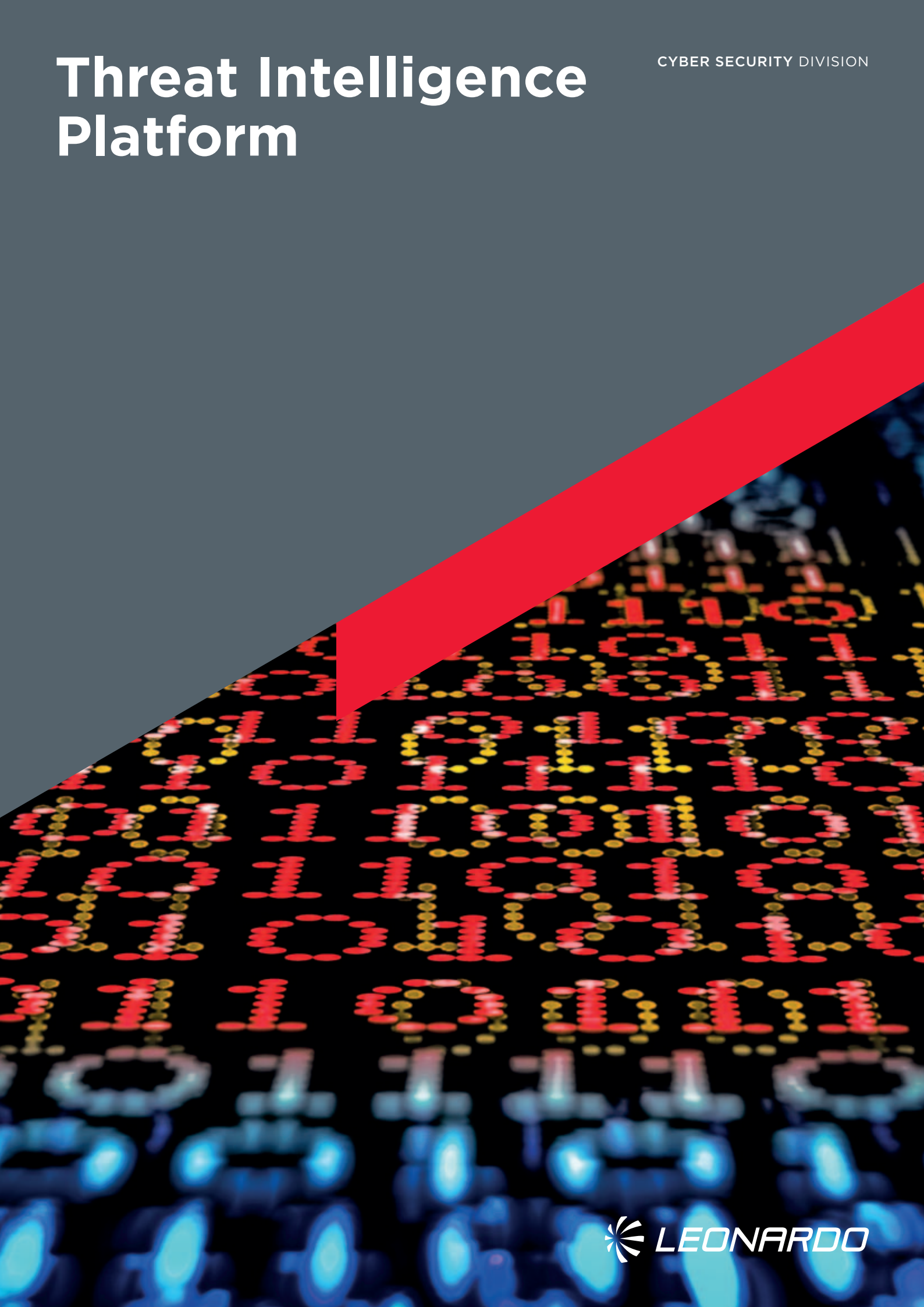
Threat Intelligence Platform

CYBER SECURITY DIVISION



LEONARDO

The cyber protection of governments, critical national infrastructures and large strategic enterprises is related to the whole threat life cycle management and Threat Intelligence represents the first and fundamental step. Threat Intelligence is crucial within the cyber protection process because it allows a proactive, aware and integrated vulnerabilities and incident management.
Cyber-attacks are exponentially growing in terms of involved subjects, reasons, strategies and methodologies increasing the asymmetry between attackers and victims.

