# La Gestione della Security nelle Infrastrutture Critiche – Esperienza Enel

**Master Homeland Security – Università Campus Bio-Medico**
**Roma, 6 Ottobre 2017**

**Ing. Francesco Ceccarelli**
**Head of Security**

## Agenda

L’attuale approccio alla Security aziendale

La Security in una Energy Company e la realtà Enel

Security Management

Q&A


Reactive
Proactive
L’attuale approccio della
Security Aziendale
enel

# L’attuale approccio alla Security aziendale

## Il cambio di paradigma

La sfida attuale per la Security aziendale si gioca soprattutto sul piano della **prevenzione,** per effetto della rapida evoluzione delle minacce, della dinamicità dei metodi di attacco, dei relativi livelli di sofisticazione (es. cyber threats) e capacità di impatto sul raggiungimento degli obiettivi di business.

L’obiettivo è quello di aumentare la capacità del sistema e dell’organizzazione di **dare risposte forti a segnali deboli.**

E’ necessario evolvere da un approccio “reattivo” ad un **approccio “proattivo”**. La proattività deve coinvolgere l’intera organizzazione. Ciascun componente dell’organizzazione deve essere parte attiva, responsabile e consapevole del processo di Security.

# L’attuale approccio alla Security aziendale

## *Success Factors*

| INIZIATIVA | APERTURA | RESPONSABILITA’ | MISURA |
|---|---|---|---|
| ▪ Non aspettare che qualcosa accada<br>▪ Raccogliere ed interpretare i “segnali deboli”<br>▪ Valutare i trend delle minacce ed i punti deboli dell’organizzazione | ▪ Dialogare internamente con tutte le componenti dell’organizzazione<br>▪ Conoscere il business e gli obiettivi strategici dell’azienda<br>▪ Analizzare il contesto esterno di riferimento | ▪ Definire ed attuare un modello di comportamento orientato alla sicurezza (non solo di “regole”)<br>▪ Promuovere la formazione: insegnamento al “saper essere” e non al “saper fare” | ▪ Definire, misurare e monitorare indicatori di performance, utili per il miglioramento continuo |

# L’attuale approccio alla Security aziendale

*«Studio, sviluppo ed attuazione delle strategie, delle politiche e dei piani operativi volti a **prevenire, fronteggiare e superare** eventi in prevalenza di natura dolosa e/o colposa che possono danneggiare le risorse materiali, immateriali, organizzative e umane di cui l’azienda dispone o di cui necessita per garantirsi una adeguata capacità concorrenziale nel breve, nel medio e nel lungo termine» (UNI 10459)*

**Security aziendale**
come parte integrante del **sistema di controllo interno** e di **gestione dei rischi operativi**

# L’attuale approccio alla Security aziendale

## Il contributo della tecnologia

La tecnologia fornisce un **contributo significativo** per il processo di trasformazione ed evoluzione della Security aziendale, nonché per il raggiungimento degli obiettivi di protezione delle risorse umane, materiali ed immateriali.

Tuttavia la sola tecnologia, per quanto sofisticata, non è **mai sufficiente** per prevenire, fronteggiare e superare gli eventi che potrebbero compromettere o alterare la capacità d’impresa dell’azienda, **se non affiancata e bilanciata da adeguate azioni di natura organizzativa, gestionale e comportamentale**.

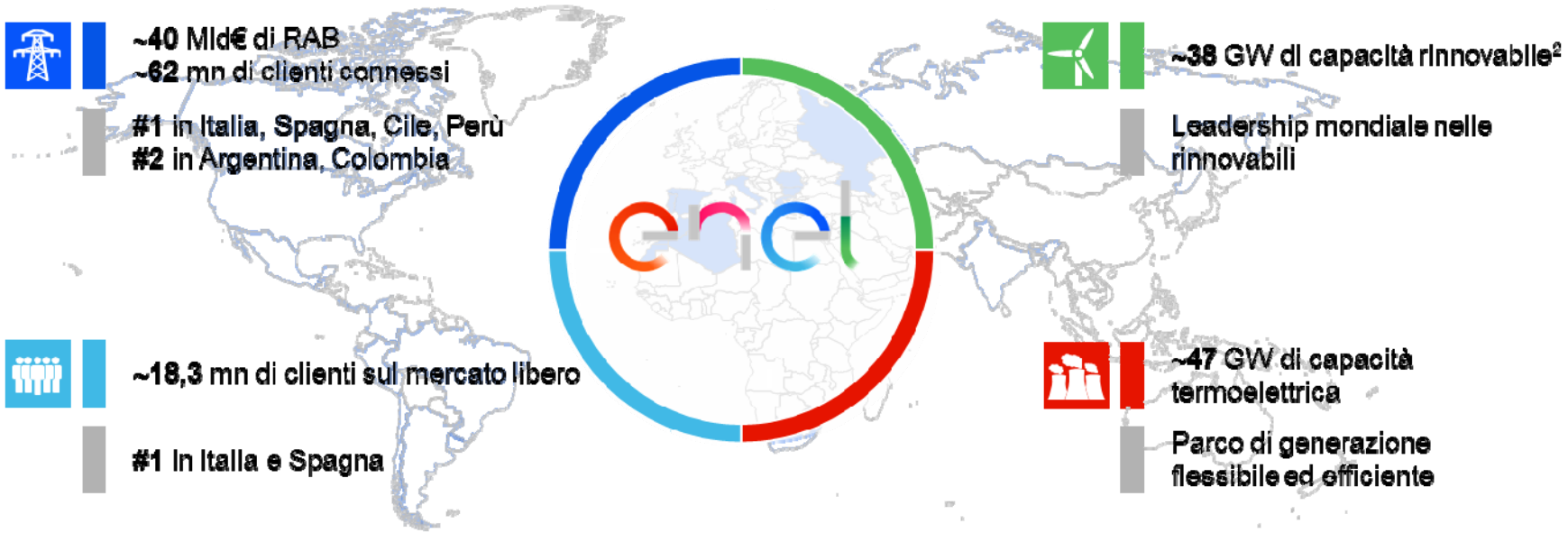
Un efficace governo dei rischi si ottiene sempre attraverso un adeguato mix di azioni:

- **tecnologiche**
- **organizzative**
- **gestionali**


La Security in una
Energy Company

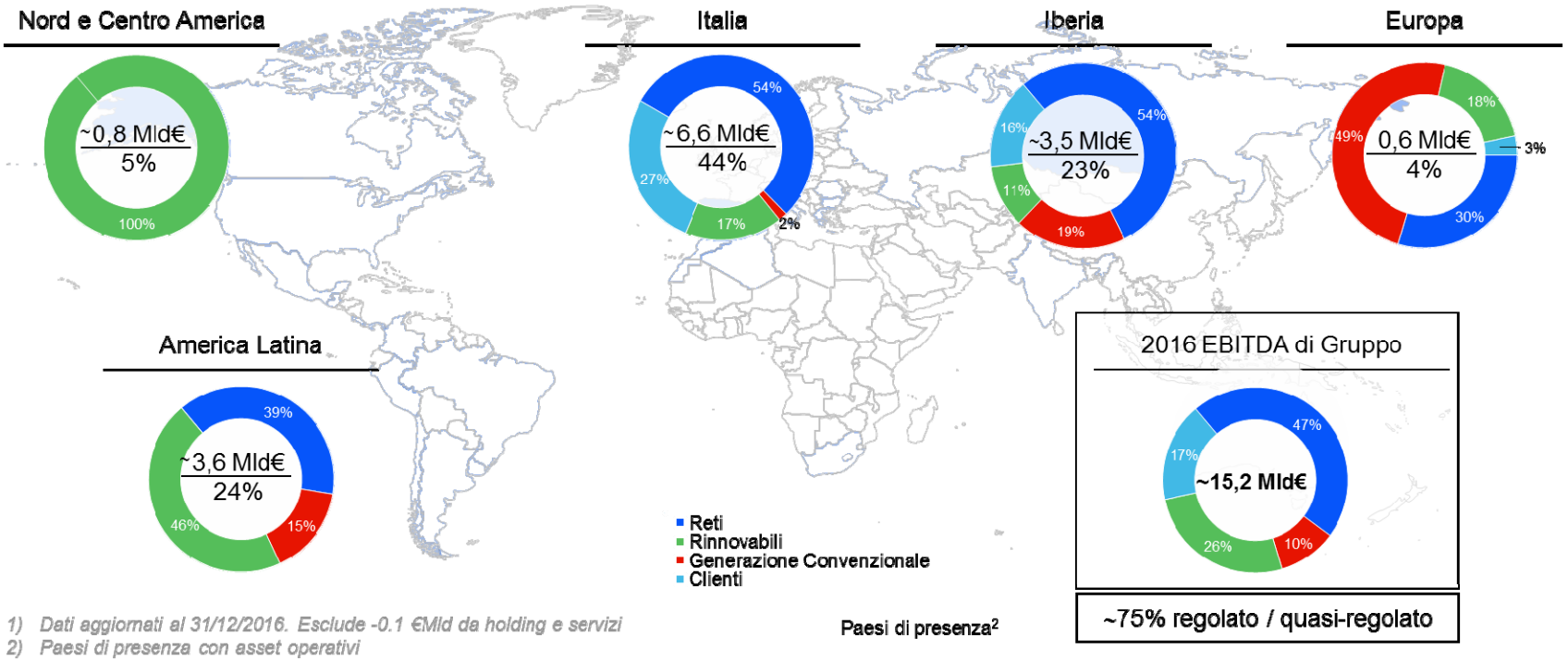
# Enel oggi[1]

