LEONARDO CYBER & SECURITY SOLUTIONS

# CYBER SECURITY

## SERVICES CATALOGUE

LEONARDO

## CONTENTS

1. INTRODUCTION 3

2. IDENTIFY 5
- Security Strategy and Governance 5
- Cyber Risk Assessment and Risk Management 6
- Certifications and Compliance 7
- Cyber Security Assessment Laboratory (LVS) 8
- Red Teaming 9
- Threat Intelligence 10

3. PROTECT 11
- Security Architecture 11
- Cyber Security Solution Design 12
- Cyber Security Delivery 13
- Device Management Services 14
- System Management Services 15

4. DETECT 16
- Real Time Security Monitoring (RTSM) 16
- Threat Intelligence 17

5. RESPOND 18
- Crisis Management, Training & Security Awareness 18
- Computer Security Incident Response Team Services 19

6. RECOVER 20
- Crisis Management, Training & Security Awareness 20
- Computer Security Incident Response Team Services 21

7. SECURITY DASHBOARD 22

# 1. INTRODUCTION

Leonardo's Service Catalogue provides a comprehensive range of cyber security solutions, structured in a way that reflects the delivery organisation.

- **Cyber Resilience & Consulting:** helping organisations to understand and manage the cyber risks that they are exposed to. We can provide a Security Management System to ensure that the level of security adopted is in line with the organisation's security strategy, business objectives, laws and regulations, along with elements to increase the Cyber Resilience of IT/OT systems and advanced support for the management of emergency situations resulting from serious IT attacks.

- **Design & Build:** supporting both private and public sector organisations in defining and designing cyber security infrastructures and platforms, to assure the protection of information and systems, in full compliance with security requirements and reducing the residual cyber security risk to acceptable levels.

- **Managed Security Services:** Leonardo Security Operation Centre (SOC) provides managed services, designed to configure and continuously monitor Customers' security systems and devices, promptly identify breaches in security policies and apply immediate and appropriate remediation actions. These services include Managed Endpoint Detection Response services that provide customers with fast and effective protection for their endpoints, through the cloud-native cross correlation of data coming from the endpoints network under monitoring.

Each of the above service groups are categorised in services families, composed of individual services.
Leonardo Cyber Security Catalogue is mapped into international frameworks, such as NIST, providing an holistic approach to cyber security across five key areas:

- IDENTIFY: the assets that support your critical business processes and the associated cyber risks.

- PROTECT: your infrastructure through the adoption of skills, processes and technologies to make it intrinsically secure.

- DETECT: in advance any internal or external cyber security attack against your organisation.

- RESPOND: effectively, improving your cyber crisis management capabilities and defining an appropriate incident response strategy.

- RECOVER: your capabilities and services that were impacted by a cyber-security incident, enabling you to quickly resume to 'business as usual'.

The following table provides a high level mapping between Leonardo Cyber Security Services Families and the NIST Framework.

| SERVICES GROUP | SERVICES CATEGORY | NIST PHASE |
|---|---|---|
| CYBER RESILIENCE & CONSULTING | Security Strategy and Governance | Identify |
| | Cyber risk assessment and risk management | Identify |
| | Certification and compliance services | Identify |
| | Cyber Security Assessment Laboratory (LVS) | Identify |
| | Crisis Management Training & Security Awareness | Respond<br>Recover |
| CYBER DESIGN & BUILD | Cyber Security Architecture | Protect |
| | Cyber Security Solution Design | Protect |
| | Cyber Security Delivery | Protect |
| MANAGED SECURITY SERVICES | Real Time Security Monitoring Services | Detect |
| | Device Management Services | Protect |
| | System Management Services | Protect |
| | Red Teaming Services | Identify |
| | Computer Security Incident Response Team Services | Respond<br>Recover |
| | Threat Intelligence Services | Identify<br>Detect |
| | Security Dashboard | Identify<br>Detect<br>Protect<br>Respond<br>Recover |

