



Proteggere le CNI: Leonardo Business Driven Cybersecurity



"It would seem that Caesar's recurrent and deep-rooted fault was his concentration in pursuing the objective immediately in front of his eyes to the neglect of his wider object. "
— B.H. Liddell Hart, Strategy

Scenario: gli Incendi Boschivi su larga scala

- Il fenomeno degli incendi boschivi su larga scala ha acquisito sempre più importanza a causa di diversi fattori, tra cui:
 - Gli effetti del cambiamento climatico
 - L'urbanizzazione
 - Il degrado del paesaggio
 - Azioni dolose o colpose da parte di singoli o gruppi di persone
- Questi cosiddetti "Mega-fuochi" sono particolarmente distruttivi e difficili da controllare con le tecnologie e sistemi attualmente disponibili per i Vigili del Fuoco e gli altri Enti coinvolti nell'emergenza.
- Il progetto AF3 intende fornire un significativo miglioramento
 - Nell'efficienza delle operazioni antincendio
 - Nella protezione della vita umana
 - Nella salvaguardia dell'ambiente e dei beni
- Fattori abilitanti
 - Sviluppo di tecnologie innovative
 - Sviluppo di mezzi per garantire un elevato livello di integrazione tra sistemi esistenti e nuovi.

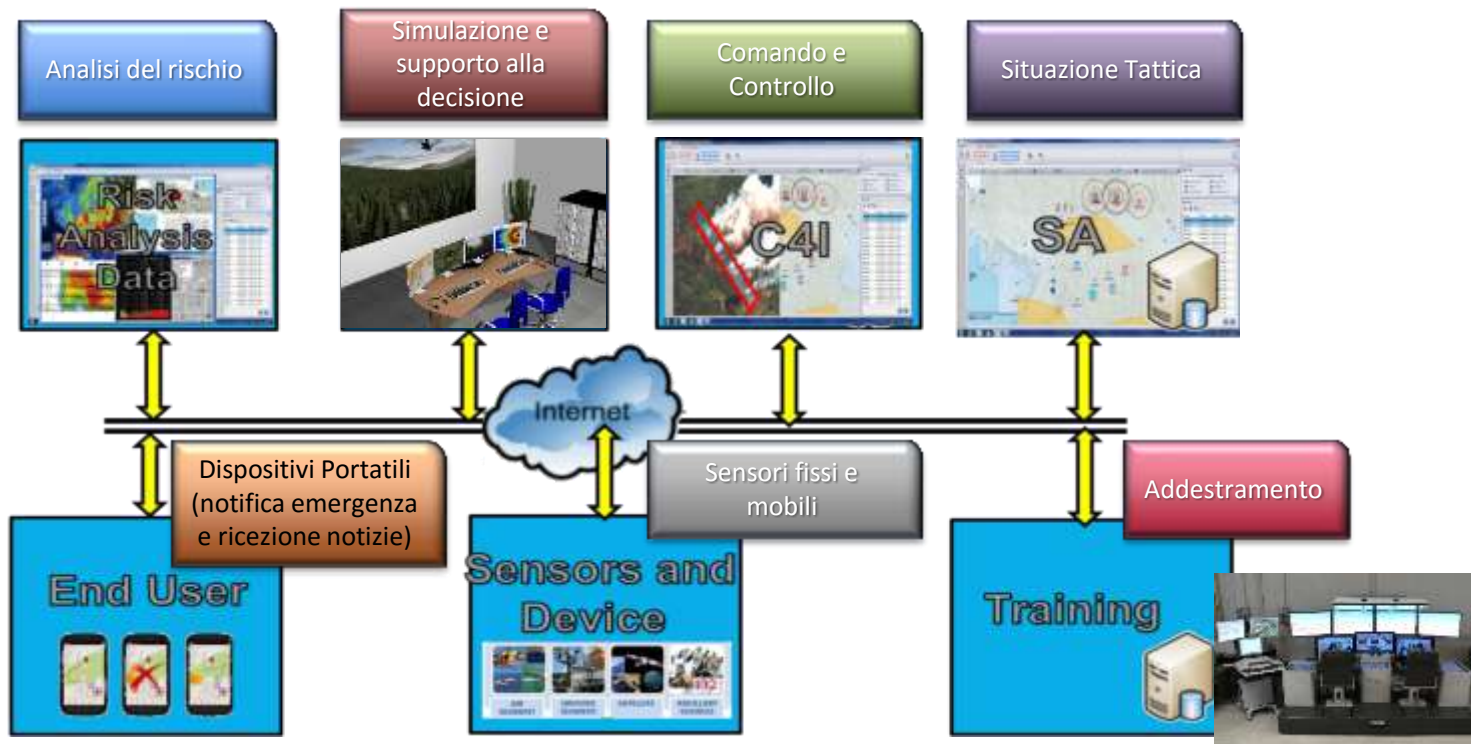


Aree di azione del Progetto AF3

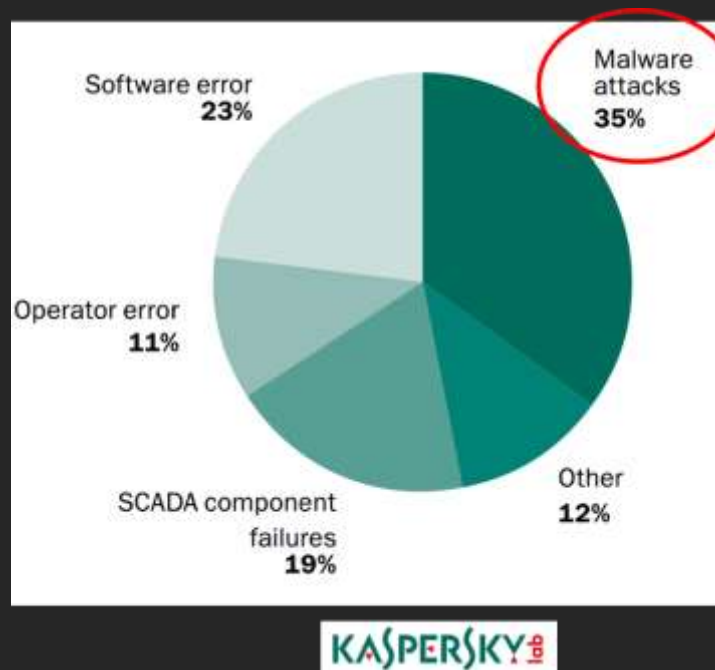
- Il progetto AF3 si concentra sulle seguenti aree:
 - **Diagnosi precoce e monitoraggio:** l'integrazione e implementazione di sistemi diversi, tra cui satelliti, aerei, UAV, e sistemi di terra mobili e fissi per la diagnosi precoce del fuoco e per il monitoraggio della propagazione del fumo e di nubi tossiche.
 - **Innovazione nelle contromisure passive:** costituzione di linee difensive preventive tramite capsule per evitare la diffusione del fuoco dall'area boschiva alle aree popolate.
 - **Innovazione nelle contromisure attive:** implementazione del nuovo sistema AAFF (Advanced Aerial Fire Fighting) per disperdere in modo accurato e sicuro materiali estinguenti da alta quota da parte di aerei ed elicotteri in qualsiasi condizione.
 - **Gestione integrata delle situazioni di crisi:** coordinamento generale di tutti gli aspetti dell'operazione e implementazione di **sistemi di Simulazione per il supporto alla decisione.**
- I risultati di AF3 saranno convalidati da prove intermedie durante il progetto, e da una dimostrazione finale con prove di volo ed esercitazioni sul campo.



