LEONARDO CYBER & SECURITY SOLUTIONS

LEONARDO END POINT SECURITY

LEONARDO

LEONARDO END POINT SECURITY (LENS)

Cyber threats are constantly evolving. They can originate from various sources, using multiple vectors and shaping into different forms. In recent years, there has been a significant increase in the number and sophistication of cyber-attacks. This is due to a number of factors, including the growing digitalization of our society and the increasing use of emerging technologies.

Particularly, the growth of the Industrial Internet of Things (IIoT) has accelerated the convergence of the once separate domains of IT and OT. Today cyber-physical systems are connected to an array of sensors and tools that gather, analyse and communicate data with other devices and systems to improve output, quality, and consistency. The gains in efficiency come at a price, however, as increased connectivity sensibly expands the attack surface for threat actors.

By connecting legacy operational devices to the modern Internet, the IT-OT convergence has opened a new threat landscape as adversaries' target organizations leveraging their augmented attack surface.

In this threatening and constantly changing scenario, it is vital for organizations to obtain valuable and actionable information, and to be able to use them to rapidly implement targeted defence and containment action.

This can be achieved using advanced tools capable of detecting anomalies at an early stage, near the point of intrusion, in order to prevent attackers from moving laterally within the victim's network eventually compromising the entire ecosystem in which it operates.

INTEGRATION WITH THE CYBER THREAT INTELLIGENCE SYSTEM (CTIS)

LENS is natively integrable with the Leonardo Cyber Threat Intelligence System (CTIS). The CTIS is based on a single knowledge base containing all information related to victims and threat actors, together with their capabilities and the infrastructures leveraged.

The system 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 identifying new cyber threats and effectively countering threat actors.

The CTIS is designed to manage the entire intelligence cycle. To pursue this objective, it provides the capability to manage collection plans, orchestrate the collection, processing, and dissemination of information, leveraging a flexible and scalable knowledge base built on top of a customizable ontology.

This is one of the key features of the Cyber Threat Intelligence System. In fact, Leonardo starts from the assumption that no "one-size-fits-all" ontology exists that can represent all use cases in the cyber field and that it may be necessary, in the future, to adapt the ontology over time to meet new customer needs.

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

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

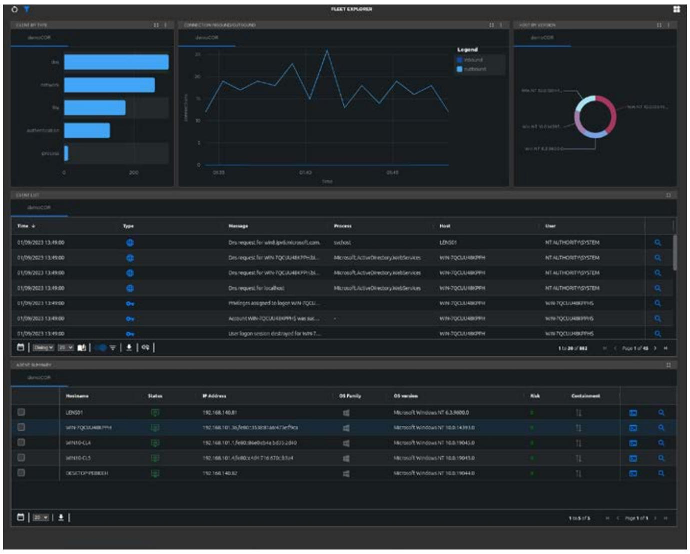
- The CTIS can analyze IPs and domains by retrieving information from the LENS server. For this purpose, a LENS analyzer has been developed to be launched on entities of type IP or domain to create entities in CTIS related to the IP or domain being analyzed.

LEONARDO END POINT SECURITY (LENS)

LENS is the Leonardo flexible and **innovative Endpoint Detection & Response (EDR) tool allowing to collect telemetry and interact with deployed agents**. It is designed to **continuously monitor end-user devices' behavior** identifying suspicious patterns **in order 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 to determine the recovery path for the systems involved in the incident.

LENS can be installed on **various types of end point** (IT clients and servers and OT devices and network elements) **with different operational system to guarantee information "actionability"** as it enables early anomaly detection and supports immediate implementation of the most appropriate response and containment actions.



