LEONARDO CYBER & SECURITY SOLUTIONS

SUITE DEFENCE4FUTURE

LEONARDO

La digitalizzazione e la conseguente iper-connessione hanno significativamente impattato il settore della Difesa che ha dovuto, da un lato, adeguare i propri processi e le proprie infrastrutture per sfruttarne i vantaggi, dall'altro predisporsi ad affrontare le nuove minacce alla sicurezza nazionale provenienti dal cyberspazio. Gli attacchi informatici sono in continua crescita e si basano sempre più su minacce ibride cioè su azioni condotte da attori governativi, o finanziati da essi, progettate per rimanere al di sotto della soglia di rilevamento e di attribuzione.

Leonardo supporta la Difesa nello sviluppare e accrescere le competenze e capacità necessarie per affrontare il rischio cyber-fisico agendo in veste di:

- **system integrator**, coinvolgendo proattivamente tutti i partner nazionali e internazionali che possono contribuire in modo significativo ai programmi della Difesa;
- **fornitore di tecnologia**, progettando e sviluppando prodotti, sistemi, servizi e soluzioni che contribuiscono alla sovranità digitale nazionale e sovranazionale.

L'APPROCCIO DI LEONARDO AI RISCHI CYBER-FISICI

Leonardo adotta un approccio strutturato e globale alla sicurezza volto a migliorare le capacità della Difesa in tutti i domini. Secondo questo paradigma, il dominio cibernetico mette a disposizione strumenti, competenze e capacità di "intelligence" necessarie non solo per condurre operazioni nel cyberspazio, ma anche per garantire la continuità delle operazioni negli altri domini.

Poiché la sicurezza del cyberspazio è sempre più sinergica con quella dello spazio fisico, per proteggere efficacemente gli asset infrastrutturali della Difesa, è essenziale indirizzare queste due realtà in modo parallelo e coordinato. Ciò è possibile non solo attraverso piattaforme in grado di raccogliere i dati provenienti da sensori fissi e mobili sul campo, ma anche grazie a sale di controllo innovative che raccolgono, integrano e analizzano le informazioni provenienti dal mondo fisico e virtuale.
Tali sale di controllo integrano anche procedure operative, processi di supporto alle decisioni, e sistemi di comunicazioni radio, garantendo una maggiore situational awareness e un processo decisionale informato.

BENEFICI

- Incremento continuo dei livelli di resilienza cibernetica di tutti gli asset infrastrutturali della Difesa (basi militari, porti e aeroporti) attraverso l'adozione di modelli e strumenti innovativi da applicare anche alla supply chain.
- Riduzione dei rischi cyber-fisici facendo leva su una situational awareness completa e multi-dominio.
- Disponibilità di informazioni ad alto valore aggiunto che possono essere utilizzate per attuare rapidamente azioni e politiche di prevenzione mirate.
- Attuazione tempestiva delle attività di risposta agli attacchi e contenimento degli impatti, con la possibilità di gestire localmente i dati critici, comprese le azioni di rimedio e i risultati dell'analisi dei malware.
- Miglioramento delle capacità di cyber defense e di cyber warfare del personale della Difesa, attraverso strumenti innovativi di modellazione e simulazione per la generazione automatica di teatri di addestramento altamente complessi (digital twin).

