ITHUM
it'sforhuman

Operational Technology

Comprendere e gestire gli scenari di rischio Cyber

29 maggio 2024

Relatore: **Francesco Tozzi**, Deloitte

Con il patrocinio

Agenda

- 17.00 Presentazione
- 17.10 Speech
- 17.45 Feedback / Prossime iniziative
- 17.50 Dibattito - Q&A
- 18.15 (circa) Saluti

Relatore: Francesco Tozzi – (LinkedIn)

Moderatore: Marco CIAMPI – (LinkedIn)

Scrivere a eventi@ithum.it per:
- Attestato di partecipazione finale
- Slide
- Registrazione
- Info corso

Focus dell'Incontro

Informazioni di Contatto e Profilo

Francesco Tozzi, *Director*

ftozzi@deloitte.it

+39 3346541428

- **Global Sales** e **GTM Emerging Technology Leader**
- **Leader** dell'offering italiana in **Italian Emerging Technology**
- **10 + anni** di **esperienza** in ambito **Cyber Security**, in particolare per quanto concerne attività di **Cyber Risk Management** e definizione di programmi di **Cyber Security** per **aziende** operanti nel **settore industriale**, sia a livello nazionale che internazionale
- Responsabile della gestione di **progetti** inerenti le **infrastrutture critiche** e lo **sviluppo** di **capability** in ambito **Cyber Security** in ambito **ICS industrial control systems**

Deloitte.

Agenda

L'**obiettivo** dello speech è provare a **rispondere** ad alcune **domande** riguardanti il **mondo OT** e le relative **implicazioni** in ambito **Cyber** ad esso riferite:

1 | COMPRENSIONE DEL CONTESTO

***Cosa** significa **Operational Technology**? Quali sono le **peculiarità** del mondo OT?*

2 | RISCHI DEL MONDO OT

***Quali** sono i **principali rischi** che impattano il mondo OT?*

3 | FRAMEWORK REGOLATORIO

***Come** è **regolamentato** il mondo OT?*

4 | CISO CHALLENGE

***Quali** sono le **principali sfide** che i **CISO** devono affrontare?*

5 | MITIGAZIONE DELLE SFIDE

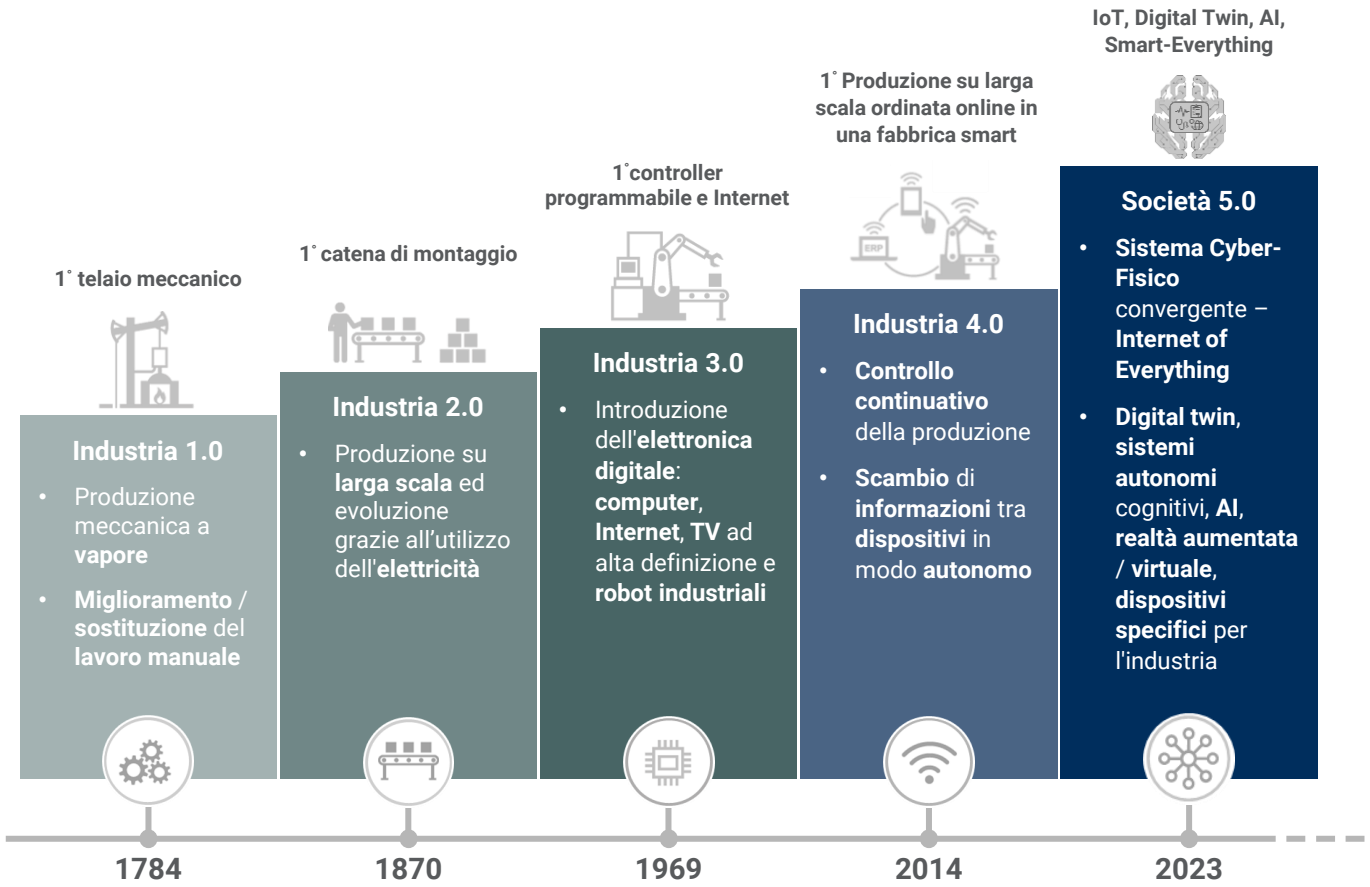
***Come** possono essere **superate** tali **sfide**?*

1 | Comprensione del Contesto

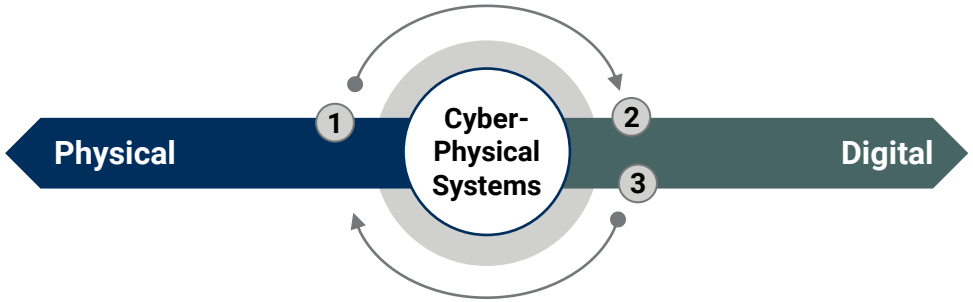
*Cosa significa **Operational Technology**? Quali sono le **peculiarità** del mondo OT?*

