Deloitte.

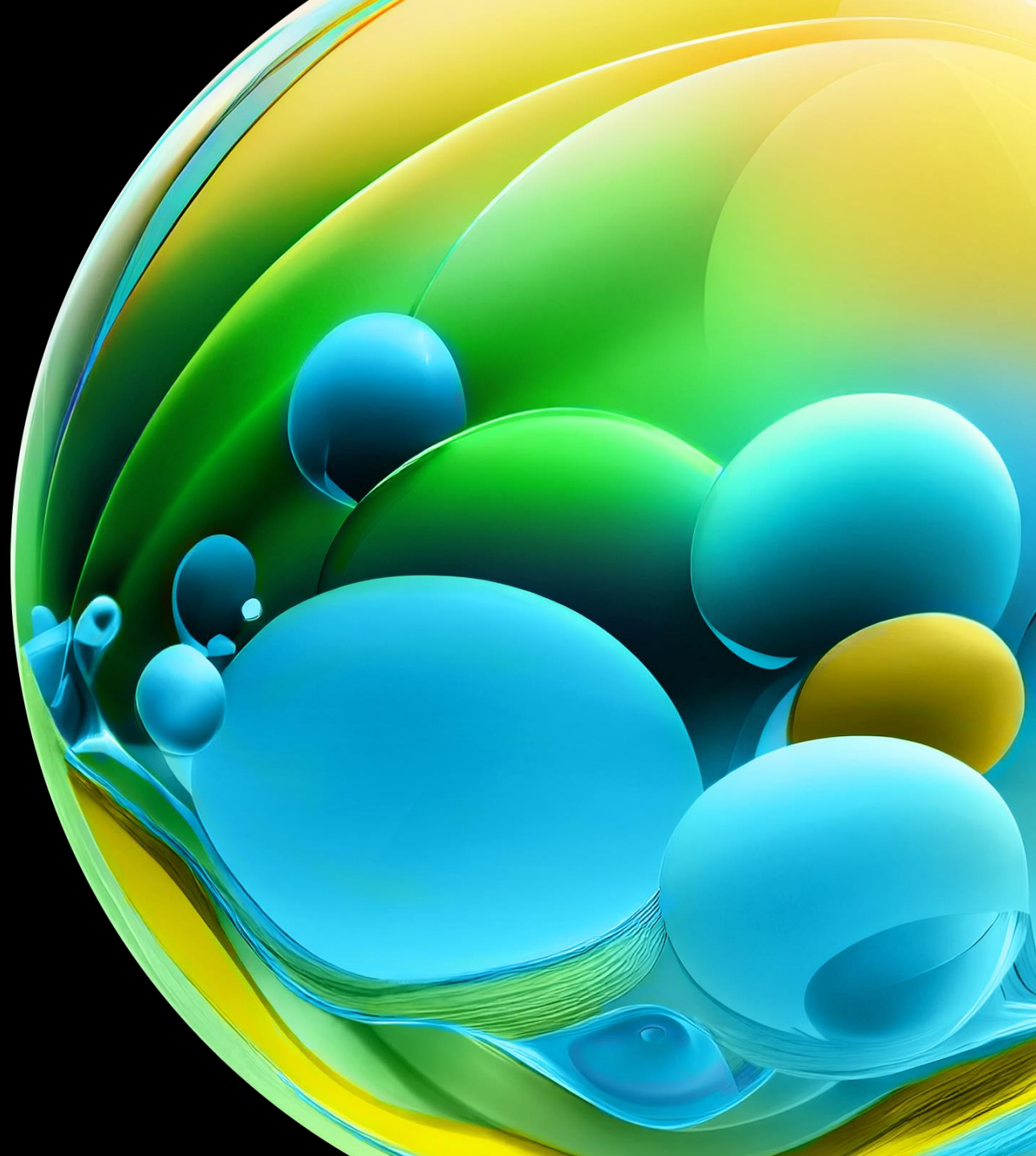
CAMERA DI COMMERCIO CUNEO

Gli impatti delle nuove normative sulla cybersecurity negli ambienti OT/IoT

Camera di Commercio di Cuneo

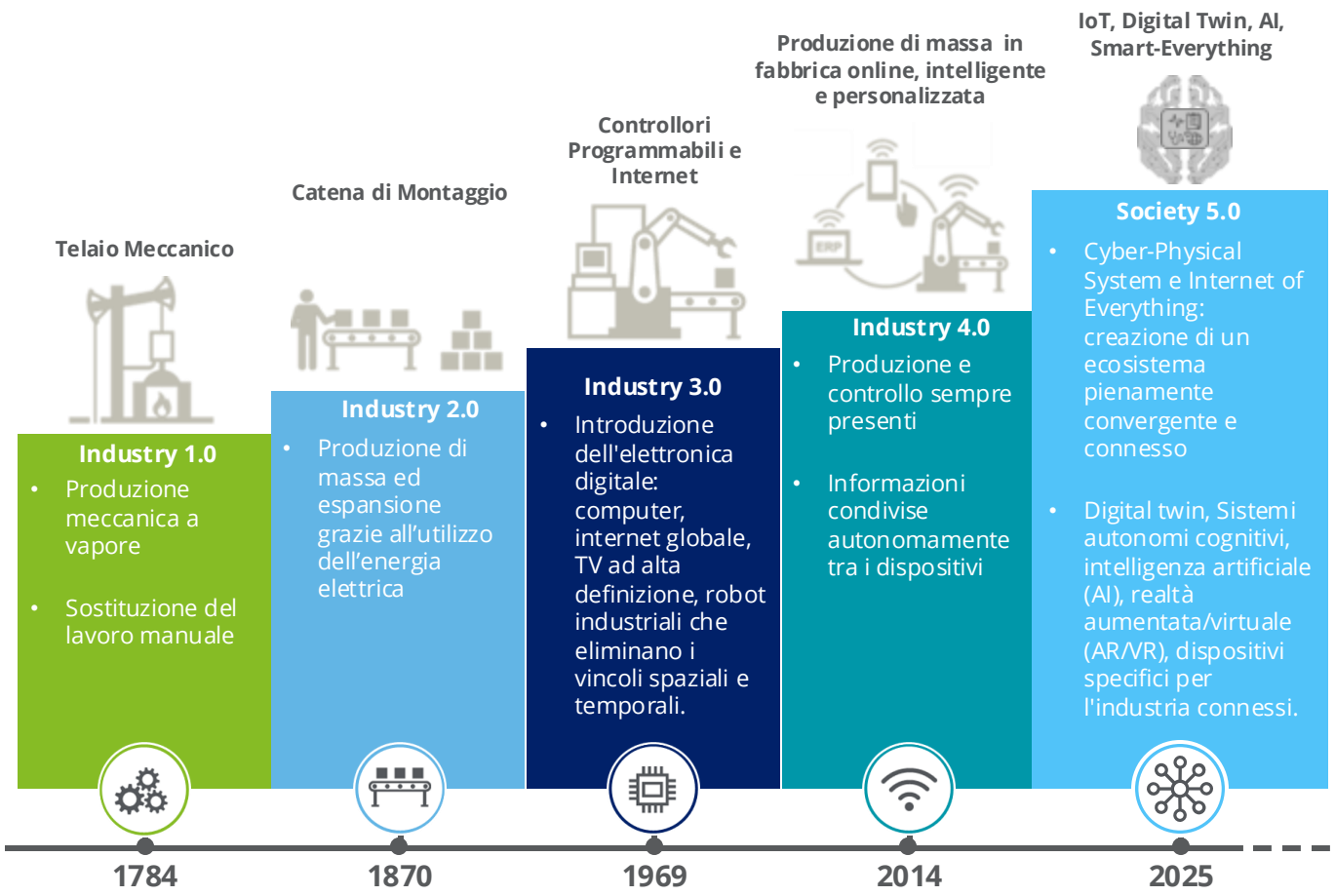
30/01/2025

Perchè ne parliamo?

