


# Cyber Security Solutions

CYBER SECURITY DIVISION

Solutions for the protection of information



The image shows a person in a dark room, likely a control room or server room, looking at a computer monitor. The monitor displays network traffic logs and a table of data. The logs show various network events such as 'ack 572150 win 16088', 'ack 67081 win 32768', and 'P 572150:572411(261)'. The table has columns for 'Disposition', 'Reference ID', and 'Original ID'. The background is dark with some blurred lights, suggesting a technical environment.

Disposition	Reference ID	Original ID
Not set	0000172869	0000172869
Not set	0000172869	0000172869
Normal Activity	0000172867	0000172867
Normal Activity	0000172868	0000172868
False Positive	0000172865	0000172865
Normal Activity	0000172864	0000172864
Normal Activity	0000172864	0000172864
Not set	0000172863	0000172863
False Positive	0000172862	0000172862
False Positive	0000172861	0000172861
False Positive	0000172860	0000172860
False Positive	0000172859	0000172859
False Positive	0000172858	0000172858
False Positive	0000172857	0000172857
Normal Activity	0000172856	0000172856



## INFORMATION AND DATA SECURITY SOLUTIONS

We provide integrated cyber security solutions for the protection of information and data, mobile infrastructures, Industrial Control/SCADA systems and industrial networks.

### THE SCENARIO

Government, defence, energy transmission and distribution networks, telecommunications, transport management infrastructures, the health care system and the financial sector are becoming increasingly complex and interdependent.

A malfunction in such critical infrastructures, even for a limited period, would have a negative impact on the economy, cause financial losses and, in certain cases, would put the security and safety of people, information and property at risk.

In light of the pervasive cyber threat, organisations are being forced to review their approach to managing risk and are identifying strategies to reduce the vulnerability of key infrastructure, with the general focus moving away from defending IT assets, to protecting services by upgrading analysis and monitoring capabilities.

Security is even more critical for organisations that store customers' sensitive data, because national and international laws and regulations make organisations and their managers legally responsible for security and privacy violations. Businesses therefore need to ensure their security systems are coherent with the latest regulations and legislation.

## EXPERIENCE

The company has more than 25 years' experience working in cyber security. Drawing on a dedicated organisation, a consolidated approach and constant investment in resources and technology, we provide public and private organisations with a comprehensive security strategy and solutions covering organisational, technological and compliance issues.

Our approach focuses on understanding the threat our customers face, their tolerance to risk, specific needs, main concerns and unique business drivers, with careful adaptation of our solutions and processes accordingly.

The customer retains total control over strategic decisions and benefits from a personalized combination of services, delivered to the highest standards of quality and expertise.

Experience gained in various market sectors including Defence, Banking and Finance, Public Safety & Security, Telecommunications, Emergency Services, Energy and Gas Production and Distribution, Health Care, Transport, enables us to understand both the business and security needs of key infrastructures.

Close collaboration with top security players, universities and research centres has enabled us to develop solutions that combine advanced technology with innovative computing systems to manage risk and prevent attacks.

Our cyber intelligence solutions provide real time analysis of large amounts of web information (open, deep, dark), correlation of open and closed sources and crosscorrelation of significant events coming from different domains to build a real time, continuously updated high level view of the security situation and real support to critical decision making.



# REFERENCE MODEL

Expertise, tools, infrastructure and managed services solutions are offered through a team of highly qualified certified specialists. Our approach includes a wide range of services which will provide an organisation with an assured security strategy which complies with all of their security objectives through: assessment of the ICT estate; risk analysis and management; design, implementation and management of secure networks; protective monitoring; training and assistance.

## CERTIFICATIONS AND STANDARDS

- › UNI EN ISO 9001:2008
- › Information security: ISO/IEC 27001:2005
- › SOA: OS19 category - VI grade
- › Business continuity - BS 25999-2
- › Safety - OHSAS 18001
- › LSR18.6E certified datacentre infrastructure (Lampertz room)
- › Resilient infrastructure with disaster recovery datacentre and UPS.

# PROFESSIONAL SERVICES

## CYBER ADVISORY SERVICES

The company delivers professional services developed specifically for organisations that want to have full assurance of effective information protection measures and to improve them in line with business needs. A qualified team has developed a full set of skills including deep technical, regulatory and organisational experience.

