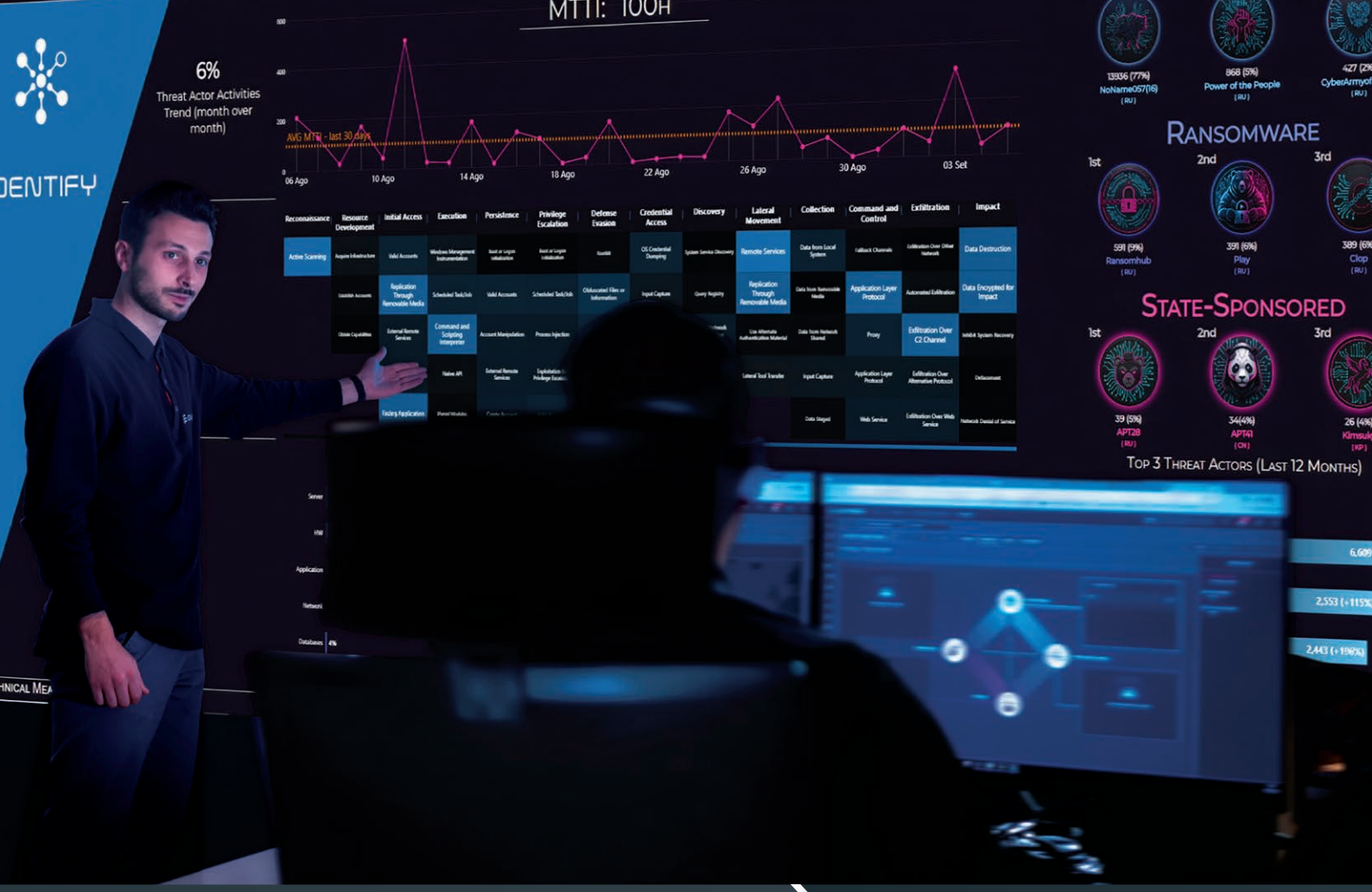


CYBER & SECURITY SOLUTIONS

GC Platform

Leonardo Cyber Defence Platform

LEONARDO

The global geopolitical landscape is experiencing unprecedented instability. Hybrid warfare operations, AI-driven cyber offensives, and coordinated influence campaigns have become core instruments of strategic competition. Critical infrastructures — energy, transport, space, telecommunications, finance — and European institutions are increasingly targeted by state-sponsored actors pursuing persistent access to national critical infrastructures and aiming to conduct disruptive activities below the threshold of open conflict. At the same time, hacktivist collectives leverage digital platforms to conduct highly visible campaigns driven by political or ideological motivations.

