CYBER & SECURITY SOLUTIONS

LENS

Leonardo End Point Security

LEONARDO

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 several 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 rely on a myriad of sensors and tools to gather, analyze and communicate data. This interconnection drives improvements in output, quality and consistency. However, this increased connectivity comes at a price: a broader and more complex attack surface, which cyber adversaries are quick to exploit. The IT-OT convergence, and especially where legacy systems are exposed to modern network environments, introduces new vulnerabilities that demand a robust and unified cyber defense strategy.

In this dynamic and threatening scenario, organizations need enhanced visibility across all network layers to detect threats before they escalate, along with simplified management of segregated and resource-limited systems. It is vital to obtain valuable and actionable information and be able to act on it quickly through agile tools that reduce noise, eliminate false positives, and help analysts focus on what truly matters.

The ability to detect anomalies near the point of intrusion, including advanced threats such as zero-day exploits, sophisticated malware, and APTs, is essential to prevent lateral movement and limit the risk of widespread compromise. At the same time, organizations must ensure continuity of operations with solutions that remain effective even under attack or in degraded conditions.

Fast and automated remediation actions, tailored to specific technology domains, can significantly reduce incident response times and minimize the operational impact of cyber-attacks.

END POINT PROTECTION FOR A CONVERGED WORLD

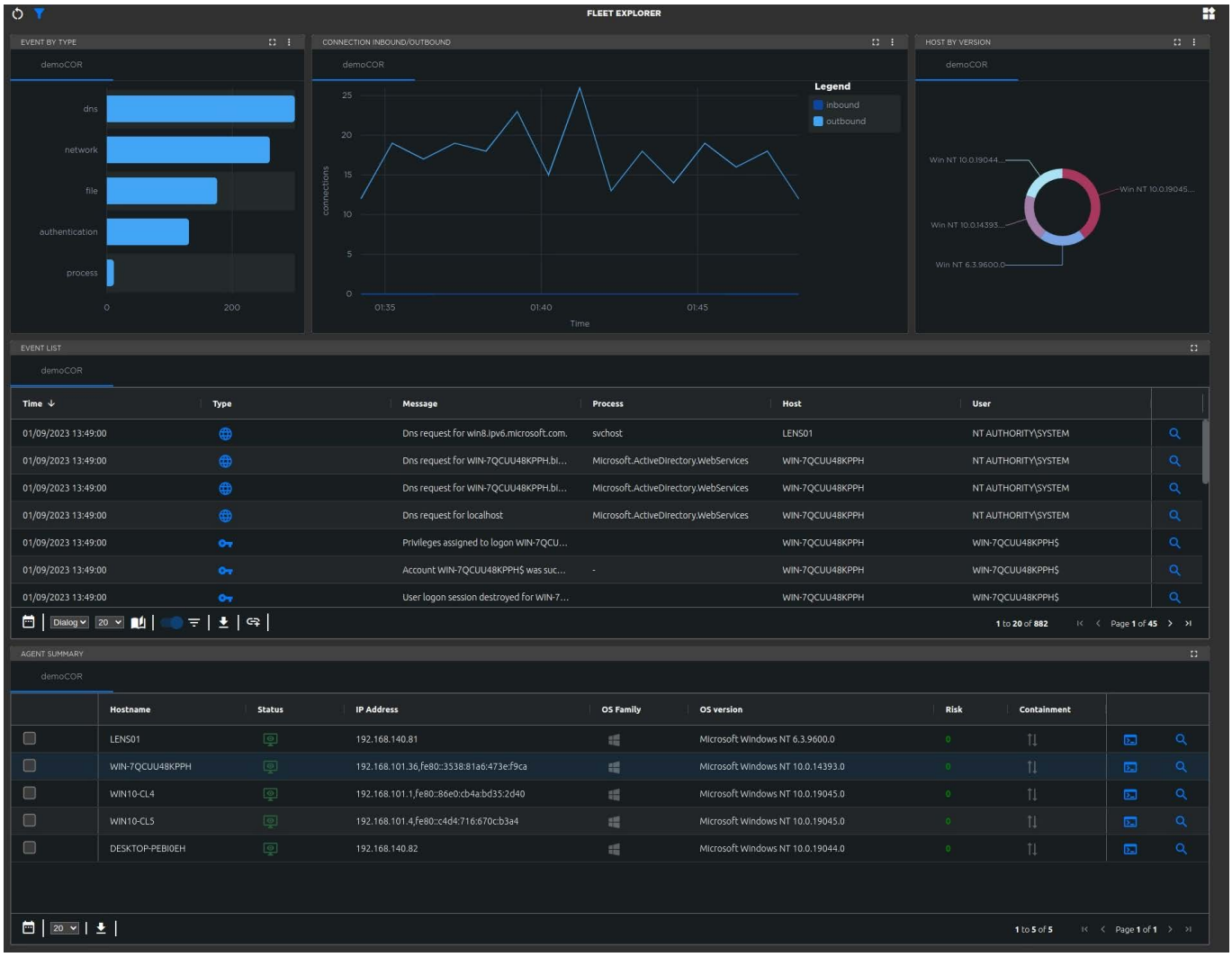
LENS is Leonardo's flexible and multi-functional Endpoint Detection & Response (EDR) platform designed to monitor and protect both OT and IT environments. By collecting telemetry and interacting with deployed agents and probes, LENS enables early detection of anomalies and intrusions, supporting timely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

