CYBER & SECURITY SOLUTIONS

C-THINK

Leonardo Cyber Threat Intelligence

LEONARDO

Cyber threats are increasingly hybrid and complex, combining disinformation, cyberattacks, and even military operations—often conducted over extended periods and in a coordinated manner.

Adversaries now have greater economic and technological resources and are increasingly skilled, motivated, and highly organized. State-sponsored actors increasingly collaborate with cybercrime groups, leveraging their advanced tools to launch simultaneous, coordinated attacks against strategic national infrastructures.

Such actions threaten the sovereignty of nations and supranational organizations, offering hostile states, terrorist groups, and criminal actors an effective, low-cost, and relatively anonymous way to influence geopolitical balance.

In this constantly evolving threat landscape, it is vital for organizations to gain timely, actionable intelligence that enables rapid, targeted defense and containment measures.

ENABLING INFORMATION AND COGNITIVE SUPERIORITY

C-THINK is Leonardo's next-generation platform, designed to support analyst teams operating in high-confidential environments. By combining advanced automation and orchestration capabilities, it enables the prediction and prevention of the threats most likely to impact an organization, while supporting the adoption of proactive security measures.

To achieve this, C-THINK leverages both standard analysis models—such as the Diamond Model, STIX, and MITRE ATT&CK—and sector-specific frameworks developed for specialized contexts, including space systems and disinformation campaigns. By integrating Open-Source Intelligence (OSINT) and Social Media Intelligence (SOCMINT), C-THINK enhances situational awareness and expands visibility into emerging and evolving threats. At the same time, C-THINK ensures full interoperability with LENS and Leonardo's wider Cyber & Resilience ecosystem, allowing for seamless coordination between tools and operational functions.

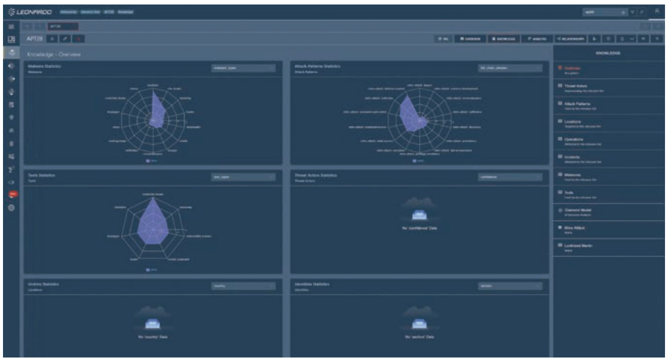
C-THINK can be deployed on-premises, offered as a SaaS, or provided as a fully managed service, depending on customer requirements.

APPROACH

C-THINK is built on an end-to-end approach that spans the entire Cyber Threat Intelligence lifecycle. The platform collects data from both internal and external sources, processes and analyzes them through advanced automation and orchestration, and finally disseminates actionable insights to analysts and security systems. This ensures that organizations can predict and prevent the most likely threats while enabling proactive and timely defense measures.

01. Plan & Direct

The process begins with the planning and coordination of intelligence activities. Analysts can define and monitor intelligence requirements and requests for information, ensuring that collection efforts are always aligned with operational and strategic priorities. The platform also makes it easy to assign and track tasks, while continuously monitoring performance trends. This structured approach ensures that intelligence operations remain focused, measurable, and adaptable to evolving needs.



C-THINK knowledge dashboard interface

02. Collect

At the collection stage, C-THINK consolidates a wide range of data sources into a single knowledge base. External threat intelligence feeds, internal cybersecurity data, and user-supplied inputs are automatically integrated through a highly configurable ontology, which extends and customizes the STIX 2.1 standard.

The system provides a rich library of connectors for the automation of feeds, fully supporting open formats such as MISP, STIX, SIGMA, and YARA. In addition, robust REST APIs allow seamless integration with third-party systems and deduplication of entities, ensuring clean, consistent, and reliable data for analysis.