Fasi Chiave dell'Evoluzione Tecnologica

La **rivoluzione industriale**, guidata da **progressi tecnologici** che consentono alle macchine di **eseguire autonomamente azioni complesse**, **trasforma** il **concetto** originale di **sicurezza informatica**



Il **Sistema Cyber-Fisico** non si limita al mondo industriale, ma considera anche **problemi sociali** attraverso l'**integrazione** di **spazi fisici** e **virtuali**. La **Società 5.0** è una società in cui le **Tecnologie Emergenti** vengono **attivamente utilizzate** nella **vita quotidiana**, nell'**industria**, nell'**assistenza sanitaria** e in **tutte** le **sfere pubbliche**



1. *Definizione del Digital Record*
Acquisizione di **informazioni** dal **mondo fisico** per creare un **record digitale** dell'**operazione fisica** e della **rete** di **approvvigionamento**

2. *Analisi e Visualizzazione*
Condivisione di **informazioni** tra le **macchine**, permettendo di svolgere **analisi avanzate** e visualizzare **dati in real-time** da fonti multiple

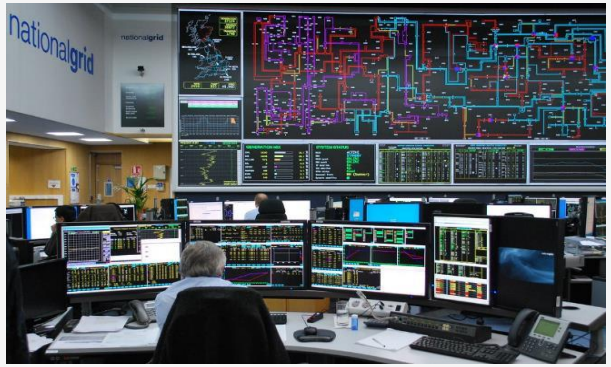
3. *Generazione del Movimento*
Utilizzo di **algoritmi** e **automazione** al fine di **tradurre decisioni** e **azioni** dal **mondo digitale** al mondo **fisico**

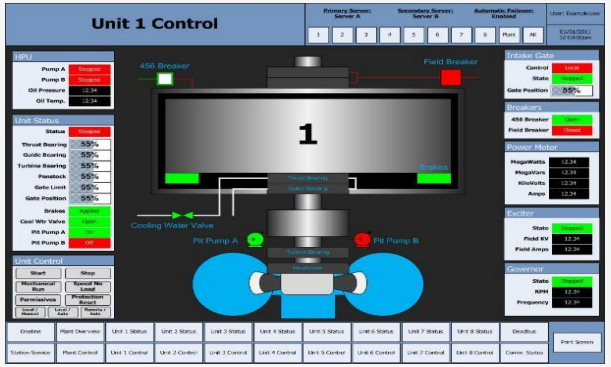
1 | Comprensione del Contesto

*Cosa significa **Operational Technology**? Quali sono le **peculiarità** del mondo OT?*

Definizione & Termini

Per **comprendere** e **gestire** la **complessità** che caratterizza il **mondo OT**, è innanzitutto necessario **definire** un **vocabolario comune**, evitando così confusione legata all'utilizzo di differenti terminologie





Definizione

L'espressione Operational Technology si riferisce ad una **combinazione** di **componenti** di **controllo** (e.g., elettrici, meccanici, idraulici, pneumatici e digitali) che **interagiscono** con il **mondo fisico** attraverso la **rilevazione** o la **generazione** di **modifiche**, grazie al **monitoraggio** ed al controllo dei dispositivi fisici, dei processi e degli eventi. Ci si riferisce altresì a diversi **sistemi di controllo** inclusi **SCADA**, **DCS** e **PCS**, spesso presenti nel settore industriale

OT	Operational Technology	**PCS**	Process Control System
ICS	Industrial Control Systems	**SCADA**	Supervisory Control & Data Acquisition
IACS	Industrial Automation and Control Systems	**DCS**	Distributed Control System
IA	Industrial Automation	**IIoT**	Industrial Internet of Things

1 | Comprensione del Contesto

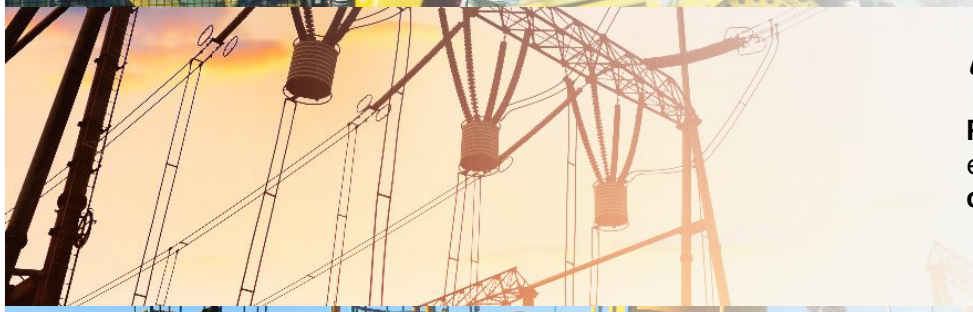
*Cosa significa **Operational Technology**? Quali sono le **peculiarità** del mondo OT?*

Tipologie di Network Industriali

Esistono infatti **diverse tipologie** di **reti industriali**, ognuna delle quali presenta **caratteristiche differenti**, **diversi sistemi di controllo industriali** e, conseguentemente, **diverse necessità**, anche in ottica di **sicurezza Cyber**

Discrete Manufacturing

Reti industriali utilizzate negli **impianti** di **produzione** che producono **oggetti discreti** di varia natura, ad esempio le automobili. Le **linee** di **assemblaggio** sono **gestite** tipicamente da **singoli PLC** o, nelle fabbriche più avanzate, da **robot SCARA connessi**



Utilities

Reti industriali funzionali alla **distribuzione** su vasta scala di **servizi essenziali**, come acqua, acque reflue, energia elettrica e gas naturale, sia per i cittadini che per l'industria. Di solito, le **utility grid** sono **monitorate** e **controllate** da sistemi di **Supervisory Control And Data Acquisition** (**SCADA**)

Chemical Processing

Reti industriali finalizzate al **controllo** di **macchinari** presenti in **impianti chimici**, **raffinerie** e altre **industrie** che coinvolgono la **lavorazione** di **beni** come **alimenti** e **bevande**, **farmaci**, etc. Tali reti sono differenziate a seconda che si tratti **di produzione continua** (grandi quantità, produzione permanente) oppure al **trattamento per lotti** (piccole quantità, oggetti creati in diverse postazioni di lavoro). Gli impianti di lavorazione chimica sono generalmente **monitorati** e **controllati** da **Distributed Control Systems** (**DCS**)

1 | Comprensione del Contesto

*Cosa significa **Operational Technology**? Quali sono le **peculiarità** del mondo OT?*

