2001 – Administrative liability of legal persons, companies and associations without legal personality
- Legislative Decree 196/2003 – Personal data protection code
- Legislative Decree 262/2005 – Protection of savings and regulation of financial markets
- Legislative Decree 81/2008 – Protection of health and safety in the workplace;

2.1 METHODOLOGICAL REFERENCES

2.1.1 OSSTMM

The OSSTMM (Open Source Security Testing Methodology Manual) is a certification provided by ISECOM (the Institute for Security and Open Methodologies), an international community for research and collaboration on security, established in January 2001.

It is a peer-reviewed methodological approach used in the field of computer security systems and is based on performing security tests and analysis on infrastructure and IT assets to arrive at verified facts; these facts provide useful information in measurable terms for the improvement of operational security.

The use of the OSSTMM standard, in compliance with relevant regulations, allows the achievement of consistent and repeatable results, providing an understanding of the countermeasures to be implemented, the extent to which the system is exposed to possible attacks, and therefore how to achieve maximum security.

2.1.2 OWASP

The **OWASP Testing Guide** is a framework for testing the security of applications and network infrastructure developed by OWASP (The Open Web Application Security Project), a non-profit foundation whose activities are centred on the production of resources, articles and material related to information security issues.

OWASP has compiled a classification of the security threats considered most critical:

- SQL Injection
- Broken Authentication and Session Management
- Cross Site Scripting
- Insecure Direct Object Reference
- Security Misconfiguration
- Sensitive Date Exposure
- Missing Function Level access Control
- Cross Site Request Forgery
- Using Components with Known Vulnerabilities
- Unvalidated Redirects and Forwards

2.2 MODES OF DELIVERY

2.2.1 PROACTIVE SECURITY SERVICES

Through the services of the INSIDE Cyber Security Division, we can assess the vulnerability of your systems and perform careful diagnostic analysis to determine the appropriate measures to ensure the security of your information property.

PENETRATION TEST

The Penetration Test is a service for assessing the security of a system or network through the simulation of an external or internal attack by a threat agent. The aim is to highlight the weaknesses of the platform, providing the greatest amount of information on the technological vulnerabilities that have enabled unauthorised access: it essentially involves putting ourselves in the shoes of the hacker, who exploits detected vulnerabilities to obtain information required for access to the computer infrastructure.

VAM – VULNERABILITY ASSESSMENT AND MITIGATION

The Vulnerability Assessment and Mitigation (VAM) method adopted by the INSIDE Cyber Security Division consists of a series of non-invasive activities aimed at **evaluating the effectiveness and strength of the security systems** used by your company, and identifying known vulnerabilities in case of a cyber attack. These initial intervention phases are followed by the adoption of countermeasures aimed at improving the security of your systems.

VAM should be implemented in various stages throughout the year, since the technology is constantly developing, as are the tools used to attack systems.

The INSIDE Cyber Security Division develops the following levels of VAM:

- **Database**: our analysis focuses in particular on the DBs mostly commonly used by companies (Microsoft SQL Server, Oracle, SYBASE Server, etc.). The assessment is done using highly sophisticated tools and software, and includes an automatic scan of these databases to identify and analyse weak points that are prone to attack. All companies “store” their business information in these types of databases, which, being constantly reorganised for better use, are exposed to attacks by parties with malicious intent, such as competitors.
- **Telephone Network**: an attack on a telephone network is commonly known as ‘war dialling’. It is a frequently used form of computer attack, as the telephone network is more vulnerable due to the presence of bugs. The attack involves automatic scanning of an entire telephone network, including switchboards, modems and telephone equipment.

WEB APPLICATION PENETRATION TESTING

With the advent of e-commerce, companies are increasingly using the web to promote and sell their products and/or services. The INSIDE Cyber Security Division conducts prevention and safety activities on all the web applications used by companies.

The process involves scanning and monitoring all the sections of the web application, with particular attention to areas protected by usernames and passwords, which, when entered, allow access to the services offered through HTTP or HTTPS protocols.