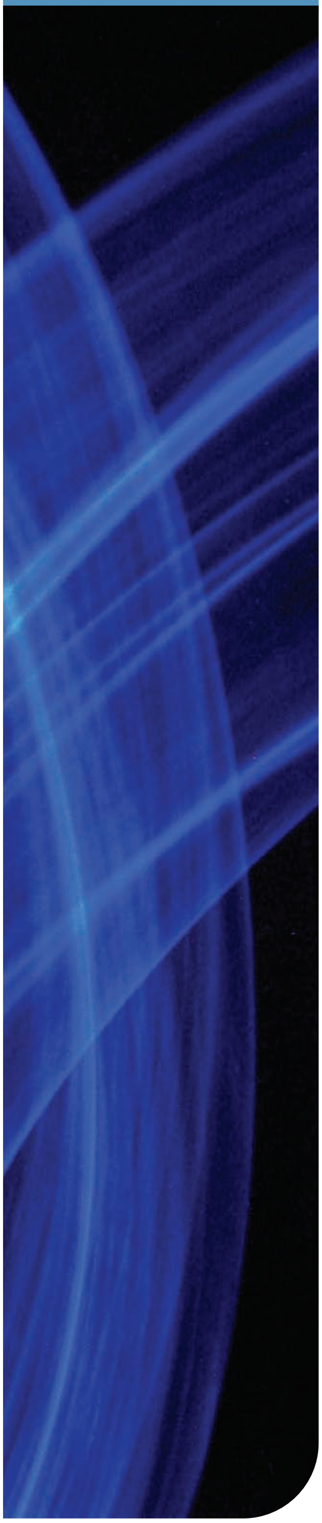
Leonardo Cyber Security Service Families are presented in accordance with the NIST Framework phases, with each Family organized into a separate sheet providing further information, and an accompanying service list. The Security Dashboard service, which applies to all phases of NIST Framework, is described in a separate chapter at the end of the document.

# 2. IDENTIFY

## SECURITY STRATEGY AND GOVERNANCE

CYBER<br>RESILIENCE<br>&<br>CONSULTING

The Security Strategy and Governance services support organisations in defining and maintaining a Security Management System, capable of ensuring that a level of security of their activities and support infrastructures is adopted in line with their security strategies and business objectives, as well as with applicable laws and regulations.



### Services' Deliverable

- Cyber security organisation chart
- SOC/CERT constituency
- Cyber security maturity models
- Security policies, procedures and guidelines
- Security processes design

### Benefits

- Defined strategy to underpin all security and assurance activities.
- Identification of key areas that need security investment, based on industry best practice.
- Contextualized security requirements enabling all activities and solutions to be designed and operated within an endorsed security policy.
- Definition of the organisational model for all the actors involved in the prevention, management and normalization of emergency states.

### Services Included

**Security Strategy:** definition of a set of security objectives that must be met, for an organisation, service, program, team or project.

**Cyber Security Maturity Assessment:** specialist support for carrying out an assessment in order to:

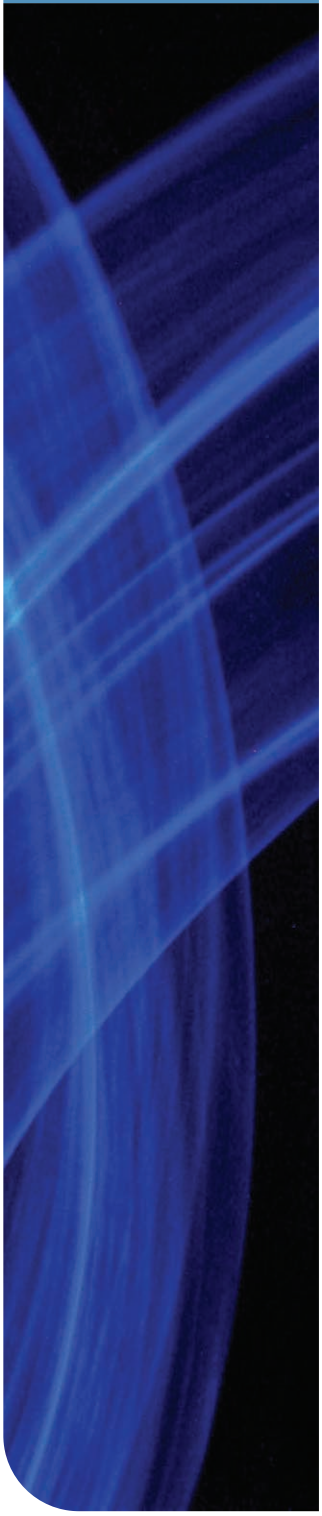
- identify the reference security standard to be adopted;
- understand the level of compliance or maturity of the Organisation;
- identify possible corrective actions with respect to the solutions and standards used by the organisation;
- support the organisation to prioritise and plan the implementation of the corrective actions.

**Security Policy Development:** development of a security policy suite specific to the business, that defines the high-level security requirements across all relevant aspects of security.

**Security Processes & Procedures Design:** creation of a security process suite with defined process owners for all security activities.

CYBER RESILIENCE & CONSULTING

# CYBER RISK ASSESSMENT AND RISK MANAGEMENT



The Cyber Risk Assessment and Risk Management services enables organisations to define a Cyber Risk Management framework, according to the ISO 31000 standard. It also enables the execution of the security risk assessment, with the aim of identifying possible cyber security threats and their consequences, along with a prioritized list of countermeasures to be implemented, aimed at ensuring the right balance between cost-benefit.