Caratteristiche del Mondo OT

In generale, il **mondo industriale** presenta delle **caratteristiche specifiche** che lo **differenziano** dall'**ambito IT/Corporate** e che rendono necessarie delle considerazioni diverse nella modalità di **gestione** della **Cyber Security**

Ecosistema di Stakeholder

L'**ecosistema** di **Stakeholder chiave** per la gestione del mondo industriale comprende l'**Ingegneria**, la **Manutenzione**, **l'Esercizio**, l'**IT Locale**

Asset OT

Gli **strumenti digitali** a **supporto** del **processo** sono **differenti** da quelli del **mondo IT** e presentano un **diverso ciclo di vita** dell'asset, che può durare **decenni**

Delocalizzazione Geografica

Il **processo industriale** si sviluppa su una **porzione** di **territorio** più o meno **estesa**, quindi anche gli strumenti digitali **non** si trovano sempre e **solo** in **un Data Center**

Competenze Specifiche

Si richiedono conoscenze **specifiche** dei processi industriali, di **Industrial Automation** e di architetture industriali per **gestire** gli **incidenti** e per le **attività** di **Recovery**

Health & Safety

I **temi** di **Health and Safety** sono **fondamentali** e **prevalgono** su qualsiasi altra attività nel mondo industriale

2 | Rischi del Mondo OT

*Quali sono i **principali rischi** che impattano il mondo OT?*

Falsi miti e Punti Critici

Le **reti industriali** (OT), **storicamente isolate** dal mondo esterno, sono diventate **sempre più vulnerabili** agli **attacchi di sicurezza** così **sfatando** alcuni **falsi miti** e mettendo in **luce** alcuni **punti critici**

FALSO MITO #1

"I sistemi di controllo industriale non connessi ad Internet"

RED ALARM

Circa il **90%** dei **sistemi di controllo industriale** sono **collegati** alla **rete aziendale (IT)**, che presenta numerosi **collegamenti internet**. Spesso il **supporto remoto** viene fornito tramite **connessioni internet non affidabili**

FALSO MITO #2

"I sistemi di controllo industriale sono protetti da un firewall"

RED ALARM

L'**implementazione** di un **firewall non** è **sufficiente**, poiché spesso sono **configurati** in **modo errato**, consentendo a qualsiasi traffico di rete di entrare e uscire. Inoltre, i firewall **non** sono **sufficienti** per affrontare le **minacce più recenti**

FALSO MITO #3

"Gli hacker non conoscono i sistemi di controllo industriale "

RED ALARM

L'hacking non è più solo un passatempo, i **criminali informatici** mossi da **interessi economici** guardano alle industrie non preparate come bersagli facili. Inoltre, le **informazioni** sul funzionamento di sistemi ICS e su protocolli **industriali** sono **gratuite** e **disponibili** sul web

FALSO MITO #4

"La nostra azienda non è un target"

RED ALARM

Nessun settore industriale è **immune** agli **attacchi informatici**. La presenza di sistemi informatici rende le aziende vulnerabili e, soprattutto, strumenti di **Cyber Warfare disponibili** su **Internet** potrebbero facilmente **colpire sistemi connessi** in modo **non mirato**

FALSO MITO #5

"I nostri sistemi di sicurezza ci proteggeranno"

RED ALARM

I **moderni sistemi** di **sicurezza (SIS)** si basano su **microprocessori** e sono configurati tramite **sistemi programmabili** gestiti da **PC** con **sistema operativo Windows**. Ciò significa che potrebbero essere **vulnerabili** agli **attacchi informatici**, come ad esempio il **malware Triton**

Punti Critici Cyber Security

- *__Disponibilità__ ed __integrità__ sono __priorità__ nei sistemi di controllo industriale*
- *Il __malfunzionamento__ dei __sistemi__ di __controllo industriale__ potrebbe __danneggiare__ le __persone__ e l'__ambiente__*
- *I __sistemi produttivi__ spesso __non__ possono essere __spenti__ per installare __patch__ e __aggiornamenti di sicurezza__*
- *Gli __Stakeholder__ che gestiscono i processi OT __non hanno sempre__ un __background informatico__ e __non__ sono sempre __consapevoli__ dei __rischi Cyber__*
- *L'attuale __base industriale globale__ (es. asset connessi) potrebbe essere __troppo grande/complessa__ da gestire*

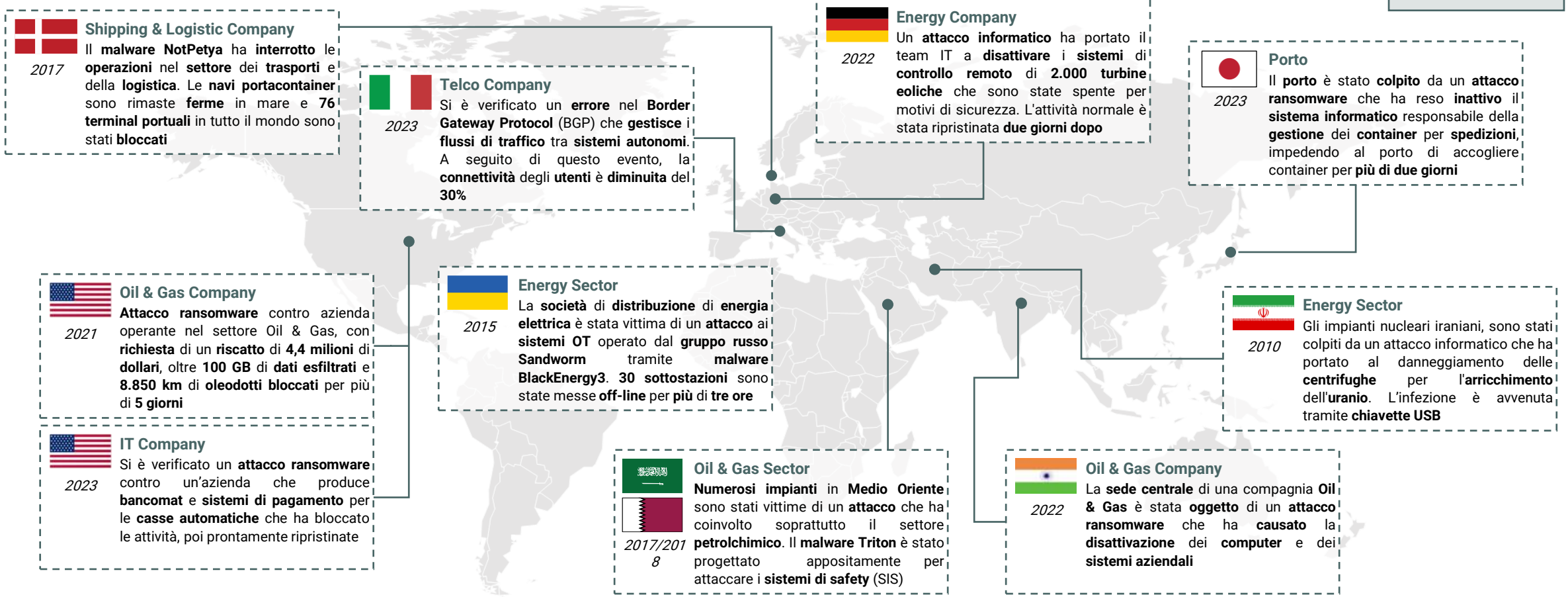
2 | Rischi del Mondo OT

*Quali sono i **principali rischi** che impattano il mondo OT?*

Esempi di Incidenti Cyber

Negli ultimi anni le **organizzazioni** operanti in **ogni settore** sono state prese di **mira** da **attacchi informatici** che possono causare **gravi conseguenze finanziarie**, **operative**, **legali**, **reputazionali**, di **sicurezza** e **ambientali**