The work involves the following security fields:

- Scanning of sensitive data sent via the application and exposed to risk of interception by malicious parties, through an examination of the HTML code, scripts or other information that can be obtained through debugging mechanisms;
- Thorough analysis of interactive fields between the application and the user to identify any gaps created by (in)voluntarily input;
- Authentication procedures;
- Resolution of issues related to a specific session, such as timeouts, logouts, hijacking, logins using unverified addresses, etc.
- Validation and alterability of data;
- Execution of commands in unexpected areas of the application, for example, through specific SQL strings, which can lead to the direct manipulation of the database, with the possibility of acquiring, modifying and deleting stored data;
- Incorrect or inappropriate interactions with the operating system (shell escape).

THREAT DETECTION & ANALYSIS

Through its Threat Detection & Analysis procedure, the INSIDE Cyber Security Division can detect and analyse any hostile hardware or software devices (such as viruses) that are potentially capable of damaging or exporting sensitive data in computer systems affected by threats.

ETHICAL HACKING

Ethical Hacking consists in the simulation of an internal or external malicious attack, depending on the type of exposure risk identified in the computer system, and includes human as well as technological aspects, for example, the Social Engineering method.

Social Engineering is a series of psychological techniques used by a Social Engineer to deceive the recipient into performing certain actions (such as issuing access codes, or opening malicious attachments or site containing diallers, etc.).

The attack includes an initial phase, known as footprinting, consisting in the collection of information about the victim (e-mail address, phone numbers, etc.) and the subsequent assessment of its reliability. Once the victim has fallen into the trap, through the false sense of confidence induced by the Social Engineer, the computer system can then be accessed and violated.

No particular computer skills are needed to perform this activity, as knowledge of the person's psychology is sufficient (normal computer intrusion tools may already have been tried, unsuccessfully): the Social Engineer exploits certain impressions of the victim, such as guilt, innocence or ignorance.

CODE REVIEW

Through its Code Review service, the INSIDE Cyber Security Division detects **vulnerabilities in source code**, thus limiting the costs due to production of the program.

The activity consists of an initial analysis of the application, using tools to simulate execution of the code and detect any vulnerabilities that may be present. A second phase searches for vulnerabilities that may not have been identified in the initial analysis.

SECURITY EVALUATION

For its Security Evaluation service, the INSIDE Cyber Security Division uses highly skilled technicians working in a laboratory environment to evaluate **the safety levels of hardware and software applications, processes and, platforms** by identifying any vulnerabilities that are present and implementing existing security procedures.

IT RISK MANAGEMENT

Through its IT Risk Management process, the INSIDE Cyber Security Division **identifies risks** (vulnerabilities, threats, etc.) due to corporate IT investments (Risk Assessment) and defines the best strategies for governing them (Risk Treatment), thereby increasing the level of security required by IT infrastructure.

SECURITY AUDIT

The Security Audit service provides a technical assessment of an organisation's security policy based on a combination of Penetration Testing and Risk Assessment activities. It basically involves **accurate identification of vulnerabilities in the computer system** through precise optimisation of the execution of technological checks, thereby strengthening its risk assessment capacity.

HIGH LEVEL SECURITY CONSULTING

The specialised staff of the INSDE Cyber Security Division offer **consulting services** on any computer security issues that may not be covered by the services described above.

2.2.2 ATTACK VECTORS - for the Penetration Test and Web Application Penetration Test services

The Cyber Security Division uses the attack vector technique – of which there are several, depending on the device for which the service is intended – to simulate the activities of a threat agent that accesses an IT system in an unauthorised manner.

Some of the attack vectors used are listed below:

- **Infrastructure**: IP, VPN, Wi-Fi, SCADA, etc.
- **Applications**: Web, Database, Client-Server, etc.
- **Telephony**: PBX, RAS, APN, BlackBerry, VoIP, etc.
- **Others**: Human, Physical, Video Surveillance, Biometrics, etc.