Attackers are increasingly organized groups that conduct large scale, territorial and target independent actions aiming to maximize profit.
Moreover, all government institutions and national strategic organizations have become potential targets also for organized «state-sponsored» criminal groups that pursue specific interests using the cyber space as a battlefield between States.

In this scenario having a Threat Intelligence Platform, able to continuously monitor multiple information sources, is essential to effectively predict cyber threats and prevent potential cyber-attacks.
The analysis and correlation of the information gathered increases cyber situational awareness and operational defence capabilities maximizing the resilience of governments an organizations.

THREAT INTELLIGENCE PLATFORM

Through the monitoring and analysis of large amounts of open source information, Leonardo's Threat Intelligence platform provides Government Agencies and Critical National Infrastructures with advanced on premises tools aimed to predict and prevent cyber threat as well as to identify attackers, motivations, dynamics and characteristics of cyber-attacks.
Our Threat Intelligence Platform enables intelligence analysts to find the right information and transforming it into actionable intelligence thanks to innovative visual analysis tools. It is based on a unique knowledge base integrating open web data and specific cyber security information using a unique cyber ontology accessible to analyst using natural language.

APPROACH AND SKILLS

The system processes information and data through an end-to-end flow ranging from the collection of open sources information to the building of a knowledge base to carry out analysis and reasoning.

- **Intelligent data collection:** open and multiple sources are continuously monitored by Leonardo's systems to capture behaviour and information also using crawlers based on proprietary technologies able to capture even high-volatile information from open sources including deep web and darknet.
- **Knowledge base building:** data and information are normalized, indexed and classified, to extract entities that feed a knowledge base that can integrates also information specifically related to the cyber security domain.
- **Knowledge base analysis & correlation:** the knowledge base's contents are deeply analysed to extract from them the information of interest using proprietary tools of visual link analysis and semantic engines.

› **Reasoning:** machine learning tools and virtual assistants, support intelligence analysts in deductive reasoning and in scenarios' understanding, through innovative visual analysis, semantic reasoning techniques and the support of a virtual assistant.

Leonardo can offer to its customers both design & build professional services and on site ongoing support provided by highly skilled intelligence analysts. Leonardo analysts have an in-depth expertise on data normalization, ontologies and taxonomies structuring, big data processing technologies. They are also highly skilled in vulnerabilities and threats analysis with specific competences on the most advanced techniques used to launch cyber-attacks.

MAIN FUNCTIONALITIES

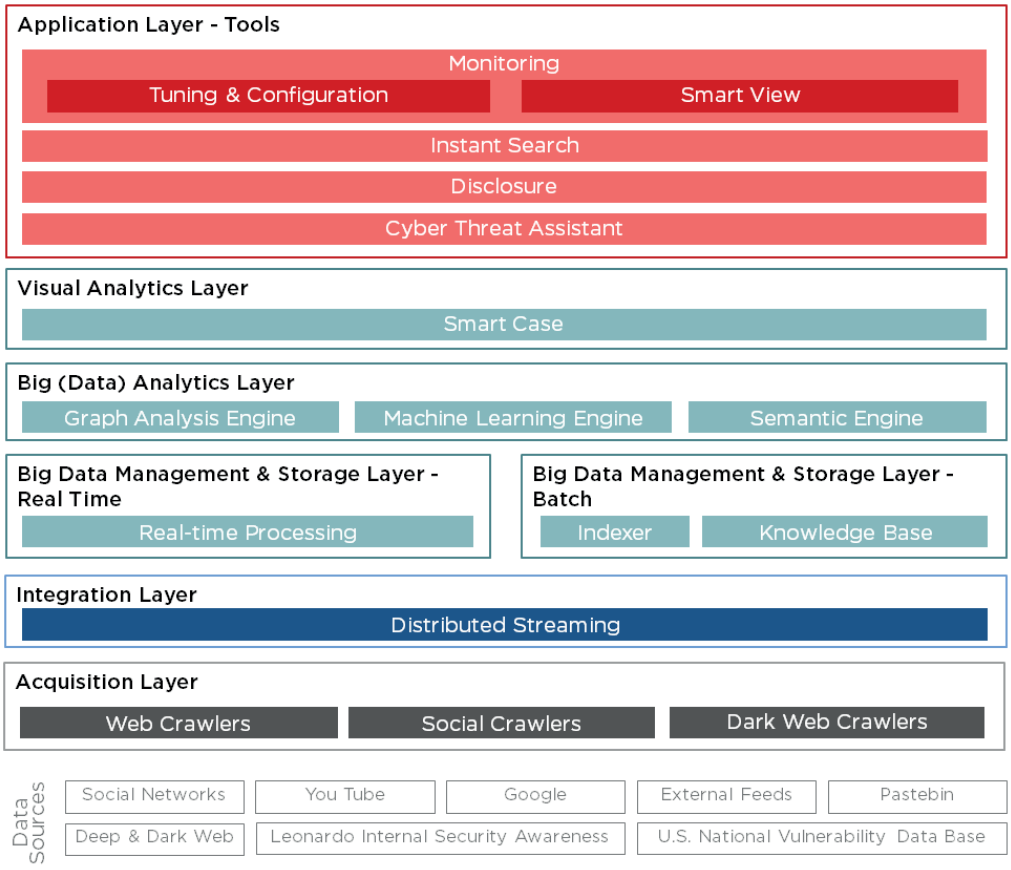
Leonardo's Threat Intelligence Platform includes a set of functionalities to enhance analysts' capabilities and highlight deductions, new links and "hidden" information.