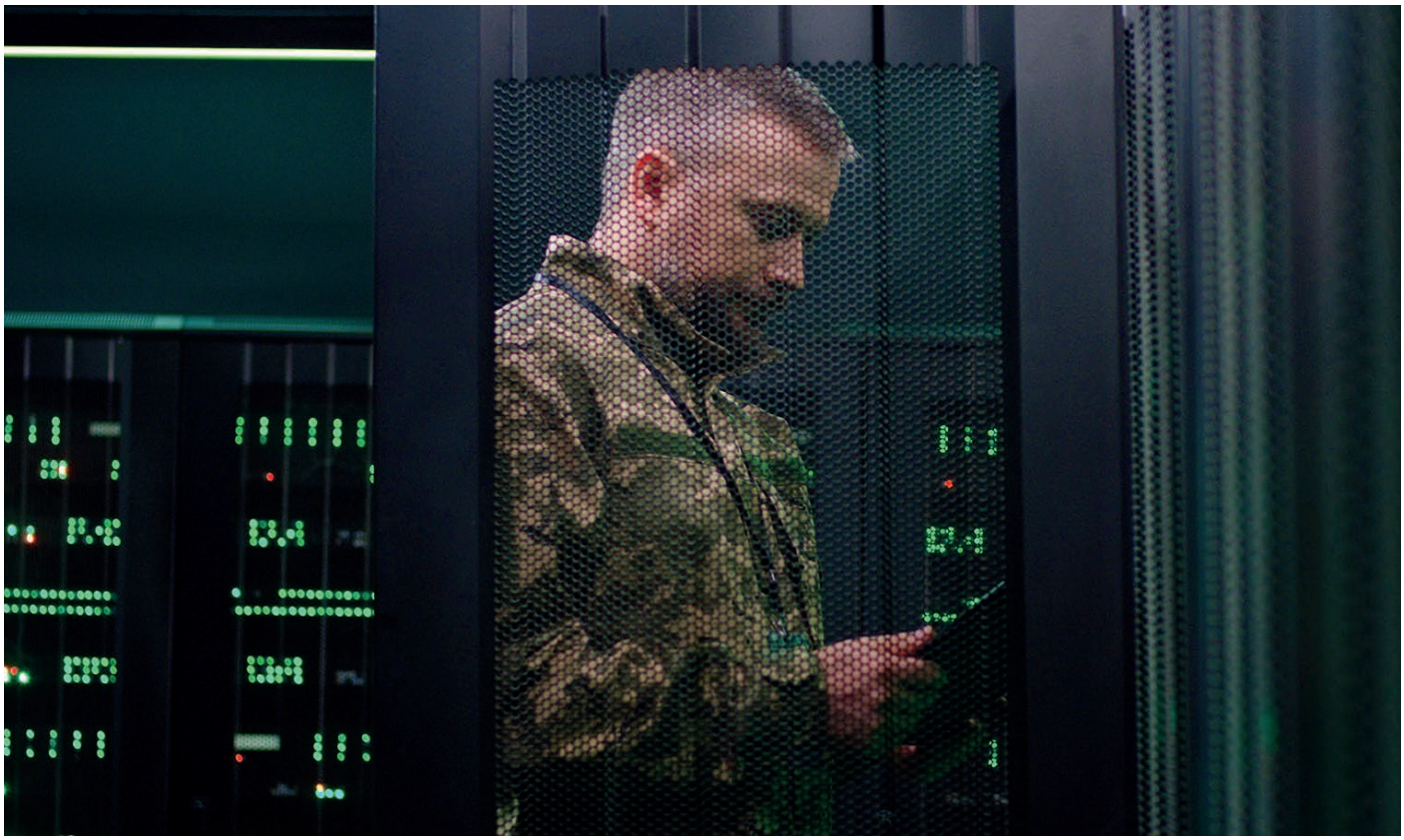
L'identificazione degli asset infrastrutturali critici, la quantificazione degli impatti causati dalla loro compromissione e la definizione di linee guida per garantirne la resilienza cyber-fisica costituiscono un punto particolarmente complesso, ma fondamentale, per rafforzare i sistemi informativi della Difesa. Si tratta di un processo che richiede necessariamente anche il coinvolgimento dell'intera filiera di approvvigionamento per l'adozione di politiche "secure by design" lungo tutto il ciclo di vita dei sistemi.

Per supportare la Difesa nella verifica della resilienza operativa e nella definizione di piani di business continuity e disaster recovery, le soluzioni di Leonardo garantiscono:

- riproduzione di scenari realistici attraverso tecniche di virtualizzazione che consentono di testare la resilienza di contesti operativi anche estremamente complessi e basati su tecnologie legacy;
- processi di valutazione cooperativa, competitiva e tecnologica grazie all'integrazione di ambienti virtuali e fisici esterni;
- elevato riutilizzo delle infrastrutture e delle architetture virtualizzate per effettuare test e valutazioni periodiche che consentono un miglioramento e un aggiornamento continuo dei sistemi;
- supporto nelle attività di verifica della resilienza operativa e nella definizione di attività di business continuity e di disaster recovery;
- possibilità di avvalersi delle potenzialità delle infrastrutture Cloud in termini di flessibilità e scalabilità garantendo la sicurezza, interoperabilità e federabilità delle infrastrutture della Difesa;
- garanzia della sostenibilità e della sicurezza delle infrastrutture energetiche della Difesa per fronteggiare possibili interruzioni nell'approvvigionamento.