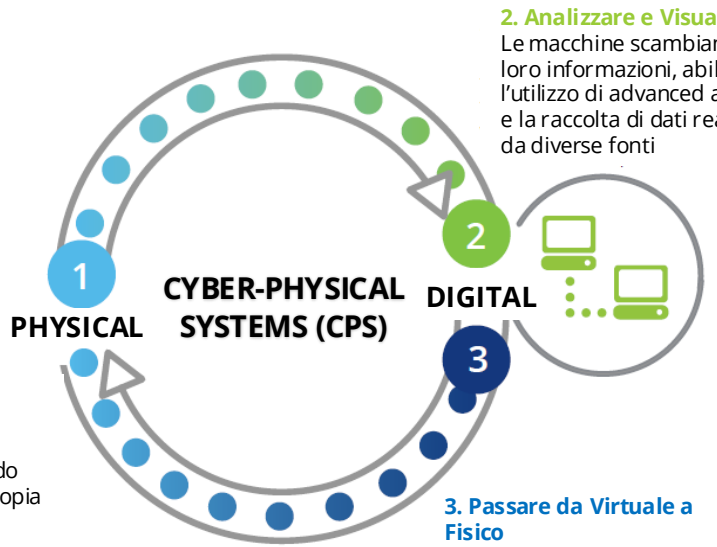


La rivoluzione Industriale, guidata da avanzamenti tecnologici in cui le macchine diventano abbastanza intelligenti da eseguire autonomamente azioni complesse, trasforma il concetto di Cyber Security

Fasi Chiave della Rivoluzione Industriale



Processo Fisico-Digitale-Fisico



1. Creare una copia digitale
Raccolta delle informazioni dal mondo fisico per creare una copia digitale

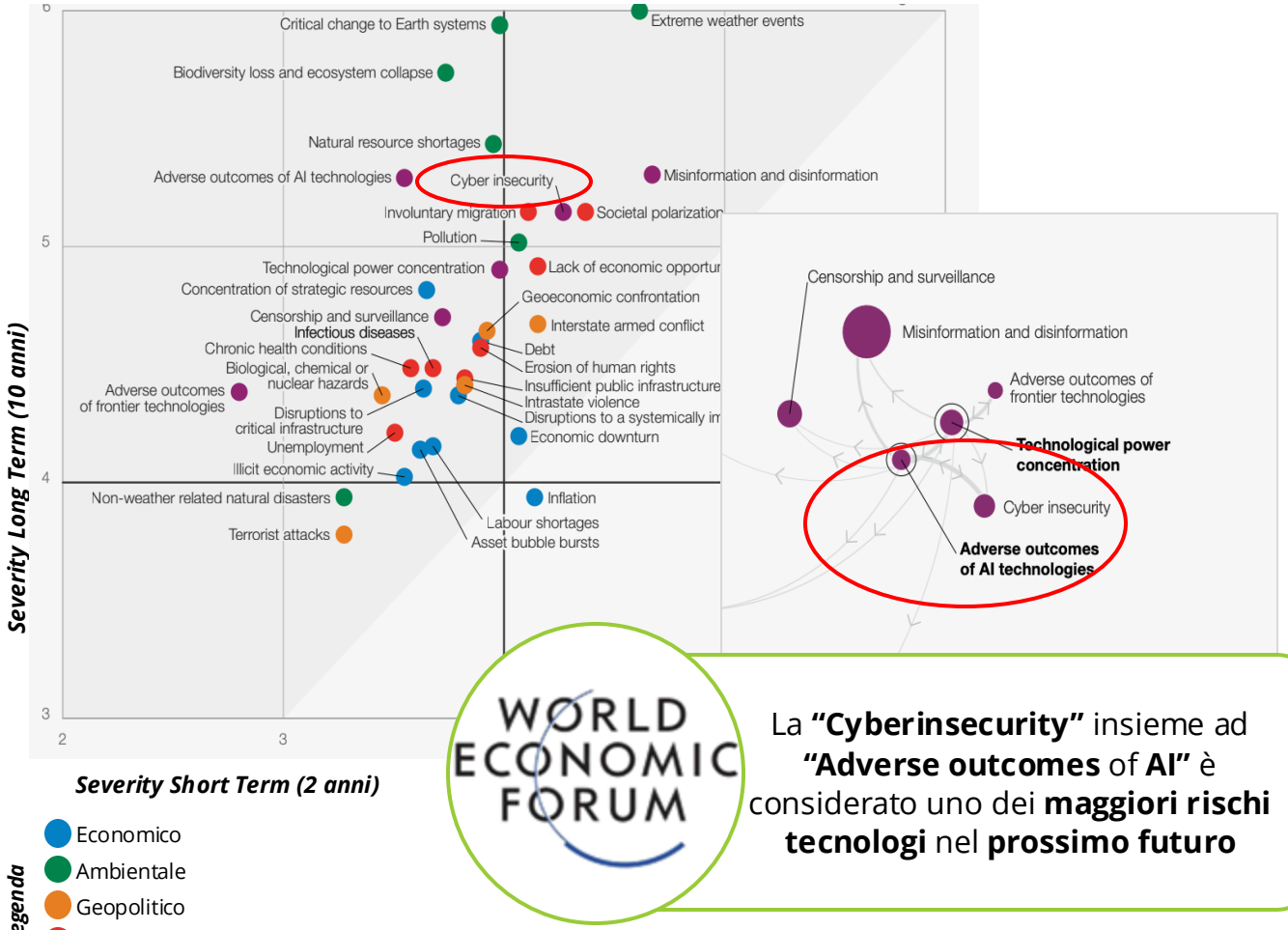
2. Analizzare e Visualizzare
Le macchine scambiano tra di loro informazioni, abilitando l'utilizzo di advanced analytics e la raccolta di dati real-time da diverse fonti

3. Passare da Virtuale a Fisico
Le decisioni dal mondo virtuale grazie all'applicazione di algoritmi vengono traslate nel mondo fisico generando azioni con impatti reali

I sistemi Cyber Fisici non sono limitati al settore industriale, ma **risolvono problemi sociali** attraverso **l'integrazione** degli **spazi fisici** e **virtuali. La Società 5.0** è una società in cui le **Tecnologie Emergenti** sono **utilizzate attivamente** nella **vita** quotidiana**, nell'industria,** nella **sanità** e in **tutte** le **sfere pubbliche**