## Services' Deliverable

- Risk Management Methodology development
- Risk Assessment activities and Reporting
- Risk Mitigation prioritization and roadmap development

## Benefits

- Risk-based approach to security investment allowing informed choices about when to accept, reduce or avoid security risks.
- Understanding gaps in security governance and risk management architecture that present cyber vulnerabilities.
- Proactive risk management in line with industry best practice.

## Services Included

**Risk Management Framework Definition:** creation of a security risk management framework that allows consistent and accurate measurement and communication of security risks to the business. The risk management Framework includes the impact domains and tiers of impact alongside the risk assessment methodologies. This requires a detailed understanding of how security incidents are most likely to impact on the business objectives.

**Risk Assessment:** identification, assessment and evaluation of the security risks attracted by an area of the business and the impact of these risks on the business objectives.

**Risk Management:** expert advice and guidance on appropriate risk response options to help inform and guide operational security risk management.

# CERTIFICATIONS AND COMPLIANCE

Our certification and compliance services enable organisations to deliver services that comply with regulatory and legal requirements, and/or mandated standards and frameworks.

## Services' Deliverable

- Standard and regulation compliances

## Benefits

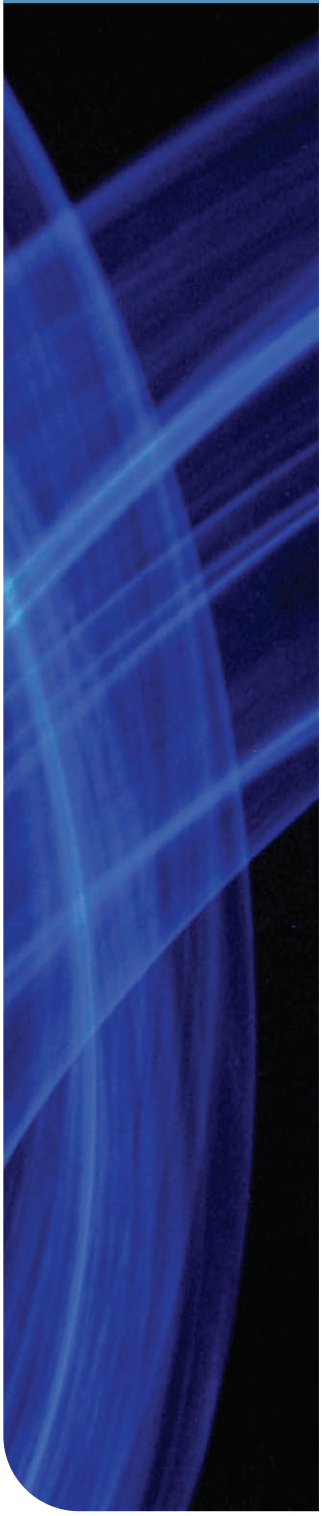
- Compliance of the organisational model and technological infrastructure to current regulations.
- Reduction of compliance risks and fines.

## Services Included

**Audit and Compliance:** audit of the managed service (to be repeated at regular intervals or in the case of significant changes in the service) to ensure that all people, policy and technology information controls implemented are in line with the mandated requirements.

**Support to ISO 27001 and 22301 Certification:** development of a security policy suite specific to the business that defines the high-level security requirements across all relevant aspects of security.

**GDPR Compliance:** specialist support to comply the European Regulation on the Protection of Personal Data (GDPR) and Legislative Decree 196/2003 and subsequent amendments.



# CYBER SECURITY ASSESSMENT LABORATORY (LVS)

The Cyber Security Assessment Laboratory (LVS) provides the following activities:

- within the “National Scheme” for the assessment and certification of the security of systems and products in the IT sector, managed by the Certification Body established within the Higher Institute of Communications and Information Technologies (ISCOM) of the Italian Ministry of Economic Development.
- providing specialist support, to the Operators of the Essential Services (OES) for compliance with the provisions of Legislative Decree 18 June 2018, n. 65 with which the Directive (EU) 1148/2016 (so-called NIS Directive).

## Services’ Deliverable

- Product/System Certification Support

## Benefits

- Increased competitiveness of the product/system.
- Adoption of a well-defined and documented development environment and process, of which will also benefit products that are not submitted to such certification.
- Improved level of trust in the system/product.

## Services Included

**Evaluation:** aims to carry out the evaluation activity within the Certification process of a product / system in accordance with the international standard ISO / IEC IS-15408 (Common Criteria).

**Consulting:** aims to support the organisation in dealing with the Evaluation and Certification processes, both in the commercial and defence fields, by providing specialist resources.

**Compliance D.Lgs. 65/2018 implementing NIS Directive and Law 133/2019:** aims to provide specialist support for compliance with the provisions of Law 133/2019 and Legislative Decree 18 June 2018, n. 65 with which the Directive (EU) 1148/2016 (so-called NIS Directive)  was implemented in the Italian and UK legal system.