Operatore globale diversificato




*1. Dati al 31/12/2016; 2. Capacità consolidata (35,9 GW) e gestita (1,9 GW) che include 24,9 GW di grande idroelettrico; 3. Presenza con asset operativi.*

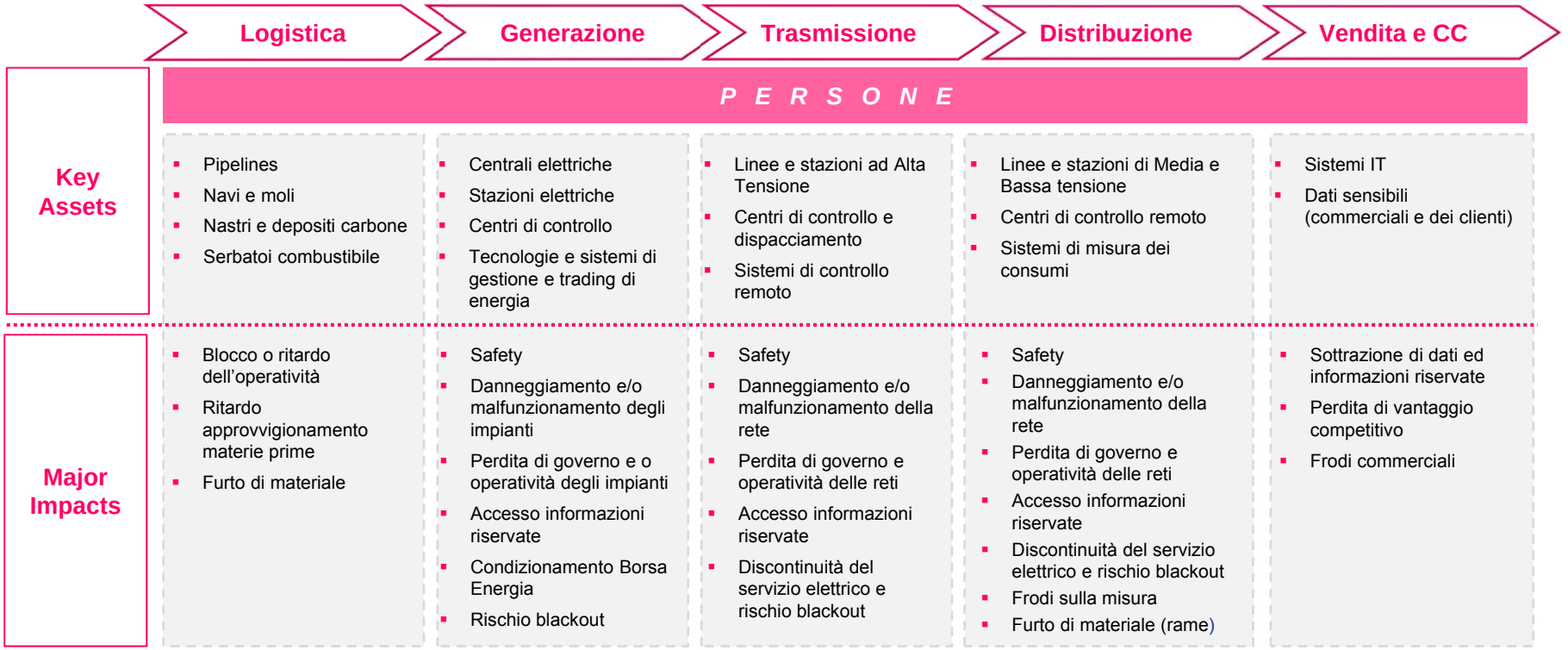
# Enel oggi[1]




1) *Dati aggiornati al 31/12/2016. Esclude -0.1 €Mld da holding e servizi*
2) *Paesi di presenza con asset operativi*

# La Security in una Energy Company

## Protezione della catena del valore



# La Security in una Energy Company

## Uno scenario in forte evoluzione

## Fattori intrinseci

Le trasformazioni del mercato dell'energia ed i cambiamenti nei processi aziendali hanno determinato nuove forme di **rischio per la sicurezza**


**Liberalizzazione del mercato** della produzione e vendita di energia, con conseguente scenario competitivo

**Interconnessione con reti pubbliche** delle reti di controllo della distribuzione e produzione di energia

Digitalizzazione dei processi gestionali e produttivi (IoT)


Espansione in **Paesi emergenti**

# La Security in una Energy Company

Uno scenario in forte evoluzione

## Fattori esterni

Nuove forme di minaccia e/o maggiore incidenza di minacce già presenti

**Furto di materiale metallico**

**Frodi di energia**


**Cyber attack**
(Energy company tra le più colpite)

**Terrorismo**

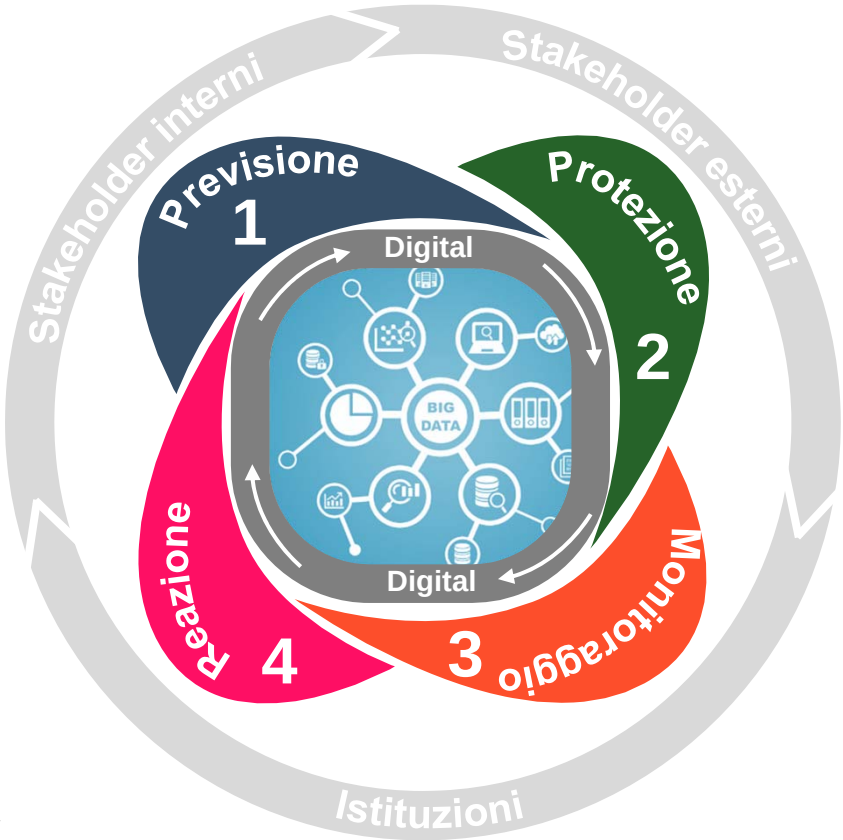

SECURITY
MANAGEMENT
enel

# Security Management

## Le fasi del processo

- Intelligence
- Identificazione e valutazione dei rischi

- Gestione incidenti ed eventi critici




- Mitigazione dei rischi:
  - protezione delle persone
  - protezione delle infrastrutture
  - protezione informazioni e beni immateriali

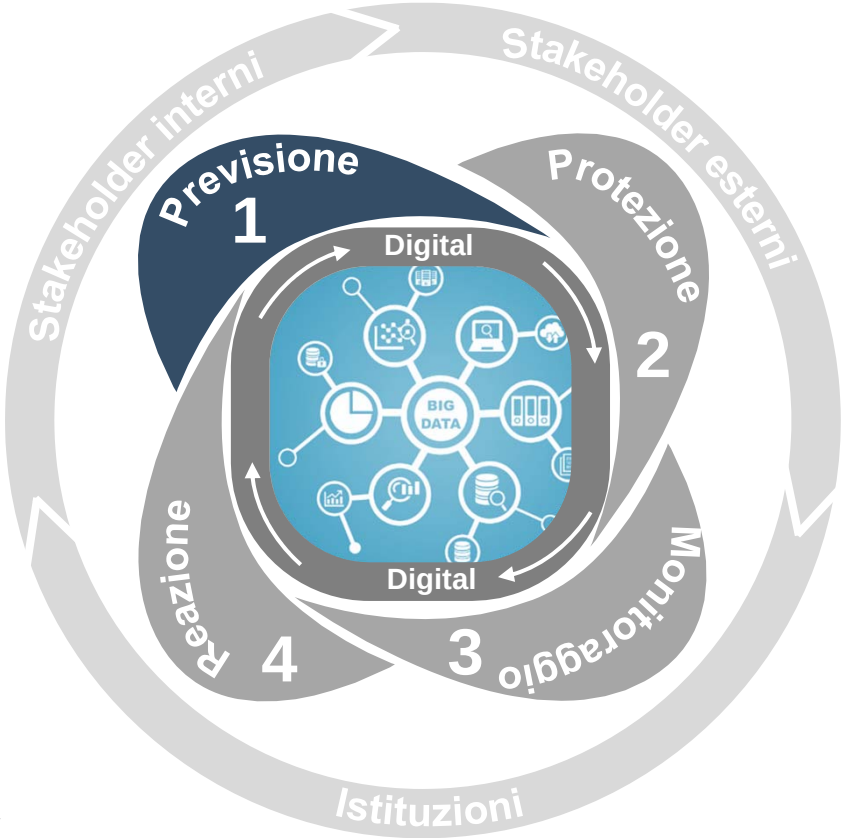
- Misura del rischio residuo
- Event detection

1

# Intelligence/Valutazione del rischio

- **Intelligence**
- **Identificazione e valutazione dei rischi**

- Gestione incidenti ed eventi critici




- Mitigazione dei rischi:
  - protezione delle persone
  - protezione delle infrastrutture
  - protezione informazioni e beni immateriali

- Misura del rischio residuo
- Event detection

1

# Intelligence
## Obiettivi

La Business Intelligence è la **raccolta, la correlazione e l'analisi di dati** ed informazioni provenienti da diverse fonti, finalizzata a ricavare notizie utili per un processo decisionale.

