THREAT INTELLIGENCE SOLUTIONS

Cyber protection for Governments, Critical Infrastructures and large strategic national enterprises is related to the whole threat life cycle and management, Threat Intelligence represents the first step. Threat Intelligence is crucial within the cyber protection process because it allows a proactive, aware and integrated management of vulnerabilities and response to incidents, leveraging on a sound framework of cyber threats contents and attackers.

Cyber attacks are various, they are growing exponentially in terms of involved subjects, reasons, strategies and methodologies used, resulting in an increasing asymmetry between attackers and victims. Attacks are carried out with the aim of disrupting vital services to citizens, stealing sensitive data, damaging reputations and undermining citizens' trust in Institutions. In addition, the network is used to address criminal and terrorist activities and actions.
As a result, it is increasingly important to be able to fully understand cyber threats' characteristics to manage them effectively and ensure the protection and resilience of critical infrastructures and national organisations, such as airports, ports, power plants, telecommunications companies and banks.

In this context, the adoption of Threat Intelligence solutions allows a critical infrastructure to continuously monitor the multiple sources of information related to cyber threats and potential attacks. Their analysis and correlation through Threat Intelligence solutions increases the effectiveness of situational awareness and operational defence capabilities with the goal of maximising the organisation's resilience.

THREAT INTELLIGENCE SOLUTIONS

THREAT INTELLIGENCE SOLUTIONS

Leonardo's Threat Intelligence Solutions include systems and services based on the monitoring and analysis of large amounts of open source data, deep and dark web, aimed at detecting cyber attacks being prepared and information illegally stolen and published on the web. The solution also provides a comprehensive overview on brand or event sentiment, and the prevention of cyber frauds carried out through the Internet.

The Threat Intelligence solutions significantly enhance the predictive capabilities of Leonardo's Next Generation Security Operation Center (NextGen SOC) with services proactively targeting the detection of cyber threats, the management of vulnerabilities and the response to security incidents.

LEONARDO APPROACH AND SKILLS

Leonardo approach to Threat Intelligence is either tactical or strategic, based on the customer's perception of Cyber Security and according to his organisational and financial commitment.

Through a **tactical approach**, the customer is automatically informed in advance of any dangerous vulnerabilities and potential data loss due to cyber threats or of the sentiment about a brand or a product. The initial investment for Threat Intelligence solutions can be progressively increased.

On the other hand, a **strategic approach** strengthens the customer's ability to monitor the progress of cyber threats over time in order to prevent particularly expensive events, such as sophisticated cyber attacks, counterfeiting and online identity theft, leveraging on automatic analysis and correlation tools, and the support of specialists and experienced intelligence analysts. Since the human factor is essential, even though edge technologies such as artificial intelligence are used to enhance research and highlight deductions, new links and information, Leonardo's analysts team operates through the Intelligence Operation Center supported by next generation SOCs.

The system processes information and data through an end-to-end flow ranging from the collection of open sources information (OSINT), to the building of a knowledge base to carry out analysis and reasoning. Both artificial intelligence techniques and a big data analytics engine are used for the purpose.

Intelligent data collection: open and multiple sources are continuously monitored by Leonardo's systems to capture behaviour and information also using cognitive agents to enhance collection abilities, if ready-to-use information sets are not available.
Knowledge base: a single knowledge base with a common language is built through the classification and the semantic analysis of multimedia content, collected and integrated with information specifically related to the cyber security domain.
Analysis & correlation: the drill down analysis, the semantic understanding and the information correlation are implemented using a high computing capacity and proprietary advanced analitics tools based on graph theory (case manager).
Reasoning: artificial intelligence, in the form of machine learning tools and virtual assistants, supports intelligence analysts in deductive reasoning and in scenario understanding, from the deduction of

new logical consequences, called inferences, to the interpretation of information sets built throughout the process of intelligent information transformation.