03. Process

Collected data is processed through a powerful knowledge graph data model and a flexible processing engine. This enables advanced data enrichment with an innovative event-based approach and a comprehensive library of processing tools. The platform's robust architecture makes it easy to extend and customize these tools as needed.

Automatic and recursive enrichment can be fully customized, providing a unified workspace that adapts to each analyst's role and responsibilities. Information access and workflows are managed according to a "need-to-know" and "need-to-share" principle, ensuring both effective collaboration and strict confidentiality.

04. Analyze

The analysis phase transforms information into actionable intelligence. Analysts can navigate the knowledge base visually through an advanced graph interface or interact via REST APIs for technical queries. A powerful search engine supports complex queries, helping analysts quickly identify and correlate relevant data across vast datasets.

C-THINK also provides a dedicated workspace for structured threat analysis, where entities, evidence, and findings can be organized into comprehensive cases. Collaboration is strengthened through an advanced editor that enables analyst to work together, streamlining the creation of accurate and consistent intelligence reports. This integrated environment accelerates threat identification, improves team efficiency, and ensures that insights are delivered in a form directly usable for both tactical and strategic decision-making.

05. Disseminate

In the dissemination phase, C-THINK ensures that intelligence reaches the right people and systems at the right time. Analysts receive automatic notifications on topics relevant to their activities, ensuring timely awareness without information overload. Customized reports further provide tailored insights for technical teams, managers, and auditors.

At the same time, C-THINK delivers structured intelligence feeds directly to SIEMs, firewalls, EDRs, and other security systems, thanks to its built-in automation and orchestration functions. This dual approach—human-centric reporting and machine-to-machine integration— ensures that intelligence is not only generated but also made immediately actionable across the organization.