LENS provides deep and contextual insight through a visual environment that supports security experts in assessing threats, selecting the most effective mitigation strategies, and determining the optimal recovery path for affected systems. Its compatibility with both ICT and ICS networks ensures comprehensive protection across converged infrastructures, including legacy systems and modern digital environments.

The platform integrates automated anomaly detection with a powerful query language, giving analysts the ability to filter billions of events and focus on relevant evidence with precision and speed. Detection and response rules can be adapted dynamically at runtime, allowing targeted monitoring and remediation activities either locally on endpoints or centrally, according to operational needs.

LENS offers extensive capabilities for searching, querying, and analyzing historical data, while the automated distribution and updating of agents and detection algorithms ensure efficiency and scalability. Strong integration with Leonardo's Cyber Threat Intelligence system further enhances situational awareness, while interoperability with the proprietary Leonardo VBrain platform and third party solutions enables the coordinated management of logical and physical security in a unified framework.

Depending on customer requirements, LENS can be deployed on-premises, offered as a SaaS, or provided as a managed service.



LENS Main Dashboard

INTEGRATION WITH THE C-ThInk

LENS is integrable with the Leonardo Cyber Threat Intelligence system (C-ThInk). C-ThInk 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 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.

C-ThInk 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 C-ThInk. 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 C-ThInk is “bidirectional,” as it involves the mutual enrichment of their respective knowledge bases.

MAIN FUNCTIONALITIES

LENS supports security specialists throughout all phases of cyber threat management, providing an operational environment that enables timely assessment and execution of the most appropriate mitigation actions.

1. DETECTION

LENS agents continuously monitor endpoints, automatically detecting and reporting malicious behaviors and suspicious activities. Telemetry collected by the agents, is stored for historical analysis. Threats are identified based on a set of known detection rules, ensuring effective and timely alerts.