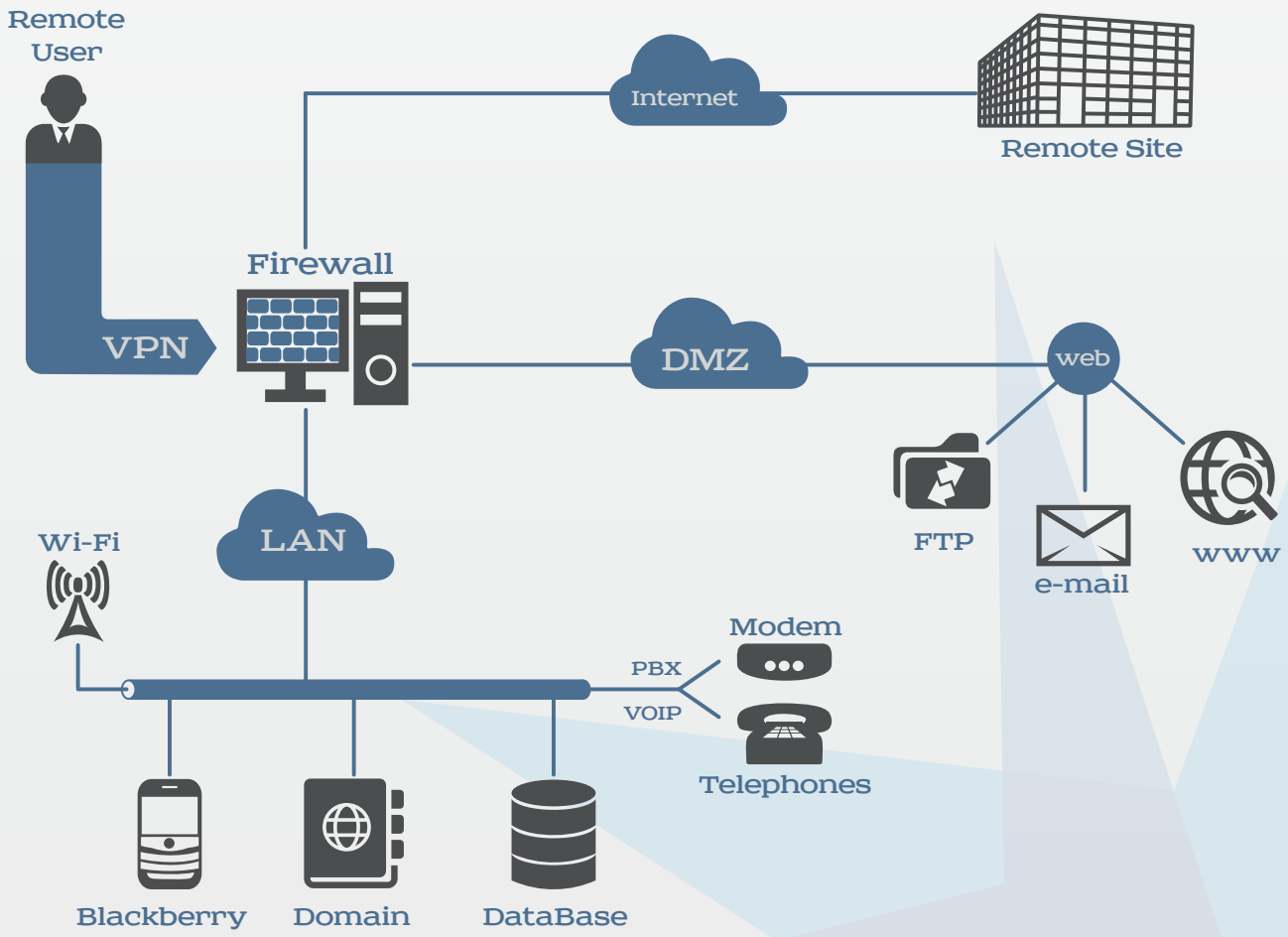


Image 2. Main attack vectors

In some cases we prefer to run tests from a privileged position, using standard access credentials, to evaluate the possibility of circumventing the authentication and authorisation mechanisms in use.