NON ESAUSTIVO



Shipping & Logistic Company

2017

Il **malware NotPetya** ha **interrotto** le **operazioni** nel **settore** dei **trasporti** e della **logistica**. Le **navi portacontainer** sono rimaste **ferme** in mare e **76 terminal portuali** in tutto il mondo sono stati **bloccati**

Telco Company

2023

Si è verificato un **errore** nel **Border Gateway Protocol** (BGP) che **gestisce** i **flussi di traffico** tra **sistemi autonomi**. A seguito di questo evento, la **connettività** degli **utenti** è **diminuita** del **30%**

Energy Company

2022

Un **attacco informatico** ha portato il team IT a **disattivare** i **sistemi** di **controllo remoto** di **2.000 turbine eoliche** che sono state spente per motivi di sicurezza. L'attività normale è stata ripristinata **due giorni dopo**

Porto

2023

Il **porto** è stato **colpito** da un **attacco ransomware** che ha reso **inattivo** il **sistema informatico** responsabile della **gestione** dei **container** per **spedizioni**, impedendo al porto di accogliere container per **più di due giorni**

Oil & Gas Company

2021

Attacco ransomware contro azienda operante nel settore Oil & Gas, con **richiesta** di un **riscatto** di **4,4 milioni** di **dollari**, oltre **100 GB** di **dati esfiltrati** e **8.850 km** di **oleodotti bloccati** per più di **5 giorni**

IT Company

2023

Si è verificato un **attacco ransomware** contro un'azienda che produce **bancomat** e **sistemi di pagamento** per le **casse automatiche** che ha bloccato le attività, poi prontamente ripristinate

Energy Sector

2015

La **società** di **distribuzione** di **energia elettrica** è stata vittima di un **attacco** ai **sistemi OT** operato dal **gruppo russo Sandworm** tramite **malware BlackEnergy3**. **30 sottostazioni** sono state messe **off-line** per **più** di **tre ore**

Energy Sector

2010

Gli impianti nucleari iraniani, sono stati colpiti da un attacco informatico che ha portato al danneggiamento delle **centrifughe** per l'**arricchimento** dell'**uranio**. L'infezione è avvenuta tramite **chiavette USB**

Oil & Gas Sector

2017/2018

Numerosi impianti in **Medio Oriente** sono stati vittime di un **attacco** che ha coinvolto soprattutto il settore **petrolchimico**. Il **malware Triton** è stato progettato appositamente per attaccare i **sistemi di safety** (SIS)

Oil & Gas Company

2022

La **sede centrale** di una compagnia **Oil & Gas** è stata **oggetto** di un **attacco ransomware** che ha **causato** la **disattivazione** dei **computer** e dei **sistemi aziendali**

2 | Rischi del Mondo OT

*Quali sono i **principali rischi** che impattano il mondo OT?*

Cyber Kill Chain

Con l'obiettivo di **comprendere meglio** gli **incidenti** in **ambito OT** e la loro **evoluzione**, nel 2015 il **SANS Institute**, dal cui rapporto trae ispirazione la rappresentazione seguente, ha adattato la **Cyber Kill Chain** della Lockheed Martin al **mondo industriale**

I - Cyber Intrusion Preparation and Execution			
Lockheed Martin's Cyber Kill Chain	**ICS Cyber Kill Chain**		**Fasi**
RECONNAISANCE	*PLANNING*		*L'attaccante raccoglie informazioni sull'obiettivo (ad esempio tramite OSINT)*
WEAPONIZATON	*PREPARATION*		*L'attaccante modifica un file o assegna priorità agli attacchi futuri*
DELIVERY	*CYBER INTRUSION*	ATTEMPT	*L'attaccante interagisce con la rete da attaccare*
EXPLOIT			*L'attaccante utilizza diversi mezzi per eseguire azioni dannose*
INSTALL/MODIFY		SUCCESS	*L'attaccante installa una nuova funzionalità o ne modifica una esistente*
COMAND & CONTROL(C2)	*MANAGEMENT & ENABLEMENTX*		*L'attaccante gestisce l'accesso ottenuto dopo l'intrusione*
ACT	*SUSTAINMENT, ENTRENCHMENT, DEVELOPMENT & ESECUTION*		*L'attaccante esegue funzionalità aggiuntive, trova nuove apparecchiature, passa da una rete all'altra, ecc...*
II – ICS Attack Development and Execution			
	ICS ATTACK DEVELOPMENT & TUNING		*Viene sviluppata una funzionalità su misura per influenzare i sistemi Industriali*
	VALIDATION		*L'attaccante ha la prova che le sue azioni creano disruption*
	ICS ATTACK		*L'attaccante agisce sul sistema Industrial Target*
			La funzionalità malevola è avviata e/o avvengono le modifiche
			Viene sferrato l'attacco per intaccare la disponilità e l'integrità del sistema

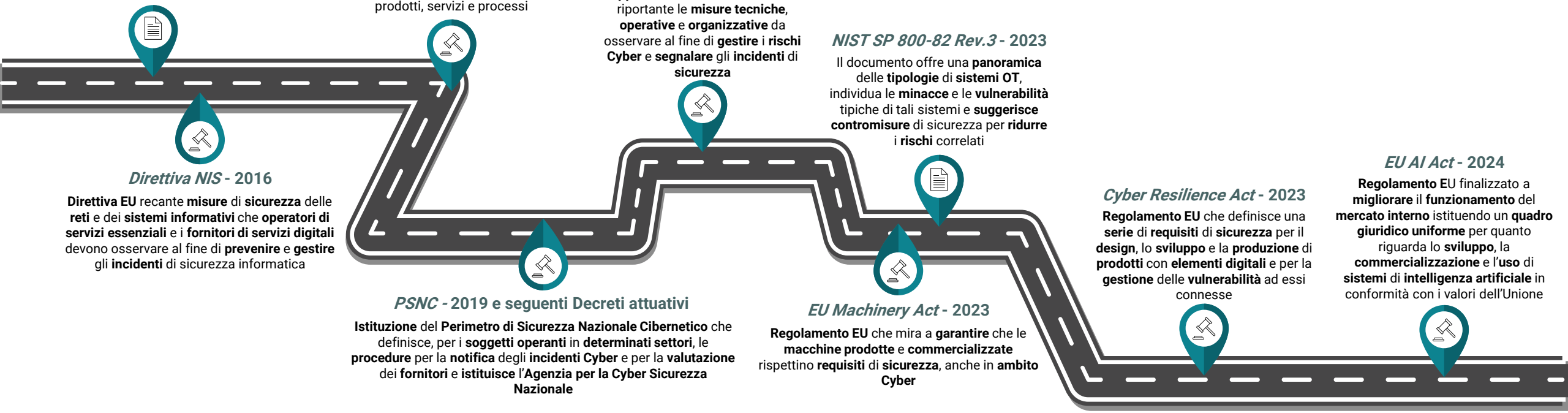
3 | Framework Regolatorio

*Come è **regolamentato** il mondo OT?*

Principali Regolamenti e Standard

Al fine di **disciplinare** la **complessità** che caratterizza il **mondo OT**, diverse **autorità** hanno elaborato **regolamenti** e **standard** la cui **conformità** o **osservanza** permette di **accrescere** la **resilienza Cyber** degli ambienti e di **garantire conformità** ai **requisiti di sicurezza**