A livello mondiale la «cyberinsecurity» è considerata uno dei maggiori rischi tecnologici futuri, continuano ad aumentare gli attacchi informatici verso tutti i settori industriali e il costo del cyber crime aumenta

Severity Relativa del Rischio in un periodo 2-10 anni



WORLD ECONOMIC FORUM

La **"Cyberinsecurity"** insieme ad **"Adverse outcomes** of **AI"** è considerato uno dei **maggiori rischi tecnologi** nel **prossimo futuro**

Attacchi Cyber: Alcuni Numeri

+ 23% di **attacchi cyber**

*(primi **6 mesi** del **2024**)*

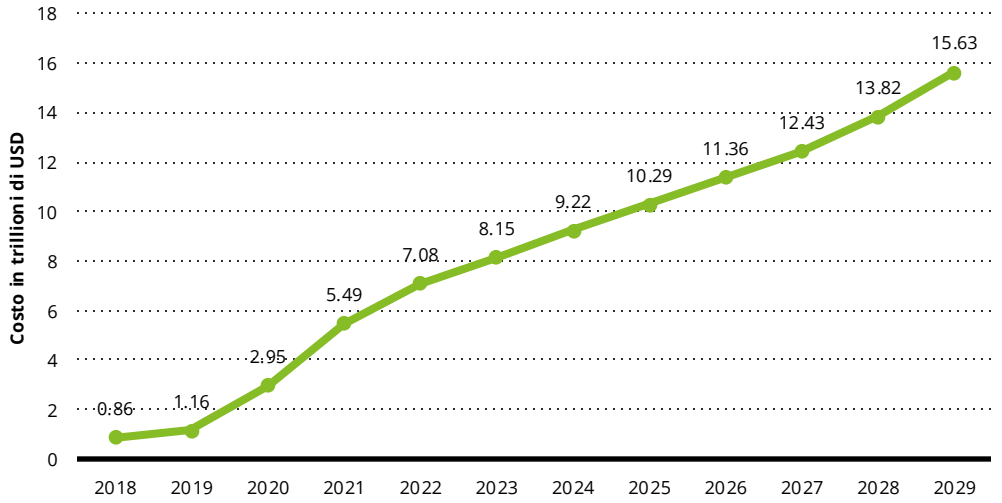
Nel Mondo, il settore **sanitario** il più **colpito (+ 83%)**

$2.4M

Costo medio di un attacco ransomware

In Italia, +**50**% di attacchi **ransomware** su sistemi OT/IoT

Costo del Cyber Crime (2018-2029)



Per disciplinare questa complessità, diverse autorità hanno elaborato regolamenti e standard la cui conformità permette di accrescere la resilienza Cyber e di garantire conformità ai requisiti di sicurezza

NON ESAUSTIVO

Legenda

Regolamenti | Standard

ISA/IEC 62443 - 2009

Set di **standard** che definisce **processi** e **requisiti** di **sicurezza** in ambito **IACS**. Principio fondamentale è il concetto di **responsabilità condivisa** a garanzia della **sicurezza**, **integrità** e **affidabilità** dei **sistemi di controllo**

Direttiva NIS - 2016

Direttiva EU recante **misure** di **sicurezza** delle **reti** e dei **sistemi informativi** che **operatori di servizi essenziali** e i **fornitori di servizi digitali** devono osservare al fine di **prevenire** e **gestire** gli **incidenti** di sicurezza informatica

Cyber Security Act - 2019

Regolamento EU che mira a **rafforzare** la **resilienza** dell'**Unione** agli attacchi informatici e a **creare** un **mercato unico** della **sicurezza Cyber** in termini di prodotti, servizi e processi

PSNC - 2019 e seguenti Decreti attuativi

Istituzione del **Perimetro di Sicurezza Nazionale Cibernetico** che definisce, per i **soggetti operanti** in **determinati settori**, le **procedure** per la **notifica** degli **incidenti Cyber** e per la **valutazione** dei **fornitori** e **istituisce** l'**Agenzia per la Cyber Sicurezza Nazionale**

Direttiva NIS 2 - 2024

Estensione dell'**ambito** di **applicazione** della **Direttiva NIS** riportante le **misure tecniche**, **operative** e **organizzative** da osservare al fine di **gestire** i **rischi Cyber** e **segnalare** gli **incidenti** di **sicurezza**

NIST SP 800-82 Rev.3 - 2023

Il documento offre una **panoramica** delle **tipologie** di **sistemi OT**, individua le **minacce** e le **vulnerabilità** tipiche di tali sistemi e **suggerisce contromisure** di sicurezza per **ridurre** i **rischi** correlati

EU Machinery Act - 2023

Regolamento EU che mira a **garantire** che le **macchine prodotte** e **commercializzate** rispettino **requisiti** di **sicurezza**, anche in **ambito Cyber**

Cyber Resilience Act - 2024

Regolamento EU che definisce una **serie** di **requisiti** di **sicurezza** per il **design**, lo **sviluppo** e la **produzione** di **prodotti** con **elementi digitali** e per la **gestione** delle **vulnerabilità** ad essi connesse