Gestione integrata delle situazioni di crisi



Il contesto di riferimento



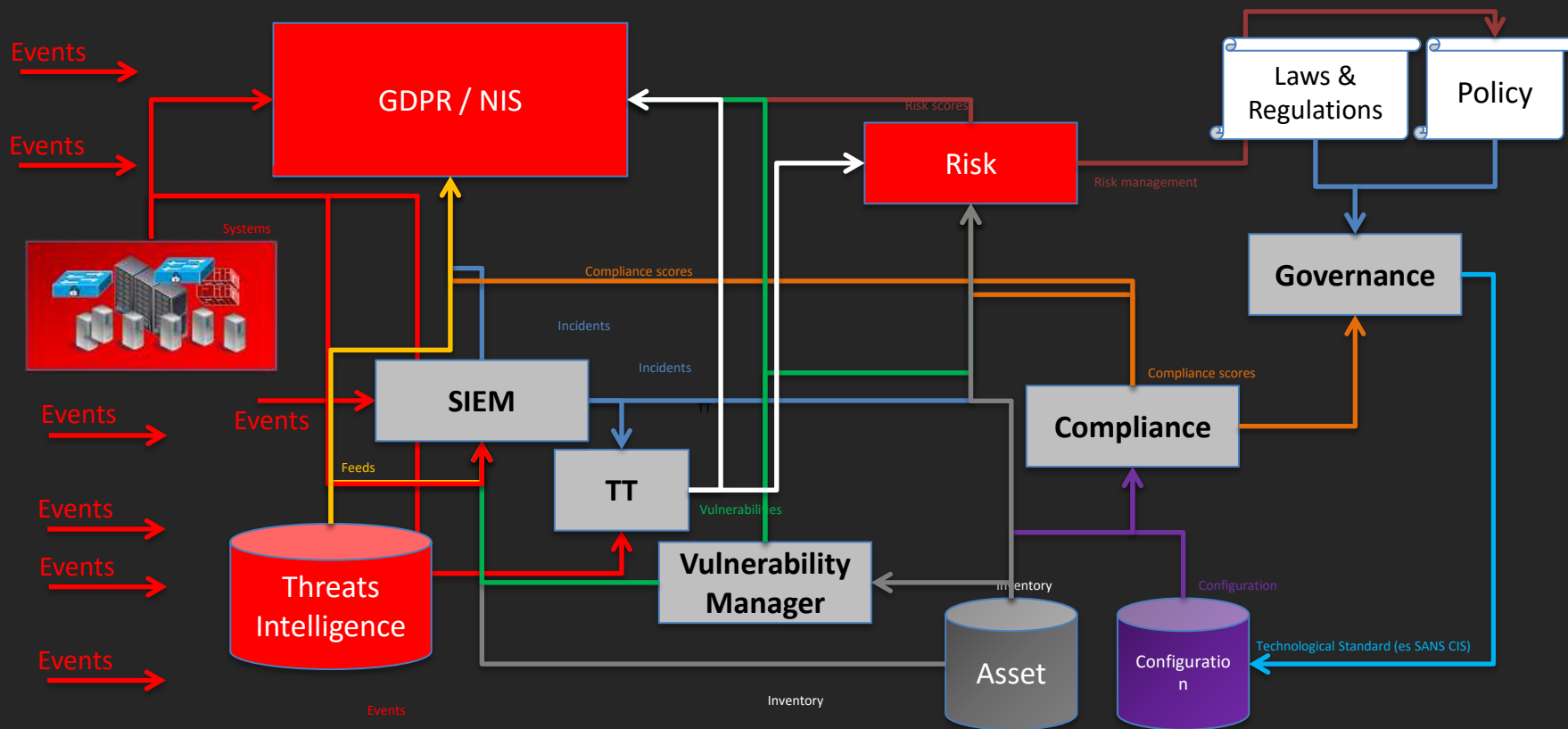
35% attacchi Cyber

Stato di fatto

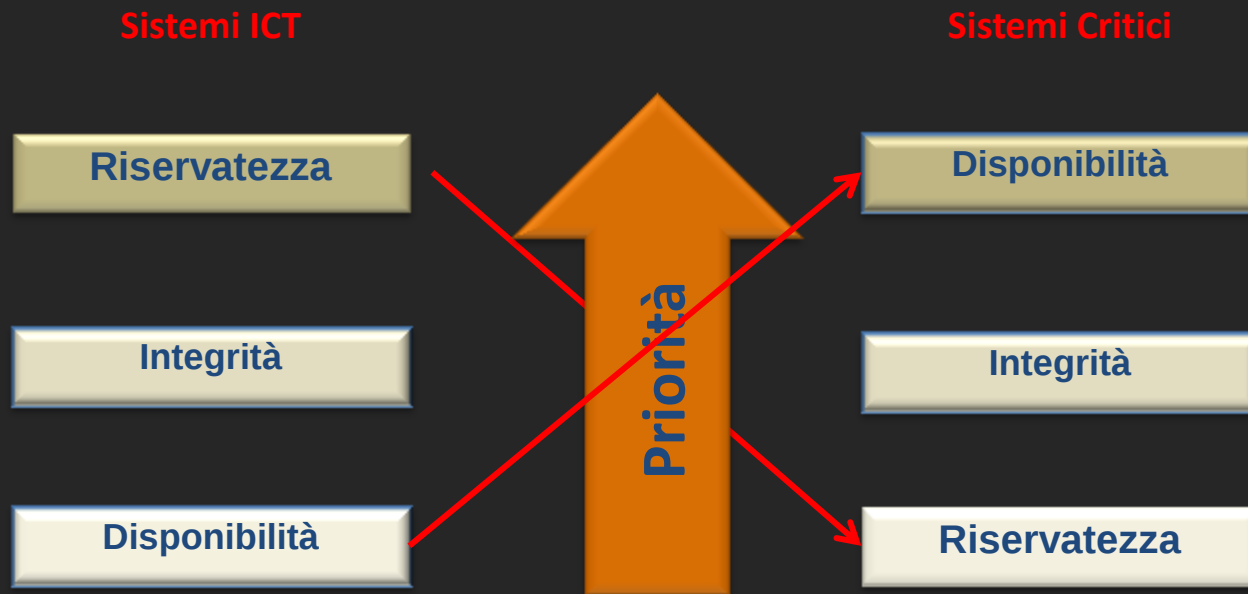
L'analisi di Kaspersky mostra che gli incidenti in ambito ICS/CNI sono provocati