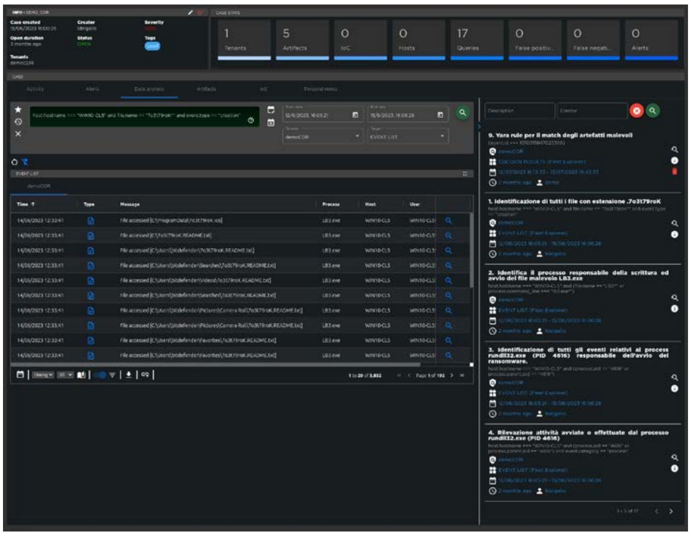
LENS Main Dashboard

LENS is a **highly flexible security system**:

- It has a **practical query language** that, in addition to the automatic anomaly detection mechanisms, allows the operators to acquire a complete view of all monitored systems and to focus their analysis, among billions of events, on the evidence of interest.
- It allows to implement **specific monitoring and remediation tasks directly on the end-points and/or at the central level**, with the possibility of instantiating them at run-time. In this way, it allows an easy and punctual adaptation of the monitoring and analysis techniques according to the specific needs and context.

MAIN FUNCTIONALITIES

- **Detection & Behavioral Analysis**: LENS supports the search performing a behavioral analysis on the large amount of events automatically collected and analyzed by the system, with the objective to identify any possible signal of suspicious behaviors, attributable to known threats.
- **Rapid Incident Analysis**: each single identified event is logically included in the context of the entire set of events detected over time. This, together with the possibility of visualizing data through multiple dashboards, enables quick evaluation and validation of even the most complex attacks, and the assignment of the right intervention priorities.
- **Effective Response and Mitigation**: enables the implementation of immediate containment actions through targeted interruption of processes, or isolation of compromised endpoints from all network activities, with the exception of monitoring connections.
- **Investigation Activities Support**: allows the analyst to collect information of interest in a case and to select it by means of advanced query tools in order to obtain really valuable and immediately usable information.
- **Tailored Threat Hunting Activities**: it supports a very accurate anticipation of the threats allowing the early preparation of detection and mitigation logics with a high degree of customization according to the infrastructure to be protected and the the Customer's threat profile.
- **High Interoperability**: LENS interoperates with the entire IT and OT security stack by forwarding events and raw data acquired from the protected end-points to SIEM systems.



LENS Investigation Dashborad

ARCHITECTURE

LENS architecture is multi-tenant, i.e. it allows the management of several tenants in a segregated manner. Analysts, if authorized, can therefore share information among several tenants.

- **Agents**: collect telemetry and send them to server. They are designed to be as "stealthy" as possible to minimize CPU and RAM occupancy. These features also ensure that the system is extremely 'silent' to avoid compatibility problems.
- **Proto Server**: enables secure and encrypted communication between agent and central system. This allows commands to be sent to endpoints in near real time.
- **Server**: analyses events and applies logic looking for patterns and meaningful sequences managing data lake, performs computation (e.g. risk score) and provides search tools. The server interoperates with agents installed on the endpoints via customized gRPC (Google Remote Procedure Call) protocol, which ensures compact data streams, reduced memory occupancy and bidirectional streaming functions. The server can perform automatic actions or request operator intervention (via WebGUi or CLI). Actions can include Cocoon deployment, dangerous code removal, malwares' deception and other program execution.
- **Automation**: server-side plugins enable event post-processing and correlation.
- **Web GUI**: provides user friendly interaction for data navigation and command execution. A visual analysis environment, configurable and customizable via widgets, provides a user-friendly interface for understanding and navigating the history of events unfolding in the control perimeter, interacting with individual agents and executing specific commands.
- **Cocoon**: DLL-level intelligent plug-in performing autonomous specific actions.

COCOONS

The continuous evolution of cyber threats requires extremely flexible and evolving defense tools. To meet this requirement LENS provides the Cocoon mechanism: a protected execution environment within the agents where plugins can be installed. They can be deployed through standard languages and allow to implement additional processes to agents' basic functionalities in order to realize specific control and reaction logics. These plugins can be loaded at runtime into the agents through the Web GUI. Cocoons can be instantiated either permanently in the agents, or loaded into the dynamic reference memory, to leave them with minimal visibility to an attacker. The Cocoon environment has security mechanisms capable of handling any plugin errors and safeguarding the continuity agent's operation. Plugins can also be developed by the end user, with the possibility of relying on Leonardo professional services dedicated to this activity.

KEY BENEFITS

- Early detection of new attacks by acquiring and correlating data to provide actionable information on application behaviour and file system usage.
- Timely implementation of customizable detection rules and response activities to respond to specific customers' needs.
- Integration with other vendors' EDR capabilities, if needed, optimizing customers' past investments.
- Local management of vulnerability data and information, detection rules and response actions
- Natively integrable with the Leonardo Cyber Threat Intelligence System

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.