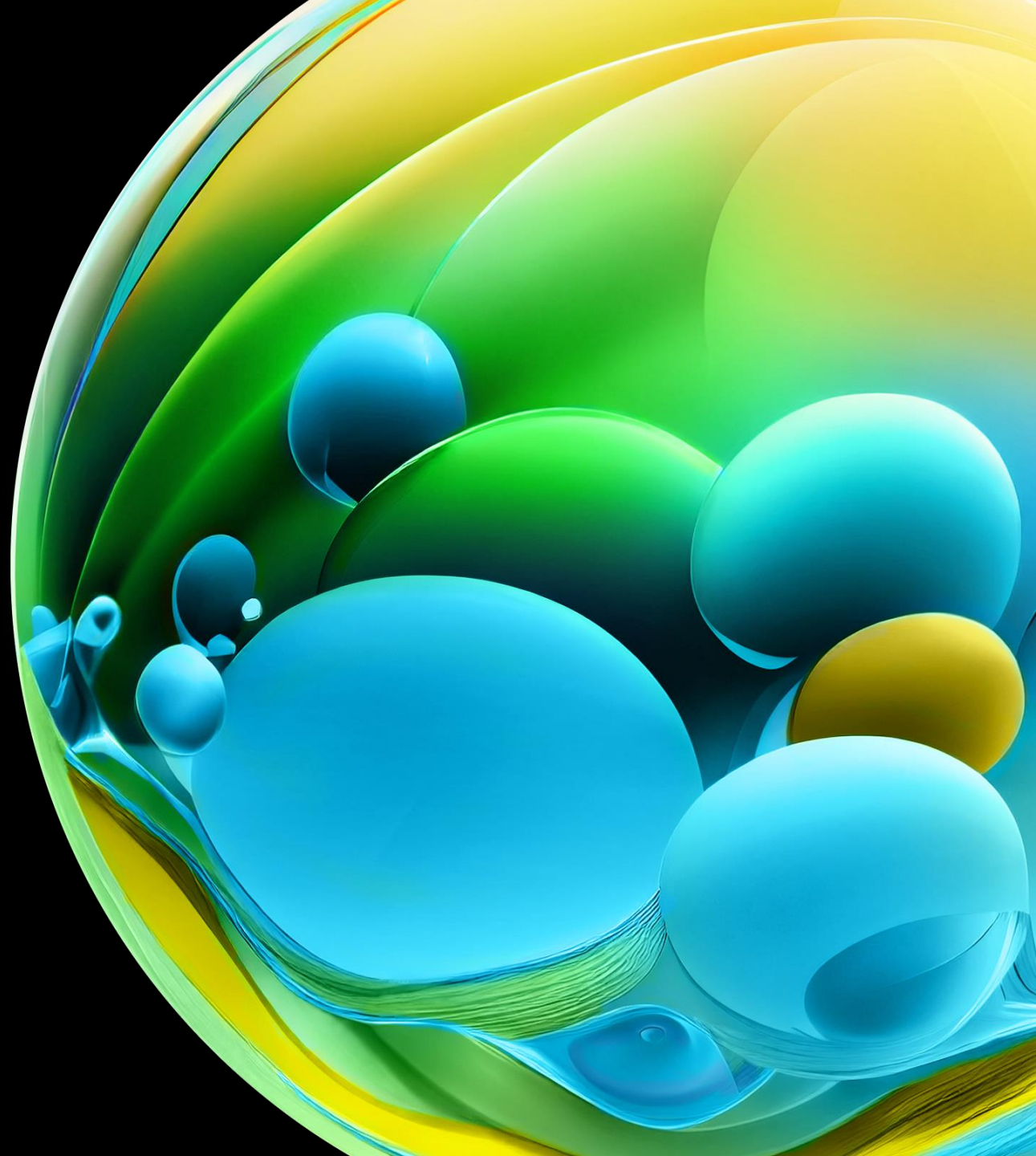
EU AI Act - 2024

Regolamento EU finalizzato a **migliorare** il **funzionamento** del **mercato interno** istituendo un **quadro giuridico uniforme** per quanto riguarda lo **sviluppo**, la **commercializzazione** e l'**uso** di **sistemi** di **intelligenza artificiale** in conformità con i valori dell'Unione

E ancora...

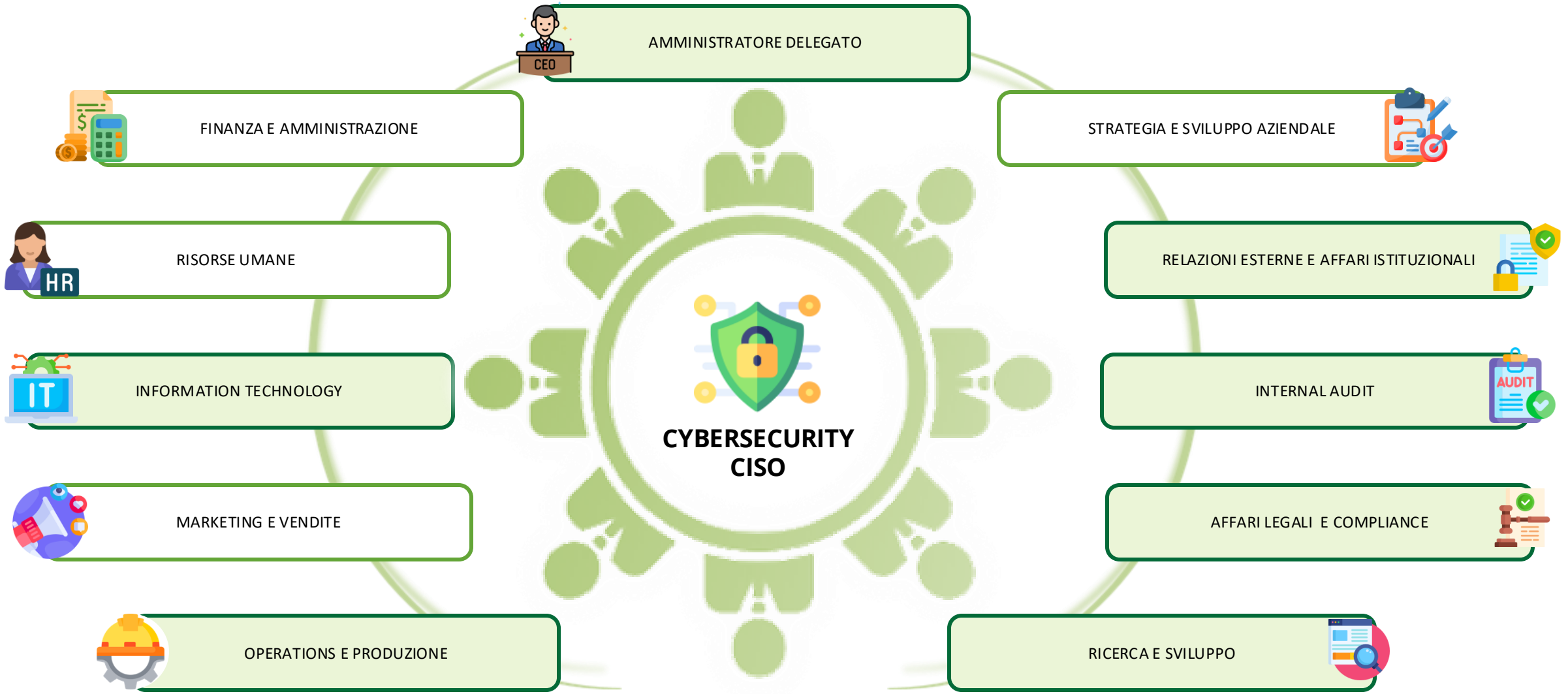
NIST *for IoT* | CEN CENELEC *EN18031* | ISO IEC | ISA *62443* | ETSI | enisa

Sfide per le Aziende



La corretta gestione della cyber security oggi non risulta più uno sforzo esclusivo del CISO ma vede coinvolti tutti gli Stakeholder aziendali, che devono dare il loro contributo, essenziale per la compliance e la sicurezza

Stakeholder Aziendali Coinvolti nella Cyber Security



Infatti, sono numerose ed eterogenee le sfide che le aziende devono affrontare per mettere in sicurezza il loro ecosistema e per poter ottenere risultati è fondamentale collaborare

Sfide Aziendali in un Ecosistema connesso OT/IoT

BUILDING A NEW CULTURE

È fondamentale o[illegible]

DON'TS

- **Dare** per **scontato** che tutti gli **Stakeholder conoscano** le nuove normative cyber
- **Sviluppare** la **strategia** evolutiva **senza** coinvolgere nuovi interlocutori (R&D, COO, CTO, ecc.)
- **Non definire** una **strategia** di **Training** & **Awareness** specifica

DOS

- **Considerare** i potenziali **impatti** di **business** derivanti da **tematiche Cyber**
- **Introdurre KPI** di alto livello
- **Definire** un **modello organizzativo OT/IoT**
- **Organizzare corsi** di **formazione** in ambito **Cyber OT/IoT**