da diversi fattori di cui bisogna tener conto:

- Errori Operativi
- Problemi con il processo di Upgrade
- Misuse & misconfiguration
- Malware & exploits: zero-days

Il contesto

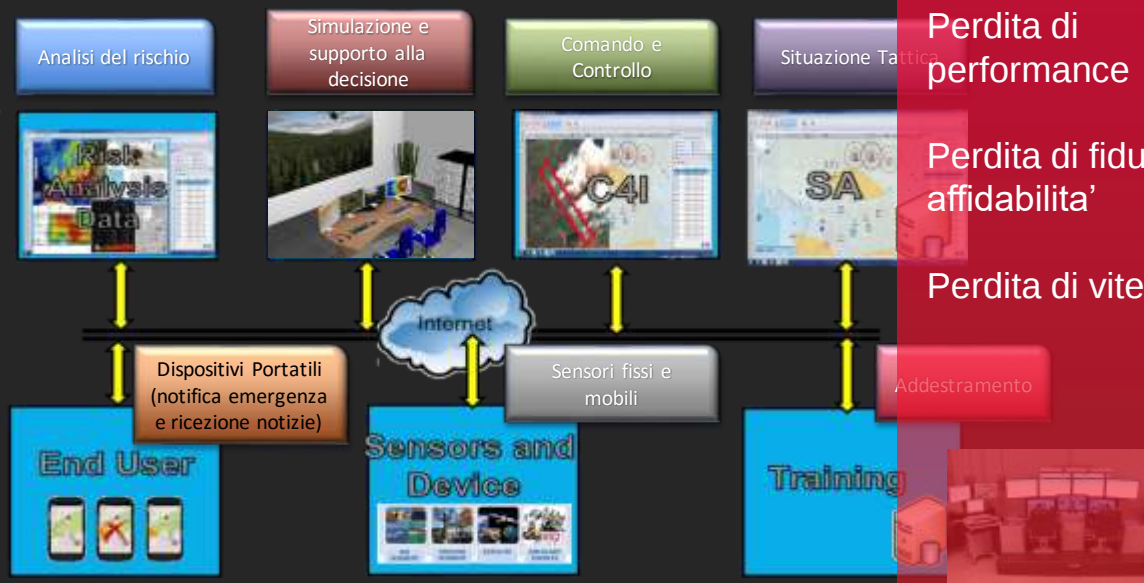


Il nuovo paradigma



Secure By Design : che significa?