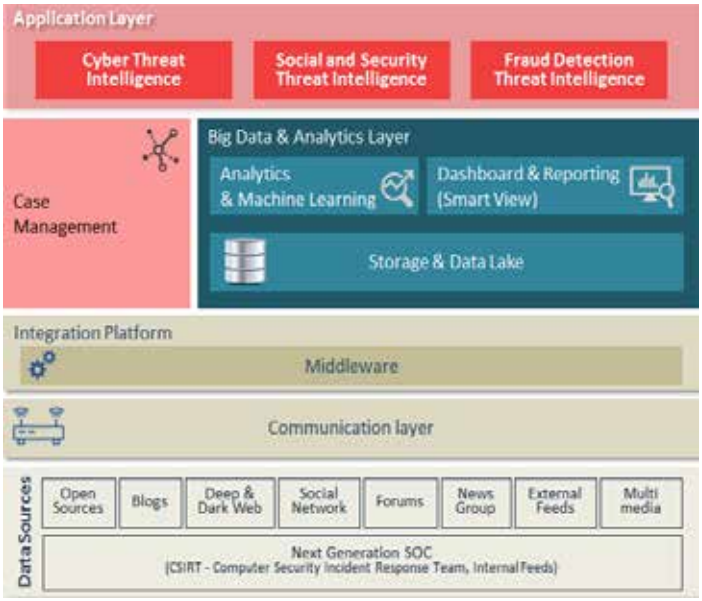
FUNCTIONALITIES AND ARCHITECTURE

Leonardo's Threat Intelligence Solutions include three sets of functionalities that can be selected according to customer's context and requirements. Each set is configurable into single services designed to operate in specific application scenarios, in cloud or on premises, depending on the operating context:

- **Cyber Threat Intelligence:** detects new vulnerabilities, cyber attacks being prepared and information illegally stolen from companies and organisations posted on the Internet, through the continuous monitoring of web and darknet sources and the real-time analysis of huge amounts of data searching for possible clues.
- **Social and Security Threat Intelligence:** acquires, analyses and correlates information on open sources in order to offer a complete overview of the online sentiment related to socio political events. This contributes to improve the awareness of imminent potential threats against the customers' assets.
- **Fraud Detection Threat Intelligence:** prevents internet frauds relevant to phishing campaigns, domain hijacking and theft of digital identities through the continuous monitoring of web and darknet sources aimed at identifying attackers and improving the customers' ability to protect themselves against internet frauds.

The platform architecture includes the following layers:

- **Data sources:** open sources continuously monitored to gather information (feeds, etc).
- **Integration & Communication:** it enables the connection of heterogeneous cyber information sources with the processing, correlation and analysis infrastructure.
- **Big data analytics & Case management:** it represents the big data and advanced analytics engine where the collection, normalisation, analysis and visualization of data are fulfilled to support the applications providing functionalities and services.
- **Application:** it includes the applications implementing Threat Intelligence functionalities.



SERVICES AND SUPPLY MODELS

The customer can choose, according to the specific sector and its peculiar needs and requirements, to install a Leonardo Threat Intelligence system on premises and to include, in addition to the design & build of the solution, also on site ongoing support provided by Leonardo (**on premises model**). Selecting the **full-outsourcing model**, the customer can decide to use a subset of services with pre-configured functions based on specific application scenarios of interest and receive automatic reports that can be used without the support of analysts.

Customers can also decide to implement the system at their premises and simultaneously make use of Leonardo's infrastructure only for those services that require high computing capacity without facing additional costs (hybrid model).

Leonardo's Threat Intelligence on-premises model is better suited to the needs of Law Enforcement and Intelligence Agencies for counter terrorism activities and for the support of investigation and crime preventing activities. On the contrary, hybrid or remote models, best meet protection and cyber resilience needs of critical infrastructures and multi-national strategic enterprises with international networks.