**IERI** — **Supporto ai processi decisionali militari**

**OGGI** — **Supporto ai processi decisionali aziendali**

**Business Intelligence**

- Raccolta ed analisi di dati su competitor, mercato, clienti e stakeholder.
- Raccolta ed analisi di dati su **potenziali minacce per gli asset dell'azienda**

Ruolo del Security Manager

1

## Intelligence
Obiettivi (esempi)

| | |
|---|---|
| **Analisi delle controparti** | Valutazione di eventuali **rischi reputazionali** per l'azienda conseguenti all'instaurazione e/o al proseguimento di rapporti commerciali o di collaborazione con terze parti (fornitori, business partner, ecc.) |
| **Threats Analysis** | Ricerca ed analisi di **nuove forme di minaccia** per gli asset aziendali e monitoraggio della loro evoluzione nel tempo |
| **Travel Security** | Analisi dei **contesti sociali, politici, economici** dei Paesi in cui è attivo il business aziendale, ai fini della protezione del personale inviato in trasferta |
| **Monitoraggio della reputazione** | **Monitoraggio sul web e stampa** della reputazione del brand e delle figure manageriali chiave dell'azienda |

1

## Intelligence

Metodi: le fonti da utilizzare

### Fonti interne

- Log di sistema
- Anomalie di sistema
- Sistema di security incident reporting
- Alert sistemi antifrode
- Controllo degli accessi
- …..

### Fonti esterne

**Open**

- Social Network
- Stampa
- Blog, Forum
- Wikis
- …..

**Certified**

- Camera di commercio
- Liste internazionali
- Catasto
- …..

**OSInt**

*Open Source Intelligence*

1

## Intelligence
Metodi: le fonti da utilizzare

### Elementi caratteristici delle fonti Open

- Sono accessibili pubblicamente
- Sono numerose ed eterogenee
- Potrebbero essere non attendibili o pilotati da attori ostili (es. fakenews)
- Sono spesso ridondanti
- Sono destrutturate

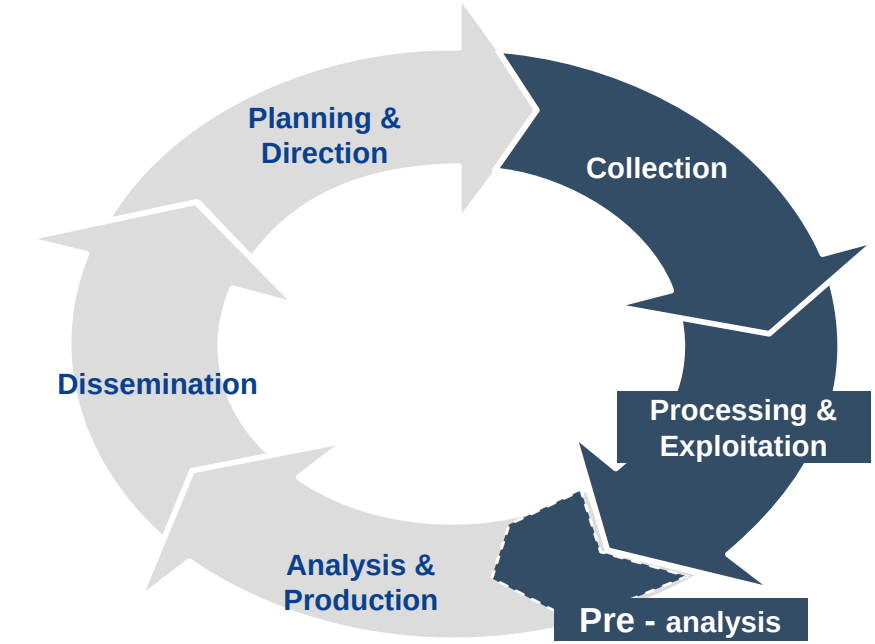
**Analisi complessa rispetto a quella delle fonti chiuse**

Le recenti tecnologie rappresentano un rilevante fattore abilitante per l'**OSInt**,
ma non va dimenticato l'apporto delle fonti umane (**HUMInt**-Human Source Intelligence)
ed il contributo dell'esperienza.

1

# Intelligence

## Metodi: il processo e gli strumenti




**Contributo dell'esperienza**

**Contributo della tecnologia**

- Importazione dati dalle fonti di interesse
- Integrazione e correlazione
- Estrazione informazioni di interesse (Security Analytics)

1

# Intelligence

## Gli strumenti di supporto

### Motore semantico

Consente la raccolta **di testi** da fonti aperte (stampa, web, social, ecc.) e la relativa analisi e **classificazione in base ai concetti in essi contenuti** e secondo specifiche tassonomie (standard o costruite ad hoc per Enel).

- **Ricerche rapide di concetti ed entità** (es. Persone Giuridiche, Persone Fisiche, Associazioni)
- **Servizio di e-mail alert,** in presenza di nuovi documenti inerenti a temi di specifico interesse

### Motore di correlazione

Consente di **rappresentare graficamente le relazioni** tra le informazioni provenienti da fonti eterogenee (interne ed esterne), allo scopo di:

- individuare rapidamente collegamenti tra entità
- Identificare nodi e punti di aggregazione

- Connessione automatica con **banche dati esterne certificate (es. camera commercio) e con banche dati interne**

1

# Identificazione e valutazione dei rischi

## Obiettivi

**Verificare il livello di esposizione ai rischi** di Security dei processi aziendali, allo scopo di identificare quelli per i quali è necessario intervenire con priorità

L'attività è fondamentale per indirizzare le successive fasi di pianificazione degli interventi, sulla base di un **criterio costo/beneficio**

L'attività dovrebbe essere eseguita con **cadenza periodica** e comunque al verificarsi di significative modifiche dell'assetto aziendale (es. nascita di nuovi processi di business, introduzione di nuovi sistemi informatici, avvio di nuove infrastrutture, ecc.)

1

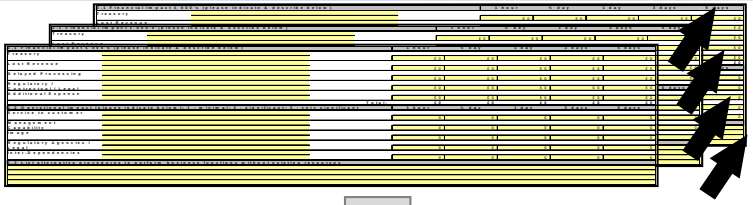
# Identificazione e valutazione dei rischi

## Metodi: la Business Impact Analysis

La **BIA** assicura che **le misure a protezione delle minacce**, siano in linea con la mission, gli obiettivi, gli obblighi di legge per l'ambito definito. Consente di concentrare le risorse aziendali sui processi di business maggiormente critici.

### 1°step

**Identificazione** dei **processi**, dei **sotto-processi**, delle **informazioni** gestite e scambiate, fino ad identificare gli asset di supporto **(applicazioni informatiche, infrastrutture, ecc.)**



### 2°step

**Stima degli impatti sui processi di business** (economici, di immagine, conseguenze legali, safety…) conseguenti alla mancata disponibilità degli asset di supporto e alla violazione di integrità e riservatezza delle informazioni trattate

| Availability Impact | Insignificant | Minor | Moderate | Major | Catastrophic |
|---|---|---|---|---|---|
| Total Impact = Financial Impact Score + Maximum Non Quantifiable Impact | 1 | 2 | 3 | 4 | 5 |
| **Integrity Impact** | **Insignificant** | **Minor** | **Moderate** | **Major** | **Catastrophic** |
| Sensible Data | | | | X | |
| Proprietary Information | X | | | | |
| Unique Information | X | | | | |
| **Confidentiality Impact** | **Insignificant** | **Minor** | **Moderate** | **Major** | **Catastrophic** |
| Sensible Data | | | | | X |
| Proprietary Information | | | | X | |
| Unique Information | | X | | | |