NON ESAUSTIVO



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 - 2022

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 - 2023

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

4 | CISO Challenge

***Quali** sono le **principali sfide** che i **CISO** devono affrontare?*

Sfide per i CISO

In considerazione del **contesto** in **continuo mutamento** e dei **rischi** che caratterizzano il **mondo OT**, sono diverse le **sfide** che i **Cyber Information Security Officer** devono **affrontare** e **gestire**

BUILDING A NEW CULTURE

È fondamentale ott

DON'TS

- **Dare** per **scontato** che gli **Stakeholder** di **impianto conoscano** la **funzione Cyber**
- **Sviluppare** la **strategia** evolutiva **senza** coinvolgere **Stakeholder** OT
- **Non definire** una **strategia** di **Training** & **Awareness**

DOS

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

RISK AS A KEY

Le **attività** di **Risk Mana** sono

DON'TS

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

DOS

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

MANAGE THE UNMANAGED

Spesso le **reti industria** estite

DON'TS

- **Sottostimare** la **complessità** dell'**ambiente industriale**
- **Non conoscere** quali sono gli **asset** presenti all'interno della **rete**
- **Non prevedere** delle **attività** di **manutenzione** e **aggiornamento**

DOS

- **Implementare soluzioni** che garantiscano **visibilità** sull'**ambiente**
- **Definire** e **mantenere** un **Asset Inventory**
- **Pianificare** nel dettaglio gli **opportuni interventi**, **coinvolgendo** tutti gli **attori** rilevanti

VENDOR COLLABORATION

Gli **OEMs gestiscon** gli

DON'TS

- **Non considerare** la dimensione **Cyber** nell'**interazione** con le **Terze Parti**
- **Non intrattenere** un **rapporto continuativo** con gli **OEMs**, **evitando** il **coinvolgimento** degli **Stakeholder** vicini ai processi industriali

DOS

- **Inserire clausole Cyber** all'interno dei **contratti**
- **Rafforzare** la **collaborazione** con gli **OEMs** per **gestire** potenziali **eventi** di **sicurezza**
- **Richiedere** agli **OEMs trasparenza** rispetto alle **attività** di **manutenzione** svolte

5 | Mitigazione delle Sfide

*Come possono essere **superate** tali **sfide**?*

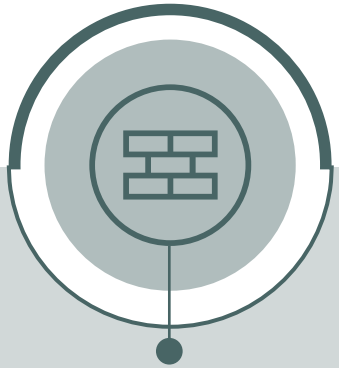
Attività di Mitigazione

Tali **sfide** possono essere gestite mediante l'**esecuzione** di **attività** che, dal punto di vista **organizzativo** e **tecnologico**, sono funzionali ad **ottenere visibilità** sul **contesto organizzativo**, **accrescere** il **livello** di **sicurezza** dell'**ambiente** e garantire il **monitoraggio**

UNDERSTAND

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

- **Valutare** il **livello** di **maturità** attuale **Cyber OT**, **definire** di un **modello Target** e **formulare** delle **azioni** di **rimedio**
- **Definire** un **modello operativo** che consideri anche la dimensione **Cyber OT**
- **Valutare** i **rischi Cyber OT** e garantirne la gestione mediante la **definizione** di **azioni** di **mitigazione**



SECURE

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

- **Definire** un **Asset Inventory dettagliato** che permetta di **garantire visibilità**
- **Allineare** l'**architettura** al **modello Purdue** e **definire requisiti** di ***Security by Design***
- **Implementare soluzioni** tecnologiche volte ad **accrescere** il **livello** di **sicurezza** dell'ecosistema, ad esempio soluzioni per l'**accesso remoto sicuro**
- **Valutare** l'**esposizione** alle **vulnerabilità** mediante l'esecuzione di attività specifiche, passive o attive

FORTIFY

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

- **Garantire** il **monitoraggio** in **real-time** degli **eventi** di **sicurezza**
- **Gestire** gli **eventi** di **sicurezza** rilevati in modo **tempestivo** al fine di **assicurare** la **continuità operativa**