## RED TEAMING

MANAGED SECURITY SERVICES

Red Teaming services focus on finding security flaws that can be exploited by malicious attacks, testing in advance the measures already adopted by organizations. These services aim at providing customers with a comprehensive picture of their security posture in terms of protection capabilities, vulnerabilities, secure software development and internal users' security awareness.

### Services' Deliverable

- One time or periodical reports
- Security Posture and Risk level reporting
- Simulated phishing/attack campaigns

### Benefits

- Detection of security vulnerabilities that an attacker could potentially exploit to access the system.
- Supporting developers to identify vulnerabilities in the early stages of development.
- Capability to test applications while they are running to find vulnerabilities (no source code needed).
- Mitigation of the attack potential through simulations involving company employees.
- Decrease in the exposure level to cyber risks.

### Services Included

**Vulnerability Assessment:** identifies vulnerabilities in customer systems and defines a repair plan, prioritising patch activities based on the criticality of the identified security issue.

**Vulnerability Management:** periodic security status evaluation of the infrastructure, identifying corrective actions for any anomalies detected, through targeted prevention campaigns and effective patch management processes, within an ITIL compliant environment.

**Penetration testing:** understands the actual security posture of a system by attempting to exploit identified vulnerabilities.

**Static Application Security Test:** application source code analysis during coding and design, without "running" the application, revealing security vulnerabilities and weaknesses in the code.

**Dynamic Application Security Test:** applications behaviour analysis -both during the test phases and during the operational phases. This includes simulations of attacks against the application and analysing the reactions of the application in order to determine the precise level of vulnerability.

**Social Engineering:** assessing the awareness and attentiveness of the customer's employees with respect to cyber-security issues, by conducting simulated attack campaigns that enable employees to identify and avoid potential malicious elements in the future.

MANAGED SECURITY SERVICES

# THREAT INTELLIGENCE

The Threat Intelligence Services monitor and analyse large amounts of data, both open source and on the deep and dark web, to prevent cyber-attacks that use malware specific to the technologies used by the customer.

## Services’ Deliverable

- Periodical or event-based threat intelligence reports
- Tailored Investigation reports on customer request

## Benefits

- Early cyberattacks identification.

## Services Included

**Early Warning (Security Bulletins):** acquires application/infrastructure security data from several sources in real time, to identify new vulnerabilities and general purpose Indicators of Compromise.

**Early Warning (Advanced):** through the configuration of targeted searches, this service aims to prevent cyber-attacks that use malware specific to the technologies used by the customer

## SECURITY ARCHITECTURE

CYBER
DESIGN &
BUILD

Our Security Architecture services assist organisations in building and implementing appropriate security controls into the business information and technical architectures. This ensures security is aligned with, and supports the business objectives.

### Services' Deliverable

- Cyber security architecture

### Benefits

- Guarantees that the company's safety posture is aligned with and supports the business objectives.

### Services Included

**Security Architecture Vision and Pattern:** enables changes in information and technology architectures to be supported in parallel with changes to the security architecture. This ensures transformational changes to the business remain appropriately secure throughout their implementation.

**Security Architecture Design:** defines the high-level and low-level security design of a particular solution, that details the security controls employed and their relationship to the functional information and technology architecture.

**Security Architecture Review:** provides assurance that the security controls within the in-scope estate achieve sufficient risk mitigation whilst also delivering value. Where this is not the case, the review highlights the principal risks to the estate alongside a remediation roadmap.

CYBER DESIGN & BUILD

# CYBER SECURITY SOLUTION DESIGN

Cyber Security Design services support organisations in defining and designing cyber security infrastructures, guaranteeing the protection of information and systems, compliance with security requirements and reducing the residual cyber security risk to acceptable levels.

## Services' Deliverable

- Cyber security high-level design
- Cyber security compliance matrix

## Benefits

- Requirements analysis and design of secure infrastructures.
- Security best practices for technologies deployment.
- Professionals and engineers support with specific skills for secure solutions design.

## Services Included

**Cyber Security Solution High Level Design:** supports customers in defining / revising their cyber security architecture to implement appropriate technological countermeasures to reduce cyber risk.

**Cyber Security Compliance Matrix:** ensure security requirements are implemented and addressed into the Solution Design.

# CYBER SECURITY DELIVERY

Cyber Security Delivery services (build) supports customers in implementing security infrastructures and platforms that guarantee the best level of protection for systems and information according to best practice standards and mitigate the overall identified cyber risks to the agreed level.