RISK AS A KEY

Le **attività** di **Risk M[illegible]ent**

DON'TS

- **Limitare** la **discussione** sulla **gestione** dei **rischi Cyber** alle **sole funzioni tecniche**
- **Non coinvolgere** i **Risk** e **Business Owner** nella **definizione** delle **strategie** di **mitigazione** dei rischi Cyber OT/IoT

DOS

- **Definire** una **metodologia** di **Cyber Risk Assessment integrata** con il processo **ERM**
- **Definire Key Risk Indicator** specifici per i rischi **Cyber OT/IoT**
- **Definire strategie** coerenti per il **trattamento** del **rischio**

MANAGE THE UNMANAGED

Spesso l'ecosistem[illegible]T è

DON'TS

- **Sottostimare** la **complessità** dell'**ambiente industriale/connect ed products**
- **Non conoscere** quali sono gli **asset** presenti all'interno dell'ecosistema
- **Non prevedere** delle **attività** di update/ **manutenzione continua** per **OT/IoT**

DOS

- **Implementare soluzioni** che garantiscano **visibilità** sull'ecosistema integrato e avere un inventario OT/IoT completo
- **Pianificare** nel dettaglio gli **opportuni interventi**, **coinvolgendo** tutti gli **attori** rilevanti

VENDOR COLLABORATION

Gli **OEMs** e i produtto[illegible]ositivi

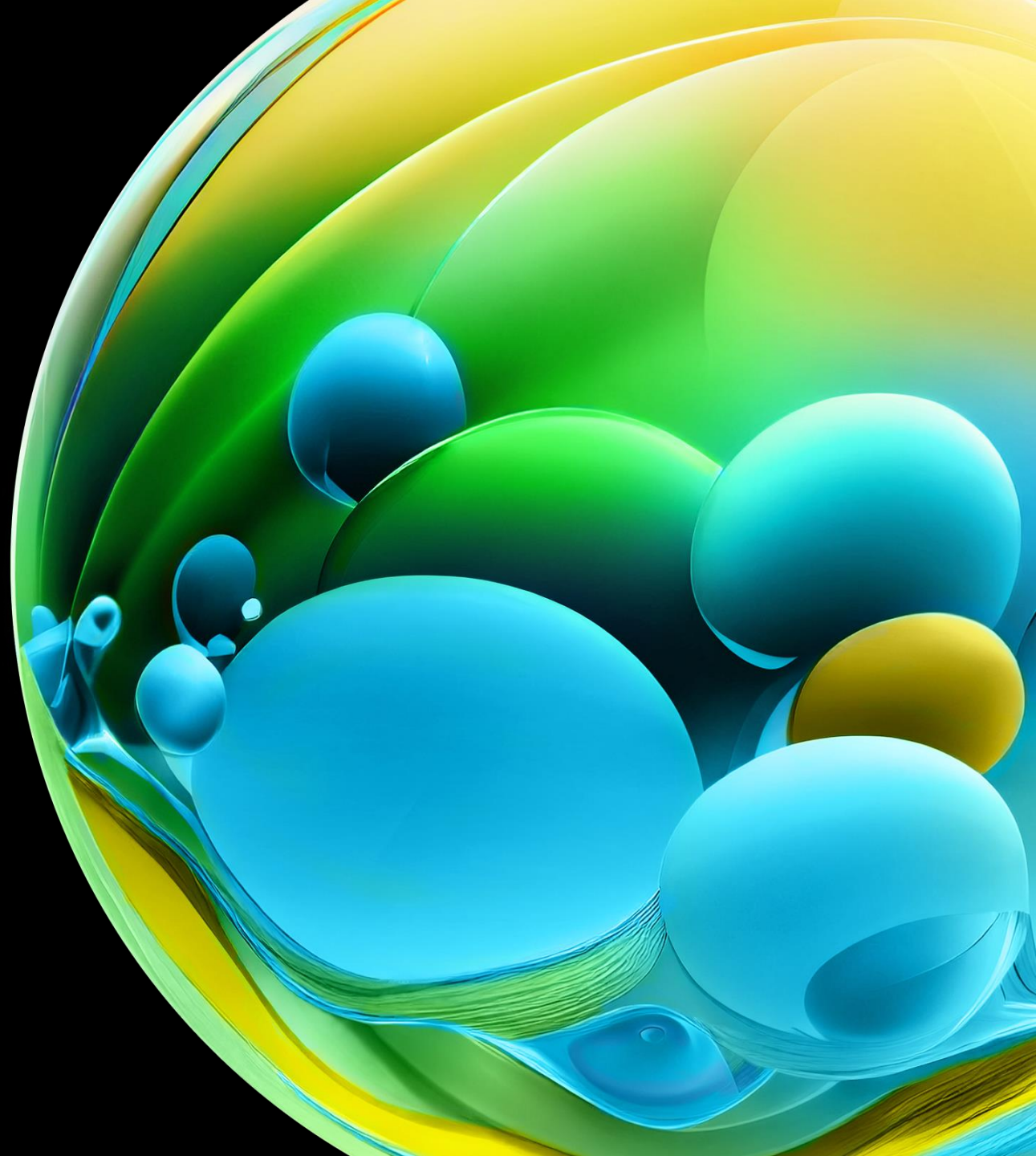
DON'TS

- **Non considerare** la dimensione **Cyber** nell'**interazione** con le **Terze Parti (OEMs** e **produttori IoT)**
- **Non intrattenere** un **rapporto continuativo** con gli **OEMs/Produttori evitando** il **coinvolgimento** degli **Stakeholder** vicini al mondo OT/IoT