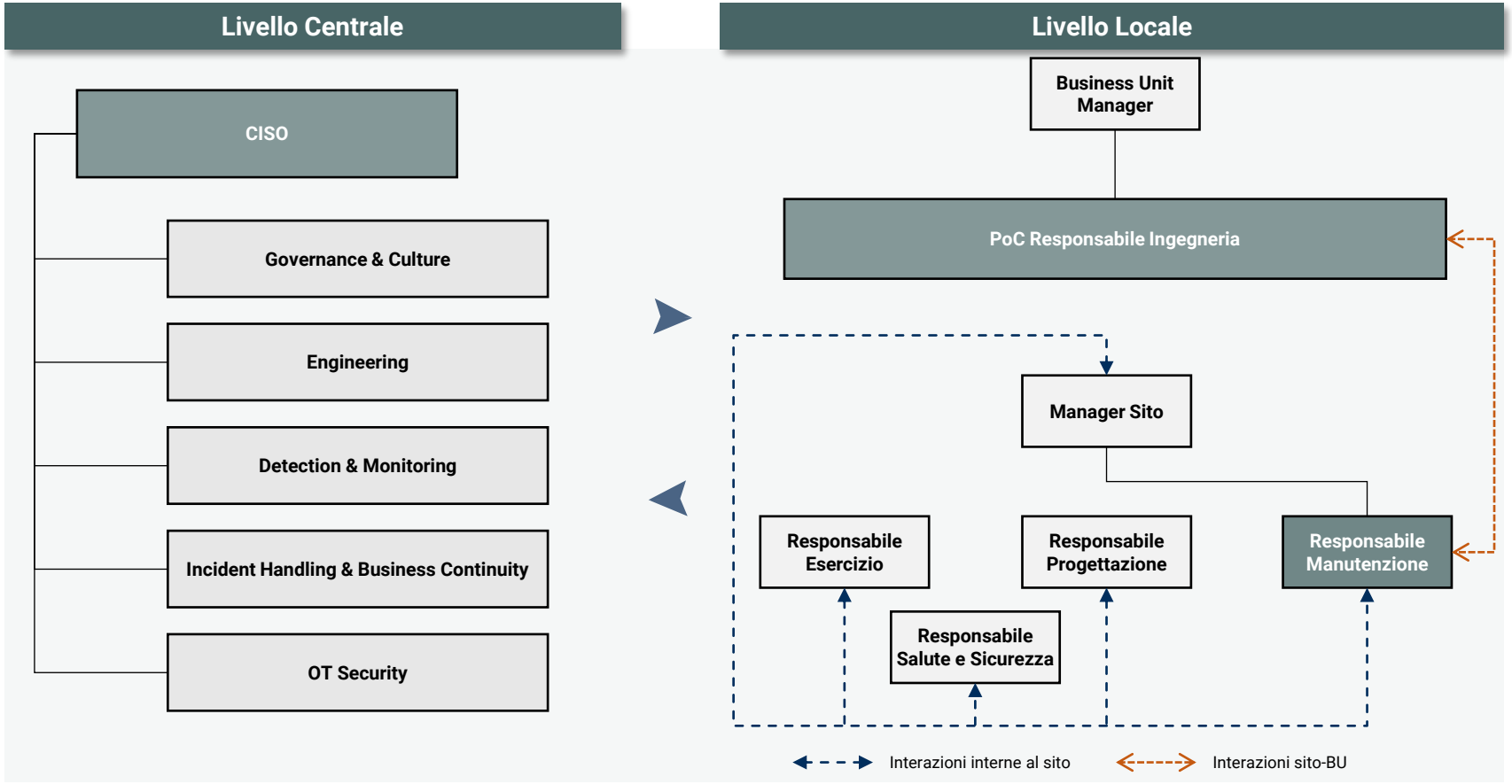
5 | Mitigazione delle Sfide

*Come possono essere **superate** tali **sfide**?*

Modello Operativo OT

Illustrative

La definizione del **modello operativo OT** permette di identificare il **modello di interazione** tra gli **Stakeholder**, sia a **livello centrale** ovvero di **Headquarter** che a **livello locale** ovvero di **Business Unit / impianto**, al fine di **gestire** in **modo efficiente** i **processi** in ambito **OT Cyber Security** e formalizzare **ruoli e responsabilità**



Il modello operativo mira a individuare le **interazioni** tra **livello centrale** e **locale** considerando i seguenti **processi** in ambito **Industrial Cyber Security**

1. **Cybersecurity Organization, Roles and Responsibilities**
2. **Cybersecurity Risk Management**
3. **Cybersecurity Training & Awareness**
4. **Timely Response to Cybersecurity Events**
5. **Cybersecurity Aspects of Business Continuity**
6. **Personnel & Third Parties Procedures**
7. **Cybersecurity Policy and Procedures**
8. **Network Security**
9. **Logical Access Control**
10. **System Development & Maintenance**

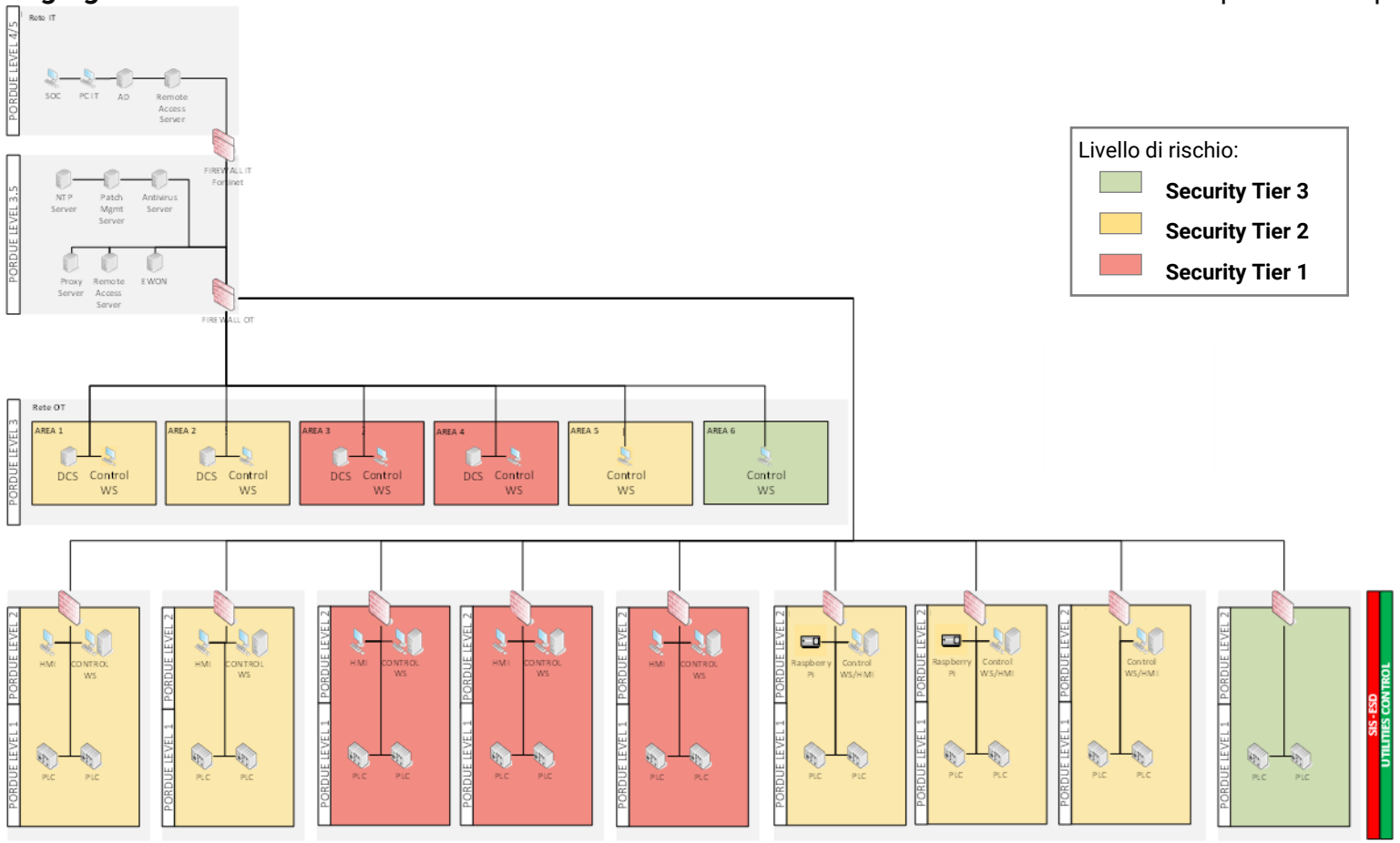
5 | Mitigazione delle Sfide

*Come possono essere **superate** tali **sfide**?*

Blueprint Architetturale

Illustrative

La **progettazione** dell'**architettura Blueprint** mira a definire, sulla base del **modello Purdue**, la **segmentazione** dei **componenti di rete** al fine di ottenere la **segregazione ottimale** in **zones and conduits** e individuare le **contromisure di sicurezza** da implementare per aumentare la sicurezza dell'ecosistema