› **Tuning & Configuration:** it allows to configure ontologies and taxonomies used by the system to acquire and process information from open sources, on the basis of customers' needs.
› **Smart View:** this dashboard enables analysts to monitor the information acquired over time and to identify anomalies through aggregated views that simplify the analysis of huge data samples.
› **Disclosure:** it allows access to reports published by companies and organizations operating in Cyber Security and Threat Intelligence areas with the aim of improving analysts' prevention and detection capabilities.
› **Instant Search:** this function can instantly searches information related to topics of interest by analyzing and correlating information from several info providers selected on the basis of customer's needs.
› **Smart Case:** advanced tool to support the complex cases' analysis, allows to define and consolidate all the significant elements for the analysis and to highlight the relations of interest.
› **Cyber Threat Assistant:** virtual assistant designed to support Intelligence analysts during their daily activities, allows access to the contents of the knowledge base using natural language and is able to activate tasks autonomously to integrate missing information.

ARCHITECTURE AND TECHNOLOGIES

Designed to continuously monitor, collect and analyse huge amounts of open heterogeneous information, the platform architecture and includes the following layers:

› the acquisition layer gathers data from open sources through cognitive agents to collect, autonomously and anonymously, information of interest defined on the basis of specific configurations.
› the integration layer manages and integrates the data flows, making them available to the different processing components.
› the big data analytics layer includes advanced analytics engines aimed to execute specific classification/clustering algorithms with the aim of effectively extracting their intrinsic value.
› the visual analytics layer provides an interactive visualization of data sets in order to highlight and intuitively represent information extracted from analytics engines.
› the application layer consists of advanced tools and applications implementing threat intelligence functionalities.



The Threat Intelligence platform includes a semantic engine trained through machine/deep

learning algorithms to interpret natural language with the aim to understand the sentiment of discussions, categorize documents by topic and perform semantic searches on specific topics of interest.
The platform uses artificial intelligence also to support the analysts' activity through the automatic integration of available information and the autonomous execution of tasks with the aim of answering questions for which there is no direct evidence.
Semantic reasoning techniques are implemented to deduce logical consequences starting from the contents of the knowledge base that represents and integrates, using a single ontology, freely accessible data on the web and specific information coming from cyber security domains.

BENEFITS

- Identification of authors, motivations, dynamics and characteristics of cyber-attacks against governments, critical national infrastructures and strategic companies.
- Prediction and prevention of cyber-attacks taking advantage of customer's application vulnerabilities through specialized malware.
- Identification, prevention, management and analysis of threats to national and international security coming from cyber-criminal groups.
- Protection of events, 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 Platform is 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.

For more information please email:
ict-cyber@leonardocompany.com

Leonardo S.p.a.
Via Enrico Mattei, 21 - 66013 Chieti Scalo (CH) - Italy
Tel. +39 0871 58541

MM08965 09-19

LEONARDO