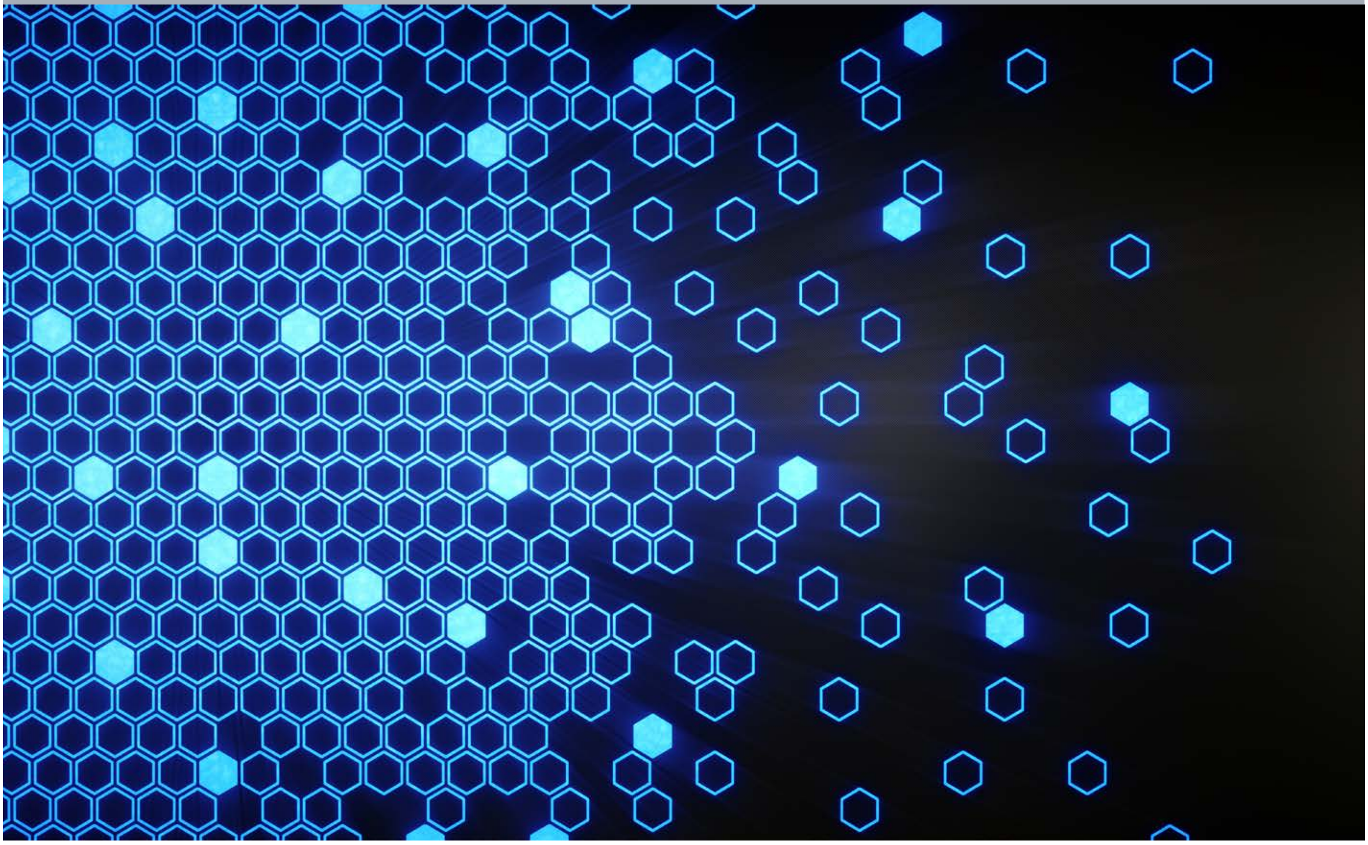
INTEGRATION WITH LENS

C-THINK is interoperable with LENS, the Leonardo's multi-functional Endpoint Detection & Response (EDR) platform for both IT and OT environments. By collecting telemetry and interacting with deployed agents and probes, LENS enables early detection of anomalies and intrusions, supporting timely response and containment based on fully customizable rules.

Through an intuitive visual environment, LENS provides contextual insight that helps security experts assess threats, select effective mitigation strategies, and determine recovery paths. Its compatibility with both ICT and ICS networks ensures comprehensive protection across converged infrastructures, including legacy environments and advanced digital systems.

The platform combines automated anomaly detection with a powerful query language, allowing analysts to filter billions of events and focus on relevant evidence with speed and precision. Detection and response rules can be adapted dynamically at runtime, enabling targeted monitoring and remediation both locally and centrally.

Integration with C-THINK is bidirectional, ensuring mutual enrichment of their knowledge bases and strengthening situational awareness across the entire security ecosystem.

