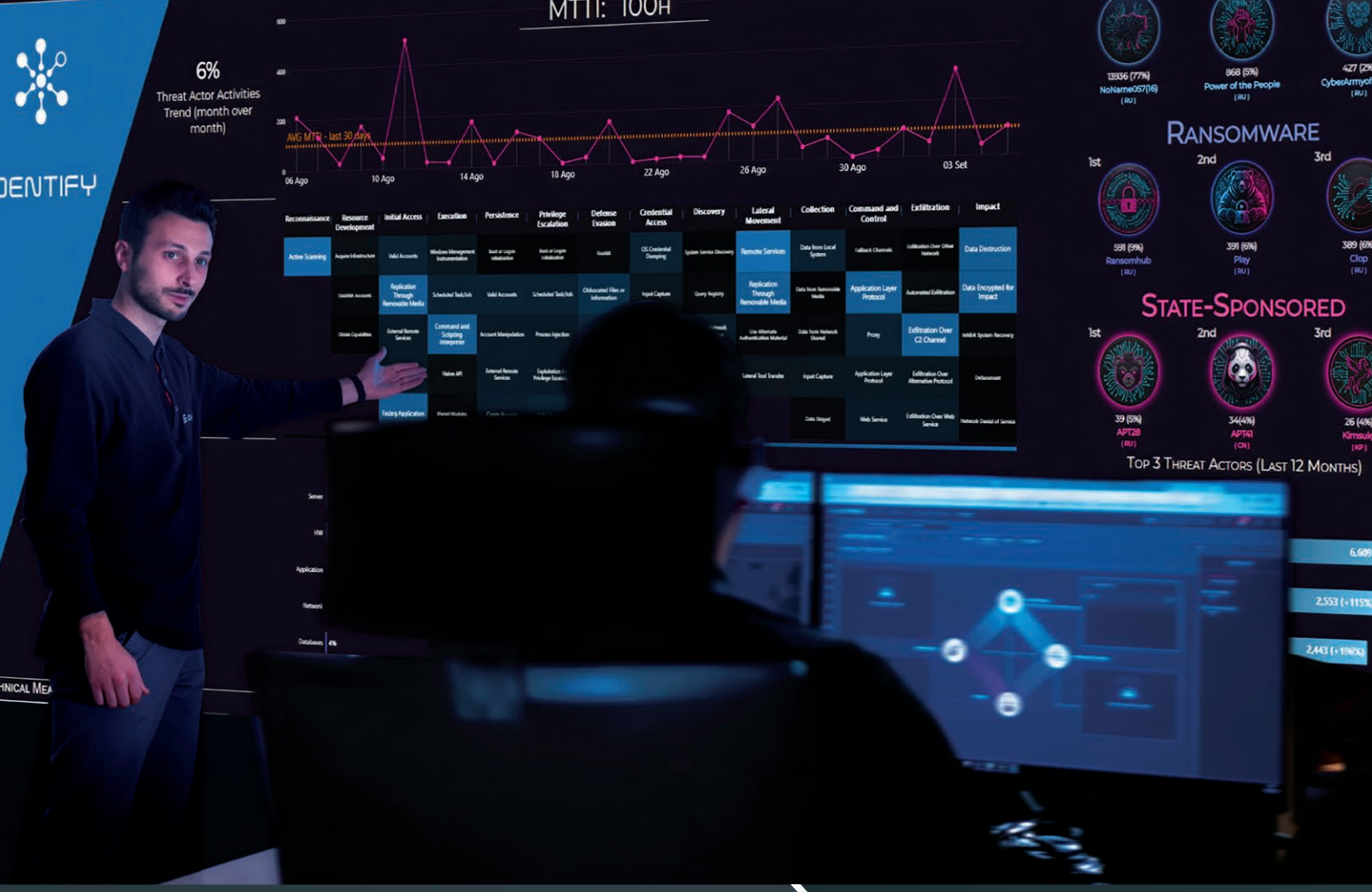


CYBER & SECURITY SOLUTIONS

GC Platform

Leonardo Cyber Defence Platform

LEONARDO

Il panorama geopolitico globale sta attraversando una fase di instabilità senza precedenti. Le operazioni di guerra ibrida, le offensive cyber guidate dall'Intelligenza Artificiale e le campagne di influenza coordinate, sono ormai strumenti centrali della competizione strategica.
Le infrastrutture critiche — energia, trasporti, spazio, telecomunicazioni, finanza — e le istituzioni governative sono sempre più spesso bersaglio di attori state-sponsored interessati a ottenere accesso persistente alle infrastrutture critiche nazionali e a condurre attività di disturbo sotto la soglia del conflitto aperto.
Parallelamente, collettivi hacktivisti sfruttano le piattaforme digitali per lanciare operazioni ad elevata visibilità, motivate da finalità politiche o ideologiche.
In questo scenario, serve un nuovo paradigma di cyber defence: integrato, automatizzato, intelligence-driven e orientato ai risultati, capace di trasformare dati tecnici in risultati immediatamente misurabili. Un modello progettato per rafforzare la resilienza, garantire la mission assurance e proteggere la sovranità digitale europea.

A SINGLE PANE OF GLASS FOR PREEMPTIVE DEFENCE

La GC Platform è la nuova piattaforma di Cyber Defence di Leonardo, progettata per garantire la gestione end-to-end dell'intero ciclo di vita della cybersecurity e garantire una reale Cyber Mission Assurance a organizzazioni mission-critical e infrastrutture strategiche.

Nata per superare la sfida della frammentazione tecnologica, la piattaforma integra e orchestra le capacità cyber già presenti presso il Cliente in un unico ecosistema intelligente e orientato ai risultati, migliorando l'efficienza operativa.

Al suo cuore opera il sistema multi-agentico proprietario di Leonardo basato su Intelligenza artificiale: una rete coordinata di agenti autonomi, ma cooperativi, in grado di osservare, interpretare e agire trasversalmente a tutte le fasi di gestione della minaccia.