DOS

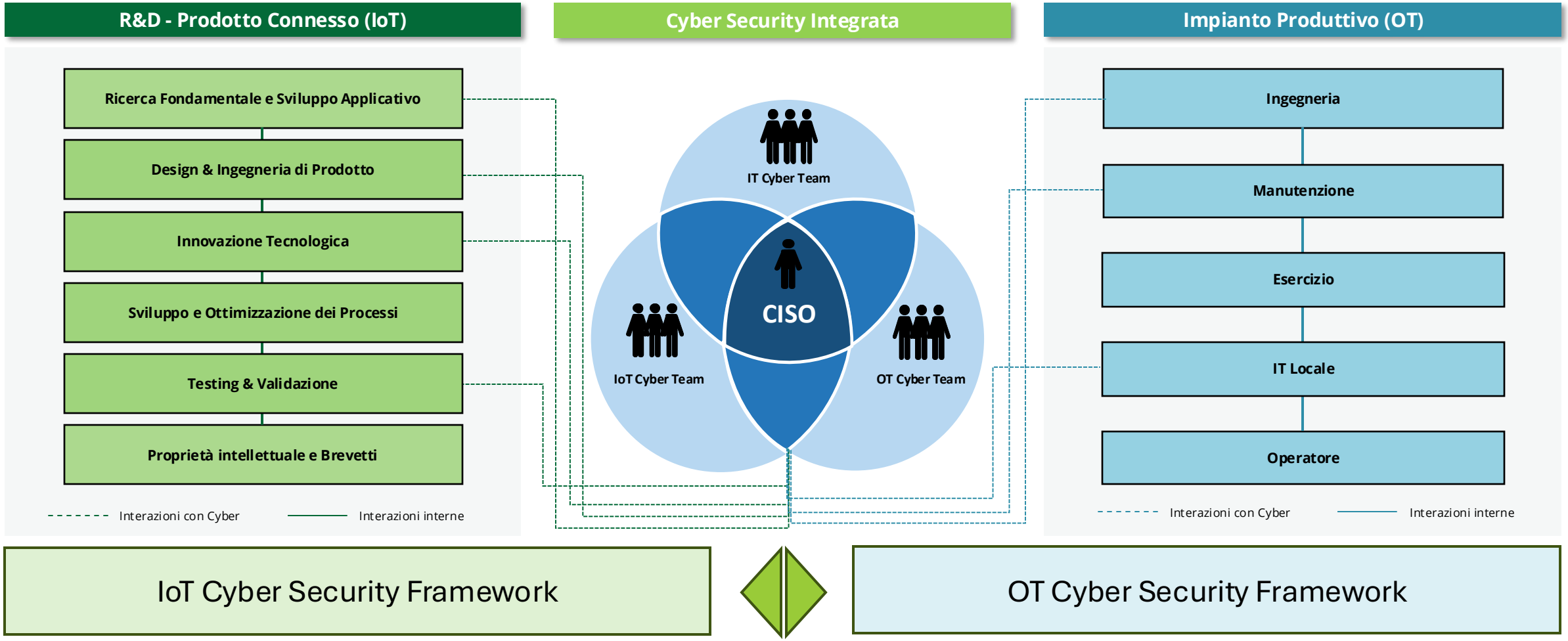
- **Inserire clausole Cyber** all'interno dei **contratti**
- **Rafforzare** la **collaborazione** con gli **OEMs/ produttori** di **dispositivi connessi** per **gestire** potenziali **eventi** di **sicurezza** e richiedere **trasparenza** sulle **attività** di **manutenzione/aggio rnamento**

Come Superare le Sfide



La prima sfida, è la realizzazione di un modello operativo cyber integrato che chiarisca l'interazione tra Stakeholder, necessaria per gestire i processi di OT/IoT Cyber Security e garantire la compliance

Modello Operativo integrato OT/IoT



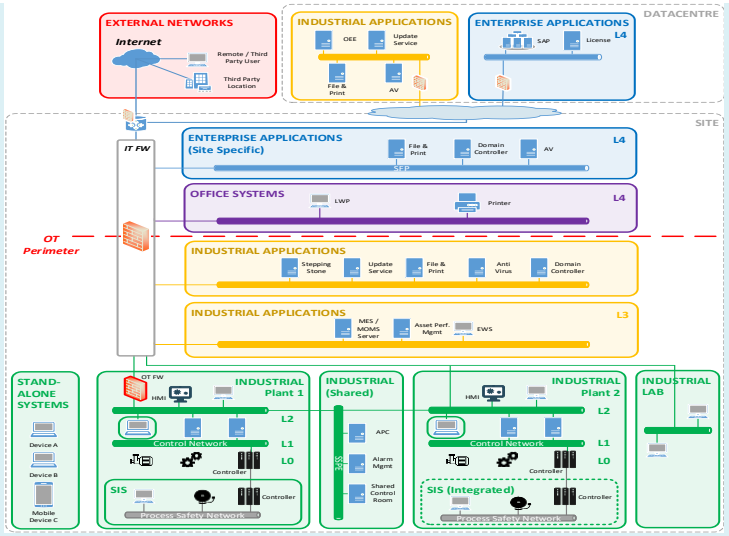
IoT Cyber Security Framework

OT Cyber Security Framework

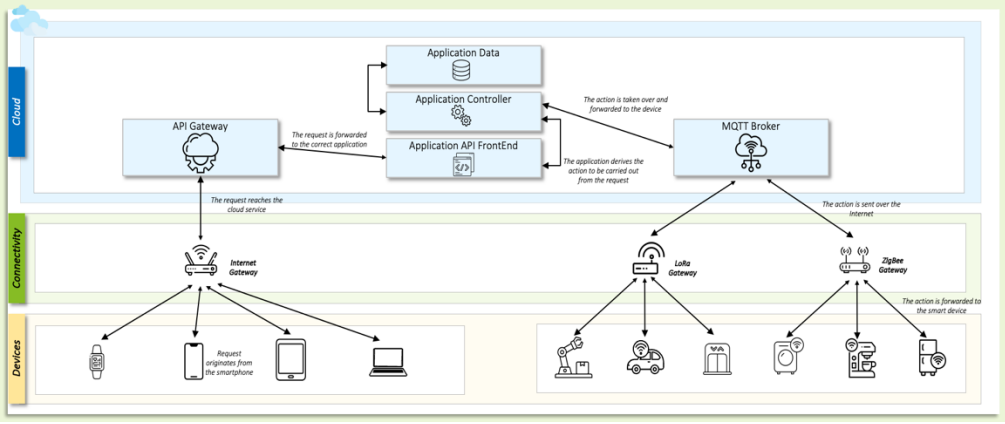
La messa in sicurezza del mondo OT/IoT richiede innanzitutto la protezione di tutto l'ecosistema integrato realizzata tramite l'implementazione di Blueprint Architetturali Cyber e specifiche misure

Messa in Sicurezza dell'Ecosistema - Blueprint Architetturale Cyber

Ecosistema OT - Esemplificativo



Ecosistema IoT - Esemplificativo



Misure di Sicurezza per OT

- **Segmentazione** della **rete**
- Sicurezza dei **sistemi obsoleti/legacy**
- **Controllo Accessi**
- **Patch** Management e **Gestione Vulnerabilità**
- **Monitoraggio** Continuo
- **Training** & **Awareness**
- **…**

Misure di Sicurezza per IoT

- **Segmentazione** Rete e **Protezione Comunicazioni** inclusi ambienti **Cloud**
- **Autenticazione** Forte e **Gestione Password**
- **Compliance** e **Certificazioni**
- **Monitoraggio** Continuo
- …

In aggiunta, per i prodotti connessi IoT è necessario definire requisiti di sicurezza applicabili sin dalla fase di design e durante tutto il loro ciclo di vita incluse le fasi di manutenzione e dismissione

Requisiti di Sicurezza dei Prodotti Connessi

Ciclo di Vita del Prodotto

Planning: Analisi di mercato per identificare le esigenze del cliente, le opportunità di mercato e le tendenze del settore

Requirement Gathering: Raccolta informazioni necessarie per individuare le feature prodotto e

Analysis: Analisi delle feature di prodotto da realizzare, dei requisiti architetturali e dell'effort necessario per la realizzazione