## Services' Deliverable

- Cyber security low level design
- Cyber security implementation document (as-built)
- Test book
- Test delivery report

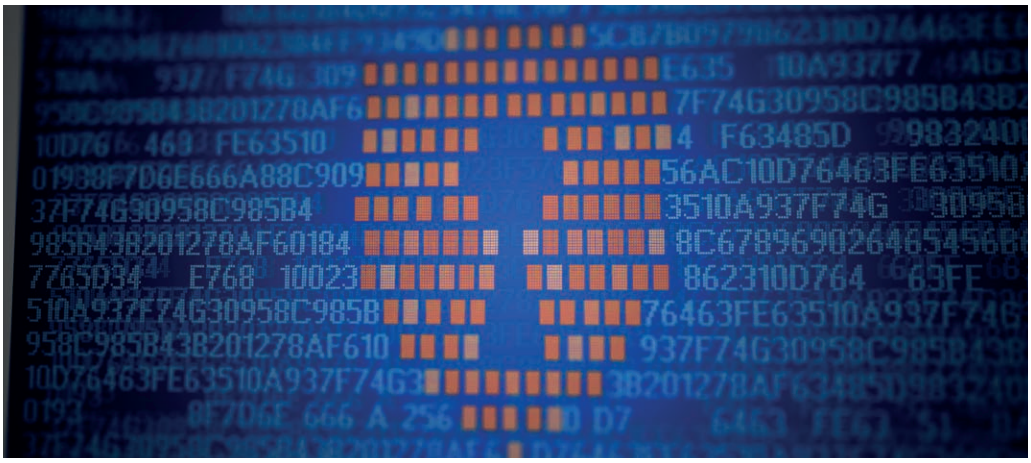
### Benefits

- Specialised cyber security professionals and network engineers, with specific skills for the implementation of secure infrastructures.
- Once delivered and tested, the infrastructures can be managed by the customer's operating structures supported by Leonardo specialists, if required.

## Services Included

**Cyber Security Solution Low Level Design:** detailed design of the technological solution based upon previously defined cyber security technological countermeasures, security requirements and reference architecture.

**Cyber Security Solution Implementation:** on the basis of the low-level design, implements the platforms, verifies their operation and effectiveness, as well as integration with the remaining ICT infrastructure.



MANAGED SECURITY SERVICES

# DEVICE MANAGEMENT SERVICES

Device Management Services provide perimeter protection of our customers' IT/OT infrastructure. These services help manage security policies of protection devices, according to international best practices and customers defined profiles, providing daily consultancy into the security model validation.
The Device Management services also play a key role into containment and remediation of security incidents phases dynamically changing security policies in order to protect against new security threats.

## Services' Deliverable

- Security policy advisory and review
- Change management
- Problem solving
- Software patching and maintenance

## Benefits

- Highly flexible maintenance and management of the customer's firewall infrastructure.
- Ability to block access to potentially malicious websites.
- 360-degree protection for all vulnerabilities typically found in web applications.
- Significant savings in the costs of updating the firewall policies and the reduction in the probability of creating incorrect configurations.
- Easy identification of exposures deriving from incorrect firewall policy configurations.

## Services Included

**Next Generation Firewall:** supports the maintenance and management of the customer's firewall infrastructure.

**Web Application Firewall:** allows analysts to define application protection rules by analyzing their normal use as well as to act proactively and promptly in the event of attacks.

**Security Web Gateway:** blocks the access to potentially malicious websites by automatically updating database and recognizing the download of potentially harmful applications through real-time traffic analysis.

**Security Policy Review:** ensures that firewall configuration and rule set meet security best practices and corporate compliance requirements.

# SYSTEM MANAGEMENT SERVICES

The System Management Services manages all detection platforms and systems, and plays an important part in the security alarms visibility scope.

Their main objective is to organise and manage customers' log sources to collect all relevant security events in order to generate notable and reliable security alarms leveraging on up to date correlation rules, technological capabilities of main detection solutions on the market and Security Operation Centre engineers' skills and knowledge base.

## Services' Deliverable

- Log sources integration and management
- Log parsing and correlation.
- On-prem and Cloud Security platforms change management.
- Design and implementation of Deception scenarios

## Benefits

- Real time identification and response of cyber threats, targeting the endpoints.
- Detection of emerging threats and trends through logs analysis.
- Protection of sensitive or critical corporate information.
- Block and discourage internal and external attackers.
- Effective application of corporate security policies when accessing the cloud resources

## Services Included

**Log Management:** receives and archives security logs from the customer's platforms, predominantly to meet regulatory obligations and to address control and monitoring activities.

**SIEM as a service:** helps organisations meet compliance requirements and improves the logging and monitoring configuration strategy in order to detect emerging threats and trends.

**Data Loss Prevention:** enables data protection, both from unauthorised accesses and from violations of security policies.

**End Point Detection & Response:** continuously collects and stores data from endpoints in a cloud-based centralised database and then analyses them to reveal potential threats and cyber issues.

**Deception:** creates an attractive scenario for potential cyber attackers in order to monitor their behaviour, discovering as much information as possible about previously unknown hacking strategies.

