Security & Privacy by Design

CYBER SECURITY DIVISION

LEONARDO

Digitalisation, together with the wider adoption of advanced technologies (mobile, cloud, analytics, social collaboration), useful for communication and continuous exchanges with outside world, considerably increases risks and vulnerabilities for critical and strategic national infrastructures. These circumstances cause security incidents with pervasive and relevant impacts on vital services for social functioning and therefore with unpredictable domino effects.

In a context where cyber attacks, with the specific goal of disrupting services for the citizens, are growing, market analysts and cyber security experts announce that these attacks will be more focused on application vulnerabilities.
These trends are determined both by the increasing number of software platforms used to run the core processes of critical service infrastructures and by software quality policies and related investments focused mainly on correcting functional defects and application logic performance rather than realizing design and implementation practices to guarantee code security.

SOFTWARE & APPLICATION SECURITY SUITE

This idea of software security opens to innovative technological paradigms such as "secure by design software" (software development life cycle including security issues controls and running applications checks) and "privacy-by-design" (the inclusion of privacy starting from business processes design and supporting IT applications).
Software security is thus built on a strategic approach applied to application security that is addressed at the early stages of the software platform development and is integrated throughout the software entire life cycle making it intrinsically secure.

Leonardo new "software and application security suite" provides a framework that enables governments and critical infrastructures to equip themselves with secure digital platforms.
It uses a methodology already tested and a set of professional and application services throughout the software life cycle. The customers are also supported by a team of cyber security and software development experts minimising both economic damages resulting from cyber attacks and reputation related problems associated to potential incidents.

LEONARDO METHODOLOGY AND SKILLS

Leonardo software and application security methodology is focused on the **SSDLC model (Secure Software Development Life Cycle)** which combines the traditional software development cycle with security services that guarantee the development of secure code, the early detection and resolution of potential security breaches.

These services help to protect applications against data loss and internal or external attacks. Leonardo proprietary methodology guarantees conformity to the fundamental pillars of confidentiality, integrity and availability of data and systems and allows the design, the development and the release of "Secure by Design" software thanks to an approach structured into operational phases and supported by dedicated services.

1. **Assess security requirements:** software requirements analysis, including security and privacy.
2. **Design & Analyse the threat:** software design based on the requirements highlighted in the analysis, cyber threat modeling, countermeasures plan to be adopted and design review.
3. **Write & test the code:** software development through code programming, source code analysis and review.
4. **Stress the code:** test of implemented software and vulnerabilities identification to verify the correspondence to the requirements identified during the analysis phase.
5. **Fix & release the code:** software release after the removal of identified vulnerabilities in the source code and the consequent handover test passing.
6. **Monitor the security:** implemented software checking and vulnerabilities identification to determine the correspondence to the requirements identified during the analysis phase.

Leveraging the experiences gained in systems, services and integrated solutions design and implementation both for the defence sector and for public and private agencies in the civil sector, Leonardo develops secure by design platforms taking advantage of professionals with highly specialised skills being able to identify security issues and vulnerabilities, to define security requirements and to use methodologies, tools and techniques for secure development, analysis and remediation of the source code such as Security Consultants, Ethical Hackers, Security Architects, Web Security Experts and Security Specialists.

SERVICES

Leonardo's software and application security suite includes application, infrastructural and professional services guaranteeing "Secure by Design" design and development, analysis and review, continuous monitoring and data protection for systems and service infrastructures. The suite includes the following services:

- **Secure by Design Development** such as Risk Assessment, Vulnerability Assessment, Threat Analysis, Static & Dynamic Analysis, Software Remediation, Patching Update and Security Training. These services are aimed at secure software design through the identification of security requirements, the developing and testing of the code and the releasing of secure software, according to the methodology, the technologies, the skills and the experiences of the software & Application Security Suite.

- **Security Application Analysis**, such as Design Review, Penetration Test, are aimed at the analysis of the source code and at the identification of vulnerabilities within applications through the use of static and dynamic analysis techniques, the review of the architecture on the basis of application security requirements and the remediation of the code for existing software.

- **Security Monitoring** such as Data Loss/Leak Prevention, Database Security, EndPoint Protection, Web Application Firewall Management, Secure Web Gateway, Advanced Threat Protection, and Real Time Security Monitoring, are aimed at vulnerabilities exposure status control and at the application and infrastructural security status monitoring for data protection from unauthorized access.
  The suite also implements functionalities for the simulation of attacks, for the access restriction to potentially malicious sites and for preventive checks against data exfiltration/corruption.

PRIVACY BY DESIGN

The inclusion of privacy starting from the software design phase is specifically addressed by a dedicated suite that ensures the compliancy of Public Administrations and Companies with the regulatory requirements of the European regulations on the protection of personal data (GDPR).

1. ASSESS SECURITY REQUIREMENTS
2. DESIGN THE THREAT
3. TEST THE CODE
4. STRESS THE CODE
5. FIX THE CODE
6. MONITOR THE SECURITY

The Privacy by Design suite of services supports the customer during the Assessment, Design, Implementation and Monitoring operational phases.

The **Privacy Assessment** services map the processing of employees' personal data and roles within the organisation, analyse the allocation of personal data in applications and infrastructures and identify the technical features and the gap analysis on non-conformities in terms of security.

The **Privacy Design** services include the design of the Privacy Governance system in terms of roles, responsibilities, skills and processes including the upgrade of infrastructures and applications.

Implementation and continuous updating of the new Privacy Governance system in terms of PIA implementation (Privacy Impact Assessment), application and infrastructure development and audit are managed through the **Privacy Implementation & Monitoring Services.**

BENEFITS

- Adequate level of applications and systems intrinsic security in order to prevent any attempt to exfiltrate data.
- Evaluation and validation, from the application security point of view, of internal and third parties developments, in order to ensure the compliance with the best practices in application and infrastructure security for systems and services.
- Minimisation of interrupt in service provision by monitoring and controlling web accesses.
- Protection of data and information assets through proactive actions on critical processes.
- Compliance with technical and organizational security measures, established by the GDPR regulation.

LEONARDO'S OFFER PORTFOLIO

Leonardo protects Governments, National Critical Infrastructures and National Strategic Industries against cyber threats and attacks using its technology and experience in cutting-edge cyber security and critical IT systems, all crucial for the operation and service continuity for citizens and countries.

Organized into two different lines Business-driven Cyber Security and Critical Information Systems, Leonardo's Portfolio leverages the main emerging technologies and the most up to date technological paradigms to offer solutions, platforms and services able to support customers' secure digital transformation.

The Security & Privacy by Design suite is part of the Critical Information Systems offer, including:

- Solutions and services for the secure digitisation of processes, infrastructures and applications and integrated digital transformation programs of strategic national customers.
- Secure-by-design systems developed using analytics, big data & IoT technologies to support the operation/provision of core services of critical and government infrastructures also during their path to digital transformation.

For more information please email:
securityandinformation@leonardocompany.com

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

leonardocompany.com

LEONARDO