- Unpatched software
- Misconfigured security software
- Unauthorized software
- Unnecessary network services
- Unnecessary system functions
- Outdated software
- Software failures
- Hardware failure in preventing malicious intrusion
- Ineffective controls



Perdita di capacità'

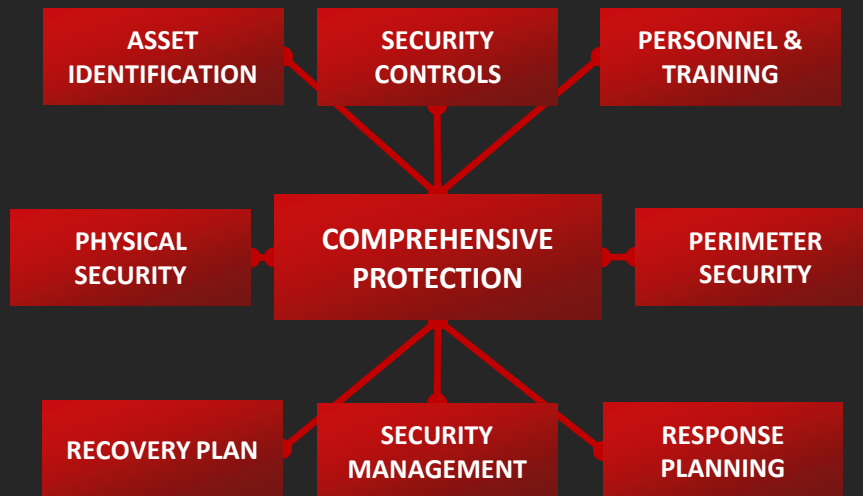
Perdita di performance

Perdita di fiducia e affidabilità'

Perdita di vite

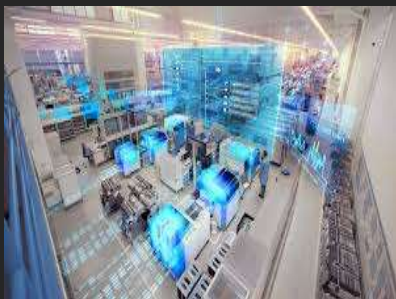
Cybersecurity testing of about 45 U.S. D.o.D. systems in 2014 showed the need for improvements in order to assure secure and resilient cyber capabilities

La visione di Leonardo



Cyber Defence oggi : Real-time

- prendere decisioni in ambienti complessi dipendendo da input dinamici
- misura continua del rischio dinamico associato a ciascun'entità analizzando sia le attività rilevate sia le informazioni d'intelligence
- calcolare istantaneamente il rischio associato ad un **determinato processo di business**



OT Assets
Sensors & SCADA



IT Assets
Cyber Security

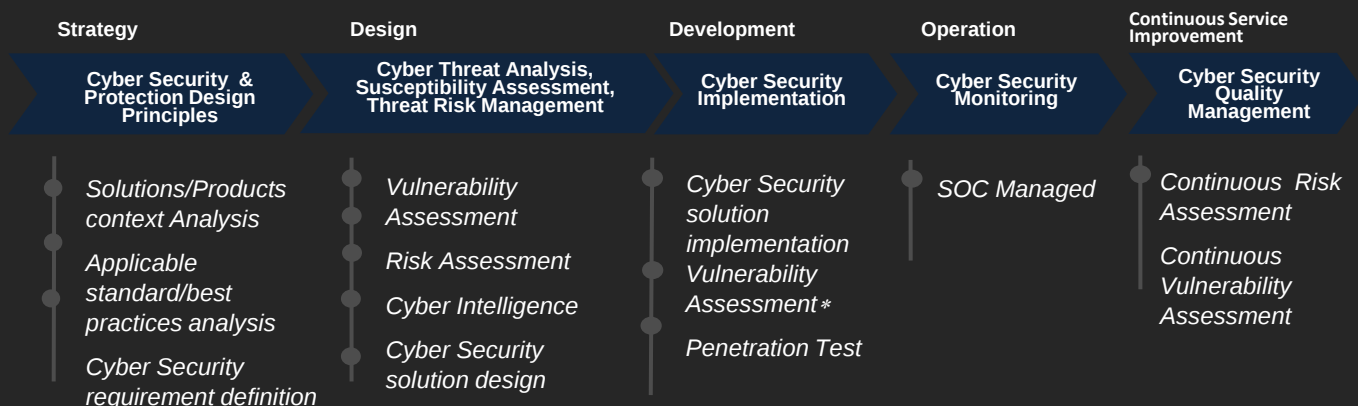


Intelligence
People & Information



Business Process Governance

Secure By Design : Reduce the attack surface



Secure by Design: Requirement, Design, Implementation, Verification

L'analisi delle vulnerabilità, ad ogni livello, sia per il codice sorgente o binario, sia per l'analisi delle applicazioni in esecuzione, nelle diverse fasi del ciclo di vita, in particolare durante le fasi di deployment e maintenance del servizio

Secure by configuration: minimal configuration enabling only the essential services

Secure by Operation: Secure Operation and Maintenance

Cybersecurity backed business
un approccio che mette al primo posto i processi di business dell'azienda (continuità operativa per la Difesa, resilienza per garantire funzionalità base per sistemi d'arma, ecc.) piuttosto che una generica protezione dai rischi

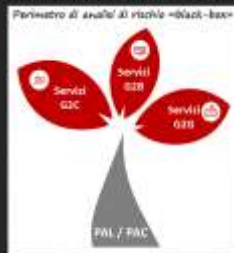
Risk Management

Fase 1

Definizione del contesto

Contesto

La definizione del contesto prevede la classificazione dei servizi erogati dalle P.A. e delle PAL/PAC oggetto dell'assessment.