### 3°step

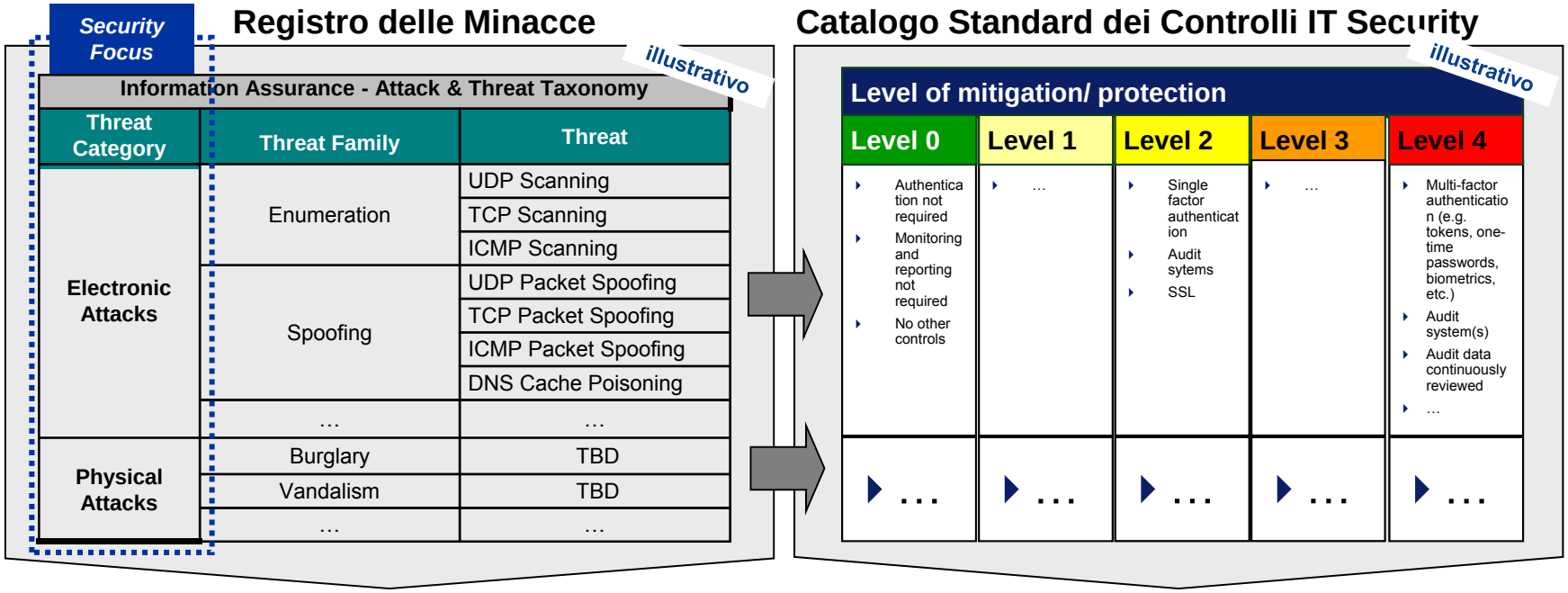
**Individuazione del livello di impatto massimo** per ogni asset secondo una metrica standard.

| Business Impact | Availability | Integrity | Confidentiality |
|---|---|---|---|
| Asset 1 | Catastrophic | Major | Minor |
| Asset 2 | Minor | Major | Insignificant |

1

# Identificazione e valutazione dei rischi

## Metodi: Matrice minacce/controlli




**Registro delle Minacce Standard**
(aggiornamento costante attraverso fonti interne ed esterne)

**Best practice e Controlli Standard**
contro le minacce identificate

1

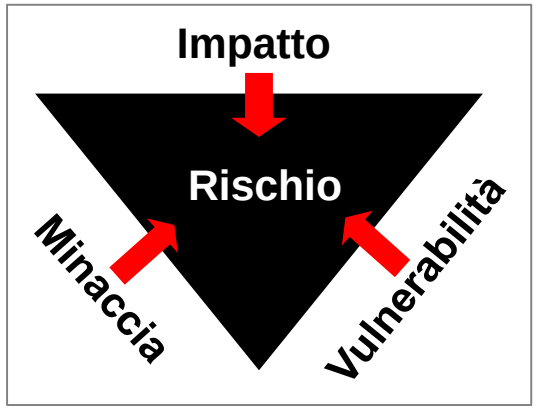
# Identificazione e valutazione dei rischi

## Metodi: valutazione dei rischi

La fase finale del risk assessment è finalizzata
**all'individuazione del reale livello di esposizione al rischio**
del processo ed alla conseguente identificazione dei controlli necessari per la sua mitigazione.

Sono presi in esame:

- i **risultati della Business Impact Analysis**
- le **minacce** possibili ed i controlli idonei a contrastarle (secondo la matrice minacce/controlli)
- il **gap** esistente tra i controlli necessari e quelli presenti



1

# Identificazione e valutazione dei rischi

## Sistemi di supporto

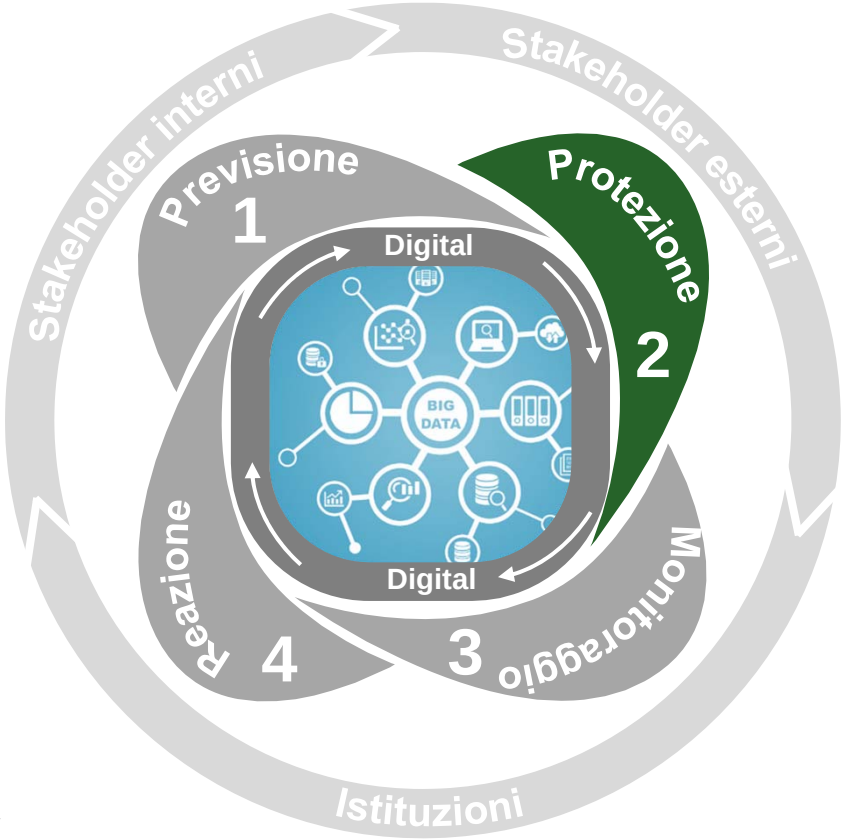
- **Sistema di anagrafica degli asset aziendali (IT e fisici)**
- **Sistema di security incident reporting**, utile per valutare la probabilità delle minacce anche sulla base dello storico degli eventi accaduti
- **Sistema per la raccolta e l'aggregazione dei risultati** della Business Impact Analysis e del Risk Assessment (dal semplice DB Access alle evolute piattaforme GRC – Governance, Risk & Compliance)

2

# Mitigazione dei rischi

- Intelligence
- Identificazione e valutazione dei rischi

- Gestione incidenti ed eventi critici




- **Mitigazione dei rischi:**
  - **protezione delle persone**
  - **protezione delle infrastrutture**
  - **protezione informazioni e beni immateriali**

- Misura del rischio residuo
- Event detection

2

# Mitigazione dei rischi

## Obiettivi

**Identificare, pianificare ed implementare le misure** di natura organizzativa, tecnica e gestionale idonee a mitigare i rischi emersi nella precedente fase di assessment, **coerentemente agli obiettivi strategici e di business aziendali**

- **Misure organizzative**: misure volte ad orientare l'organizzazione ed i comportamenti al rispetto dei principi e delle regole di sicurezza (definizione di policy, procedure, linee guida; realizzazione di interventi di comunicazione interna, ecc.)
- **Misure tecniche**: introduzione e/o adeguamento di sistemi e soluzioni volti a proteggere gli asset materiali ed immateriali rispetto a specifiche minacce
- **Misure gestionali**: iniziative finalizzate alla gestione della sicurezza che richiedono attività operative e/o l'acquisizione di servizi specifici (es. Sorveglianza, monitoraggio allarmi, ecc.)