Secure Cloud & Digital solutions

Energy Monitoring & Optimization for Decision Support (EMODS)	È la piattaforma per il monitoraggio energetico e per l'analisi dei dati di consumo delle infrastrutture. Grazie a dashboard e report personalizzabili, il sistema permette di ottenere una **conoscenza approfondita dei consumi** e una **visione completa dell'utilizzo dell'energia** anche a livello di singolo processo. Questo è utile a definire gli interventi più adeguati per ottimizzare ed efficientare i consumi, garantendo al contempo la cyber resilienza dei sistemi e delle operazioni.



Per quanto riguarda le comunicazioni infrastrutturali, destinate cioè ad usi diversi da contesti tattici ad alto impatto, la Difesa richiede soluzioni completamente integrate, affidabili e robuste, progettate per operare in basi militari, porti e aeroporti, anche in situazioni critiche. Leonardo sviluppa soluzioni di rete multi-tecnologiche, chiavi in mano, che integrano molteplici tecnologie di comunicazione cablate e wireless (TETRA e radio wireless a banda larga come LTE e 5G) che garantiscono una connettività trasparente agli utenti in ogni circostanza, incrementando la sicurezza e l'efficienza delle attività.

Leonardo è in grado di fornire alla Difesa:
- Reti di trasporto (sia cablate che wireless)
- Accesso a reti cablate (LAN) e wireless
- PAGA/PABX
- Clock distribution
- Operational communications.

Mission Critical Communications	
LTE/5G	**Le infrastrutture LTE supportano applicazioni ad alta intensità di dati.** In quest'ambito Leonardo riveste il ruolo di system integrator fornendo infrastrutture di terze parti finalizzate a garantire una copertura estesa, integrando reti commerciali e hot spot (attraverso bolle tattiche o configurazione network-in-a-box).
TETRA	**Adaptanet®** è una famiglia completa di prodotti TETRA modulari, scalabili e flessibili, in grado di soddisfare esigenze che vanno dal singolo sito alle reti nazionali. **Il sistema consente di fruire dei miglioramenti tecnologici offerti dalle comunicazioni full-IP**, ed è integrabile anche con soluzioni di dispacciamento dei terminali e applicazioni di servizio.
Network Integration	**CSP (Communications Service Platform)** consente l'integrazione di reti multi tecnologiche con gestione unificata di utenti e applicazioni; rappresenta l'elemento della **RIM (Rete Ibrida Multivettore)** di Leonardo che supporta la progressiva evoluzione dalle reti di comunicazione professionali a banda stretta a quelle a banda larga. CSP implementa la porzione LMR dello standard 3GPP LMR-IWF (Interworking Function) consentendo l'integrazione delle applicazioni 3GPP MCX.
Push-To-Talk over cellular	Il **Push-To-Talk su cellulare** è il modo per fornire servizi professionali su reti a banda larga. La **piattaforma MCX CSP** di Leonardo è una soluzione completa pienamente conforme agli standard 3GPP che consente comunicazioni mission critical su LTE e 5G. Progettata per sfruttare il potenziamento della banda larga mission critical, MCX può essere distribuita anche come applicazione OTT (Over-The-Top) su una rete commerciale, con un client Android completo e un dispatcher web based.