SERVIZI GIOVANI

ATTIVITÀ ECONOMICHE

SERVIZIO BIBLIOTECA

Indice	Relevanza	Integrità	Disponibilità
Accessibilità	3	3	3
Qualità	3	3	3
Accessibilità	3	3	3
Accessibilità	3	3	3

Indice	Relevanza	Integrità	Disponibilità
Accessibilità	3	3	3
Qualità	3	3	3
Accessibilità	3	3	3
Accessibilità	3	3	3

Indice	Relevanza	Integrità	Disponibilità
Accessibilità	3	3	3
Qualità	3	3	3
Accessibilità	3	3	3
Accessibilità	3	3	3

Valutazione impatti

Gli ambiti di analisi sono classificati in funzione dell'impatto sulla riservatezza, integrità e disponibilità delle informazioni trattate.

Fase 2

Valutazione del rischio

Tassonomia Minacce

Sono identificate le minacce che insistono sugli ambiti di analisi delle P.A.

Analisi del rischio

E' valutato il rischio associato a ciascuna minaccia sulla base della probabilità di accadimento e dell'impatto.

Fase 3

Trattamento del rischio

Trattamento del rischio

In funzione del livello di rischio e delle vulnerabilità del sistema di controllo, si determinano le principali azioni di rimedio.



Attacchi logici e/o fisici



Utilizzo improprio e/o errori



Minacce Ambientali



Legale



Esempi di risultati del Risk Assessment

Valutazione dei rischi a livello aggregato

ESEMPLIFICATIVO

Scenario	Minaccia	Descrizione generale della minaccia	Risk rating* Complessivo	Distribuzione rischi sulle minacce di dettaglio
Attacchi logici e/o fisici	Malware	Include le minacce legate a codice malevolo (viruses / worms, trojan horses / rootkits, botnet clients)	Medio	3 Medio
	Hacking	Include le minacce relative a attacchi DoS, utilizzo di credenziali non autorizzato, scanning / intercettazione della rete, modifiche al sito web / al software / alle informazioni, furto di credenziali, etc.	Alto	1 Alto 3 Medio 5 Basso 1 Molto Basso
	Minacce sociali	Include le minacce che utilizzano l'utente finale come veicolo per un attacco ai sistemi/informazioni (spoofing del sito, phishing, spam, etc.) e relative alla disclosure non autorizzata, accidentale o deliberate di informazioni aziendali.	Alto	1 Alto 2 Medio 2 Basso
Utilizzo improprio e/o errori	Utilizzo improprio	Include le minacce relative ad utilizzo non autorizzato/non consono dei sistemi informatici, sottrazione di software/informazioni.	Medio	3 Medio 1 Basso
	Errori e malfunzionamenti	Include le minacce legate ad errore utenti finali / staff tecnico, malfunzionamento HW / SW, effetti non desiderati derivanti da modifiche.	Alto	3 Alto 3 Medio 1 Basso
Minacce ambientali	Accessi fisici e furti/perdite	Include le minacce relative ad accessi fisici non autorizzati e furti/perdita di dispositivi.	Medio	3 Medio 1 Basso