In this scenario, a new paradigm of cyber defence is required: integrated, automated, intelligence-driven, and outcome-oriented, capable of translating technical data into measurable outcomes. A defence model designed to accelerate resilience, ensure mission continuity, and protect the sovereignty of the European digital ecosystem.

A SINGLE PANE OF GLASS FOR PREEMPTIVE DEFENCE

The GC Platform is Leonardo's new Cyber Defence platform, designed to deliver end-to-end management of the entire cybersecurity lifecycle and to ensure true cyber mission assurance for critical infrastructures and mission-driven organizations.

Designed to overcome the challenge of technological fragmentation — integrating and orchestrating existing cyber capabilities into a single, intelligent, and outcome-based ecosystem that eliminates silos and improves operational efficiency.

At its core, the platform leverages Leonardo's proprietary multi-agentic system based on Artificial Intelligence, a coordinated network of autonomous yet collaborative agents capable of observing, interpreting, and acting across all functions of the NIST Cybersecurity Framework 2.0. By combining advanced managed services, Leonardo's proprietary cybersecurity products, and a wide operational knowledge base, the GC Platform transforms cybersecurity from a reactive function into a proactive capability, able to predict, prevent, and counter threats, delivering measurable outcomes in terms of risk reduction, speed of response and resilience.

Fully aligned with major industry standards — including NIST CSF 2.0 and MITRE ATT&CK® — it ensures structured, auditable and compliant security operations.

The GC Platform is typically delivered as a service but can also be deployed on-premises when customers require strict data sovereignty and confidentiality.

Developed and managed in Europe, the platform leverages open-source AI models trained by Leonardo, ensuring full compliance with European regulations.

OUTCOME-BASED APPROACH

The GC Platform adopts an outcome-based approach that continuously measures cybersecurity performance, transforming operational data into measurable business-aligned results that deliver tangible value for the customer. Each function of the NIST CSF 2.0 is associated with dedicated indicators.

- → DEFense CONdition (DEFCON) — GOVERN
  Continuous alignment between services, resources and threat level
- → Mean Time to Identify (MTTI) — IDENTIFY
  Time required to recognize threats before public disclosure
- → Mean Time to Protect (MTTP) — PROTECT
  Speed in mitigating and correcting known vulnerabilities
- → Mean Time to Detect (MTTD) — DETECT
  Speed of detecting attacks and active threats
- → Mean Time to Respond (MTTR) — RESPOND
  Speed of incident containment and mitigation operations
- → Mean Time to Recover (MTTR) — RECOVER
  Speed of restoring services and operations

Continuous monitoring of these parameters enables data-driven decisions and constant improvement of the security posture.

MAIN CAPABILITIES

The GC Platform delivers continuous and adaptive defence by orchestrating all NIST functions through a cooperative multi-agentic AI system that observes, interprets, and acts in real time, eliminating technological silos and reinforcing Zero Trust principles.

GOVERN AGENT

Provides dynamic orchestration of services and configurations based on threat level and operational risk. It aggregates technical risk data from the other five agents and maps them to the business context (compliance, critical processes and economic value of assets). Classifies and maps assets based on their criticality to support prioritized intervention. It manages tickets, requests, and operational workflows, ensuring strategic visibility, prioritization, and control over the entire cyber domain.

IDENTIFY AGENT

Delivers comprehensive visibility over assets, vulnerabilities, and exposure points. Integrates open and proprietary intelligence sources to analyse emerging threat trends. When a new threat is detected, it already identifies which customer assets are vulnerable to that specific threat, based on its Techniques, Tactics and Procedures (TTPs). Continuously profiles threat actors and their TTPs, identifying vulnerabilities before public disclosure, providing a tangible advantage in proactive defence.

PROTECT AGENT

Implements proactive security controls and vulnerability remediation measures, prioritised by exposure and operational impact. The Protect agent introduces Business Risk-Based Vulnerability Remediation (RBVR) and converts Privileged Access Management (PAM) and Attribute-Based Access Control (ABAC) into an “as-a-Service” model, enabling Zero Trust enforcement. It ensures continuous protection of systems, data and operations.