Livello di rischio:

- **Security Tier 3**
- **Security Tier 2**
- **Security Tier 1**

A seconda del **livello** di **criticità** della **zona** all'interno dell'**impianto**, viene **assegnato** un **Security Tier** che va **da 1 a 3**.
Ogni **livello** prevede una serie di **contromisure suggerite** al fine di **mitigare** e **ridurre** i **rischi**:

Security Tier 3

- **Controllo accessi** | SRA, Micro-segmentazione
- **Monitoraggio attività** | Continuous Asset Monitoring, XDR, SIEM
- **Aggiornamenti di sicurezza** | Patch Management
- **Autenticazione a due fattori** | MFA
- …

Security Tier 2

- **Difesa avanzata** | XDR,
- **Autorizzazione role-based** | SRA, Micro-segmentazione
- **Analisi delle vulnerabilità** | Continuous Asset Monitoring
- **Gestione eventi di sicurezza** | XDR, SIEM
- …

Security Tier 1

- **Monitoraggio avanzato delle minacce** | XDR
- **Crittografia avanzata** | Firewall OT
- **Controllo accessi granulari** | Micro-segmentazione
- **Ripristino rapido** | Recovery Plan
- …

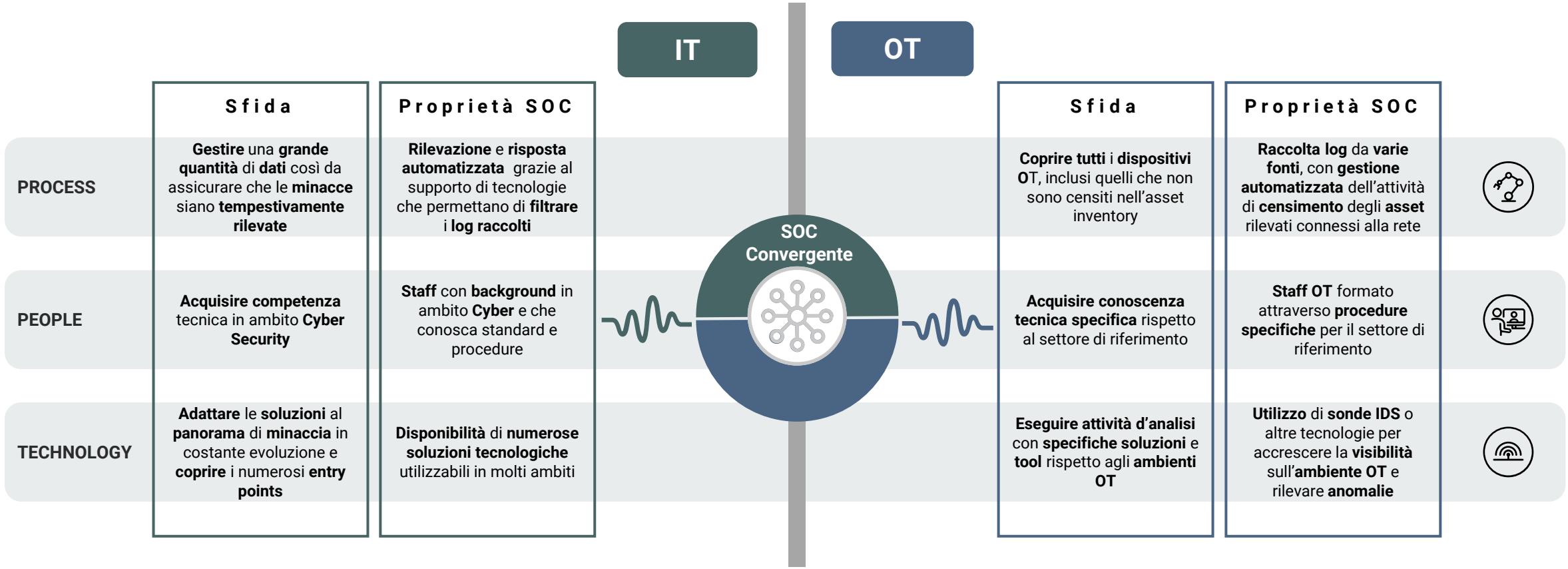
5 | Mitigazione delle Sfide

*Come possono essere **superate** tali **sfide**?*

SOC Convergente

Illustrative

La **creazione** di un **SOC convergente** consente di **rispondere** ad alcune **esigenze** che riguardano l'ambiente **IT** e l'ambiente **OT**, **conciliando** le **priorità** tra **sicurezza aziendale** e **operativa** e fornendo **visibilità completa** sull'intero **ecosistema IT/OT**



5 | Mitigazione delle Sfide

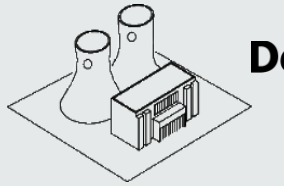
*Come possono essere **superate** tali **sfide**?*

Cyber Digital Twin

I **Digital Twin** offrono una **grande opportunità** per quanto riguarda l'**esecuzione** di **attività** di **analisi** e **monitoraggio avanzate** in un **ambiente digitale** che replica l'**ambiente fisico** e che permette lo **svolgimento** di **test** e la **simulazione** di **scenari Cyber critici** in un contesto protetto

Opportunità

- **Comprendere** l'**esposizione** al **rischio** dell'**infrastruttura** mediante la **definizione** di **scenari critici**
- **Simulare** l'**impatto** derivante dall'**applicazione** di una **patch** o l'**implementazione** di un **cambiamento senza influenzare** l'**infrastruttura fisica**
- **Simulare incidenti informatici** per **aumentare** il **livello** di **preparazione** dei **dipendenti** e **testare** il **processo** di **risposta** e **ripristino**



Deloitte.

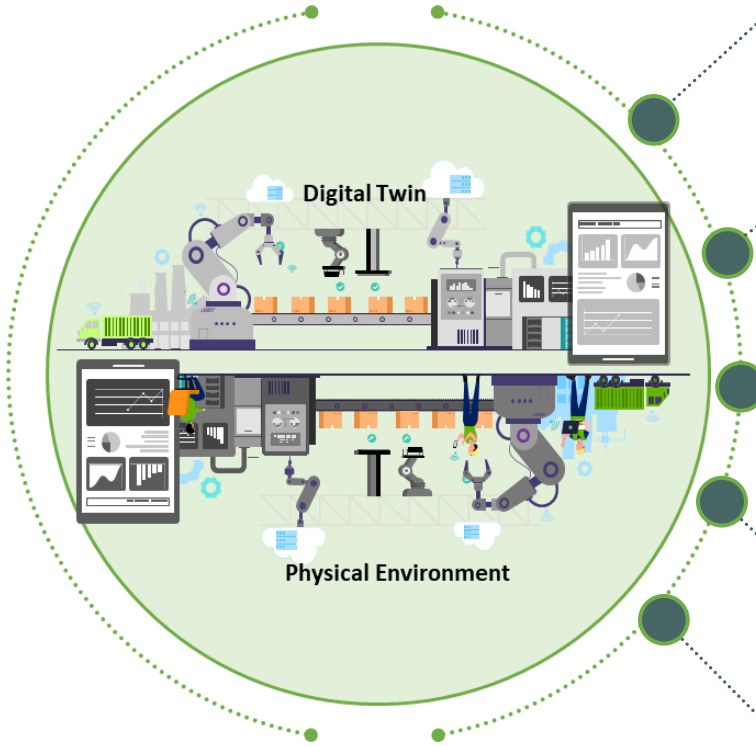
NextHub | Bari

5 | Mitigazione delle Sfide

*Come possono essere **superate** tali **sfide**?*

I Vantaggi dei Cyber Digital Twin

Le **opportunità** che derivano dall'utilizzo dei Digital Twin sono quindi numerose, ma è fondamentale che la loro **implementazione** sia **corretta** al fine di **massimizzare** i **vantaggi** e non incrementare i rischi Cyber



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

Grazie per l'attenzione!

