LEONARDO CYBER & SECURITY SOLUTIONS

CYBER INFORMATION SUPERIORITY

LEONARDO

Cyber threats are increasingly based on hybrid and complex actions that exploit disinformation, cyber-attacks, military actions, often over a long period of time and used in conjunction with each other.
Attackers have more and more economic and technological resources at their disposal, they are highly skilled, motivated and organised too. As further evidence, state-sponsored actors increasingly collaborate with cyber-crime groups to exploit their evolved tools in order to launch simultaneous and coordinate cyber-attacks against strategic national infrastructures.

These actions represent a potential threat to sovereignty of countries and supranational organizations as they offer hostile nations, terrorist organisations and criminal actors with an extremely effective, cheap and relatively anonymous way to influence geopolitical balance.
In this threatening and constantly changing scenario, is vital for organizations to obtain valuable and actionable information, which can be used to rapidly implement targeted defence and containment actions.

CYBER INFORMATION SUPERIORITY SUITE

To pursue this objective, Leonardo has designed and developed a **Cyber Information Superiority (CIS)** suite based on Information Superiority applied to the cyber domain and allowing the collection, processing and dissemination of an uninterrupted flow of huge amount of data with the ultimate goal of countering adversaries' activities.
The CIS suite consists of three modules, that aim to maximise the profitability of information both coming from the monitoring and management of corporate security infrastructures and those acquired through commercial information feeds.

- **CYBER THREAT INTELLIGENCE SYSTEM (CTIS)**, represents the core of Cyber Information Superiority suite as it is based on a single knowledge base containing all information related to victims and threat actors, together with their capabilities and the infrastructures leveraged. This platform is provided with advanced analysis modules that exploit machine learning and artificial intelligence algorithms to facilitate data analysis. These features enable the provision of global and tailored cyber threat intelligence services, which are crucial for identify new cyber threats and effectively countering threat actors.

- **LEONARDO END POINT SECURITY (LENS)**, flexible and innovative Endpoint Detection & Response (EDR) tool allowing to collect telemetry and interact with deployed agents, LENS can be installed on various types of end point (IT and OT). It guarantees the "actionability" of the information contained in the knowledge base as it enables early detection of any anomaly and supports immediate implementation of the most appropriate response and containment actions.

- **ARGO,** is a multi-sandbox solution that provides a powerful environment supporting analysts in malware classification and management performing and combining static analysis with dynamic analysis and information enrichment . Argo orchestrates the Leonardo proprietary tools with other several commercial products (antivirus and sandboxes) normalizing results to maximize analysis capabilities.

In situations where customer needs to acquire information from open sources, the Cyber Threat Intelligence System can natively integrate the Threat Intelligence System (TIS) Osint module that monitors and analyse OSINT (Open Source INTelligence) and SOCMINT (SOCial Media INTelligence) sources.

CYBER THREAT INTELLIGENCE SYSTEM

The new generation Cyber Threat Intelligence System is designed to manage the entire intelligence cycle. To pursue this objective, it provides the possibility to manage collection plans, orchestrate the collection, processing and dissemination of the information, leveraging a flexible and scalable knowledge base that is built on top of a customizable ontology. This is one of the key feature of the Cyber Threat Intelligence System platform. In fact, Leonardo starts from the assumption that “no one-fits-all” ontology exists that can represent all use cases in the cyber field, and also that it may be necessary, in the future, to adapt the ontology over time to meet new customer’s needs.

APPROACH & SKILLS

The CTIS is based on an **end-to-end process** ranging from the collection of external and internal data sources to the dissemination of information both to analysts, through reports and notifications, and to security systems by means of the integrated automation and orchestration functions.

01. Plan & Direct

Collection plans are managed and monitored developing and tracking Intelligence Requirements and Requests for Information. It is also possible to **assign tasks** to analysts as well as to manage and to monitor **trends** about the ongoing performance.

02. Collect

External Threat Intelligence, internal cyber security data sources and user supplied data are fused together in one comprehensive location, the knowledge base, that allows the definition of a **tailored ontology**. An extensive library of **dedicated connectors** provides the automation of threat intelligence feeds, with full support for MISP, STIX, SIGMA, YARA and many more “open” formats. In addition, robust and documented **REST** (REpresentational State Transfer) **APIs** allow to configure and manage tailored data integrations through a dedicated engine that allows to **deduplicate entities**.