Legend

a



Alto



Medio



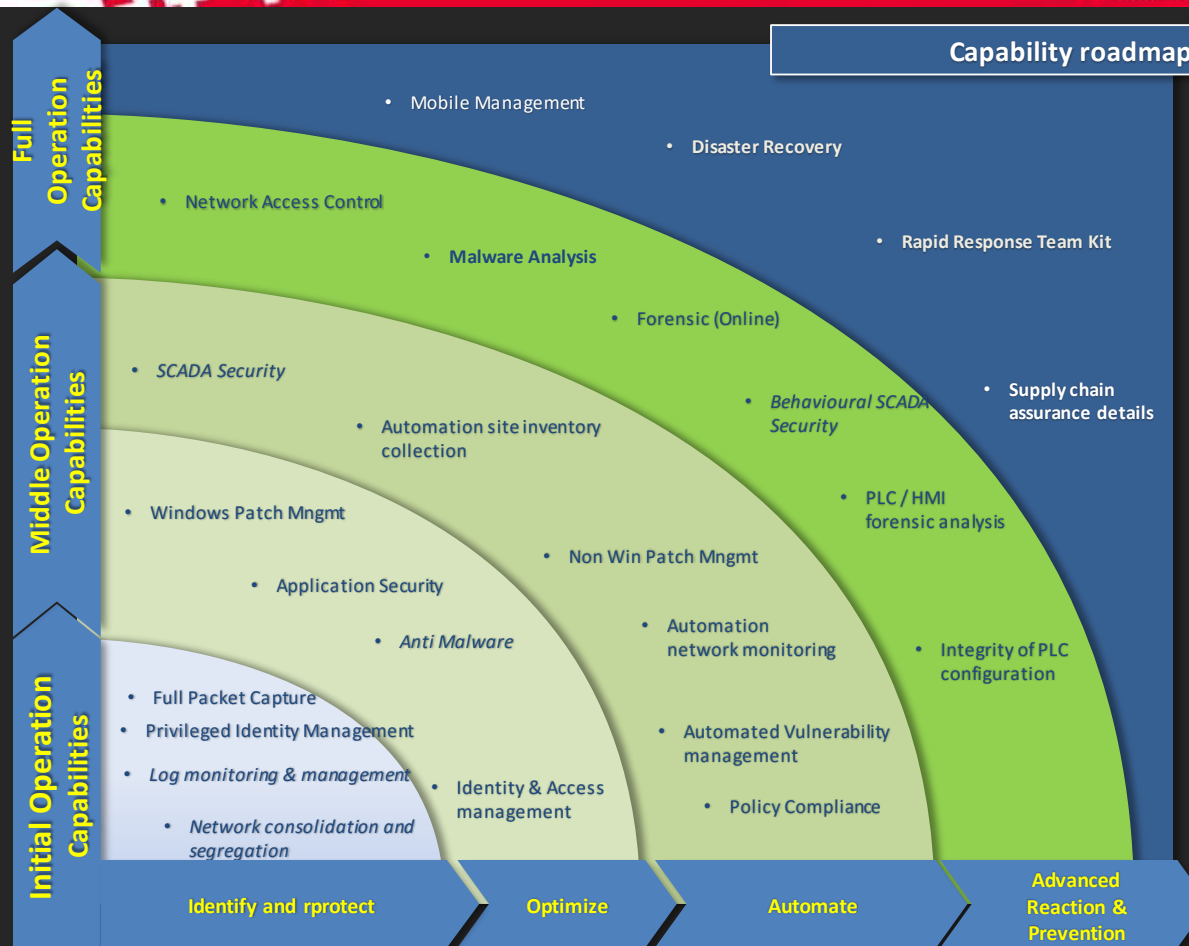
Basso



Molto Basso



* Calcolato considerando il valore massimo di rischio (worst case) riscontrato per le minacce sottostanti



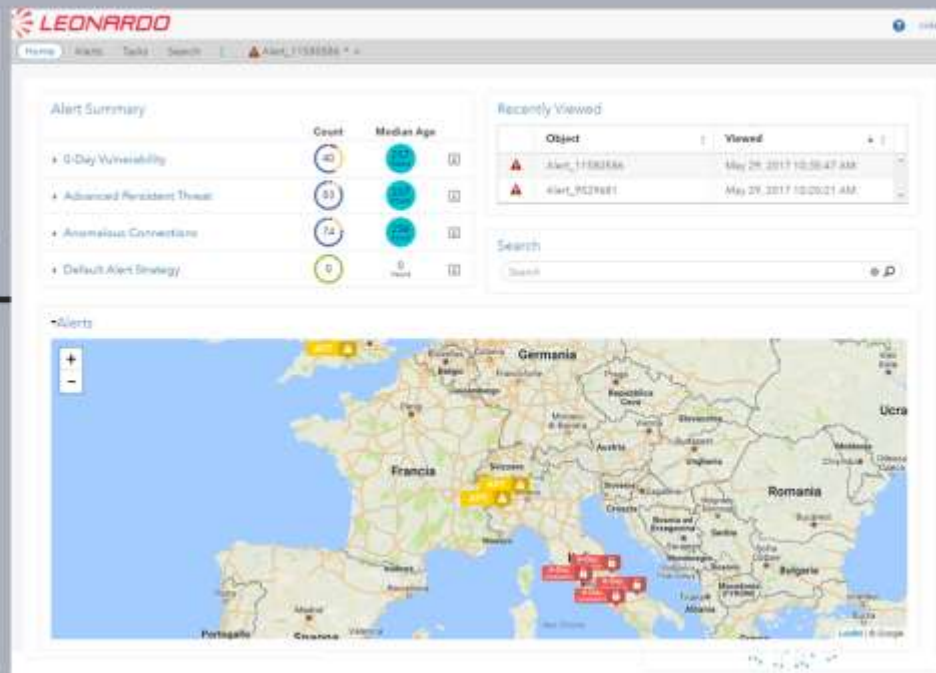
Real-time reaction on dynamic risks

Dynamic Impact Concept

The «**Dynamic Impact**» is a method to evaluate the potential damage of a Threat towards the Vulnerabilities of a Business environment.

Dynamic Risk Factor

«**Risk Factors**» are determined by the sum of different dimensional analysis: deterministic and other dynamically calculated by machine learning algorithms, clustering, ecc. to identify a Threat



Wanna Cry

Vulnerabilità 0-Day SMB
rilev. 8 Jan 2017 11:46:00

Identificazione asset a rischio alto business (sensibilità informazioni, processi critici, alto impatto disruption)