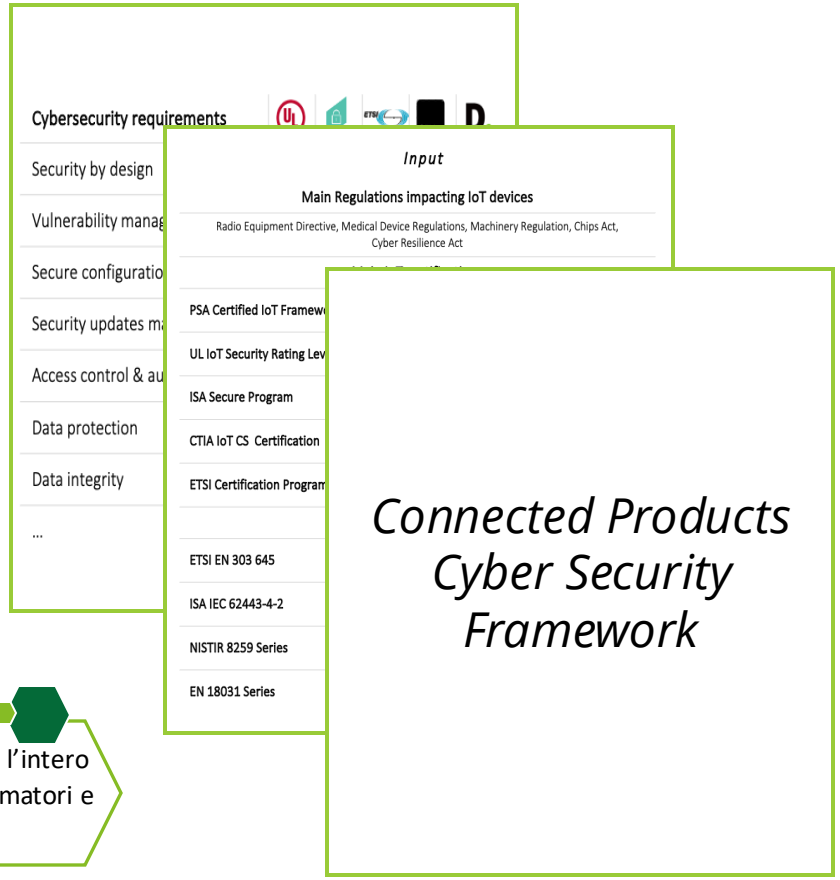
Design: creazione del concept di prodotto, e definizione dei dettagli tecnici per la sua implementazione

Development: Realizzazione di prototipi funzionali per testare le funzionalità, le prestazioni, la sicurezza e la conformità agli standard

Testing: Esecuzione di test specifici volti a verificare il funzionamento del prodotto e la sicurezza, includendo se necessario migliorie

Deployment: Avvio della produzione su larga scala, monitorando continuamente la qualità

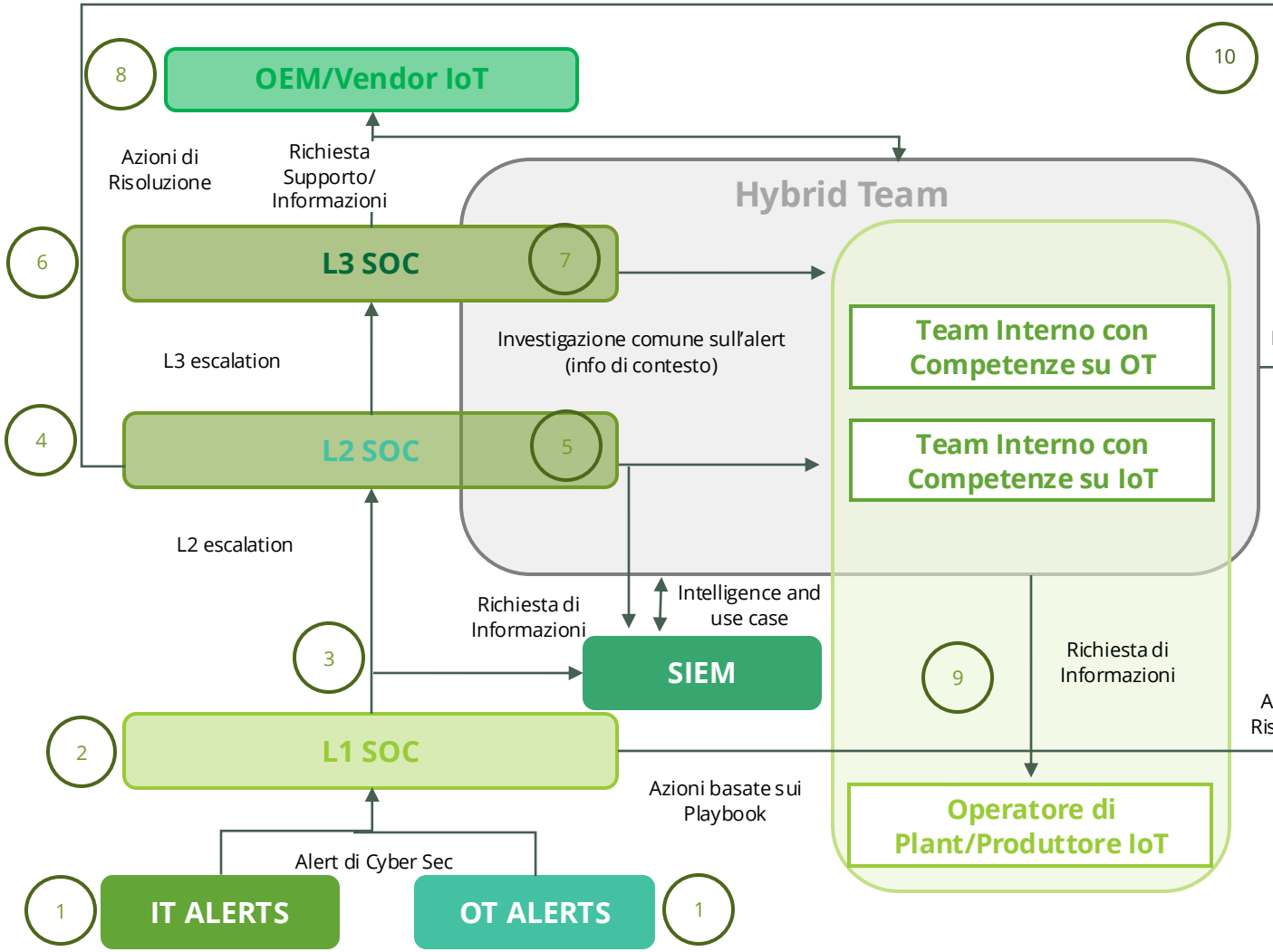
Operation and Maintenance: Supporto nell'installazione e nella configurazione, pianificazione di interventi regolari di manutenzione



Le normative oggi vigenti richiedono requisiti stringenti per garantire che i dispositivi connessi rispettino standard di sicurezza lungo l'intero ciclo di vita. L'obiettivo è quello di ridurre i rischi associati alla crescente complessità dell'IoT, proteggendo sia le aziende che i consumatori e rafforzando la resilienza dell'intero ecosistema digitale

L'ecosistema OT/IoT deve essere monitorato per prevenire e gestire efficacemente gli alert di sicurezza: la realizzazione del SOC convergente e la collaborazione di nuovi stakeholder rende possibile tutto questo