2.2.3 APPROACH

The approach developed by the INSIDE Cyber Security Division, always geared towards the assessment of the security level of the Client's IT infrastructure, operates in blind mode, through **the simulation of a "blind" attack**, i.e. without knowledge of the implementation details of the infrastructure.

2.2.4 TOOLS

The INSIDE Cyber Security Division uses the attack tools most commonly used in the market or those developed by the Security Advisory Team, included in the categories listed below:

- **Vulnerability Scanning** (Nessus, NeXpose, OpenVAS, etc.)
- **Network Scanning** (Nmap, Unicornscan, Singsing, Arp-scan, Ike-scan, p0f, etc.)
- **Web Testing** (Burp suite, Zed Attack Proxy, w3af, Skipfish, Nikto, etc.)
- **Wireless Testing** (Aircrack-ng, Kismet, Karmetasploit, etc.)
- **Phone Testing** (Minicom, WarVOX, Ward, THC-SCAN, etc.)
- **Packet Forging** (hping, Scapy, VoIP Hopper, Yersinia, ISIC, Netcat, etc.)
- **Network Sniffing** (Wireshark, Cain & Abel, Ettercap, etc.)
- **Password Cracking** (John, Rcrack, fgdump, THC-Hydra, Medusa, etc.)
- **Exploitation** (Metasploit framework, Exploit-db, private exploits, etc.)

Zero-day exploits, computer attacks that are particularly harmful to the integrity of a website and the proper functioning of an internet node, may also be used, but only at the Client's explicit request.

Only proprietary hardware and software is used, and at the conclusion of each project a **sanitisation procedure** is carried out to delete any data remaining from the operation.

2.2.5 DENIAL OF SERVICE

This project does not include testing for **Denial of Service (DoS)** attacks, unless specifically requested by the Client. These consist of malfunctions due to cyber attacks in which **the resources of an IT system** providing a service are deliberately exhausted so that it is no longer able to provide the service.

3. ACTIVITY PLAN

3.1 Preparation of the activities

In the initial phase of the project, the Security Advisory Team has to interface with the Client to gather all the information required for the task and to arrange the schedule and intervention method for each particular security operation.

3.2 EXTERNAL WEB CHECKS - for web application penetration testing

The purpose of this activity is the **analysis of web applications**, using a range of various technologies (ASP.NET, PHP, JSP, etc.), to test the security of the application components and prevent any threat agents from the Internet from gaining access to sensitive data possessed by the Client.

3.3 EXTERNAL IP CHECKS - for Penetration Tests

The purpose of this activity is to analyse systems exposed to threat from the Internet in order to assess **the security of the overall network infrastructure** and prevent unauthorised access or removal of confidential information.