THREAT INTELLIGENCE SOLUTIONS

BENEFITS

- Forecast and prevention of cyber attacks pursuing financial losses or compromising operations activities of companies or organisations taking advantage of customer's application vulnerabilities through specialised malware.
- Identification, prevention, management and analysis of threats to national and international security coming from criminal networks and organizations operating on the web and the darkweb.
- Protection of people and corporate assets from propaganda attacks by monitoring users' opinions on topics specifically identified by the customer.
- Real-time identification of frauds, identity thefts and illegal activities, damaging the company or the organization digital reputation.

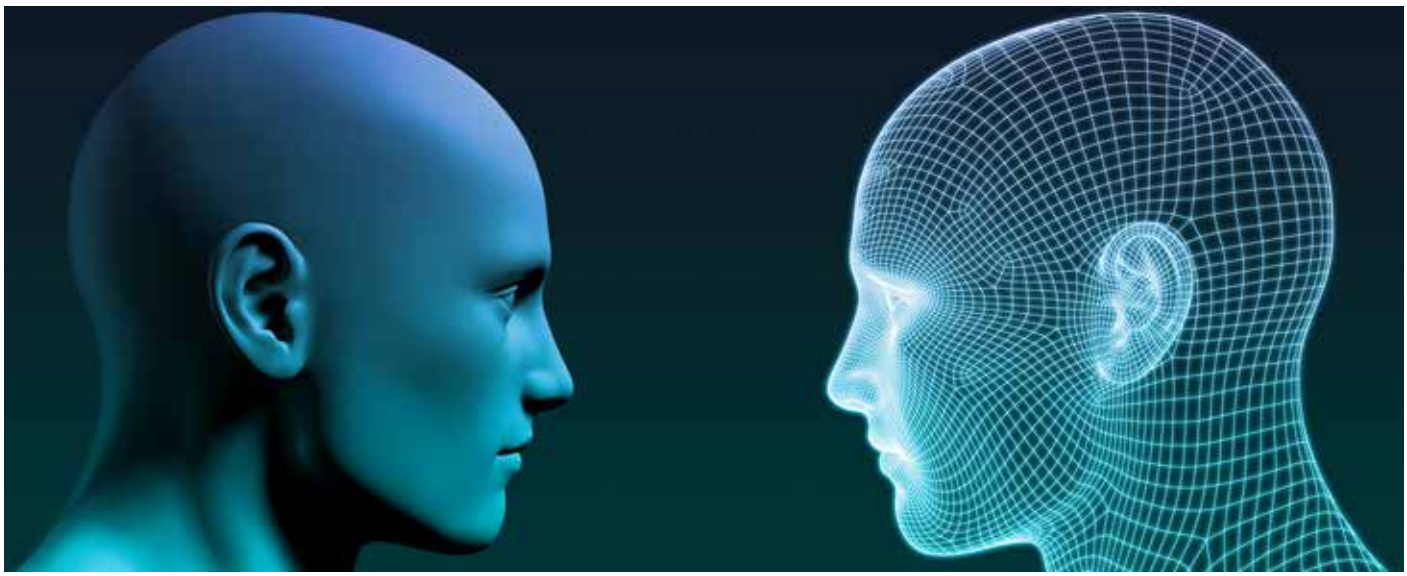
LEONARDO'S OFFER PORTFOLIO

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 Threat Intelligence Solutions are part of the Business-driven cyber security offer, including:

- **Cyber Protection & Resilience** for governments and critical infrastructures through services, tools and methodologies for the management of the entire threat life cycle and for the resilience of systems and services against cyber-attacks.
- **Intelligence & Investigation** in order to support Law Enforcement Agencies, Blue Lights e and Defence in the research, the collection and the analysis of relevant information for investigation activities, strategic intelligence and preventing crime.
- **Cyber Training** for the creation and simulation of complex cyber-warfare scenarios aiming at training operators in charge of IT/OT system security, both in the civil and military sector.



LEONARDO
CYBER SECURITY

For more information please email: securityandinformation@leonardocompany.com
Leonardo S.p.a.
Via Laurentina, 760 - 00143 Roma - Italy - Tel: +39 06 50275738 - Tel +39 06 50275685
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