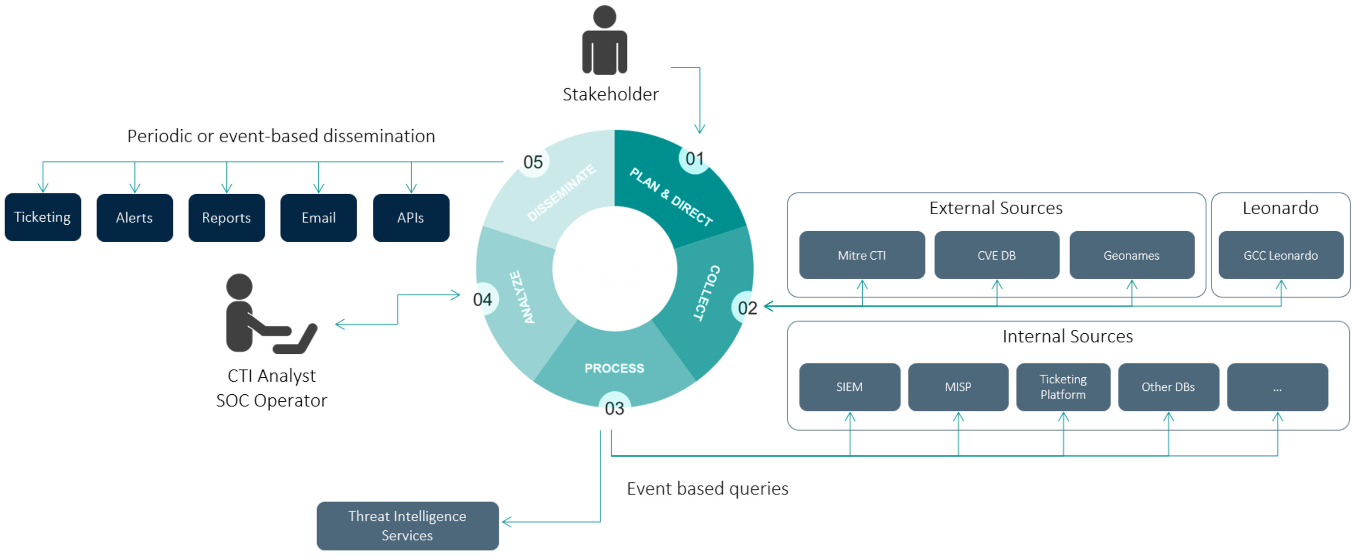


AUTOMATION & ORCHESTRATION

Effective cyber threat intelligence requires not only advanced analytical capabilities, but also the ability to automate and orchestrate the entire intelligence cycle — from the acquisition of data to its dissemination across the organization.

To meet this challenge, C-THINK integrates a powerful orchestration and automation engine, designed to be highly scalable, flexible, and adaptable to evolving scenarios. The platform automatically acquires information from both internal and external sources — including Threat Intelligence feeds, network logs, and attack reports — and enriches it with additional details such as IP reputation or correlation with known vulnerabilities.

At the same time, C-THINK coordinates the operation of different security systems — SIEM, firewalls, EDR, and SOAR platforms — creating a seamlessly connected ecosystem where intelligence becomes immediately actionable. Finally, customized intelligence is disseminated to different stakeholders, ensuring that each team — from technical operators to top management — receives the insights most relevant to their needs.



TAILORED THREAT ANALYSIS: STANDARD AND DOMAIN-SPECIFIC MODELS

C-THINK enhances threat intelligence with structured analysis based on both industry standards and domain-specific models. Standard models such as the Diamond Model, STIX 2.1, MITRE ATT&CK, and MISP ensure methodological rigor and interoperability across the cybersecurity community.

At the same time, the platform provides advanced specialization for critical domains. For instance, the **SPACE-SHIELD** framework, developed under the European Space Agency program, and **SPARTA** created by Aerospace Corporation, strengthens resilience against cyber threats targeting space infrastructures, while DISARM supports the analysis and management of risks linked to disinformation campaigns.

This dual capability—leveraging recognized standards while adapting to sector-specific challenges—makes C-THINK a versatile solution for organizations that require both breadth and depth in their cyber threat intelligence.

KEY FEATURES

→ **Native integration with data sources from Leonardo's Global Cybersecurity Center**, through the synchronization of the different C-THINK instances, to provide updated and qualified threat intelligence.

→ **Direct connection to configurable MISP servers** to share and receive structured threat information.

→ **Advanced situational** awareness through OSINT and SOCMINT integration, expanding visibility on emerging threats.

→ **Customizable modeling of threat data:** use of standard entities (e.g., STIX) or creation of new entities with specific attributes, relationships, rules, and constraints.

→ **Advanced graph-based queries** with a visual interface to define nodes, relationships, and semantic properties.

→ **Structured analysis based on standard models** (Diamond Model, STIX, MITRE ATT&CK) **or domain-specific models** (e.g., SPARTA and SPACE-SHIELD for space, DISARM for disinformation).

→ **Collaboration among analysts through shared reports and** dedicated plug-ins for inserting evidence, entities, and correlations.

→ **Interoperability with LENS** and Leonardo's cybersecurity ecosystem for seamless integration of tools and functions.

→ **Available as SaaS, on-premises, or fully managed service** to meet diverse infrastructure and organizational requirements.

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.

MM09135 10-25