**Cloud Access Security Management:** provides a 'control point' between users and the cloud provider, to intervene in the application of corporate security policies when accessing the cloud resources.

MANAGED SECURITY SERVICES

## REAL TIME SECURITY MONITORING (RTSM)

This services family represents core functionalities of real time security incident management services provided by Leonardo Security Operation Centre (SOC). They provide customers with real time notifications about security alarms, behaviour anomalies and potential threats, leveraging best of breed detection platforms capabilities and Leonardo SOC analysts' skills and knowledge base.

### Services' Deliverable

- Security alarms real time notification
- Periodical reports for misconfigurations and low severity security evidences
- Tuning process support
- First level analysis and support in security incidents

### Benefits

- Increases cyber situational awareness and faster identification of compromise when it occurs.
- Reduce the impact of security incidents through quicker more informed response.
- Continuous monitoring of endpoints' events and activities through advanced analysis

### Services Included

**Real Time Security Monitoring (RTSM):** delivers continuous monitoring of customer security devices/systems logs in order to quickly identify potentially harmful resources or events.

**Managed Endpoint Detection & Response (MDR):** to provide customers with fast and effective protection for their endpoints, leveraging Endpoint Detection and Response cloud-based technologies.

# THREAT INTELLIGENCE

The Threat Intelligence Services monitor and analyse large amounts of data, both open source and on the deep and dark web, to identify ongoing cyber-attacks or those being planned. The service also identifies cyber threat actors' activities and information illegally stolen and published on the web. The solution also provides a comprehensive overview on brand or event sentiment, and guidance on the prevention of cyber frauds.

## Services' Deliverable

- Periodical or event-based threat intelligence reports
- Tailored Investigation reports on customer request

## Benefits

- Increases cyber situational Prevention of company-owned data loss.
- Sentiment analysis.
- Black market related illegal activities identification.
- Prevention against new planned cyber-attacks.
- Protection of VIPs' and Company online reputation.
- Customer digital identity protection / identity theft identification.
- Real time detection of cyber frauds and phishing attacks identification.

## Services Included

**Data breach:** detects any data loss relating to a specific target of information through real-time monitoring of the network, including scanning of the deep and dark web.

**Brand reputation:** analyses the communications exchanged by web and social network users to understand the positioning of a company's brand in relation to its competitors.

**Black market monitoring:** analyses large quantities of information from open sources, deep and dark web, in real time, to promptly identify new black markets and illegal activities on specific issues of interest.

**Pre-planned attack:** allows you to identify and predict possible new cyber-attacks more effectively, through real-time analysis of large quantities of information from open sources and the deep and dark net.

**Brand abuse:** protects brands and public figures from the misappropriation of domain names aimed at making a profit on the transfer of the domain itself, or by causing damage to those who cannot use it.

**Identity fraud detection:** detects unauthorised use of a person's digital identity to carry out illegal activities and/or defamatory actions without the knowledge of, and to the detriment of the individual.

**Anti-phishing:** manages the detection of ongoing phishing attacks against the customer, the real-time identification of ongoing fraud towards their brand and the protection of online reputation.

CYBER RESILIENCE & CONSULTING

## CRISIS MANAGEMENT, TRAINING & SECURITY AWARENESS

Crisis Management, Training & Security Awareness services support organisations in managing the crisis situations and impact of cyber incidents as well as in the design and delivery of training activities on a range of cyber security issues and awareness campaigns to increase the cyber security awareness and competency of employees.

### Services' Deliverable

- Executive note
- Press charges for regulatory compliance
- Media statements
- Security training and courses
- Cyber exercise report

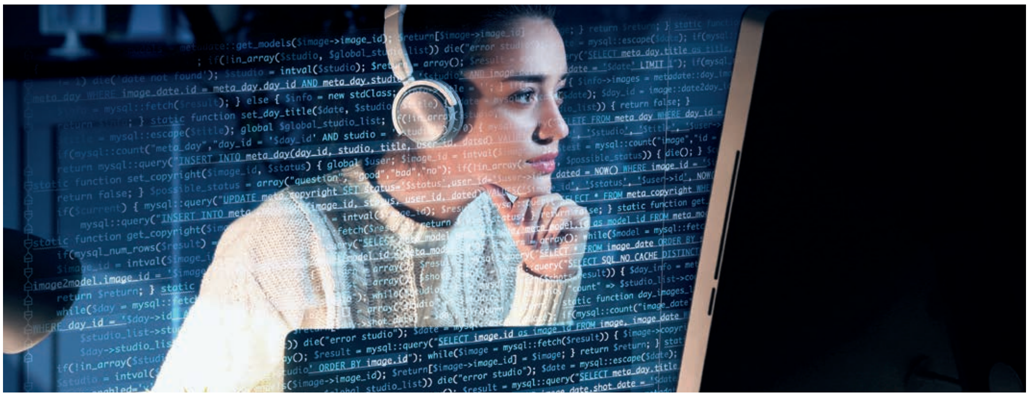
### Benefits

- Support for strategic and operational decisions to ensure operational continuity, and minimising the impact of cyber-attacks.
- Acquisition of expertise, skills and competences to adequately face a wide range of malicious events in different contexts.
- Increased awareness of cyber issues for the entire workforce.