Grazie alla combinazione di servizi gestiti avanzati, tecnologie proprietarie e un ricco patrimonio di conoscenza di dominio, la GC Platform trasforma la sicurezza da funzione reattiva a capacità proattiva, in grado di prevedere, prevenire e contrastare le minacce, producendo risultati tangibili in termini di riduzione del rischio, rapidità di risposta e resilienza.

La piattaforma è pienamente allineata ai principali standard internazionali, tra cui NIST CSF 2.0 e MITRE ATT&CK®, garantendo operazioni sicure, strutturate, auditabili e conformi.

Generalmente erogata as-a-Service, la GC Platform può essere implementata on-premises per i clienti con requisiti stringenti di sovranità e riservatezza dei dati.

Sviluppata e gestita interamente in Europa, utilizza modelli di AI open-source addestrati da Leonardo, garantendo piena conformità al quadro regolatorio europeo.

APPROCCIO OUTCOME-BASED

La GC Platform adotta un approccio outcome-based, misurando costantemente le performance cyber e trasformando i dati operativi in risultati concreti per il business. Ogni funzione del NIST CSF 2.0 è associata a indicatori dedicati.

- → DEFCON (DEFense CONdition) — GOVERN
  Allineamento continuo tra servizi, risorse e livello di minaccia
- → Mean Time to Identify (MTTI) — IDENTIFY
  Tempo necessario per riconoscere le minacce prima della loro divulgazione pubblica
- → Mean Time to Protect (MTTP) — PROTECT
  Rapidità nel mitigare e correggere le vulnerabilità note
- → Mean Time to Detect (MTTD) — DETECT
  Velocità di rilevazione di attacchi e minacce attive
- → Mean Time to Respond (MTTR) — RESPOND
  Velocità delle operazioni di contenimento e mitigazione di un incidente
- → Mean Time to Recover (MTTR) — RECOVER
  Rapidità di ripristino dei servizi e dell'operatività

Il monitoraggio continuo di questi parametri consente decisioni data-driven e un miglioramento costante della postura di sicurezza.