DETECT AGENT

Enables continuous monitoring and correlation of security events across the environment. It does not only search for known Indicators of Compromise (IOCs) but also for anomalous behaviour, anticipating the attack dynamic. It provides timely and transparent communication to the corporate roles involved in incident management.

RESPOND AGENT

Automates containment and mitigation workflows, accelerating response operations and reducing human workload. It helps the analyst build complex playbooks in real-time, significantly accelerating the response operations. Minimises incident impact through real-time orchestration between defence teams. Provides timely and transparent communication to all stakeholders.

RECOVER AGENT

Ensures rapid recovery of assets and operational environments reducing long-term impact on business performance and service availability. It manages Leonardo’s Crisis Recovery Vault (CRV), ensuring that backups of critical data are isolated, immutable, and ready for a secure, orchestrated rapid recovery. Guarantees business continuity, even under active threat conditions, maintaining trust and operational resilience throughout the recovery process.

BEYOND SERVICES: THE RISE OF THE MULTI-AGENTIC PARADIGM

The GC Platform goes beyond the traditional model based on delivering multiple services for each function, introducing a coordinated multi-agentic defensive ecosystem.

Six specialized agents operate autonomously while cooperating through a shared and continuously updated knowledge base.

Each agent contributes contextual intelligence, sharing data, decisions and insights across the entire NIST framework. This approach enables:

- → faster reactions
- → deeper situational awareness
- → adaptive resilience against evolving threats

LOGICAL MODEL

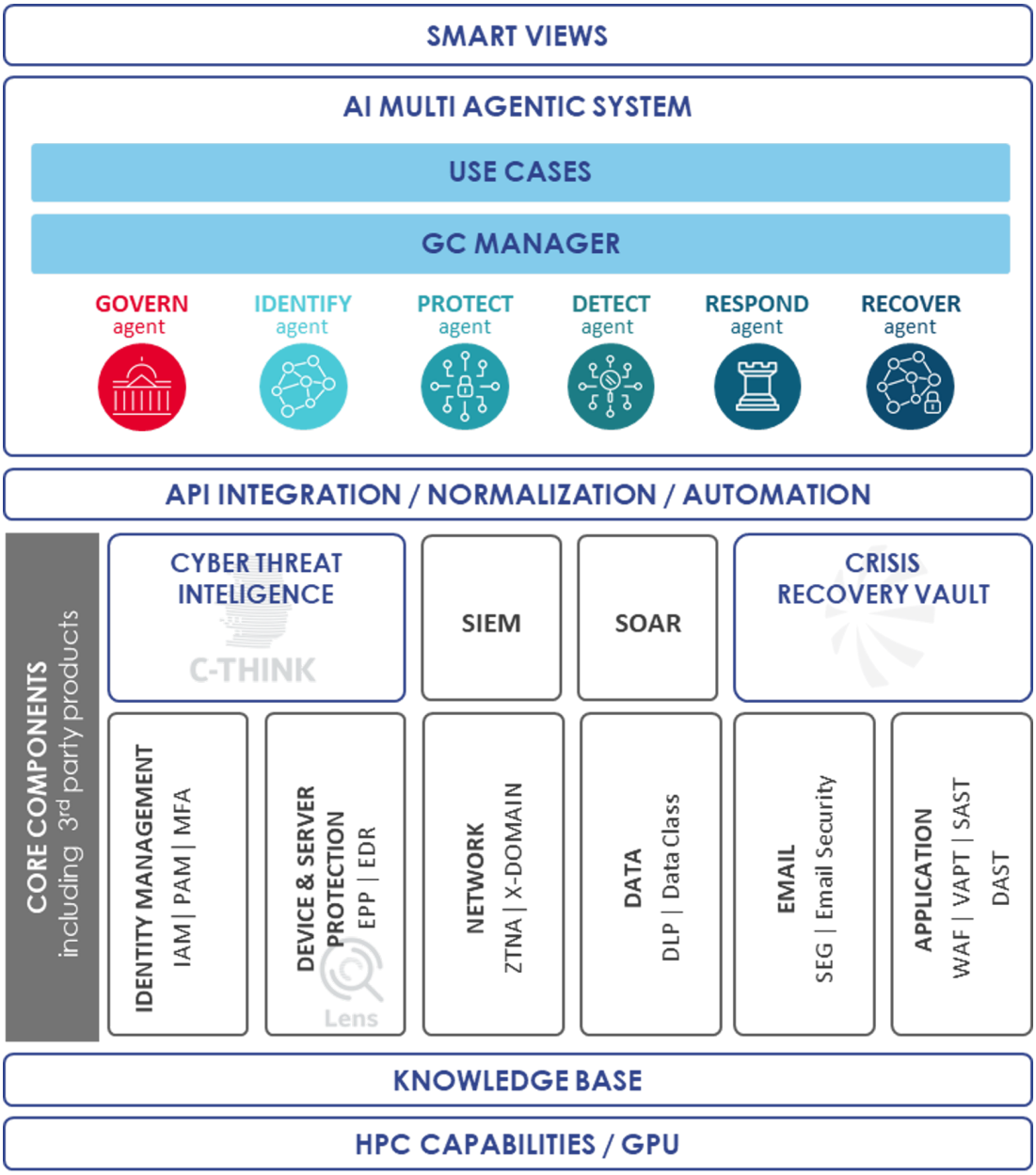
The platform is based on a logical model designed to provide unified cyber governance management, delivering full visibility across all phases of cyber threat management. To achieve this, the GC Platform integrates Leonardo solutions and third-party technologies into a federated, interoperable ecosystem independent of individual vendors. Through Smart Views and Use Cases, technical complexity becomes information immediately accessible both to analysts and strategic decision-makers.