2. HUNTING

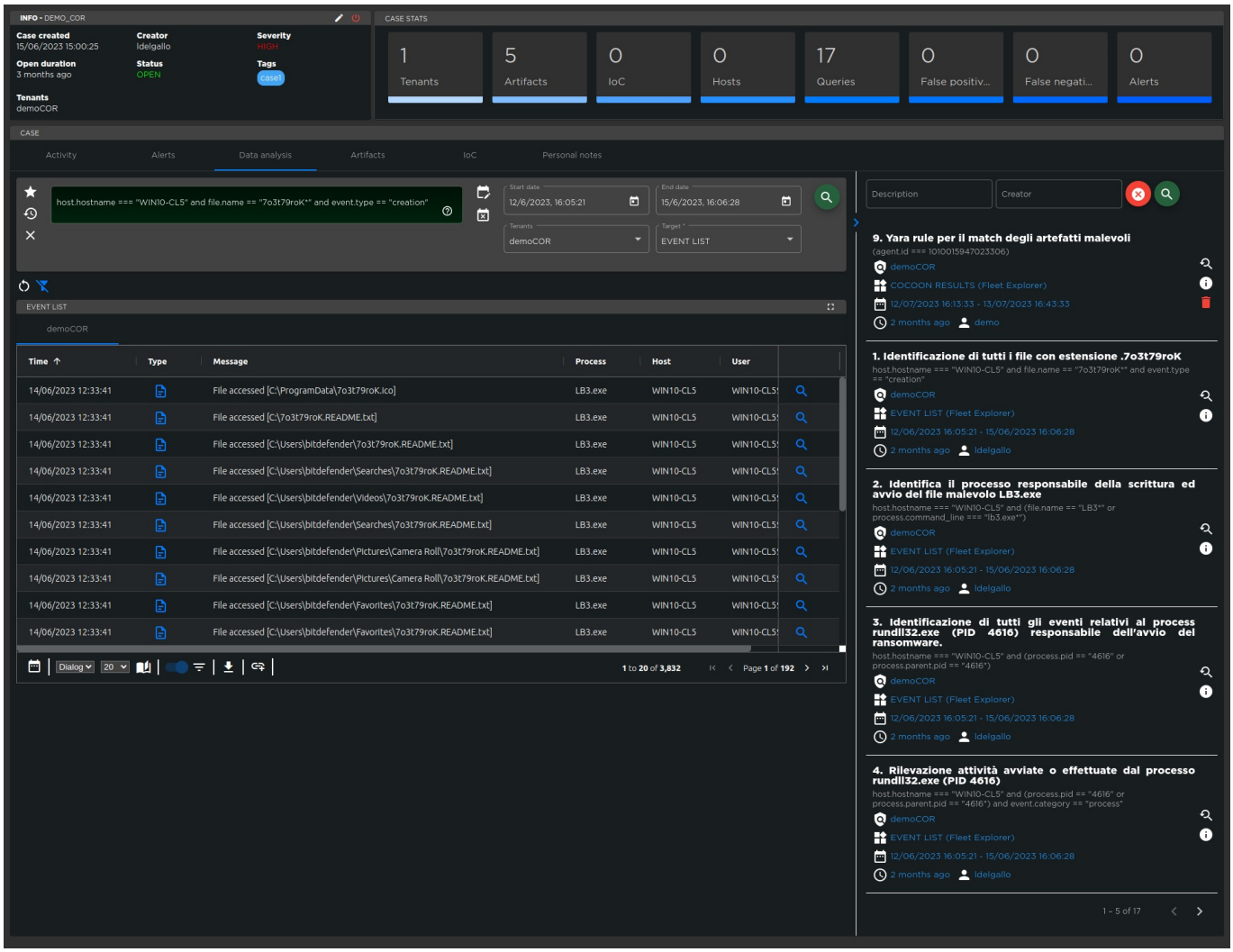
LENS empowers analysts to proactively search for hidden or emerging threats through manual and on-demand detection activities. It enables customization and development of dedicated Cocoons, such as YARA rules or Hash Finders, to enhance and tailor hunting capabilities.

3. INVESTIGATION

Analysts can open dedicated cases to aggregate and correlate incidents, events, and telemetry data from multiple endpoints. LENS provides a structured investigation workspace that enables deep forensic analysis, timeline reconstruction, and threat actor profiling.