Prioritizzazione remediation

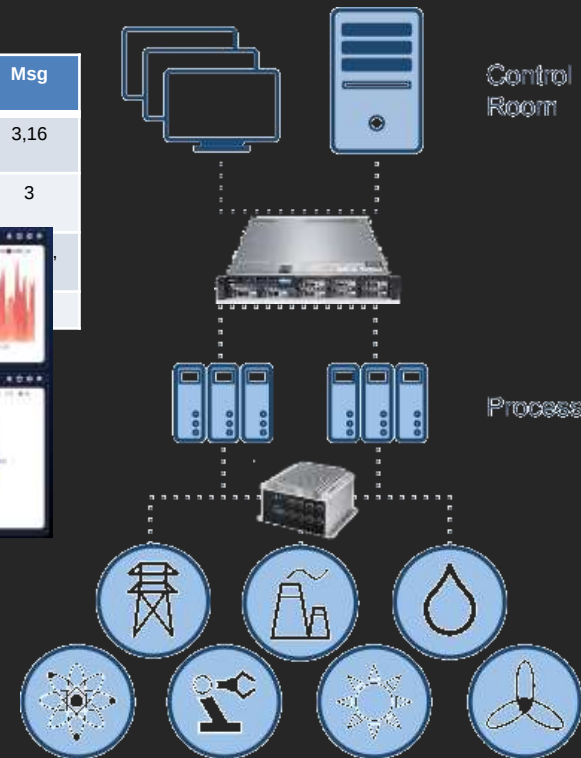
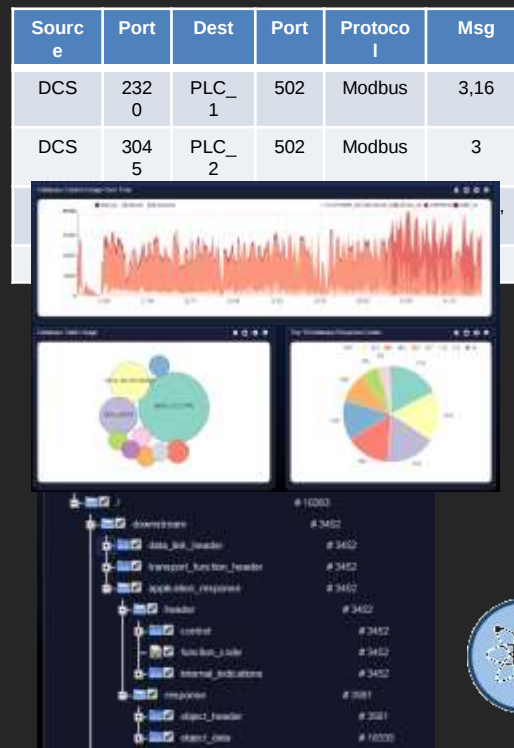
Gestione casi accessori

Impatto ransomware contenuto

Impatto finanziario e operativo limitato

Network Security Awareness

- **Awareness of the industrial network and process**
 - Quali sono i device attivi?
 - Quali protocolli e funzioni sono utilizzati?
 - Come sono modificati I valori di set-up dei processi?
- **Advanced threat detection**
 - Nuove connessioni (e.g. rogue devices)
 - Comandi inusuali (e.g. cambiamenti su PLC/RTU)
 - Valori anomali (e.g. non-compliant or harmful)
 - Exploitation di vulnerabilità (e.g. 0-days)
 - Portscan, MITM
- **Actionable security & operational intelligence**
 - Capacità di individuare la root cause di un'anomalia



Cyber Training & Cyber Range



Automazione spinta di gestione

Addestramento personalizzato tramite criteri innovativi

Modelli avanzati di rappresentazione di esigenze, scenari, tattiche ed asset

Strumenti per l'amministrazione e il monitoraggio delle attività.

Costi di esecuzione ridotti

Architettura e fruizione flessibili

L'architrate e la principale vulnerabilit  di ogni sistema sono le persone

Pi  del 90% degli attacchi che vanno a segno sono basati su vulnerabilit  ed exploit ben noti

E' necessario mantenere aggiornati i team di sicurezza anche offrendo scenari formativi che includono simulazioni di attacco e esercitazioni realmente complete.

The background features a pixelated, grayscale mountain range spanning the upper half of the image. Below the mountains, a faint compass rose is visible, consisting of a circle with several radial lines. In the top right corner, there is a solid red rectangle. The text "Alcuni esempi pratici" is positioned in the lower-left area of the image.

Alcuni esempi pratici

Case Study – Distribuzione Elettrica

AMBIENTE

CENTRO DI CONTROLLO

- Monitoraggio sistemi SCADA: DNP3 e IEC (150+ sottostazioni)

SOTTOSTAZIONI

- Monitoraggio del traffico interno: IEC 61850 e Synchrophasor

RISULTATI PIÙ SIGNIFICATIVI

- Rilevati diversi componenti in sottostazione non configurati correttamente
- Rilevata diverse RTU malfunzionanti che avrebbero potuto causare la perdita di visibilità del processo
- Rilevate connessioni Telnet non aderenti alle policy aziendali che prevedono l'uso di SSH ove possibile
- Rilevate RTU non configurati correttamente che avrebbero potuto impedire le normali operazioni di controllo sulla rete elettrica

Case Study – Distribuzione Elettrica

AMBIENTE

CENTRO DI CONTROLLO

- Monitoraggio di 150+ RTU basate su protocollo IEC 104
- Connessioni con il TSO nazionale e altri due centri di controllo regionali (2 server ICCP)

RISULTATI PIÙ SIGNIFICATIVI

- Rilevato un elevato numero di connessioni non terminate correttamente, con rischio di impedire nuove connessioni
- Rilevato problemi di connettività tra il server SCADA e diverse RTU remote (20.000 riconnessioni in un giorno)
- Rilevati tutti i tentativi di attacco: portscan, MitM, exploit di vulnerabilità software, alterazione dei processi
- Simulati e correttamente rilevati scenari di elevata importanza per il cliente: sequenze di comandi errate, errate configurazioni