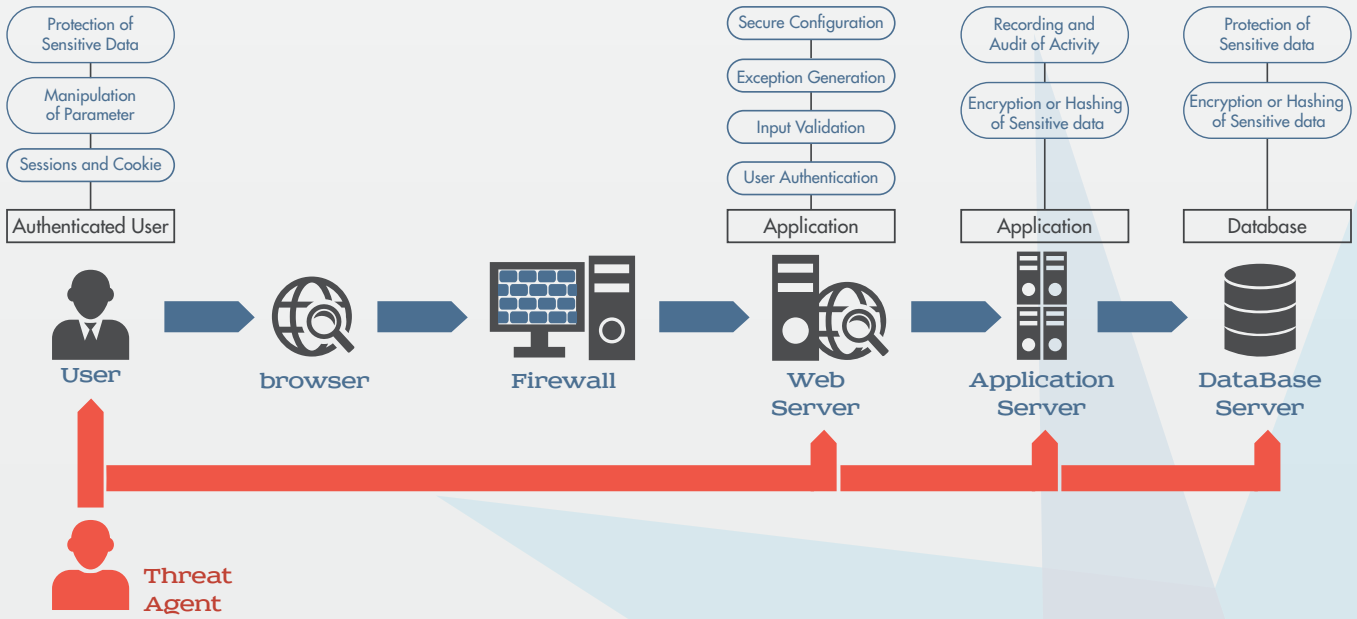


Image 3. Architecture of a web application and security measures

3.4 INTERNAL IP CHECKS - for Penetration Tests

The purpose of this activity is to analyse the systems on the Client's private network to assess the security of the overall network infrastructure and **prevent unauthorised access** or removal of confidential information.

4. DELIVERABLE

A series of information is given below regarding the final document delivered to the Client at the conclusion of the project.

4.1 TEST REPORT

On completion of all the activities, the INSIDE Cyber Security Division issues a strictly confidential report containing details of all the operations carried out and the necessary solutions for the total security of your company.

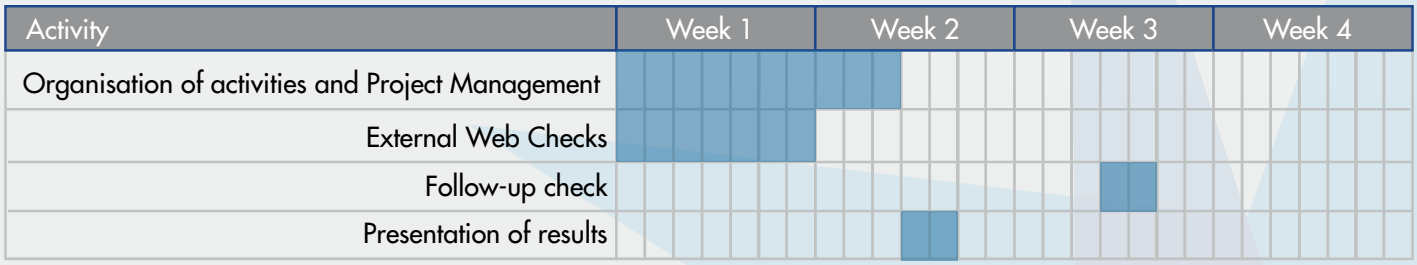
The document consists of two levels of analysis:

- **Executive Summary**: an introductory section that provides the Client with a broad overview of the main information on the security level of the structure examined, together with an indication of the risks identified, foreseeable damage and the measures to be taken to resolve problems;
- **Technical Report**: the true final document, containing a technical description of the operations performed, the critical aspects detected and details of the measures to be implemented.