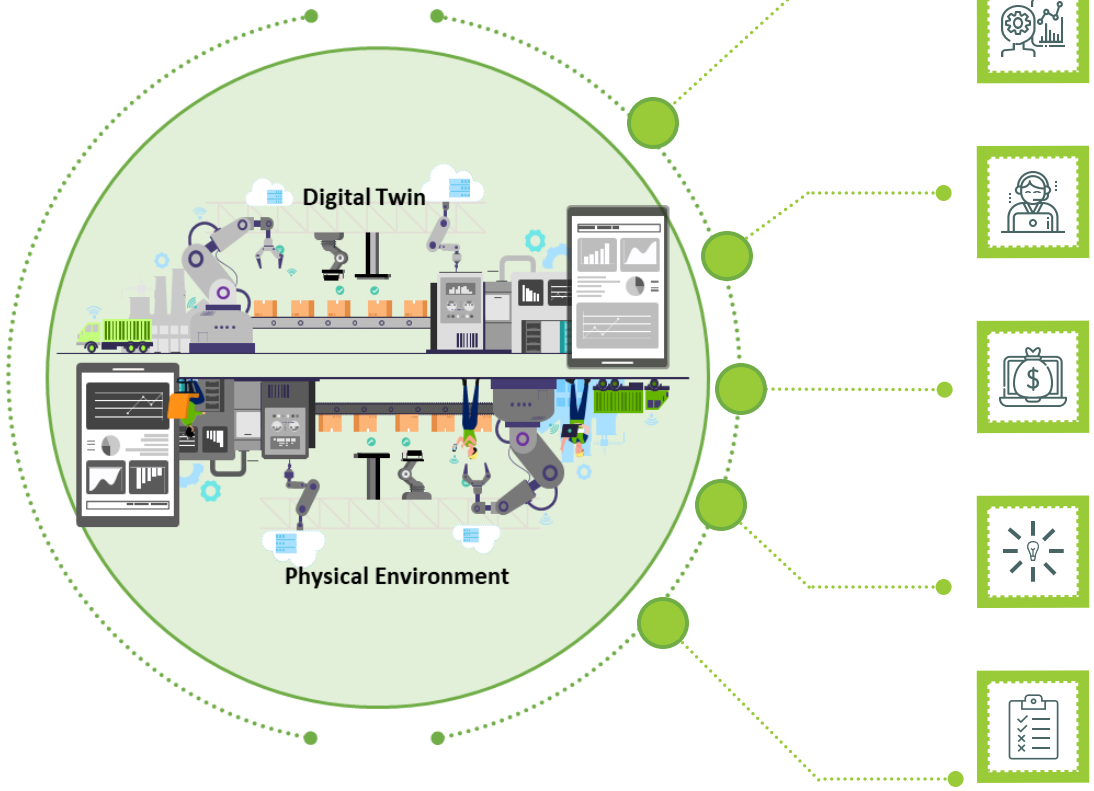
Team Coinvolti per la Risoluzione Incidenti OT/IoT in un SOC Convergente



1. Il processo inizia quando un **alert** di **security** è **generato** per l'ambiente **IT/OT/IoT**
2. Il team di L1 (**L1**) **consulta** il **playbook** e prova a svolgere la **prima risoluzione** dell'alert
3. Se necessario, **scala** al livello L2 (**L2**)
4. Il team L2 con più **esperienza**, cerca di **investigare** e **risolvere** l'alert
5. Se necessario il team L2 **svolge** delle attività specifiche in stretta **collaborazione** con I **team** del Cliente
6. Nei casi più **gravi**, è prevista la **partecipazione** dei **team L3**
7. Se necessario anche il team **L3 collabora** in maniera ibrida con i **team specializzati** del **cliente**
8. Nei casi più difficili l'incidente può **essere scalato al vendor** per trovare una risoluzione comune
9. Il team SOC insieme al cliente potrebbe chiedere **informazioni all'operatore di fabbrica** o al **produttore IoT**
10. Infine, individuata l'azione di **risoluzione** questa viene **applicate** per **risolvere l'incident**

Infine, per raggiungere una protezione avanzata, nelle realtà più mature, è utile implementare i Cyber Digital Twin che permettono di massimizzare gli effort di cyber security

Messa in Sicurezza del Cyber Physical System – Vantaggi Digital Twin



SECURE DATA
Assicurare l'**integrità** dei **dati** in entrata e in uscita, insieme alla **disponibilità** e alla **non ripudiabilità**, per **supportare** le **decisioni aziendali**

ENSURE INTEGRITY
Controllare l'**integrità** del **comportamento** del **Digital Twin** così da garantire la **visibilità** completa dell'**ambiente** e il **monitoraggio** degli **accessi**

RISK-BASED INVESTMENTS
Raccogliere informazioni in **tempo reale** sulle **vulnerabilità** per **prevedere** e **minimizzare** gli **impatti aziendali** allocando gli investimenti in modo efficace

EVENTS PREDICATBILITY
Eseguire **patching di sicurezza** avanzato e **test** di **impatto** dei **cambiamenti** per **prevedere** gli **impatti** e **prevenire** i **blocchi** della produzione

MINIMIZE DISRUPTION
Testare le **capacità** di **risposta** e **recupero** dagli **incidenti**, formando il personale in modo efficace in un ambiente protetto e realistico per evitare interruzioni

La messa in sicurezza dell'OT/IoT è un percorso graduale che inizia con la comprensione del contesto e la definizione di strategie, passa per la visibilità piena ed infine raggiunge l'apice con il monitoraggio continuo

Cyber Security OT/IoT Journey

Step 1

- **Valutare** il **livello** di **maturità** attuale **Cyber OT/IoT**, **definire** di un **modello** Operativo **Target** e **formulare** delle azioni di integrazione
- **Valutare** i **rischi Cyber OT/IoT** e garantirne la gestione mediante la **definizione** di **azioni** di **mitigazione**

Step 2

- **Definire** un **Asset Inventory dettagliato** per **garantire visibilità** sull'ecosistema OT/IoT
- **Garantire** la sicurezza dei prodotti connessi durante tutto il loro ciclo di vita e **definendo requisiti** di ***Security by Design***
- **Implementare soluzioni** tecnologiche di monitoraggio per **accrescere** la **sicurezza** dell'ecosistema OT/IoT
- **Valutare** l'**esposizione** alle **vulnerabilità** mediante l'esecuzione di attività specifiche, passive o attive su OT/IoT

Step 3

- **Monitorare real-time** gli **eventi** di **sicurezza** attraverso la realizzazione di SOC convergenti IT/OT/IoT
- Valutare l'implementazione di **Cyber Digital Twin** per la **simulare attacchi avanzati** e **testare** il **comportamento** di **misure** di **sicurezza** sull'ecosistema OT/IoT

UNDERSTAND

Comprendere** il **contesto** e **definire** una **strategia evolutiva Cyber

1

SECURE

Implementare soluzioni tecnologiche** e **misure** di **sicurezza** volte ad accrescere la **resilienza

2

FORTIFY

Monitorare** l'**ambiente** al fine di **rilevare** gli **eventi** e **garantirne** la **gestione tempestiva

3

Grazie