PRINCIPALI CAPACITÀ

La GC Platform garantisce una difesa continua e adattiva orchestrando tutte le fasi del framework NIST attraverso un sistema AI multi-agentico cooperativo che osserva, interpreta e agisce in tempo reale, eliminando i silos tecnologici e rafforzando i principi dello Zero Trust.

AGENTE GOVERN

Orchestra dinamicamente servizi e configurazioni in base al livello di minaccia e al rischio operativo dell'organizzazione. Aggrega dati di rischio tecnico provenienti dagli altri agenti e li correla con il contesto di business (compliance, processi critici, valore economico degli asset). Gestisce ticket, richieste e workflow operativi, assicurando visibilità strategica, priorità di intervento e controllo sull'intero dominio cyber.

AGENTE IDENTIFY

Garantisce piena visibilità su asset, vulnerabilità ed esposizioni. Integra fonti di intelligence aperte e proprietarie per analizzare le tendenze emergenti. Quando viene identificata una nuova minaccia, identifica gli asset del Cliente esposti alle specifiche Techniques, Tactics and Procedure (TTP), grazie all'integrazione con gli agenti Protect e Detect. Profila costantemente i threat actor, identificando vulnerabilità prima che siano rese pubbliche.

AGENTE PROTECT

Implementa controlli di sicurezza proattivi e misure di remediation prioritizzate per impatto ed esposizione. Introduce modelli Risk-Based Vulnerability Remediation (RBVR) ed eroga soluzioni di Privileged Access Management (PAM) e Attribute-Based Access Control (ABAC) as-a-Service, abilitando l'applicazione del paradigma Zero Trust. Assicura protezione continua di sistemi, dati e operazioni.

AGENTE DETECT

Esegue il monitoraggio continuo e la correlazione degli eventi di sicurezza. Non rileva solo Indici di Compromissione (IoC) noti, ma anche comportamenti anomali, anticipando la dinamica dell'attacco. Utilizza tecniche di reasoning multi-agentico per identificare anomalie basate su segnali deboli, migliorando la capacità di rilevazione precoce.

AGENTE RESPOND

Automatizza i workflow di contenimento e mitigazione, accelerando significativamente
le operazioni di risposta e riducendo il carico degli analisti. Supporta la creazione in tempo reale di playbook complessi e coordina i team di difesa. Fornisce comunicazioni tempestive e trasparenti ai profili aziendali coinvolti nella gestione dell'incidente.

AGENTE RECOVER

Garantisce un recupero rapido di asset e ambienti operativi, riducendo gli impatti di lungo periodo. Si avvale di una soluzione proprietaria di Crisis Recovery Vault (CRV), con l'obiettivo di garantire che i backup critici siano isolati, immutabili e pronti a un ripristino sicuro e orchestrato. Assicura la business continuity anche durante scenari di minaccia attiva.

OLTRE I SERVIZI: IL PARADIGMA MULTI-AGENTICO

La GC Platform supera il modello tradizionale che prevede l'erogazione di più servizi per fase, introducendo un ecosistema difensivo multi-agentico coordinato.

Sei agenti specializzati operano in autonomia ma cooperano attraverso una knowledge base condivisa e costantemente aggiornati.