5. DELIVERY TIMES

The graph shows the time taken to provide the requested services.

The activities described in this offer shall be carried out at the INSIDE headquarters or, in the case of an agreement between the parties in this regard, on the Client's own premises.



6. PROFESSIONAL FIGURES

The INSIDE Cyber Security Division includes highly specialised experts with a range of awards and certifications for security testing that vouch for their technical and professional competence and ethical values:

- CISSP (Certified Information System Security Professional)
- CISA (Certified Information Security Auditor)
- CISM (Certified Information Security Manager)
- OPSA (OSSTMM Professional Security Analyst)
- OPST (OSSTMM Professional Security Tester)
- OWSE (OSSTMM Wireless Security Expert)
- GCFA (GIAC Certified Forensics Analyst)
- ITV3F (ITIL Foundation v3)
- ISFS (Information Security based on ISO/IEC 27002)
- ISO/IEC 27001:2005 Lead Auditor (various schemes)
- PCI-QSA (Payment Card Industry Qualified Security Assessor)
- PCI-ASV (Payment Card Industry approved Scanning Vendor)

6.1 SENIOR SECURITY ADVISOR

This figure has five years of technical and organisational experience in the field of security and thus possesses the necessary requirements to identify the work activity and plan the strategies that the customer needs.

He/she possesses thorough knowledge of the security services and procedures to be implemented for the solution of all security problems; thanks to these skills and constant updating, he/she is able to **intervene dynamically in training and research activities**.

6.2 SECURITY ADVISOR

This figure has three years of technical and organisational experience in the field of security. He/she is capable of assisting the Client in the choice the services to be carried out to ensure **company security**; he/she directs the activities of the Security Expert and plays an active role in training and research projects.

6.3 SECURITY EXPERT

The Security Expert, with two years of technical and organisational experience in the field of security, has developed the capacity to **offer advice and assistance**, and provide support for the work of the Security Advisor. He/she is regularly involved in updating and research activities.

Inside
INTELLIGENCE & SECURITY INVESTIGATIONS

www.inside.agency • info@inside.agency

MAIN OFFICE

SWITZERLAND
Via Maggio, 1/C
6900 Lugano
T +41 (0)91 260 16 42
F +41 (0)91 228 03 95

OFFICES AROUND

UNITED KINGDOM
Crown House, 72 Hammersmith Rd
Hammersmith, London, W14 8TH
T +44 (0)20 75 59 13 11
F +44 (0)20 35 14 68 50

USA
6800 Jericho Turnpike, Suite 120W
Syosset, New York, 11791
T +1 (0)516 393 58 52
F +1 (0)516 393 58 19

RUSSIA
31st floor, stroenie 1, bld. 3,
Begovaya str, Moscow, 125284
T +7 (0)499 277 13 03
F +7 (0)499 287 66 00

ITALY
Via Monte di Pietà, 21
20121 Milano
T +39 (0)2 86 33 73 42
F +39 (0)2 94 75 26 15

ITALY
Via Ludovisi, 35
00187 Roma
T +39 (0)6 42 03 73 97
F +39 (0)6 94 80 17 11

UNITED ARAB EMIRATES
Building 3, Plot 598-676, Dubai Investment
Park, Green Community, DUBAI, 212880, EAU
T +971 (0)4 80 19 276
F +971 (0)4 80 19 101

HONG KONG
25 Westlands Road, Quarry Bay Berkshire
House, Unit 2402-07, 24th HONG KONG
T +852 (0)28 24 85 28
F +852 (0)37 19 81 11

SOUTH AFRICA
First Floor, Willowbridge Centre, 39
Carl Cronje Dr, Cape Town, 7530
T +27 (0)21 974 6276
F +27 (0)21 974 6101

BRAZIL
Top Center Paulista, Paulista Avenue, 854
Bela Vista – 10° floor, São Paulo, 01310-913, Brasile
T +55 (0)11 21 86 04 42
F +55 (0)11 21 86 02 99