Services include:

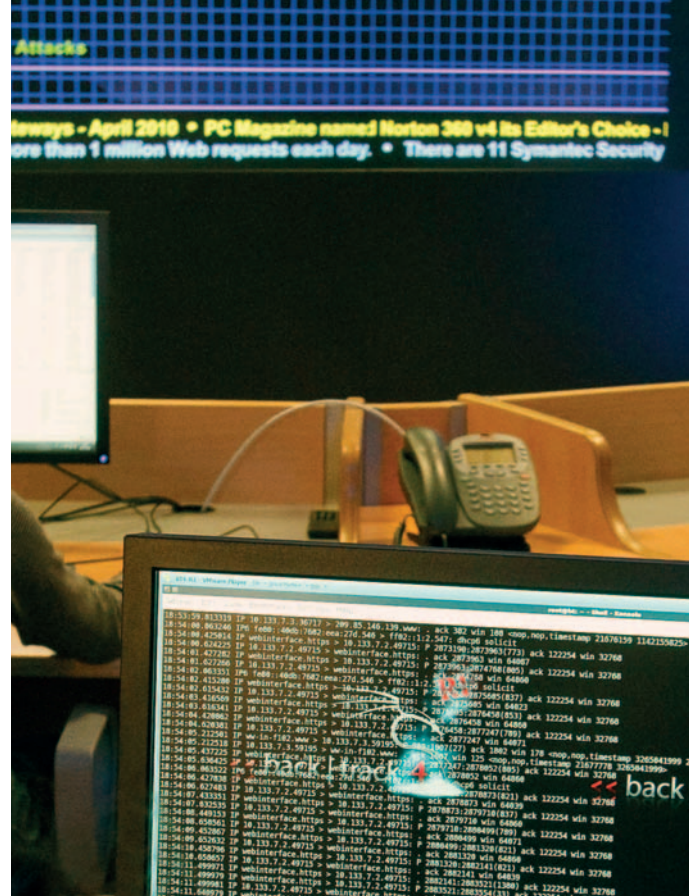
- › Security assessment and audit
- › Security governance
- › Risk analysis and management
- › Regulatory compliance
- › Certification support
- › Business continuity and disaster recovery planning
- › Information security awareness and training.

## SECURE SOLUTIONS

We offer turnkey solutions based on an analysis of customer needs, comprising architecture and design specification, implementation, and on-site integration.

Services include the design of custom SOCs, secure collaboration solutions (Unified Communication and Messaging), information management with a particular focus on document classification and protection, and secure web applications.

- › Network and application design
- › Data and network protection
- › Data loss and leakage prevention
- › Endpoint security
- › Secure/certified mail
- › Identity management, PKI and digital signatures
- › Message and document protection
- › Mobile device security & BYOD
- › Cloud security and virtual environment protection
- › Counter APT and malware analysis.



We also offer protection for both traditional ICT and Industrial Control Systems (ICS)/SCADA by leveraging a comprehensive approach:

- › Infrastructure assessment, design and review
- › Data, system and network protection
- › Deep protocol behaviour inspection
- › ICS and SCADA protection
- › Security management.

## OPEN SOURCE INTELLIGENCE

Actionable intelligence based on real time analysis of large amounts of web information (open, deep, dark), obtained through data mining, machine learning algorithms and a high performance computing framework.

- › Analysis of massive social networks
- › Network analysis for intelligence and surveillance
- › Security prevention & early warning
- › Brand protection - reputation analysis
- › Fraud & anti phishing.

## ENTERPRISE FRAUD MANAGEMENT

A series of innovative services based on the integration of technology, policy and processes to enable proactive fraud prevention and remediation.

- › Anti-phishing
- › Transaction monitoring
- › Alert management
- › Web threat detection
- › Data breach response.

# MANAGED SERVICES

## MANAGED SECURITY SERVICES

Our Security Operation Centres (SOCs) provide a flexible and comprehensive set of management and monitoring services that can be quickly tailored around an organisations' specific needs.

Security services offer efficient, around-the-clock perimeter and internal security with real-time monitoring, device maintenance, event correlation, and analysis of the customer's infrastructure and critical applications to ensure the cyber threat is pro-actively managed and attacks mitigated.

- > Firewall and IP VPN management
- > Real time security monitoring
- > Security intelligence
- > Security device maintenance
- > Ethical hacking /penetration test
- > Early warning
- > CSIRT/CERT services
- > Asset management.

We undertake evaluation of vulnerabilities in applications, taking account of the security posture of an application across the development life cycle, enabling companies to identify, eliminate, and prevent security risks in their software.

- > Web application security
- > Source code and application vulnerability assessment and Compliance.

## INCIDENT RESPONSE SERVICES

Our incident response services cover the entire spectrum from initial incident and the provision of threat intelligence, through to forensic services and advanced malware analysis to establish the nature of the attack and the attack origin:

- > Incident response services identify the most appropriate containment and reaction strategy, reducing business impact and supporting the repair and recovery of affected systems
- > Threat intelligence services gather information on both existing and emerging threats specific to your business
- > Forensic services collect, store and document all the evidence typically required for forensics activities.



For more information please email:  
[ict-cyber@leonardocompany.com](mailto:ict-cyber@leonardocompany.com)

Leonardo S.p.a.  
Via Laurentina, 760 - 00143 Rome - Italy  
Tel. +39 06 50271  
Fax +39 06 5051140

[leonardocompany.com](http://leonardocompany.com)

This document contains information that is proprietary to Leonardo - Società per azioni and is supplied on the express condition that it may not be reproduced in whole or in part, or used for manufacture, or used for any purpose other than for which it is supplied.

2019 ©Leonardo S.p.a.

MM08252 09-19

