LEONARDO CYBER & SECURITY SOLUTIONS

CYBER THREAT INTELLIGENCE SYSTEM

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 Threat Intelligence System

INTEGRATION WITH THE LEONARDO END POINT SECURITY (LENS)

The CTIS is fully integrable with the entire Leonardo product ecosystem. In particular, CTIS is natively integrated with LENS, the Leonardo flexible and innovative Endpoint Detection & Response (EDR) tool, which allows for the collection of telemetry and interaction with deployed agents. It is designed to continuously monitor end-user devices' behavior, identifying suspicious patterns to detect the most complex cyber threats.

Additionally, it provides contextual information through a visual environment that allows security experts to evaluate the most appropriate mitigation activities for the detected malicious event and determine the recovery path for the systems involved in the incident.

LENS can be installed on various types of endpoints (IT clients, servers, OT devices, and network elements) with different operating systems to guarantee information "actionability" It enables early anomaly detection and supports the immediate implementation of the most appropriate response and containment actions.

The interfacing of the CTIS with LENS is "bidirectional," as it involves the mutual enrichment of their respective knowledge bases. In particular:

- The CTIS can analyze IPs and domains by retrieving information from the LENS server. For this purpose, a LENS analyzer has been developed to be launched on entities of type IP or domain to create entities in CTIS related to the IP or domain being analyzed;

- The LENS can retrieve Yara and Sigma rules associated with specific IPs and domains from from CTIS. This occurs through the API provided by CTIS itself.

PROPOSED APPROACH

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. 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.**

Cyber Threat Intelligence System

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 system 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 system also provides intelligence feeds to SIEM, firewalls, EDRs, etc. through integrated automation and orchestration functions.

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.

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

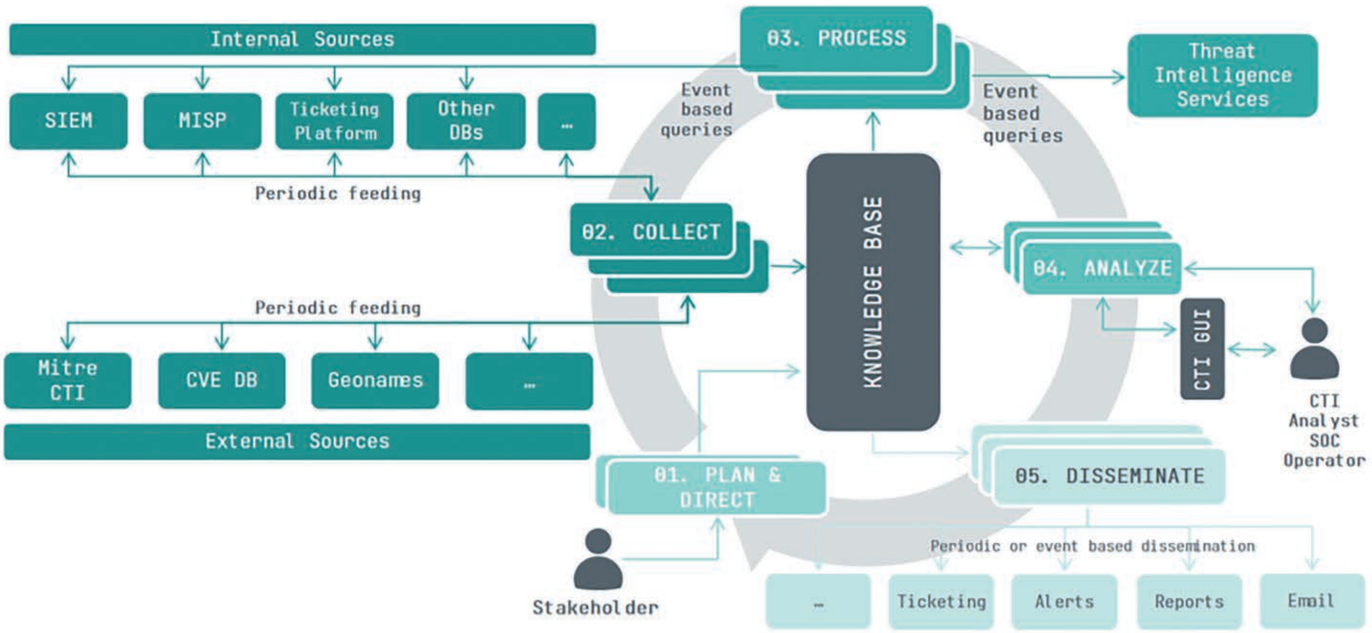
The graph data model is the heart of our solution. A flexible data storage catalogue where entity types, their attributes and the possible relationships can be defined. Each time a new entity is inserted into the graph it triggers a set of automated and configurable actions (playbooks), contextualizing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

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.



Cyber Threat Intelligence System (CTIS) Automation & Orchestration

Search Engine

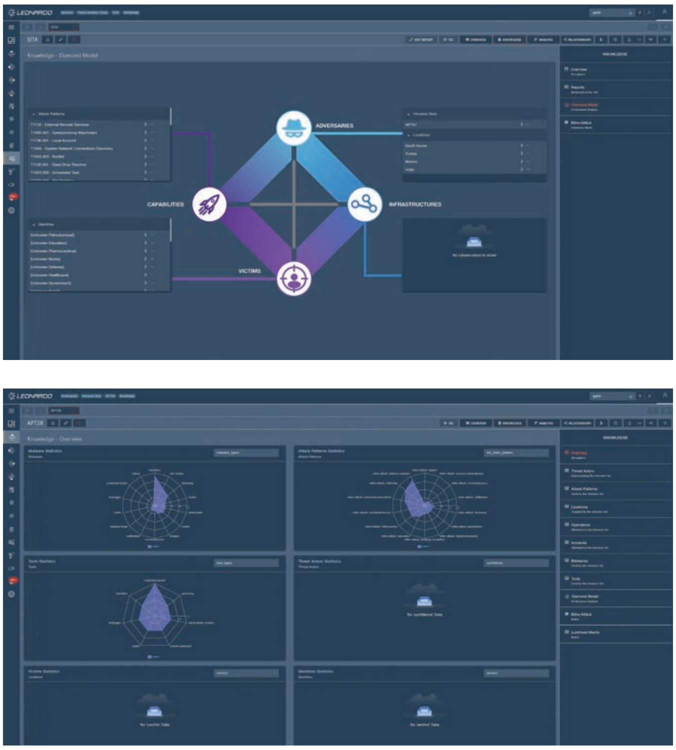
The integrated search engine leverages the ontology definition and provides matches categorized by their entity types. The text search automatically works on all the attributes defined in the ontology. Complex queries can be performed by leveraging the documented APIs.

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 system 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 THREAT INTELLIGENCE SYSTEM?

- 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.
- Natively integrable with the Leonardo End Endpoint Security

For more information:
cyberandsecurity@leonardo.com

Leonardo Cyber & 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.