Ogni agente contribuisce con intelligenza contestuale, condividendo dati, decisioni e insight lungo l'intero framework NIST. Questo approccio abilita:

- → reazioni più rapide
- → situational awareness più approfondita
- → resilienza adattiva rispetto all'evoluzione delle minacce

MODELLO LOGICO

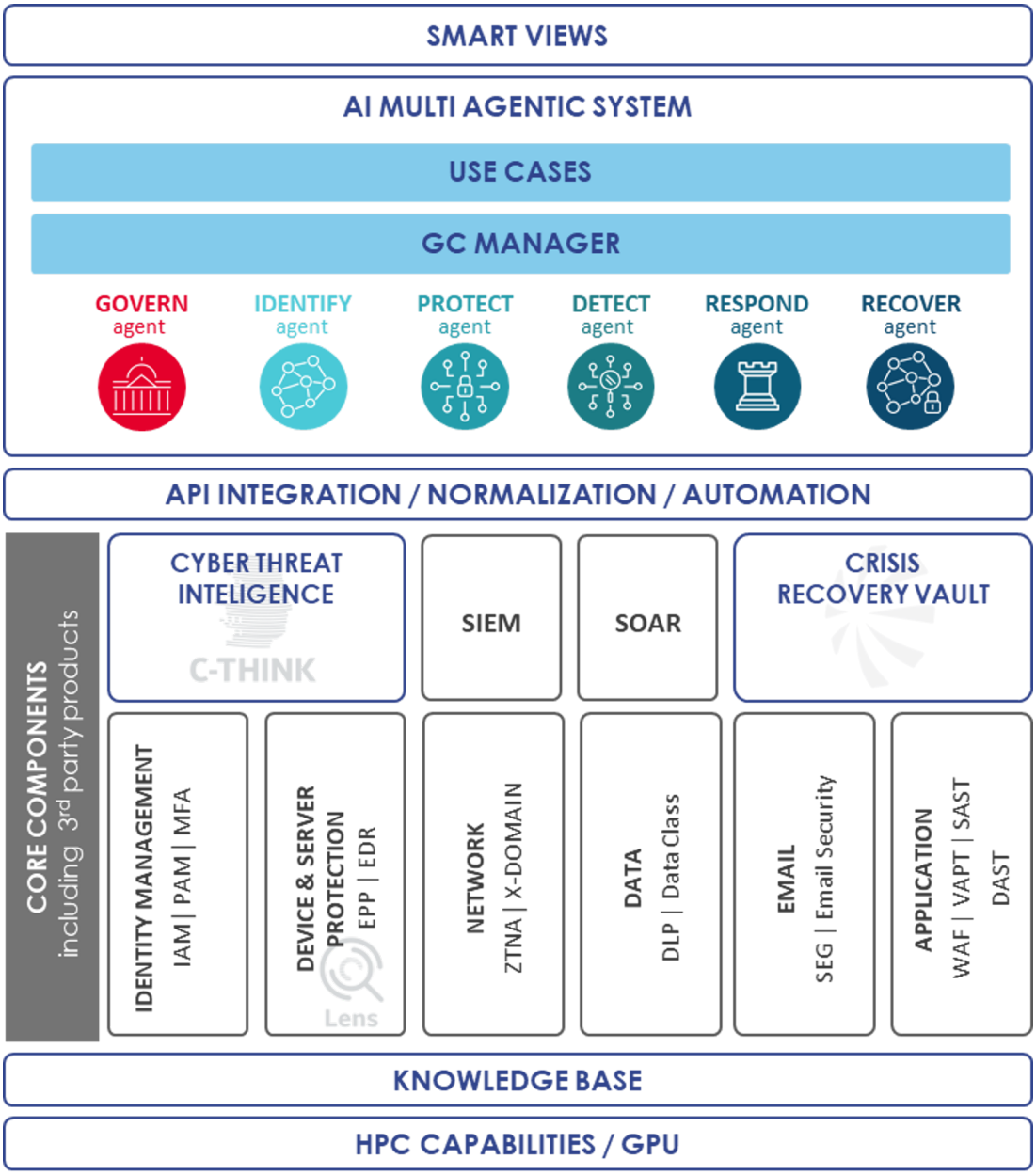
La piattaforma si basa su un modello logico pensato per offrire una gestione della governance cyber unificata, fornendo piena visibilità su tutte le fasi di gestione delle minacce cyber. A questo scopo la GC Platform integra soluzioni Leonardo e tecnologie di terze parti in un ecosistema federato, interoperabile e indipendente dai singoli fornitori. Grazie a Smart View e Use Case, la complessità tecnica diventa informazione immediatamente fruibile sia per gli analisti sia per i decisori strategici.

