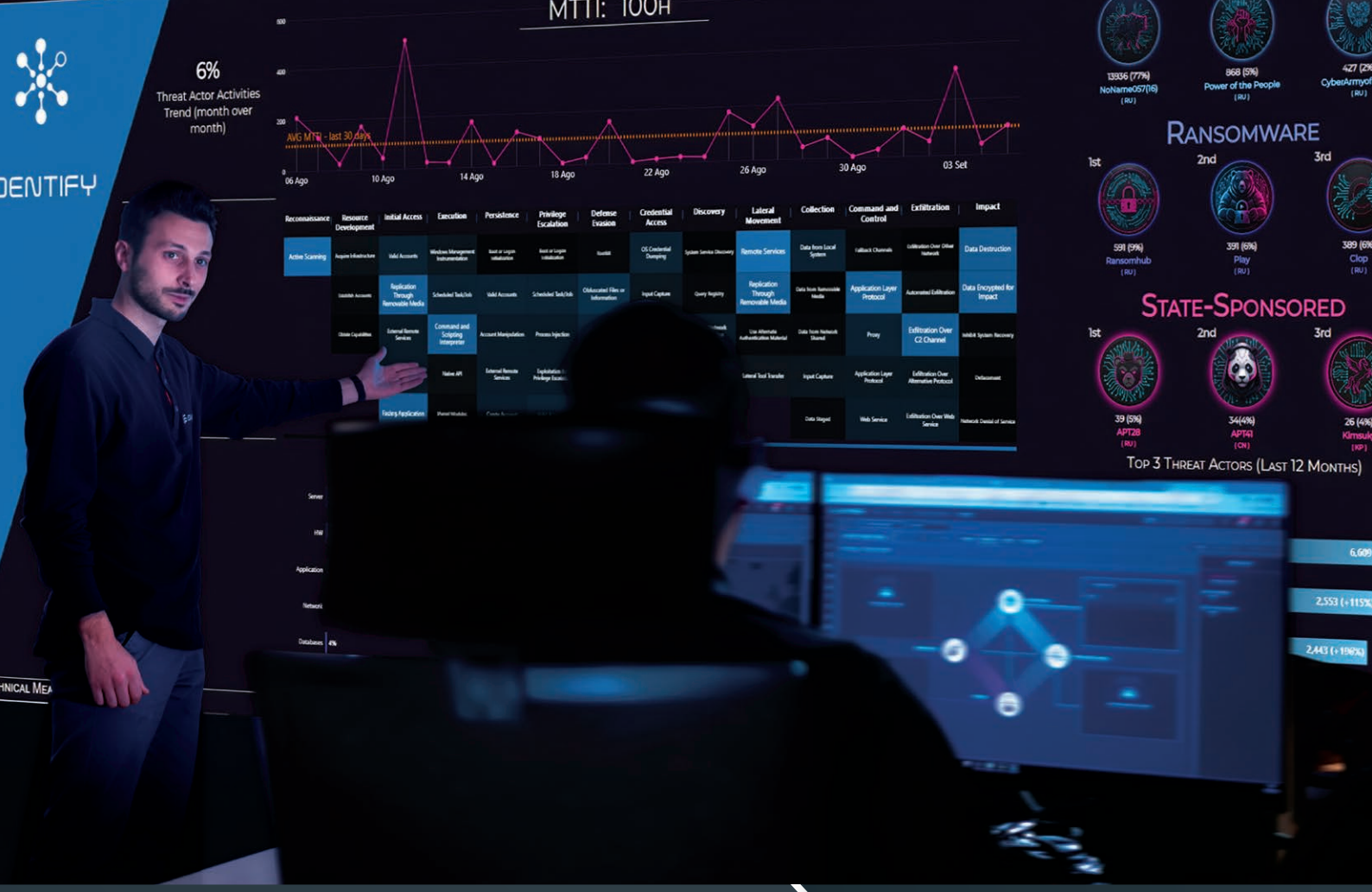


CYBER & SECURITY SOLUTIONS

GC Platform

Leonardo Cyber Defence Platform

LEONARDO

The global geopolitical landscape is experiencing unprecedented instability. Hybrid warfare, AI-driven cyber offensives, and coordinated influence operations have become core instruments of strategic competition. Critical infrastructures — energy, transport, space, telecom, finance — and European institutions are increasingly targeted by state-sponsored actors pursuing persistent access and disruption 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.

This evolution demands a new cyber defence paradigm: 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 (silos)—integrating and orchestrating existing cyber capabilities into a single, intelligent, and outcome-oriented ecosystem that eliminates silos and improves operational efficiency.

At its core, the platform leverages Leonardo's proprietary multi-agent
Artificial Intelligence, a coordinated network of autonomous yet collaborative agents capable of observing, interpreting, and acting across all phases 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 controls.

Developed and managed in Europe, the platform guarantees data sovereignty and confidentiality, leveraging 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 NIST Cybersecurity Framework 2.0 is supported by dedicated performance metrics, enabling real-time evaluation of resilience and operational efficiency.