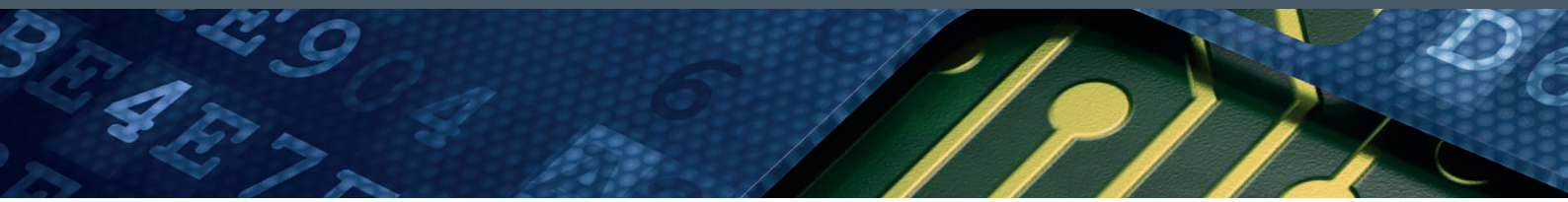
Per il settore della Difesa è fondamentale aumentare la resilienza delle proprie infrastrutture, in modo da poter anticipare, resistere e adattarsi a condizioni avverse, stress, attacchi o compromissioni. Partendo dal presupposto che è impossibile azzerare completamente i rischi cyber-fisici, è necessario garantire che le operazioni continuino anche a fronte di un attacco fisico, informatico o ibrido. Per farlo, è necessario monitorare, elaborare e analizzare continuamente un'enorme quantità di dati multidominio per estrarre, in modo tempestivo, informazioni concise, contestualizzate e immediatamente utilizzabili per supportare i processi decisionali e affrontare in modo ottimale i nuovi rischi convergenti.

Il Centro di Controllo Integrato di Leonardo è in grado di:

- integrare un numero significativo di sensori e sottosistemi diversi per raccogliere eventi e allarmi provenienti sia da domini fisici che informatici;
- filtrare e correlare gli allarmi attraverso un motore intelligente;
- rappresentare geograficamente le informazioni grazie a una interfaccia utente efficace e flessibile, integrata con un potente sistema informativo geografico (GIS);
- automatizzare le operazioni e guidare gli operatori nell'analisi del contesto seguendo le procedure operative standard e di emergenza;
- potenziare il coordinamento delle risorse dedicate alla protezione delle infrastrutture grazie all'integrazione di "Mission Critical Communication";
- tracciare e registrare tutti gli eventi per migliorare l'analisi, l'indagine e il debriefing successivi all'evento critico.

Global Monitoring	
SC2	Piattaforma orientata alla gestione della sicurezza fisica in grado di raccogliere tutti i dati provenienti da sensori fissi e mobili distribuiti sul campo (PIDS, AC, Videosorveglianza, UAV), correlare gli eventi e guidare gli operatori alla risoluzione dell'incidente grazie al sistema di workflow automatizzato (Orchestrator).
X-2030	Un nuovo **modello di sala di controllo basato sul paradigma del sistema dei sistemi**. **X-2030** integra le procedure operative, i processi di supporto alle decisioni, le comunicazioni radio e sfrutta tali tecnologie per ottenere una maggiore "situational awareness" e garantire decisioni informate. Progettato per integrare i sistemi esistenti, fornisce un'interfaccia utente innovativa basata su un assistente virtuale e sulla comprensione del linguaggio naturale.
GANIMEDE	Una soluzione per **l'analisi audio e video basata sull'intelligenza artificiale**, instanziabile attraverso diversi framework su diverse piattaforme hardware e applicabile a flussi live o registrati. I laboratori di intelligenza artificiale di Leonardo possono sviluppare e addestrare soluzioni personalizzate. **Integrato nativamente nelle piattaforme SC2 o X-2030**, Ganimede fornisce un set di API per applicazioni in sistemi di terze parti.

CYBER SECURITY & RESILIENCE: WHERE READINESS MATTERS



Nell'ambito delle numerose crisi geopolitiche in corso, gli attacchi informatici hanno spesso anticipato e supportato le strategie offensive e difensive degli avversari attraverso azioni nel dominio cibernetico in grado di causare impatti significativi anche nel mondo reale. Tali azioni risultano particolarmente efficaci a causa della difficoltà di attribuzione, aggravata da una linea di demarcazione sempre più labile tra attori governativi e non.