03. PROCESS

Incoming data are processed through a **knowledge graph** data model and a **processing engine**, allowing data enrichment with an innovative event based approach and through an **extensive library of processing tools** that can be easily extended by leveraging a robust architecture. **Automatic and recursive enrichment** can be configured at will through **playbooks**, providing a unified workspace for all members of the analysts’ team regardless of work role or experience level.

04. ANALYZE

Data and information analysis is supported by **exploratory data analysis** functionalities that allow to **navigate the underlying knowledge graph data model visually** and through REST APIs; complex queries are supported by an integrated **search engine data base**. In addition, a set of integrated tools enable to perform **manual analysis** and to organize entities, evidences and findings’ organization in a threat analysis case. Reports can be generated within the platform through an **advanced editor**.

05. DISSEMINATE

Changes related to configurable topics of interest are automatically notified to analysts with a ''need to know'' and ''need to share'' approach by creating customized reports. The platform also provides **intelligence feeds** to SIEM, firewalls, EDRs, etc. through integrated automation and orchestration functions.

AUTOMATION & ORCHESTRATION

An effective cyber threat intelligence requires to implement the entire intelligence cycle, starting from the **information requirements’ definition** and passing through **data collection, processing** or enrichment, **analysis, dissemination** and feedback.
For this reason, Leonardo's Cyber Threat Intelligence System offers all the functions necessary to orchestrate these different phases. The orchestration and automation engine has been developed to be extremely **scalable, flexible** and **extensible**.

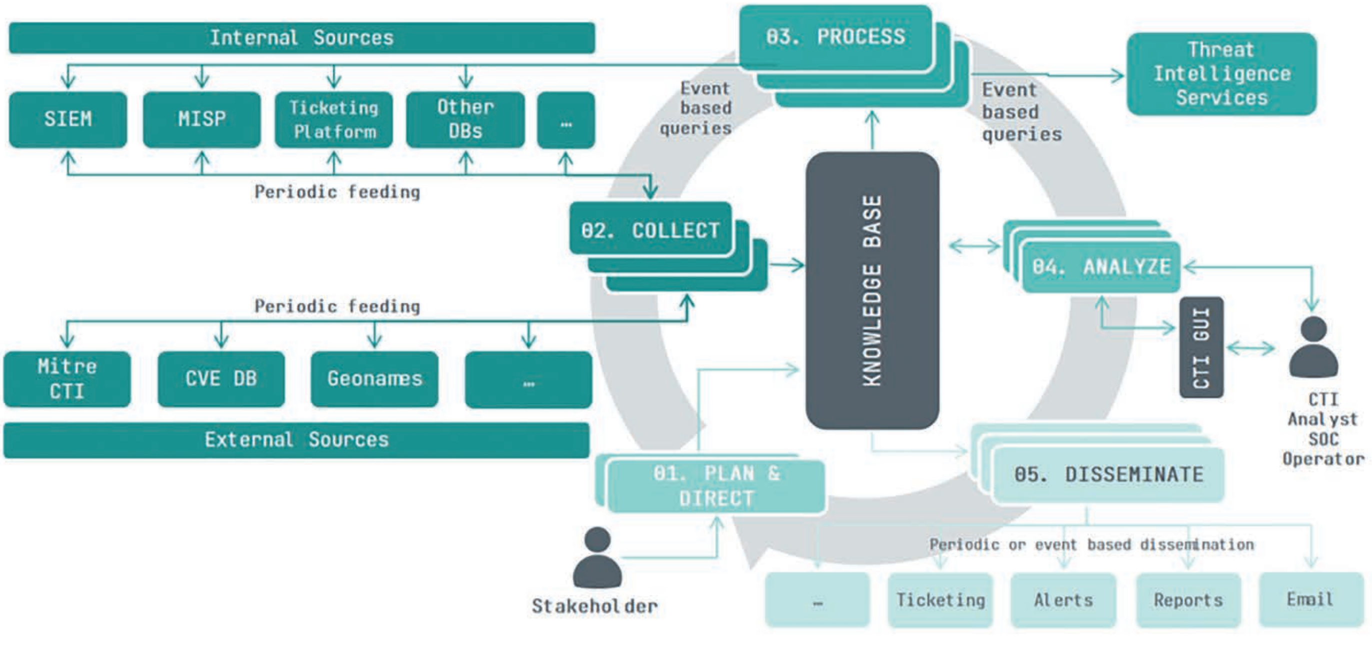
MAIN FUNCTIONALITIES

Knowledge graph modelling

The graph data model is the heart of our solution. A flexible data storage catalogue where entity types, their attributes and the possible relationships can be defined. Each time a new entity is inserted into the graph it triggers a set of automated and configurable actions (playbooks), contextualizing and enriching it with all the information made immediately available to the user.