QUESTIONARIO

- **Gradimento**
- **Newsletter**

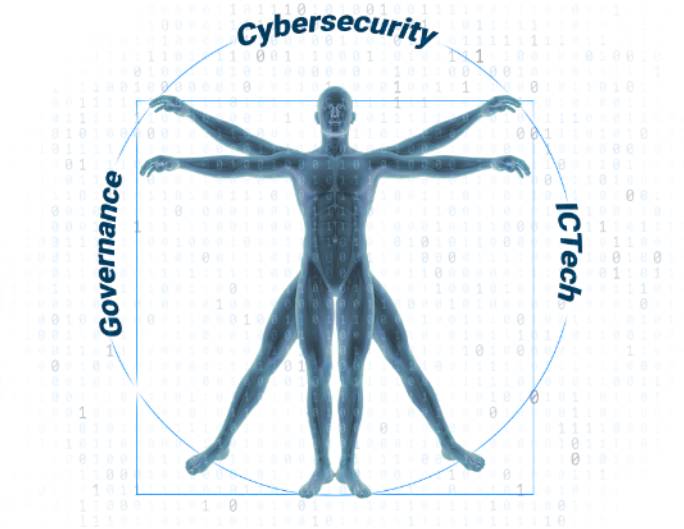
Scrivere a eventi@ithum.it per:

- Attestato partecipazione
- Slide
- Registrazione
- Info corso

ITHUM
it's for human

Founded in **2005**
by ICT professionals

Fields of interest:
Training & **Certifications**
Specialized **Consultancy**



HQ located **in Rome**
Active in Italy & Europe

Collaborative & strategic approach
to build Value

CYBER SECURITY

- IT Security
  - Attacks & Warfare
  - Defence & Analysis
  - Secure Coding
- Governance & Management
- Intelligence & Social
- Investigation & Digital Forensic

GOVERNANCE

- Management Systems ISO
  - Information Security, Business Continuity, Quality, ICT
  - Artificial Intelligence
  - Environment Social Government
- National & International Standards
  - Privacy GDPR
  - ICT Professional Profiles UNI/EN
  - HR Professional Profiles UNI
- Project Management & Framework
- Job Safety & Security
- Management & Soft skills

IT TECHNICIAN

- IT & OS Systems
- Cloud & Virtualization
- Development
- Industry 4.0
- Security DevNet
- DevOps

ithum.it

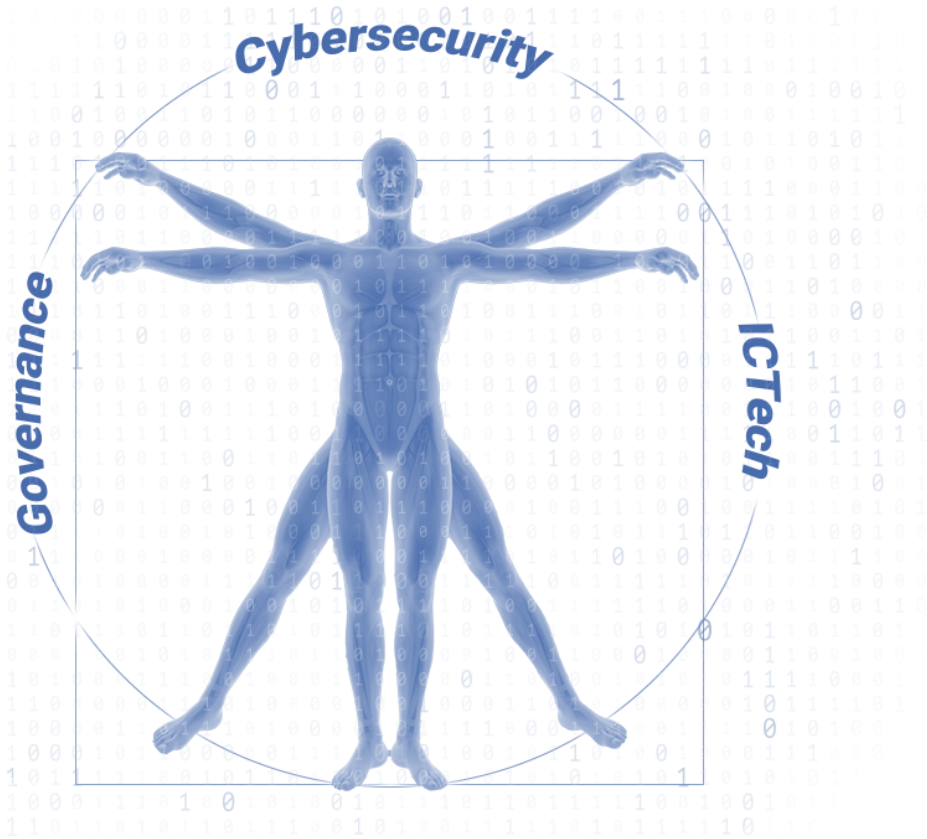
ITHUM
it's for human

(+39) 06 2158915
(+39) 06 86726329

Via Cristoforo Colombo, 149
00147 Roma (RM) Italy

informazioni@ithum.it

www.ithum.it



Corsi ICS/SCADA & Compliance Normativo

- **ICS/SCADA CyberSecurity – EC-Council**
  - Processi di automazione industriale con sistemi di controllo industriale (ICS) e sistemi di controllo di supervisione e acquisizione dati (SCADA)
- **Compliance Normativa CyberSecurity**
  - Regolamenti, Norme, Framework NIS, NIS2, CER, NIST2, ISO 27001, NIST, DORA, Golden Power, Perimetro, etc

Prossime edizioni di corsi

ICS/SCADA
28 h (4 gg)
Data partenza: martedì 25 giugno

Compliance Normativa
21 h (3 gg)
Data partenza: mercoledì 25 giugno

I nostri Webinar

21 Febbraio

Informazioni, materiali e registrazione:
https://ithum.it/innovazione-responsabile-lia-al-crocevia-di-cyber-security-sostenibilita-e-resilienza/

26 Marzo

Informazioni, materiali e registrazione:
https://ithum.it/losint-nellera-dellintelligenza-artificiale-nuove-frontiere-minacce-e-opportunita/

Q&A