In questo scenario è ancora più evidente come il dominio cibernetico svolga un ruolo particolarmente critico nella conduzione delle operazioni militari. Infatti, la disponibilità e la continuità operativa delle infrastrutture fisiche e logiche della Difesa a supporto della conduzione delle missioni nei domini nuovi e tradizionali (aereo, terrestre, marittimo, spaziale) dipende dalla disponibilità e dall'accessibilità al cyberspazio stesso.
Leonardo supporta i clienti della Difesa nella progettazione, implementazione, messa in servizio e gestione di servizi, piattaforme e soluzioni di cyber security e protezione dei dati, al fine di difendere e mettere in sicurezza le infrastrutture IT/OT militari per renderle più resilienti nei confronti di minacce informatiche nuove e estremamente complesse.
L'offerta di Leonardo comprende:

- competenze professionali specifiche e certificate per l'implementazione di infrastrutture secure by design;
- piattaforme dedicate alla previsione e identificazione di minacce avanzate e alla gestione e orchestrazione di processi di intelligence altamente strutturati;
- capacità consolidate nella progettazione e implementazione di infrastrutture fisiche e logiche per lo sviluppo di programmi ad alto livello di classifica;
- supporto alle attività propedeutiche all'ottenimento di certificazioni e omologazioni necessarie per la gestione di informazioni classificate;
- sistemi finalizzati ad ottenere elevati livelli di situational awareness nell'ambito delle operazioni cibernetiche e a supportare gli operatori nella comprensione e gestione dei rischi informatici;
- soluzione EDR (Endpoint Protection & Response) proprietaria per l'implementazione tempestiva di regole di rilevamento e azioni di risposta completamente configurabili, che garantiscono la gestione locale dei dati relativi a vulnerabilità, attività di incident reponse e analisi dei software malevoli;
- soluzione evoluta per l'analisi di malware che consente di utilizzare e integrare più strumenti da un'unica interfaccia, ottimizzando i costi di utilizzo dei COTS (Commercial Off-The-Shelf).

Cyber Security & Resilience	
Design and Build services	Questi servizi si basano su un **approccio proprietario e su un processo consolidato per la progettazione, implementazione e avviamento** di infrastrutture di cyber security presso i Clienti (SOC, CERT, IOC).
Leonardo Engineering Assurance Profile for Cyber Resilience (LEAP4CR)	Questa **metodologia, basata sui framework NIST e MITRE**, consente di valutare il **livello di cyber resilienza di un prodotto/sistema/servizio, nuovo o già esistente**. Grazie ad una visione globale della postura di sicurezza, garantisce un'efficace gestione dei rischi e **consente di implementare le tecniche più appropriate per il contenimento di determinati tipi di attacco.**
Cyber Information Superiority (CIS) suite	La suite, **basata sul paradigma della superiorità informativa applicato al dominio cyber**, è composta dall'integrazione **di tre piattaforme che permettono di svolgere attività di threat intelligence, di protezione e gestione degli end point e di analisi delle minacce informatiche**. L'obiettivo è ottenere informazioni preziose e fruibili che possono essere utilizzate per attuare rapidamente azioni mirate di prevenzione, risposta e contenimento.
Cyber Situational Awareness System (CSAS)	Il sistema è progettato per **mantenere aggiornati i team di sicurezza e i comandanti sullo stato di sicurezza del perimetro IT e per supportare il processo decisionale** in quest'ambito. Fornisce una **piattaforma di centralizzazione delle informazioni** che aggrega e rende visualizzabili i dati attraverso viste gestionali di alto livello e dashboard tecnico-operative.