Valutare il **corretto equilibrio tra tutte le componenti** (es. inutile predisporre misure tecniche se non accompagnate da efficaci procedure per la relativa gestione e controllo)

2

## Mitigazione dei rischi

Fase di realizzazione: azioni organizzative


- Definiscono i **principi** della politica di sicurezza aziendale
- Definiscono i processi, i **ruoli e le responsabilità** per la sicurezza
- Forniscono le **regole operative**

2

## Mitigazione dei rischi

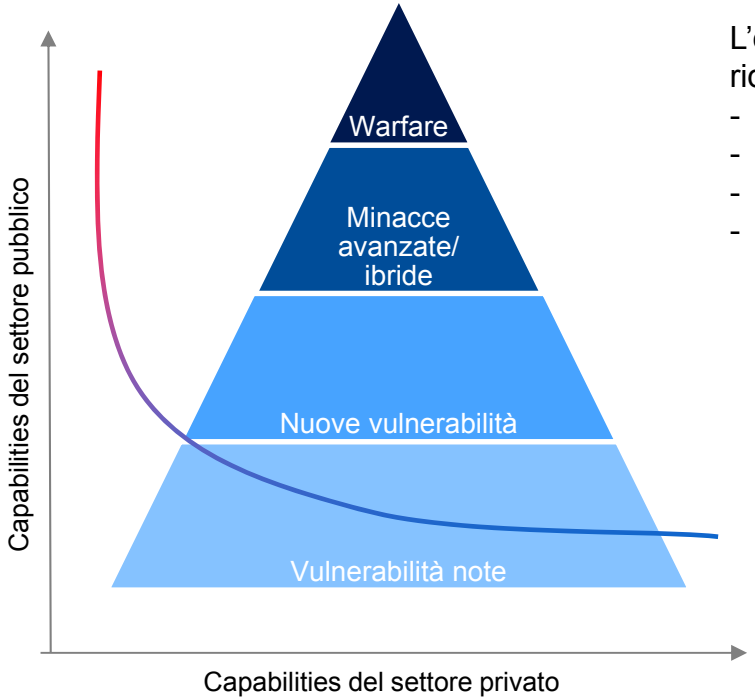
Fase di realizzazione: azioni gestionali

- **Sorveglianza** armata e non armata
- Monitoraggio e **gestione allarmi**
- Servizi di **manutenzione** impianti di sicurezza
- Accordi di PPP (Public&Private Partnership)
- Awareness and training

2

# Infosharing e PPP

## Verso un coordinamento operativo di settore




L'operatore privato di infrastrutture critiche ha un'autonomia di azione ridotta nella mitigazione dei rischi e nel contrasto delle minacce a causa di:

- risorse limitate
- natura delle minacce
- implicazioni legali
- influenza sulla supply chain

2

## Mitigazione dei rischi

Fase di realizzazione: azioni gestionali

### Awareness and training

- Diffusione e mantenimento della **consapevolezza sui rischi di sicurezza**
- Affermazione di un **“etica della sicurezza”** nei comportamenti organizzativi
- Diffusione della conoscenza su **policy, procedure ed istruzioni operative di Security**
- Informazione tempestiva in presenza di **particolari minacce** (es. propagazione di virus informatici)
- Accrescimento ed aggiornamento continuo delle **competenze del personale** che opera nella struttura di Security

2

## Mitigazione dei rischi

Fase di realizzazione: azioni tecniche

- Sistemi e soluzioni per la **protezione dei dati**
- Sistemi e soluzioni per la **protezione dei sistemi, delle applicazioni e delle infrastutture informatiche**
- Sitemi attivi per la **protezione delle infrastrutture fisiche** (antintrusione, videosorveglianza, controllo accessi fisici)
- Misure passive per la protezione delle infrastrutture fisiche (recinzioni, tornelli, ecc.)

Definire bene i requisiti, effettuare i test di collaudo, ma soprattutto **assicurare la definizione e l'applicazione delle procedure di gestione** dei sistemi e delle soluzioni di sicurezza. Spesso la loro inefficacia, soprattutto nel contesto della sicurezza fisica, è dovuta alla scarsa manutenzione!!

2

# Mitigazione dei rischi

## Protezione infrastrutture


2

# Mitigazione dei rischi

## Protezione infrastrutture

### Possibili contromisure tecniche

- videosorveglianza con software di video-analisi
- sistemi di antintrusione perimetrale
- sorveglianza con droni (per monitoraggio linee)
- rilevatori di caduta con antenna GPS integrata (per trasformatori a palo)

2

# Mitigazione dei rischi
## Protezione infrastrutture

### MoveAlarm

Rileva il movimento e la mancanza di tensione. Utilizzato per la protezione dei trasformatori su palo e cabine secondarie.

### CableAlarm

Utilizzato su linee già interrotte da precedenti furti, rileva la continuità del conduttore rimanente, evitando il reitero del furto.

### tGuard

Con funzionalità di Security e di esercizio, mappa le vibrazioni naturali delle linee aeree e segnala una variazione dovuta a tentativi di furto o, ad esempio manicotti di ghiaccio.

### Scanner laser

Per la protezione di zone aperte, permette la riduzione di falsi positivi, semplice e poco costoso da installare

### Telecamera termica

Utilizzata per la protezione, perimetrale usa l'analisi video come sensore. Punto di forza nella protezione delle centrali fotovoltaiche

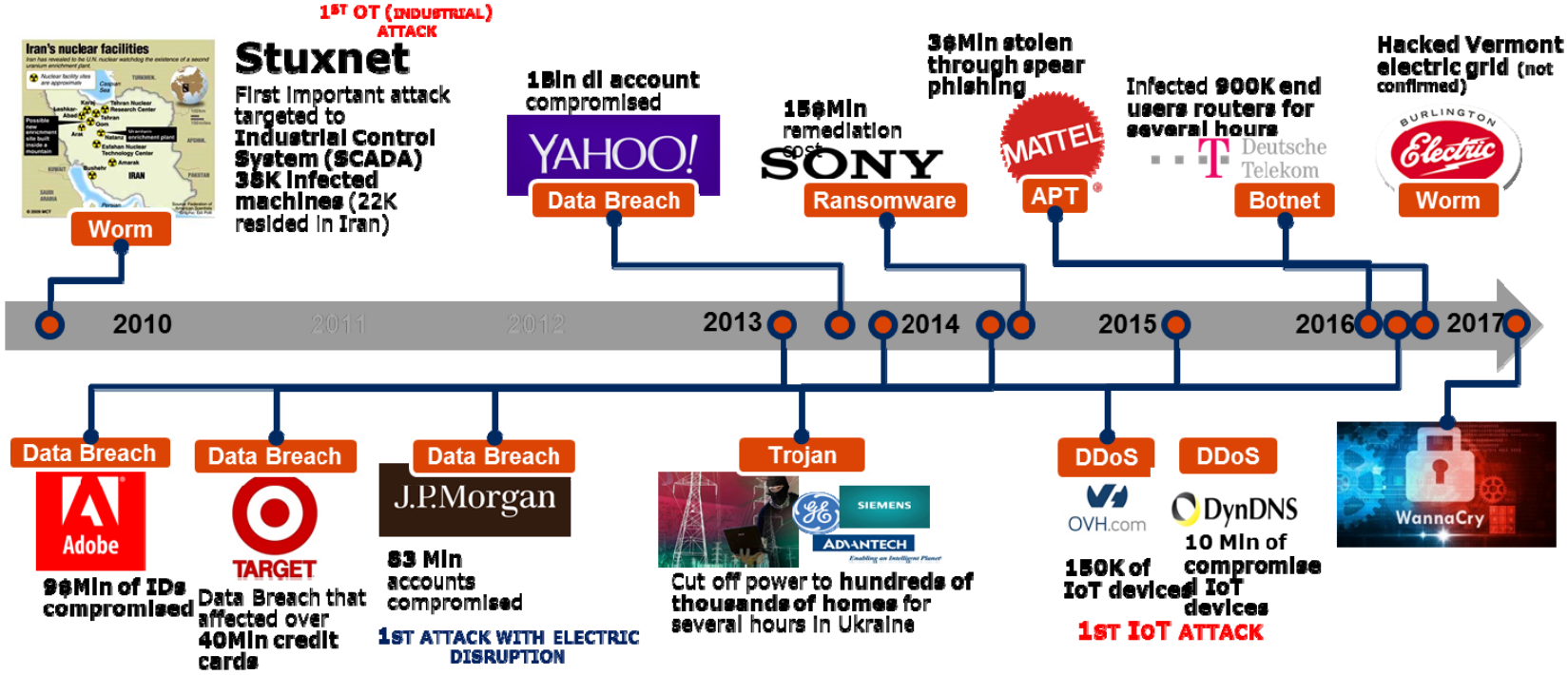
### Radar

Dedicato alla protezione del perimetro, ha il vantaggio di rilevare gli avvicinamenti al sito con largo anticipo