### Services Included

**Cyber Crisis Management:** provides specialist support for the effective management of crisis situations, that may threaten the company's services or assets.

**Cyber Training & Security Awareness:** includes basic and advanced training courses on cyber security issues, as well as awareness campaigns on a range of cyber security topics.



# COMPUTER SECURITY INCIDENT RESPONSE TEAM SERVICES

The Computer Security Incident Response Team Services (CSIRT) identify and analyse the most advanced cyber threats capable of bypassing traditional automatic defensive measures, through the identification of root cause, attacker behaviour, relevant artefacts, and compromised assets within the monitored infrastructures.
The CSIRT services deeply analyse and react to security incidents, minimising the operational and economic impacts of the security incident as effectively as possible, through the definition of the most rapid and effective incident response strategy.

## Services' Deliverable

- Artifacts analysis and reports
- Containment and mitigation activities
- Incident response reports
- Remediation and restoration technical support
- Security evidences and artifacts
- Compromise assessment report

## Benefits

- Identification of Indicators of Compromise and any containment actions to put in place.
- Capability to isolate systems while preserving evidences.
- Specialised support to carry out the remediation and restoration of systems.
- Indications regarding the actions needed to mitigate future incidents.

## Services Included

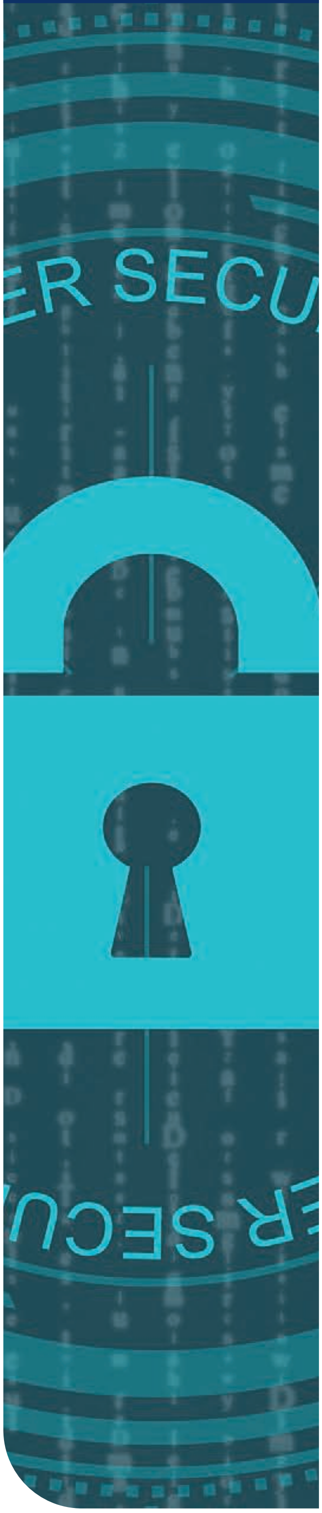
**Incident Response:** combines specialist capability in incident management and investigation to deliver comprehensive advice and technical analysis in response to any cyber security attack or breach.

**Malware Analysis:** acquires and classifies suspected malicious files (samples), provides hash control, comparison with known malware, behaviour analysis in order to identify any indicators of compromise and any containment actions to put in place.

**Threat Hunting:** proactively identifies, isolates and neutralises the most advanced cyber threats that are capable of bypassing traditional automatic defensive measures before they can cause real damage to the organization.

**Compromise Assessment:** provides the customer with a complete view of the current situation in terms of potential threats or ongoing malicious activities leveraging the capabilities of an Endpoint Detection & Response (EDR) solution.

CYBER RESILIENCE & CONSULTING



# CRISIS MANAGEMENT, TRAINING & SECURITY AWARENESS

Crisis Management, Training & Security Awareness services support companies and organisations in the management of emergencies and crises due to cyber incidents that seriously affect organisations as well as in the design and delivery of training activities on hot cyber security issues and awareness campaigns increasing the cyber security competency of internal staff.

## Services' Deliverable

- Technical incident report
- Post-crisis assessment
- Lesson learned and training activities

## Benefits

- Performance of post-crisis assessment by evaluating all aspects involved within the crisis and getting incident parameters against future occurrences.
- Activation of Lesson learned phase aimed at developing a resilient and secure cyber approach for the organization.