Le attività di formazione e addestramento svolgono un ruolo fondamentale nella prevenzione e nell'individuazione precoce delle minacce informatiche più evolute. Gli operatori dedicati alla protezione cibernetica delle infrastrutture strategiche nazionali devono essere in grado di testare e implementare in modo tempestivo, rapido e cooperativo le azioni necessarie per contenere le minacce e minimizzarne gli impatti. Per questo è necessario creare una rete culturale fatta di competenze di sicurezza integrate e condivise che contribuiscano a sensibilizzare sui nuovi rischi cyber tutti i soggetti che rivestono un ruolo chiave nel garantire la sicurezza nazionale e sovranazionale.
È quindi fondamentale investire in attività formative che, da un lato, rafforzino la conoscenza della sicurezza in termini di tecnologie, processi e normative, e dall'altro sviluppino il "fattore umano", migliorando la capacità di condividere il contesto e interpretare le informazioni, capacità fondamentali per gestire efficacemente le crisi derivanti da attacchi alla sicurezza e incidenti con impatti su larga scala.

Leonardo supporta la Difesa nel potenziamento delle competenze e delle capacità necessarie a riconoscere e affrontare i nuovi rischi cyber-fisici che minacciano la sicurezza dei Paesi attraverso un centro di formazione avanzata che offre:

- un approccio integrato e multilaterale ai temi della sicurezza globale che va oltre il concetto di erogazione di contenuti formativi su argomenti specifici;
- un ecosistema formativo dedicato a scambiare idee, migliorare le competenze dei team di difesa informatica, proporre e testare nuovi approcci e raccogliere nuovi requisiti nell'ambito della sicurezza e resilienza cibernetica;
- percorsi di formazione immersivi basati sulle competenze acquisite dai team di sicurezza di Leonardo in domini critici;
- attività di addestramento personalizzabili in base al contesto di riferimento, implementate utilizzando piattaforme proprietarie per la simulazione di contesti operativi reali;
- possibilità di configurare e generare automaticamente teatri e scenari di addestramento complessi e riutilizzabili;
- interoperabilità con orchestratori remoti e capacità native di condividere teatri di federabili con altri poligoni virtuali.

Cyber Training	
Cyber & Security Academy	Un centro di formazione innovativo per promuovere la consapevolezza in ambito cybersecurity e sviluppare le competenze tecniche e soft-skill attraverso un **portafoglio di corsi completo, erogato da formatori esperti e caratterizzato dall'utilizzo di piattaforme avanzate** per esercitazioni pratiche e immersive.
Cyber Trainer	**Piattaforma basata su cloud per formare e tenere aggiornati sia i professionisti della sicurezza che gli utenti non esperti**. Permette di gestire l'intero processo di formazione dei discenti (esigenze formative, apprendimento formale, esercitazioni, certificazione).
Cyber Range	Ambiente integrato per **simulazioni immersive e realistiche che riproducono scenari di attacco e difesa informatica** dedicato all'addestramento dei team di sicurezza e alla verifica della resilienza informatica delle infrastrutture militari.

HIGHLIGHTS

- Maturity Model proprietario e ambienti simulati estremamente realistici per testare e valutare la postura di cyber sicurezza e resilienza della Difesa in termini di persone, processi e tecnologie, nuove e/o già in uso.
- Sistemi e soluzioni interoperabili progettati e sviluppati per valorizzare dati eterogenei e multidominio al fine di ottenere un vantaggio informativo sugli attori malevoli.
- Piattaforma proprietaria che consente di svolgere esercitazioni di sicurezza informatica in un ambiente virtualizzato al fine di preparare gli specialisti ad affrontare al meglio anche attacchi informatici sistemici e su larga scala.

DIVISIONE “CYBER AND SECURITY SOLUTIONS”

Con esperienza nell’information technology, nelle comunicazioni, nell’automazione, nella sicurezza fisica e digitale, la Divisione Cyber and Security Solutions di Leonardo genera sinergie unendo le proprie competenze a supporto di agenzie, aziende e organizzazioni di pubblica sicurezza, emergenza e protezione civile.
La nostra offerta include soluzioni per la sicurezza e la protezione di infrastrutture critiche, infrastrutture di trasporto, grandi eventi e stadi, sicurezza informatica, sistemi di reti integrate e comunicazioni sicure che consentono una gestione delle informazioni sicura, affidabile ed efficiente.

Secure Cloud & Digital

Global Monitoring

Mission Critical Communications

Cyber Security & Resilience

For more information:
cyberandsecurity@leonardo.com

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

MM09151 06-23

LEONARDO