2

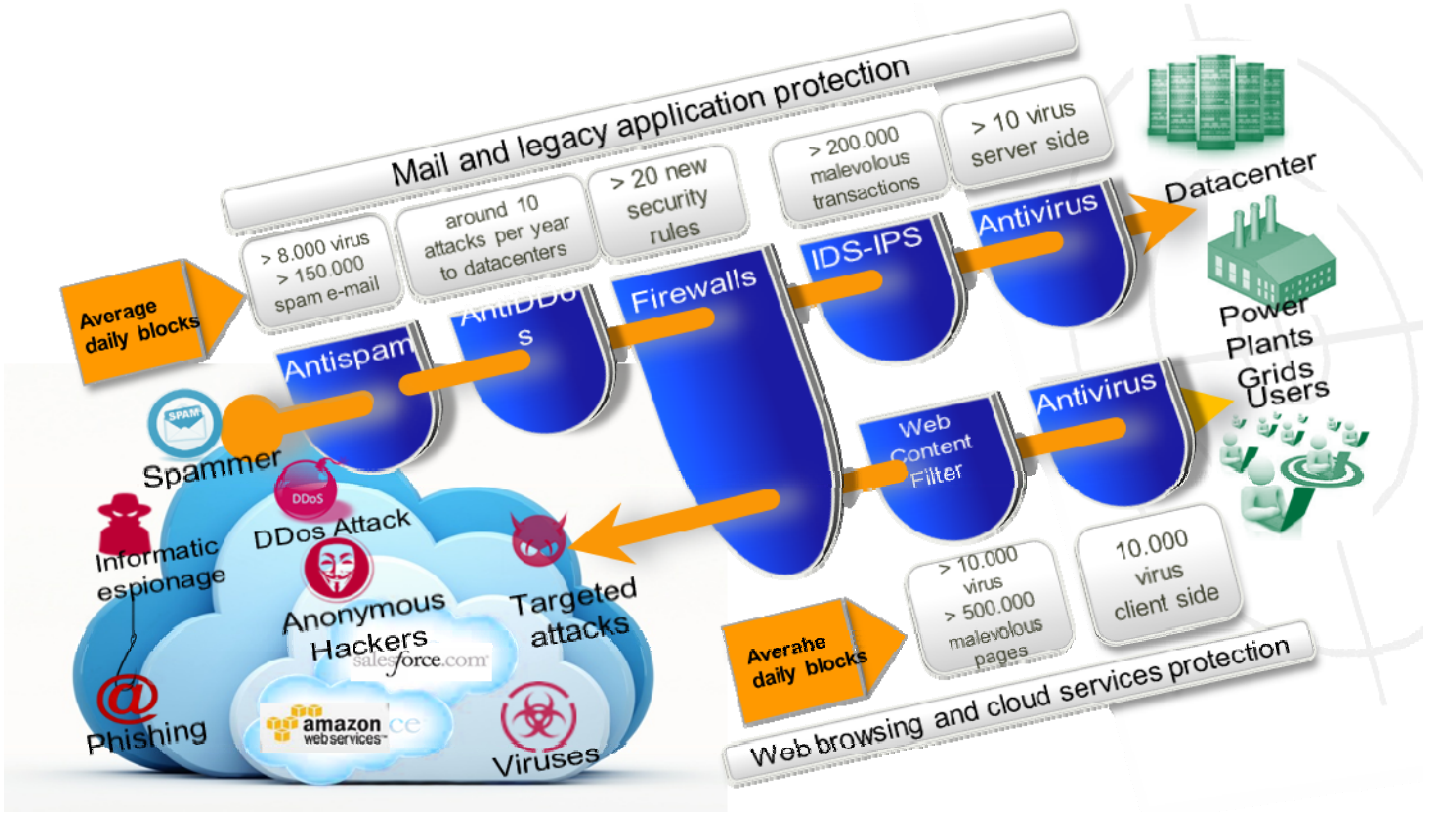
# Mitigazione dei rischi

## Protezione sistemi IT e OT



# Mitigazione dei rischi

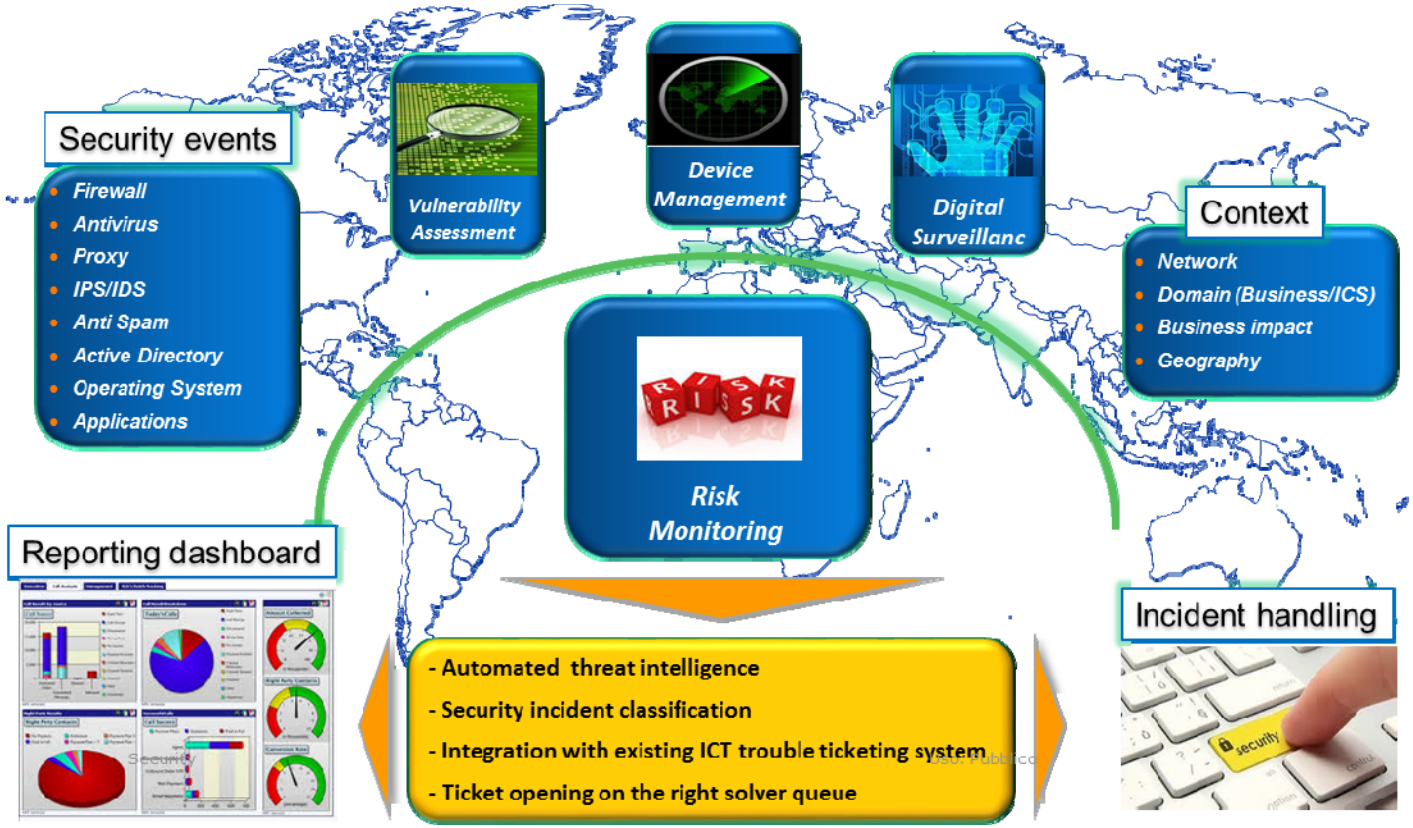
## Protezione sistemi IT e OT



2

# Mitigazione dei rischi

## Protezione sistemi IT e OT



2

# Mitigazione dei rischi

Protezione persone in viaggio

## Preparazione

Risk assessment
Vademecum
Assicurazione

## Feedback

Viaggiatori
Management
Fornitori

## Hotline

SCR 24 x 7
Reperibilità senior security

## Pianificazione

Logistica
Trasporti con autista (armato e non)
Comunicazione satellitare

## Monitoraggio

Piattaforma integrata (GTS)
OSINT
Intelligence

## Reazione

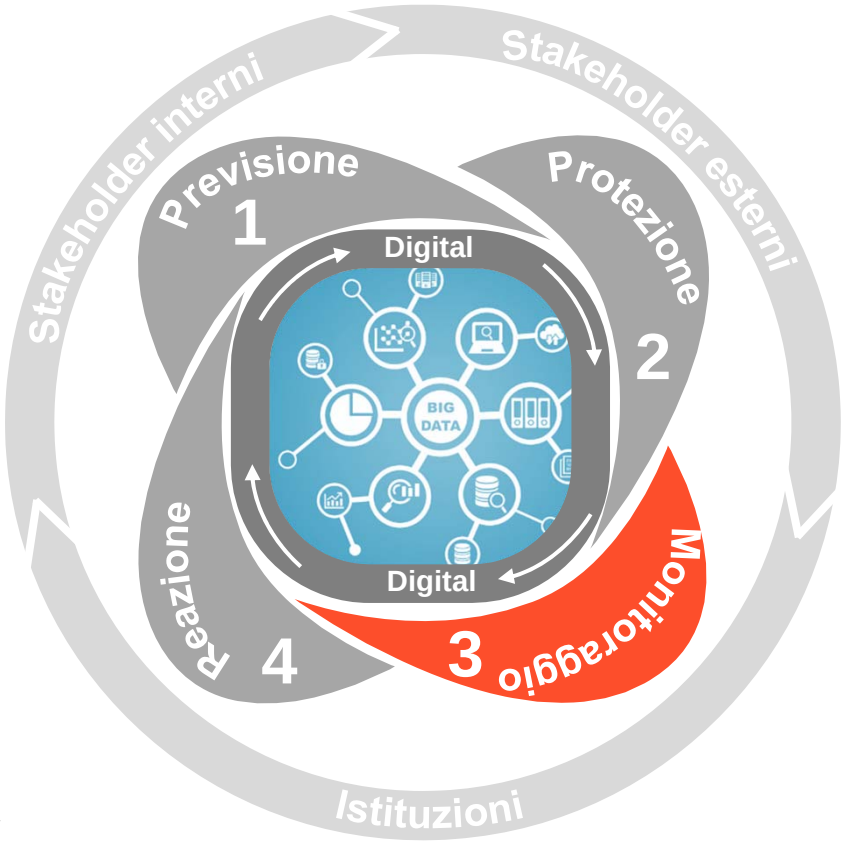
Nuovo programma di viaggio
Piani di evacuazione/esfiltrazione

3

# Monitoraggio

- Intelligence
- Identificazione e valutazione dei rischi

- Gestione incidenti ed eventi critici




- Mitigazione dei rischi:
  - protezione delle persone
  - protezione delle infrastrutture
  - protezione informazioni e beni immateriali

- **Misura del rischio residuo**
- **Event detection**

3

# Misura del rischio residuo

## Obiettivi

**Verificare l'efficienza e l'efficacia delle azioni di mitigazione del rischio**, attraverso la conduzione di test ed attività di controllo mirate a verificare:

- il livello di conoscenza ed applicazione delle **policy** e delle **procedure di sicurezza**
- il grado di robustezza delle soluzioni tecniche realizzate
- il livello di efficacia ed efficienza delle azioni gestionali adottate

L'esito di tale attività costituisce anche un **input significativo per il successivo ciclo periodico di risk assessment**

3

# Misura del rischio residuo

## Le possibili azioni

- **Vulnerability assessment e penetration test sui sistemi informatici**
- **Vulnerability assessment su siti ed infrastrutture fisiche**
- Attività di **social engineering**
- Verifica efficacia dei sistemi e delle procedure di **controllo degli accessi logici** (con particolare riferimento al rispetto del principio di **segregation of duties**)
- Verifica efficacia dei sistemi e delle procedure di **controllo degli accessi fisici**
- Controllo livelli di servizio offerti dai fornitori di **servizi di vigilanza e sorveglianza**
- Verifica livello di efficienza e manutenzione **sistemi di sicurezza fisica** (videosorveglianza, antintrusione, ecc.)