## Services Included

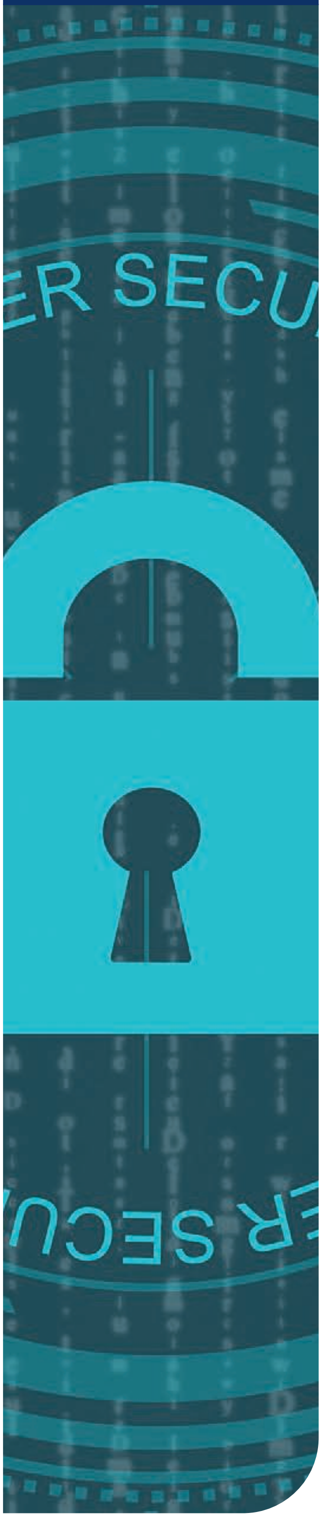
**Cyber Crisis Management:** provides specialist support to guarantee the effective recovery of the organisation's vital services or assets from crisis.

**Cyber Training & Security Awareness:** includes basic and advanced training courses on cyber security issues to support the company in improving its cyber resilience level.

# COMPUTER SECURITY INCIDENT RESPONSE TEAM SERVICES

MANAGED SECURITY SERVICES

The Computer Security Incident Response Team Services (CSIRT) identify and analyse the most advanced cyber threats that are capable of bypassing traditional automatic defensive measures, through the identification of root cause, attacker behaviour, relevant artefacts, and compromised assets within the monitored infrastructures. The CSIRT services deeply analyse and react to security incidents, minimising the operational and economic impacts of the security incident as effectively as possible through the definition of an effective recovery plan including long-term, mid-term and short terms suggested actions.



## Services’ Deliverable

- Incident response reports
- Remediation and restoration technical support
- Security evidences and artifacts

## Benefits

- Understanding of the root cause of any cyber security related incident.
- Provision of evidence to support company, regulatory or criminal investigations.

## Services Included

**Incident Response:** combines specialist capability in incident management and investigation to deliver comprehensive advice and technical analysis in the face of any cyber security attack or breach.

**Digital Forensics:** identify, collect and acquire all the evidence that demonstrates a possible compromise following an exploit by an attacker and any non-compliant use of an asset.

MANAGED SECURITY SERVICES

# SECURITY DASHBOARD

The Security Dashboard service offers flexible and configurable tools for the representation of large amounts of data both in numerical and graphical format. Dashboard tools are organised in sections, panels and configurable widgets to represent contextual information, statistics and service deliverables. Using appropriate tabs, the user can access customised views based on requested services and specific requirements.

## Services' Deliverable

- KPIs and SLAs graphical representation
- Incidents reports and data export
- Incident notification process management
- Change management process
- Threat Intelligence reports
- Actionable and Non-Actionable IoCs

## Benefits

- Self-developed tools with highly customisable and service driven functionalities.
- Ability to drill down at points of interest to show details derived from, and related to, a wide range of cyber security services from this catalogue.
- Multi Factor Authentication and/or IPSec VPN access with the highest level of protection for customer data.

## Services Included

**Next Generation SOC:** NGS portal represents the main interaction point for customer notification process and service request management. It also provides SLA and KPI overview, services statistics and reports.

**TIS-Disclosure:** threat Intelligence portal provides a customer detailed and aggregated view of intelligence, actionable information and reports, threat actors description and activities, malwares anthology and an Indicators of Compromise (IoC) database.

**SIEM Dashboards:** where applicable, customers can request access to a dashboard configured on Security Incident and Event Management platform, to take under control in real time its monitoring perimeters in terms of alarms type and severity, data sources, detection levels and statistics.

For more information:
cyberandsecurity@leonardo.com

Leonardo Cyber and Security Solutions Division
Via R. Pieragostini, 80 - Genova 16151 - Italy

This publication is issued to provide outline information only and is supplied without liability for errors or omissions. No part of it may be reproduced or used unless authorised in writing. We reserve the right to modify or revise all or part of this document without notice.

MM09090 06-22

leonardo.com

LEONARDO