- → DEFense CONdition (DEFCON) — GOVERN
  How well are services and resources aligned to the current threat level?
- → Mean Time to Identify (MTTI) — IDENTIFY
  How quickly can an incident be recognized?
- → Mean Time to Detect (MTTD) — DETECT
  How fast can an ongoing attack be detected?
- → Mean Time to Patch(MTTP) — PROTECT
  How rapidly can preventive measures be activated?
- → Mean Time to Respond (MTTR) — RESPOND
  How effectively can an incident be contained and neutralized?
- → Mean Time to Recover (MTTR) — RECOVER
  How quickly can services be restored to full operation after an incident?

By measuring these indicators continuously, the GC Platform enables customers to measure, compare, and enhance their cybersecurity posture, supporting data-driven decision-making and continuous improvement over time.

MAIN CAPABILITIES

The GC Platform delivers continuous and adaptive defence by orchestrating all NIST phases 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. 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 knows which customer assets are vulnerable to that specific Technique, Tactics and Procedure (TTP), being integrated with the Protect and Detect agents. 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 PAM and ABAC into an “as-a-Service” model, enabling Zero Trust enforcement. Reduces the likelihood and impact of cyber events through dynamic prioritisation. Ensures continuous protection of systems, data, and operations within a Zero Trust enforcement model.

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 (e.g., an administrator accessing a server at unusual times), anticipating the attack. Uses behavioural analytics and multi-agentic AI reasoning to identify anomalies beyond threshold-based detection, enhancing early threat awareness and accelerating operator decision-making.

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 DEFENCE PARADIGM

The GC Platform marks a decisive evolution from traditional "service-per-phase" delivery models, where each NIST function is operated independently.

Instead, it introduces a coordinated multi-agentic paradigm: six specialized AI agents (Govern, Identify, Protect, Detect, Respond, and Recover) work together as an autonomous but collaborative defence ecosystem.
Each agent operates within its dedicated phase, leveraging a shared and continuously updated knowledge base associated with that function, making the GC Platform not just aligned with the NIST framework, but truly built around it.

Every agent contributes contextual intelligence — analysing threats, protecting assets, detecting anomalies, responding to incidents, and securing recovery — while continuously exchanging data, context, and decisions across all NIST phases.

This collective AI enables faster reaction times, deeper situational awareness, and adaptive resilience against evolving threat, ensuring a measurable improvement in resilience and mission continuity.

LOGICAL MODEL

At the heart of GC Platform lies a logical model designed for unified governance, visibility, and intelligence. The platform consolidates Leonardo's proprietary solutions and thirdparty technologies into a federated ecosystem that ensures interoperability without lock-in. Through Smart Views and Use Cases, it transforms complex data into accessible insights for both executives and security analysts, bridging operational security and strategic decision-making.

MULTI-AGENTIC SYSTEM

The GC Platform is powered by a multi-agentic AI system composed of specialized agents operating across the different NIST functions. Each agent continuously processes contextual data and supports user interaction through natural language queries – providing an intuitive conversational experience. By leveraging a dedicated Knowledge Base that is transversal to all phases—enriched with threat intelligence reports, vulnerability information, and system logs—the system provides contextualized, proactive and decision-oriented insights that enhance collaboration and accelerate operational workflows.
For example, a user can query the GC Platform regarding the most critical assets within their perimeter.