3

# Misura del rischio residuo

## Sistemi di supporto

- **Tool per il vulnerability scanning automatico** di sistemi ed infrastrutture IT
- Sistemi di **raccolta ed analisi dei log**
- Piattaforme di **Governance, Risk & Compliance**
- Sistema di **security incident reporting**
- Sistema di **Identity and Access Management**

3

# Event Detection

## Early detection

- L'early detection di un evento potenzialmente pericoloso, di natura accidentale o dolosa, dipende dal fenomeno specifico e varia dai secondi, come ad esempio per i terremoti o effrazioni in sito o attentati terroristici, alle ore o giorni, come ad esempio per fenomeni meteorologici o pianificazione trasferte in paesi a rischio (per motivi etnici, politici, tasso criminale e terrorismo).
- L'early detection non è quindi una previsione dell'accadimento di un evento, ma dell'intensità con la quale l'evento giungerà ad un determinato sito o determinato scopo.
- L'insieme delle competenze comprende i sistemi/piattaforme di acquisizione dei segnali (Security Control Room), le reti di sensori tecnici (Infrastructure Security: impianti di videosorveglianza ed antintrusione) e «umani» (Local operations) distribuiti sul territorio nazionale, le capacità di rapida elaborazione dei dati (Intelligence & Risk Assessment) ed, infine, le strategie di gestione e comunicazione (Crisis Management).

## Accidentali


- bollettini di allerta meteo e criticità idrogeologica diramati dal DPC
- bollettini sismici emanati dal INGV
- press monitor

## Dolosi

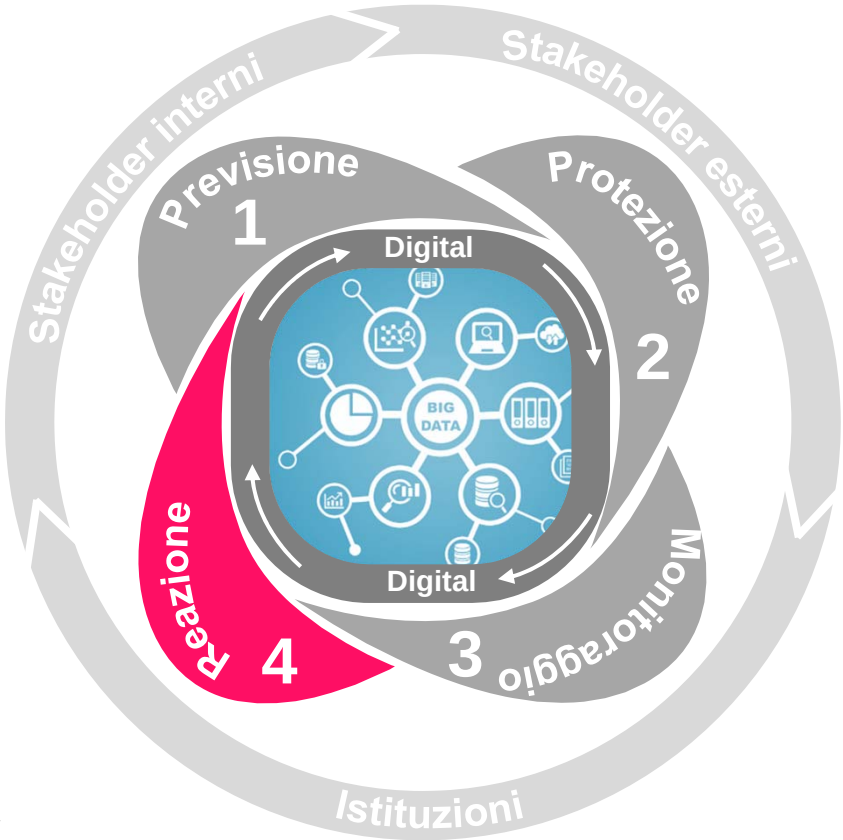
- video Ispezioni SCR
- segnali di allarme antintrusione
- informazione o avvisi dai Security Local Operations
- avvisi inviati da Prefetture, Forze dell'Ordine o altri Organi Istituzionali in merito a possibili eventi relativi ad ordine pubblico
- informazione o avvisi dalle Business Lines
- OSINT
- travel guide

4

# Reazione

- Intelligence
- Identificazione e valutazione dei rischi

- **Gestione incidenti ed eventi critici**



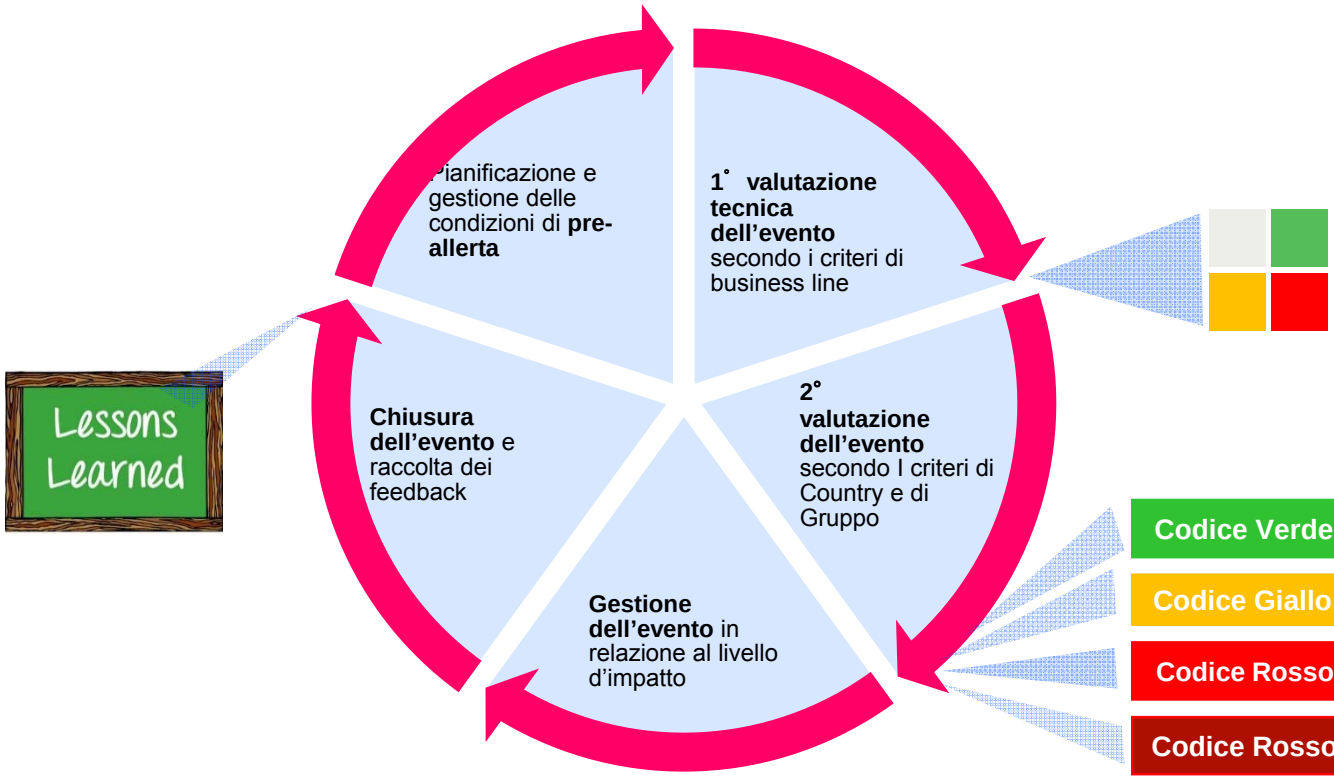

- Mitigazione dei rischi:
  - protezione delle persone
  - protezione delle infrastrutture
  - protezione informazioni e beni immateriali

- Misura del rischio residuo
- Event detection

4

# Gestione incidenti ed eventi critici

## Le fasi del processo




**Valutazione impatto di Line**

- Codice Verde di Country
- Codice Giallo di Country
- Codice Rosso di Country
- Codice Rosso di Gruppo