SMART VIEWS
Interfacce intelligenti che centralizzano la gestione del dominio cyber, aggregando log e insight da molteplici fonti e trasformandoli in indicatori outcome-based. Personalizzabili per profili manageriali e operativi, forniscono una situational awareness immediata e orientata alle decisioni.

USE CASE
Combinano agenti AI e capability cyber trasversali alle fasi NIST. Integrano e automatizzano processi, tecnologie e dati esistenti, supportando gli analisti nelle attività di detection, correlazione e remediation. Realizzati a partire da esigenze specifiche del cliente, sono pienamente riutilizzabili e adattabili in contesti diversi. Gli Use Case sfruttano il GC Manager, per l'orchestrazione multi-agentica che consente di automatizzare le attività e ampliare la visibilità sul dominio cyber.

SISTEMA MULTI-AGENTICO
La piattaforma è alimentata da un sistema AI multi-agentico. Ogni agente elabora dati contestuali e interagisce con gli operatori tramite linguaggio naturale, accedendo a una knowledge base trasversale arricchita da report di threat intelligence, dati sulle vulnerabilità e log di sistema. Fornisce insight proattivi, contestualizzati e orientati alle decisioni, accelerando i workflow operativi.

CYBER PLATFORMING
Abilita l'integrazione nativa di soluzioni Leonardo e prodotti di terze parti in un'unica architettura interoperabile. Eliminando i silos, valorizza gli strumenti già presenti presso il cliente, permette la creazione di ecosistemi cyber integrati e abilita un modello modulare on-demand basato sulle priorità operative e sul contesto di minaccia.



GC Platform - Modello Logico

ZERO TRUST

La piattaforma è progettata in modo nativo secondo il paradigma Zero Trust, con l'obiettivo di gestire, orchestrare e applicare in modo continuo architetture Zero Trust in tutti i domini operativi.

Ciò consente alla piattaforma non solo di governare e sostenere ambienti Zero Trust, ma anche di fornire servizi avanzati che estendono la protezione, la visibilità e il controllo oltre i perimetri tradizionali.

Questi servizi includono una gestione completa degli accessi privilegiati (PAM), con sicurezza quantum-ready e autorizzazione contestuale basata su modelli di controllo degli accessi basati sugli attributi (ABAC).

Attraverso l'uso combinato delle tecnologie proprietarie di Leonardo e di soluzioni di terze parti europee affidabili, la piattaforma rafforza i principi Zero Trust durante l'intero ciclo di vita della sicurezza informatica, grazie al sistema di intelligenza artificiale multi-agente cooperativo.

Nello specifico, le funzionalità della fase di Protect garantiscono l'applicazione continua, basata su policy dell'accesso con privilegi minimi, mantenendo l'integrità del sistema e rafforzando la resilienza complessiva delle infrastrutture critiche e delle organizzazioni mission-critical.

Use Case Identify Agent

KEY CAPABILITIES

- → Allineamento completo al NIST CSF 2.0
- → Multi-Agentic AI proprietaria a supporto di processi decisionali autonomi e coordinati
- → Cyber Observability unificata e cross-dominio
- → Modello di integrazione aperto e indipendente dai fornitori
- → Misurazione e governance basate sui risultati, trasformando i KPI tecnici in informazioni aziendali utilizzabili immediatamente
- → Smart View per analisti e profili executive
- → Use Case personalizzabili, modulari e riusabili
- → Zero Trust nativo
- → Sovranità digitale europea
- → Modello di erogazione flessibile: as-a-service oppure 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