SMART VIEWS
Intelligent interfaces that centralize cyber domain management by aggregating logs and insights from multiple sources and transforming them into outcome-based indicators. Customizable for both managerial and operational roles, they provide immediate decision-oriented situational awareness.

USE CASES
They combine AI agents and cyber capabilities across NIST functions. They integrate and automate existing processes, technologies and data, supporting analysts in detection, correlation and remediation activities. Designed starting from specific customer requirements, they are fully reusable and adaptable in different contexts. Use cases leverage the GC Manager for multi-agentic orchestration, enabling automation of activities and expanding visibility across the cyber domain.

MULTI-AGENTIC SYSTEM
The GC Platform is powered by a multi-agentic AI system. Each agent continuously processes contextual data and supports user interaction through natural language, accessing a cross-domain knowledge base enriched with threat intelligence reports, vulnerability data and system logs. It provides contextualized, proactive and decision-oriented insights that enhance collaboration and accelerate operational workflows.

CYBER PLATFORMING
Cyber Platforming enables the seamless integration of both Leonardo's proprietary products and trusted third-party solutions into a single, interoperable architecture. By eliminating technological silos, it enhances the value of tools already present within the customer environment, enables the creation of integrated ecosystems and supports a modular on-demand model based on operational priorities and threat context.



GC Platform - Logical Model

ZERO TRUST

The GC Platform is natively engineered around the Zero Trust paradigm, designed to manage, orchestrate, and continuously enforce Zero Trust architectures across all operational domains.

This Zero Trust by design enables the platform not only to govern and sustain Zero Trust environments, but also to deliver advanced Zero Trust services that extend protection, visibility, and control beyond traditional perimeters.

These services include comprehensive Privileged Access Management (PAM), with quantum-ready security, and context-aware authorization based on Attribute-Based Access Control (ABAC) models.

Through the combined use of Leonardo proprietary technologies and trusted European third-party solutions, the platform integrates Zero Trust principles throughout the entire cybersecurity lifecycle, orchestrated by the cooperative multi-agentic AI system.

Specifically, the Protect phase capabilities ensure continuous, policy-driven enforcement of least-privilege access, maintaining system integrity and strengthening the overall resilience of critical infrastructures and mission-critical organizations.

Use Case Identify Agent

KEY CAPABILITIES

- → Full alignment with NIST CSF 2.0
- → Proprietary multi-agentic AI system, enabling autonomous and coordinated decision-making processes
- → Unified and cross-domain cyber observability
- → Open and vendor-independent integration model
- → Outcome-based measurement and governance, turning technical KPIs into actionable business insights
- → Smart Views for analysts and executive roles
- → Customizable, modular and reusable Use Cases
- → Native Zero Trust
- → European Digital Sovereignty
- → Flexible delivery model: as-a-service or on-premises

For more information:
cyberandsecurity@leonardo.com

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

LDO_IT25_1629

leonardo.com