**Valutazione impatto di Country e di Gruppo**

4

# Gestione incidenti ed eventi critici

## Pianificazione e pre-allerta

### Pianificazione

**Un'adeguata pianificazione** è fondamentale per garantire una rapida ed efficace risposta al manifestarsi di un improvviso evento critico. Include:

- la definizione e **l'aggiornamento di procedure ed istruzioni operative**
- l'identificazione di **attori e dei loro sostituti (backup)**
- l'organizzazione di **simulazioni** periodiche, finalizzate a valutare le procedure ed identificare possibili miglioramenti.
- l'organizzazione di **sessioni di formazione** per tutti gli addetti
- la predisposizione ed il **test** degli strumenti e delle attrezzature di supporto

### Pre-Allerta

Raccolta di dati ed informazioni, sia da fonti esterne che interne, utili ad identificare situazioni che potrebbero evolvere in **possibile stato di emergenza** come, ad esempio:

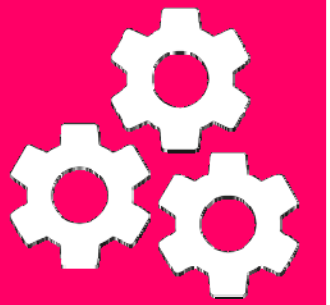
- **Bollettini di allerta meteo**
- **Allerte da Enti Istituzionali** inerenti a possibili eventi collegati all'ordine pubblico o a potenziali emergenze civili
- Raccolta di informazioni da **fonti aperte** (stampa, social, Web, etc.) collegate ad azioni organizzate che potrebbero compromettere la continuità del servizio, l'attività di business o compromettere gli interessi di Enel
- **informazioni fornite dalle linee di business globali (ad es. Produzione o Distribuzione)** inerenti a manutenzioni programmate o previsioni di fuori servizio

4

# Gestione incidenti ed eventi critici

## Valutazione

**Metodologia**



Gli eventi vengono classificati in linea con la **matrice d'Impatto** definita a livello di Country.

La valutazione si basa su:

- **elementi oggettivi** e misurabili (ad es. numero di clienti disalimentati)
- **elementi di contesto** nei quali si sviluppa l'evento (ad es. possibile impatto sull'esposizione mediatica dovuta all'evento)

La policy aziendale identifica e definisce i seguenti **codici** di classificazione:

- **Codice Verde**: emergenza gestita a livello locale
- **Codice Giallo** : attivazione del Comitato di Gestione Emergenze centrale a livello di Paese
- **Codice Rosso** : attivazione del Comitato di Crisi di Gruppo su approvazione del CEO

4

# Gestione incidenti ed eventi critici

## Risposta

## Azioni

Gli stessi codici vengono adottati anche a livello globale

- **VERDE:** l'evento ha un **impatto basso** e per essere gestito richiede solo l'applicazione delle **procedure definite**
- **GIALLO**: l'evento ha un **impatto medio** e per essere gestito richiede sia l'applicazione delle **procedure d'emergenza**, sia il **coinvolgimento dell'intera organizzazione di Country**
- **ROSSO**: l'evento ha un **alto impatto** e richiede l'attivazione di **strategie straordinarie a livello globale**

In relazione alla gravità dell'evento si Il **processo di risposta** ha l'obiettivo di **ripristinare le normali condizioni** di operatività e/o di safety, di garantire l'allineamento interno delle informazioni, di monitorare la comunicazione e le relazioni con gli stakeholders esterni, procedendo con:

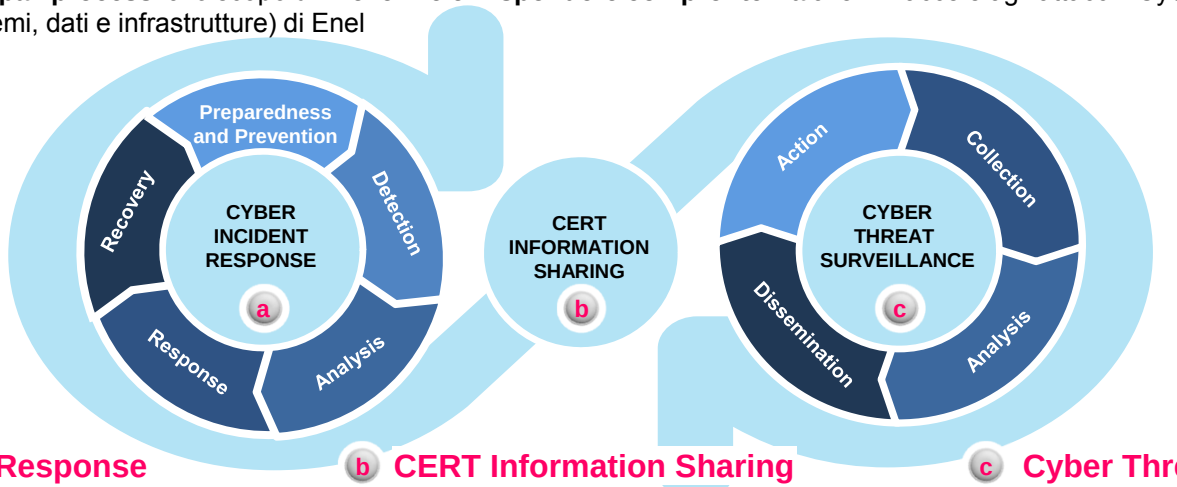
- Attivazione del **Comitato Gestione Emergenza** (locale e/o centrale e/o crisi)
- Attivazione delle **procedure di ripristino dell'operatività** su ciascuna Linea tecnica impattata
- **Identificazione del Referente** per la gestione della comunicazione con i Media
- Preparazione e distribuzione di **bollettini e/o aggiornamenti** periodici
- Partecipazione a gruppi di lavoro **con le Istituzioni** locali e/o centrali

4

# Gestione incidenti ed eventi critici

## Enel Cert

Enel CERT supporta **3 principali processi** allo scopo di **Prevenire e Rispondere con prontezza** alle minacce e agli attacchi Cyber rivolti alla **Constituency** (persone, sistemi, dati e infrastrutture) di Enel




### a Cyber Incident Response

Processo di **Prevenzione**, **Individuazione** e **Risposta** ai Cyber Incidents.
Aspetti chiave:

- **14 servizi** dal **Service Activation** al **Recovery & Lessons Learned**
- Comprensivo di tutti i **ruoli** e delle competenze multidisciplinari di Enel
- **Piena integrazione** con le **policy** Enel vigenti (Ad es. Emergency and Crisis Policy)

### b CERT Information Sharing

Processo per la **trasmissione certificata delle infomazioni** tra tutti gli **Stakeholders Interni** e relative **Controparti esterne.**
Aspetti chiave:

- CERT - Flusso di comunicazione e diffusione informazioni
- **Gestione della riservatezza** (Traffic Light Protocol)

### c Cyber Threat Surveillance

Processo di raccolta di **informazioni privilegiate** inerenti alle cyber-minacce ed agli attaccanti coinvolti, provenienti da sorgenti multiple: aperte, riservate e commerciali.
Aspetti chiave:

- Produzione di informazioni rilevanti ed utili al **Management** di Enel
- **Early detection** delle cyber-minacce con potenziale impatto per la Constituency di Enel.

4

# Gestione incidenti ed eventi critici

## Il ruolo del Security Manager

Il Security Manager definisce la procedura aziendale di crisis management e ne cura l'aggiornamento

Inoltre:

- predispone gli **strumenti tecnici e logistici** necessari per gestire le crisi (es. crisis room, sistemi di backup, ecc.)
- organizza periodiche **simulazioni** di un evento critico
- **contribuisce alla fase di valutazione** di un'emergenza
- **supporta il Vertice** nel dichiarare l'eventuale stato di crisi
- **partecipa al Comitato Emergenze**
- cura gli eventuali rapporti con le Forze dell'Ordine

**Ruolo del Security Manager**

4

# Gestione incidenti ed eventi critici

## Strumenti di supporto

### Cruscotto di Travel Security

- **Mappa interattiva di monitoraggio** delle trasferte che visualizza:
  - presenza di trasfertisti in base ai dati dell'agenzia viaggi ed alla geolocalizzazione, se attivata da App
  - **livello di rischio** dei paesi
  - **punti di interesse** (sedi Enel, aeroporti, stazioni, ambasciate, stazioni di polizia ecc.)
  - situazioni di pre-allerta in determinate zone o località
- **gestione di alert specifici** gestiti dalla Security Control Room relativi a situazioni di pre-allerta e messaggistica automatica verso il personale interessato
- **informazioni di dettaglio** relative ai trasferimenti (voli/treni ecc.), prenotazioni alberghiere ed itinerari interni di dettaglio

### Mobile App

**Aggiornamento itinerario** da parte del viaggiatore: es. in caso di mezzi di trasporto interni o alloggi non prenotabili con il sistema di prenotazione viaggi (GTM – Global Trave Management)

**Notifica di "warning"** di pre-allerta (es. manifestazioni, disordini vari ecc.);

**Lancio di SOS** in caso di emergenza


**Geolocalizzazione** mediante attivazione volontaria del tracciamento con GPS

**Gestione di chat e gruppi:** per il coordinamento delle operazioni di messa in sicurezza del personale in trasferta in situazioni di emergenza

**Messaggi ed informative** (Security Travel Guide, Security Vademecum, Health Guide)