CYBER PLATFORMING

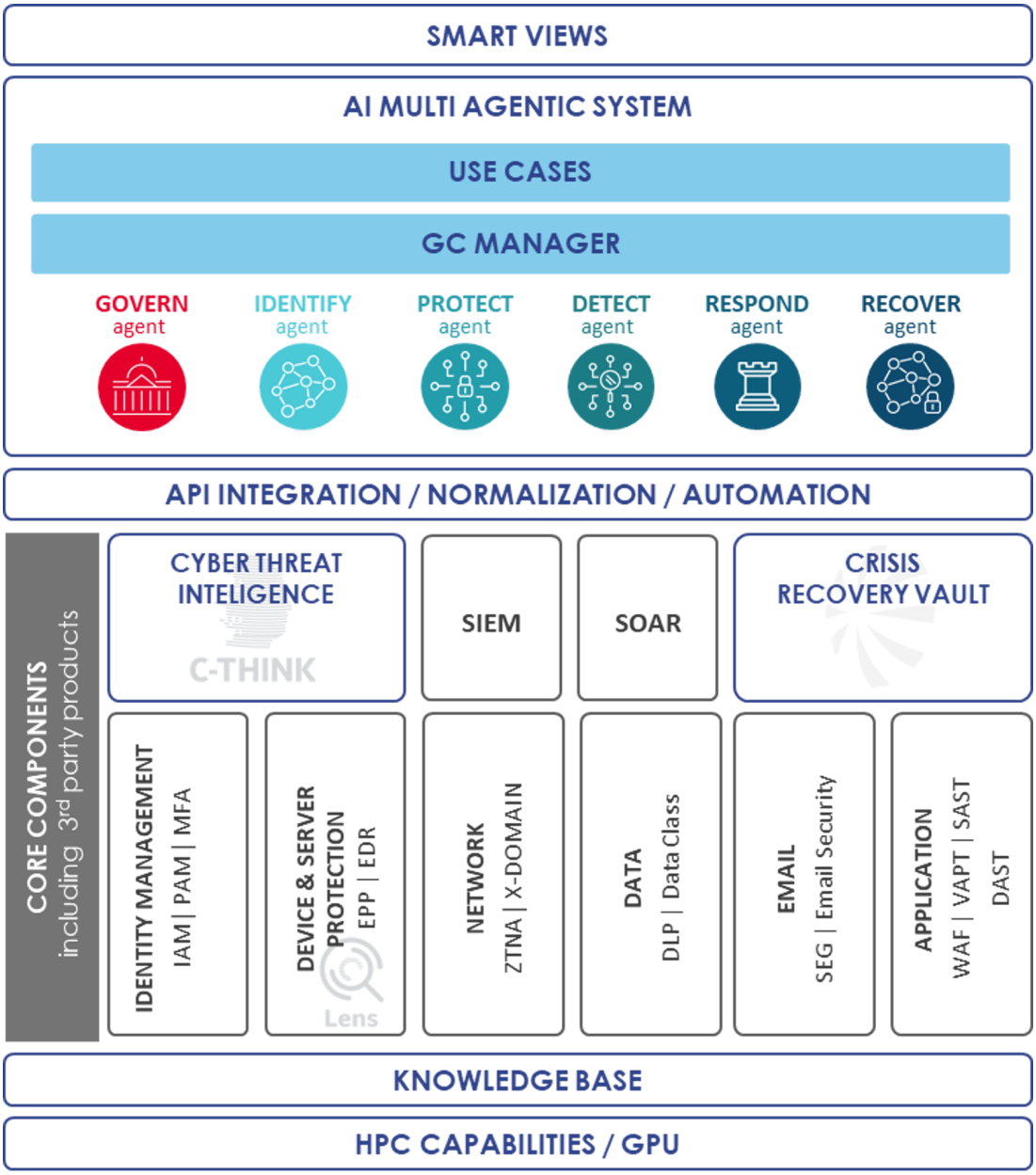
Cyber Platforming enables the seamless integration of both Leonardo proprietary products and trusted third-party solutions into a single, interoperable architecture.
By eliminating technological silos, it unifies existing customer tools while also allowing the creation of new, fully integrated cyber ecosystems. This approach maximizes protection efficiency while enhancing resilience and adaptability through a modular, on-demand model allowing customers to activate capabilities on demand, according to their operational priorities and the evolving threat context, transforming cybersecurity into a living, evolving capability.

SMART VIEWS

Smart Views are intelligent interfaces that centralize governance of the cyber domain and provide real-time monitoring of the organization's cybersecurity posture.
They aggregate logs and insights from multiple sources transforming them into outcome-based indicators that are measurable and immediately understandable.
Thanks to modularity and flexibility, Smart Views adapt to different user profiles, delivering instant situational awareness tailored to strategic and operational needs, supporting better and faster decisions across the organization.

USE CASE

Operational use cases combine AI agents and cybersecurity capabilities across different NIST phases to address real-world needs of each customer.
They provide intelligent integration and automation of data, processes, and technologies, automating repetitive activities and supporting analysts in detection, correlation, and remediation.
Use Cases are designed on specific customer requirements but remain fully reusable and adaptable in other operational contexts - allowing capability. Each use case integrates existing processes, data and technologies, leveraging the GC manager, which enables the platform's multi-agentic orchestration to automate activities and enhance visibility across the cyber domain.



GC Platform - Logical Model

ZERO TRUST

The GC Platform is natively engineered around the Zero Trust paradigm, designed to manage, orchestrate, and continuous 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 reinforces 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, providing continuous and adaptive defence across all phases
- → Proprietary multi-Agentic AI system, enabling autonomous decisionmaking and coordinated intelligence across defensive capabilities
- → Unified Cyber Observability breaking technological silos and correlating data to maximise end-to-end visibility
- → Open and vendor-neutral integration model that incorporates existing tools (SIEM, SOAR, PAM, EDR, etc.) without lock-in
- → Outcome-based measurement and governance, turning technical KPIs into actionable business insights
- → Smart Views for executive analysts, enabling real time situational awareness and mission-centric decision support
- → Modular design with customisable and reusable Use Cases, amplifying platform capabilities and accelerating scalable adoption
- → Zero Trust by design, enforcing continuous verification and least-privilege access across domains
- → European Digital Sovereignty, with open-source AI models developed and secured within EU regulatory frameworks
- → Flexible delivery as-a-service, with on-premises options for highly sensitive environments

For more information:
cyberandsecurity@leonardo.com

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

LDO_IT25_1629

leonardo.com