Case Study – Impianto Manifatturiero

AMBIENTE

PLANT NETWORK

- Dump del traffico dei sistemi di produzione
- Protocollo proprietario Siemens Step 7

RISULTATI PIÙ SIGNIFICATIVI

- Rilevato un backup completo della memoria dei PLC effettuato da due engineering workstation durante la notte (non noto al cliente)
- Rilevato un operatore forzare manualmente alcuni registri di memoria di PLC a valori statici; tali registri sono normalmente aggiornati in base allo stato dei canali di I/O (non noto al cliente)
- Rilevato l'uso di una interfaccia RPC nota per essere vulnerabile nel passato ad exploit (Server Service Remote Protocol)

Case Study – Stoccaggio Gas

AMBIENTE

RISULTATI PIÙ SIGNIFICATIVI

STOCCAGGIO

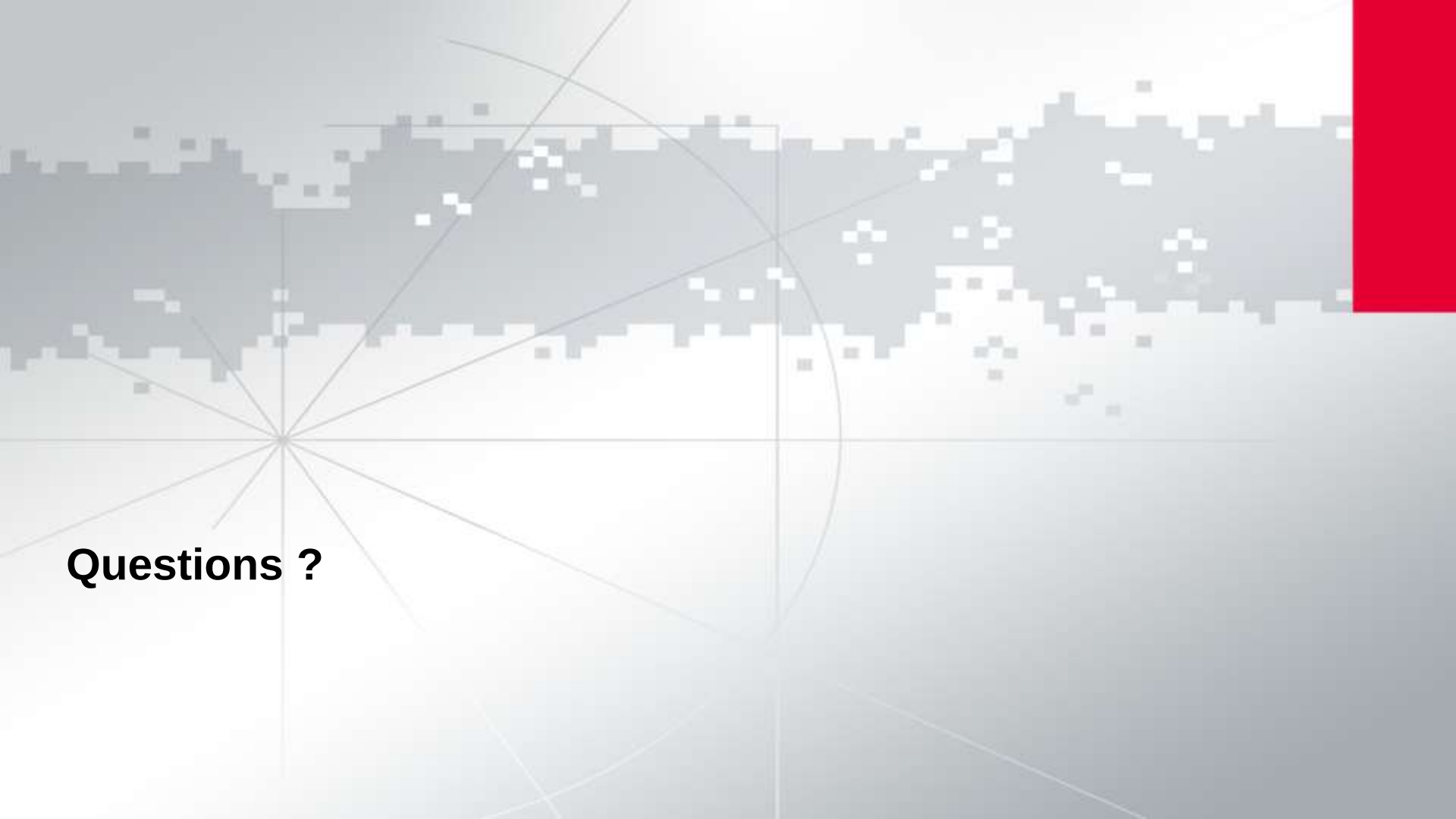
- ABB 800xA DCS
- ABB AC 800 M PLCs

- Rilevate inconsistenze tra le reti di produzione e test
- Rilevati tutti gli attacchi simulati condotti durante il PoC: malware, comunicazioni e comandi anomali
- Gli operatori utilizzano SilentDefense per effettuare cambiamenti in maniera controllata

TRASPORTO

- SCADA server connessi a ~2000 RTU

- Rilevate RTU che non utilizzavano l'estensione proprietaria al protocollo IEC 104 utilizzato dall'organizzazione

The background features a pixelated, grayscale mountain range across the top. A faint compass rose is centered on the left side. A solid red rectangle is positioned in the top right corner.

Questions ?