Integration

Baseline and specialized tools can be integrated leveraging existing connectors and APIs in such a way to provide customizable collection, processing and dissemination phases of the intelligence cycle fitting the needs of incident responders, threat intelligence analysts, Security Operation Centre operators and Chief Information Security Officers in one.



Cyber Threat Intelligence System (CTIS) Automation & Orchestration

Knowledge dashboard

The knowledge dashboard allows to analyse data related to a given entity, together with all the entities that are linked through a direct or inferred relationship. The overview panel can automatically provide charts about all the attributes of the entities defined in the ontology. This is a necessary step of any exploratory data analysis task.

Search Engine

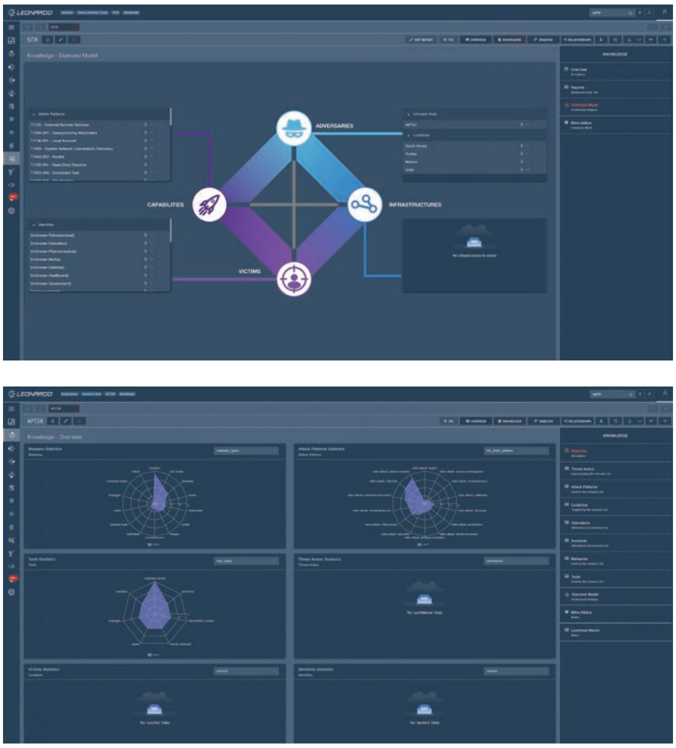
The integrated search engine leverages the ontology definition and provides matches categorized by their entity types. The text search automatically works on all the attributes defined in the ontology. Complex queries can be performed by leveraging the documented APIs.

Customizable Ontology

We start from an important hypothesis: “no one-fits-all ontology exists”. Therefore, you will be able to define your own entities, attributes and relationships in such a way to fit your own needs. Constraints, types and validation rules can be enforced on an attribute base.

Fine Grained Access Control

The platform uses both a Role Based Access Control and an Attribute Based Access Control in such a way to enforce the “need to know” and “need to share” approach. Each source of information can assign a different classification, releasability and Traffic Light Protocol (TLP) level to a single piece of data. Users gain access only to those entities and those sources defined in a customizable policy ruleset.



Cyber Threat Intelligence System (CTIS) Knowledge dashboard interface examples

WHY CYBER INFORMATION SUPERIORITY SUITE?

- Effective prediction and identification of advanced threats, designed to target a specific organization’s needs.
- Powered by the OSINT (Open Source INTelligence) and SOCMINT (SOCial Media INTelligence) collection provided by TIS Osint.
- Management of a highly structured intelligence process and orchestration of the technologies needed to instantiate it.
- Timely implementation of targeted remediation actions integrating other vendorsi’ EDRs, if any.
- Access to multiple malware analysis tools from a single dashboard, optimizing COTS (Commercial Off-The-Shelf) usage costs.
- Local management of vulnerability data, remediation actions and malware analysis.

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.

MM09135 09-23

leonardo.com