4. RESPONSE

LENS facilitates the design and execution of immediate containment actions to neutralize identified threats. In addition to automated responses, LENS provides a dedicated workspace for managing incident response. Analysts can take direct action on endpoints such as isolating compromised machines via the user interface or terminating malicious processes using PowerCLI. Custom Cocoons plugins can be developed to perform specific actions, such as blocking suspicious connections, ensuring a tailored and effective response to ongoing threats.



LENS Investigation Dashboard

COCOONS

The continuous evolution of cyber threats requires highly adaptable and constantly evolving defense tools. To meet this need, LENS introduces Cocoons.

Cocoons are dynamic libraries that extend the native capabilities of an agent, enhancing detection and response features while ensuring adaptability to emerging threats. These libraries can be securely distributed to agents from a central repository via a protected gRPC channel.

Developed using standard programming languages, Cocoons enable the implementation of customized processes that go beyond the agent's core functionalities, allowing for the creation of specific detection rules and tailored response actions. They can be instantiated either permanently within the agents, or dynamically loaded into memory, minimizing their visibility to potential attackers.

LOGICAL MODEL

LENS features a multi-tenant architecture, enabling the segregated management of multiple tenants according to the customer's specific operational needs.

The **SERVER** is the central component of LENS, responsible for managing all core system functionalities, including configuration, administration, monitoring, and detection. It is designed for deployment within a Docker-based architecture, ensuring greater robustness, scalability, and resilience against potential failures.

AGENTS are distributed components dedicated to monitoring, analyzing, and responding to security events. They are designed to operate efficiently across heterogeneous environments and are fully compatible with enterprise platforms. Agents are divided into two main categories.

IT Agents are installed on endpoint devices such as PCs and servers, which form part or all an organization's information system. These agents perform a dual function.

- They collect and transmit telemetry data for detection purposes by invoking dedicated backend services for processing and storage.
- They execute predefined actions, locally on the host system, in response to commands issued by the central server.

Developed using a dedicated Software Development Kit (SDK), IT Agents are equipped with advanced capabilities for threat detection and automated response, enabling effective and timely intervention across IT environments.

OT Agents are deployed on embedded OT systems. While they maintain the same telemetry collection and detection/response capabilities as IT agents, they are specifically designed for operational environments. They differ in terms of deployment context and the type of data they acquired and processed, ensuring compatibility with industrial control systems.

The **OT PROBES** are components designed to monitor, inspect, and analyze network traffic within industrial and operational environments. It passively intercepts and examines network flows to identify anomalies, suspicious behavior, or policy violations—without interfering with operational systems or processes. To ensure maximum deployment flexibility, the LENS OT Probe is available in two formats.

- **Physical Appliance**, a hardware-based device installed externally to the system or equipment being monitored, incorporating the probe functionality.
- **Virtual Appliance**, a software version of the probe, deployable on virtual machines within existing infrastructure.

KEY FEATURES

- → **Strong integration with the Cyber Threat Intelligence System** and the broader Leonardo cyber product ecosystem.
- → **Fully customizable rule-based response and containment actions** to address specific needs.
- → High level of robustness and **compatibility with segregated operational environments.**
- → **Applicable in IT/OT environments and even in contexts in which implementing a complex defense structure** (Security Operations Center) **is not feasible.**
- → **Option for local management of vulnerability data, detection rules, and response actions** for greater control and security.
- → **Easy integration with third-party EDR solutions** to preserve customers' existing investments.
- → **Employed to protect Leonardo's proprietary products** against cyber threats **in the fields of Mission-Critical Communications and Transportation.**
- → **Integrated management of logical and physical security through interoperability with Leonardo's VBrain** system and third-party solutions.
- → **Available as a SaaS, on-premises, or fully managed solution**, to meet different operational needs.

For more information:
cyberandsecurity@leonardo.com

Leonardo Cyber & Security Solutions Division
Via R. Pieragostini, 80 - Genova 16151 - Italy

LDO_IT23_00440 07-25

leonardo.com