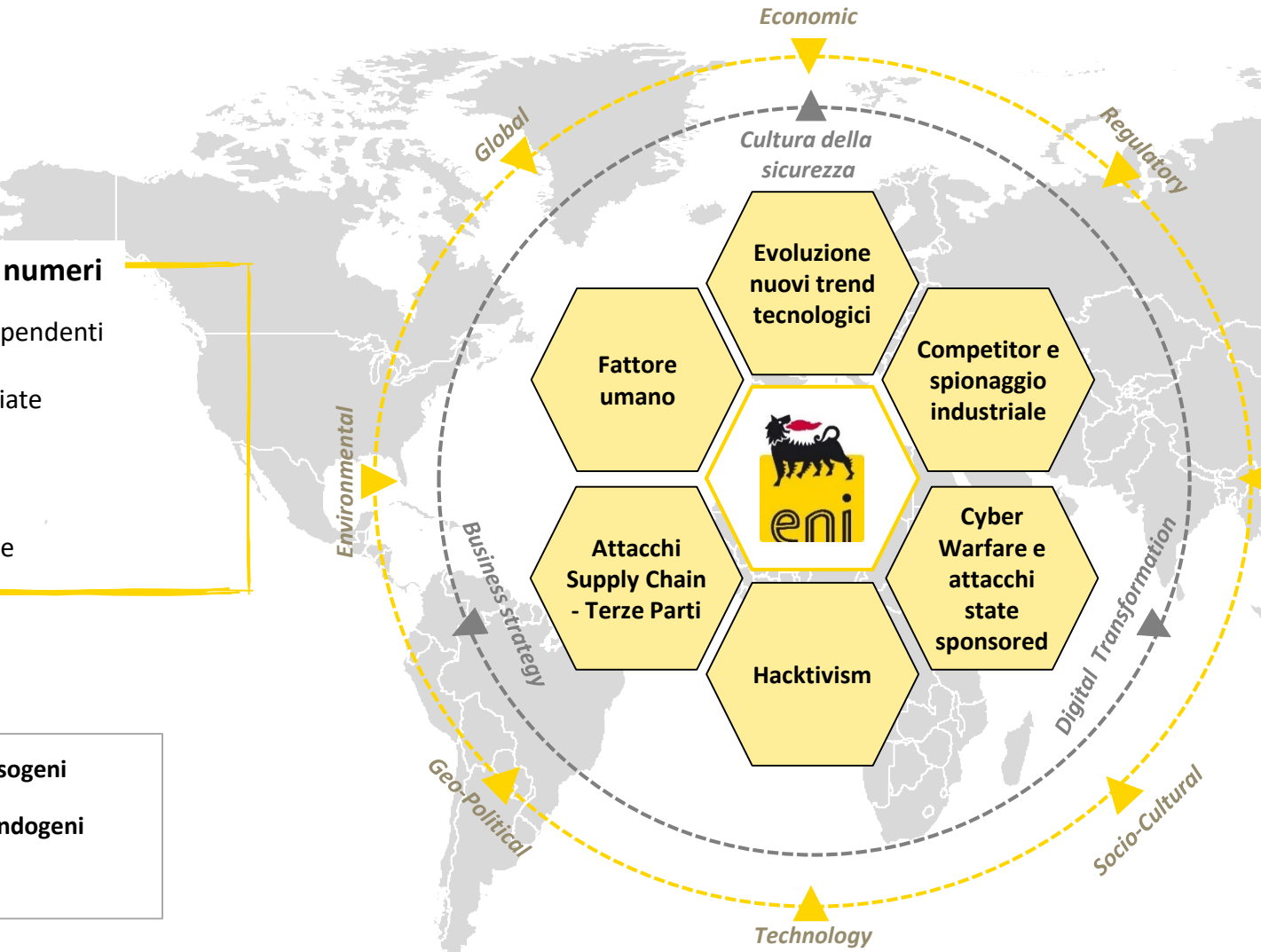
Cyber Security nelle Infrastrutture Critiche

Danno e Impatto nella Cyber Security: risposte di sistema

Roma, 20 Gennaio 2020

Contesto Eni – Panorama di minaccia e fattori endogeni ed esogeni

*Eni è una Energy Company che opera in 67 Paesi nel mondo. La presenza in **continenti** e **Paesi** differenti obbliga a fare uno **sforzo** ulteriore per **comprendere** il **contesto di minaccia** in cui Eni opera e i **principali fattori esogeni ed endogeni** che lo caratterizzano*



Eni in numeri

- ***31.000+*** dipendenti
- ***70+*** consociate
- ***67*** *Paesi*
- ***12*** Timezone

Eni gestisce e risponde ai rischi cyber, definendo una **strategia aziendale di "Cyber Defence" finalizzata a proteggere in maniera adeguata i numerosi asset che possiede in tutto il mondo**

Legenda

- **Fattori esogeni**
- **Fattori endogeni**
- **Minacce**

Contesto Eni – Complessità Tecnologica

*Lo scenario è caratterizzato inoltre dalla **complessità tecnologica** del contesto Eni che comporta il **monitoraggio** di un volume elevato di eventi*

~60.000 Mailbox

~10.000 Server

~500 Business Application

~7.000 Collegamenti Geografici

Il Green Data Center (GDC), ospita tutti i sistemi applicativi e le infrastrutture a servizio dei Business di Eni, ***in Italia e nel mondo***

Eventi di cyber security monitorati nel 2019*

Sorgenti	Cyber Security Monitoring		Cyber Security Incident
115 Miliardi Eventi di Cyber Security raccolti da **7.500** Sorgenti			
~500.000 Indicatori di compromissione gestiti	***~13.000*** Automatic Advanced Analysis and Response	***~4.000*** Security Investigation	***~500*** **Potenziali** Incidenti di Sicurezza
~1.000 Segnalazioni di minacce e report analizzati			

Incidente di sicurezza: evento o serie di eventi che coinvolgono uno o più sistemi della rete aziendale, e/o utenti, che comportino un **potenziale rischio (impatto) per la sicurezza fisica e/o informatica**

*Dati relativi al periodo Gennaio 2019 - Settembre 2019

La gestione del Rischio Cyber è parte integrante del framework aziendale

*La gestione di un **panorama** di **minaccia complesso** richiede un **approccio «risk-based»** alla Cyber Security che tenga in considerazione anche i diversi **vincoli normativi***

Eni governance on Risk and Compliance

ENHANCED GOVERNANCE ON RISK & COMPLIANCE

- Board
- Control and Risk Committee / Board of Auditors
- Chairman
- CEO
  - Risk Committee
  - Compliance Committee
  - Integrated Risk Management
  - Integrated Compliance

1° line	2° line	3° line
«Line» managers – risk owners	Risk & Control functions	Internal Audit

ENI TOP RISKS (2019)

- **20 Top risks** out of around 150 risks identified
- **Nearly 80 indicators** for top risks quarterly monitoring

Strategic Risks	Price scenario, Climate change, Stakeholder's relationship
External Risks	Country political & social instability
	Credit & Financial Risk
	Regulatory Evolution – HSE and gas & Power
Operational Risks	Blow out/accidents
	Investigations and legal procedures
	Cyber Security & other process risks

Top ten rischi operativi

Rischio di Cyber Security

La metodologia di Analisi Quantitativa del Rischio

La valutazione del rischio Cyber come passaggio da asset ICT centrico ad **approccio business centrico** secondo un approccio olistico

Approccio basato su capacità di **prevention** & **reaction**

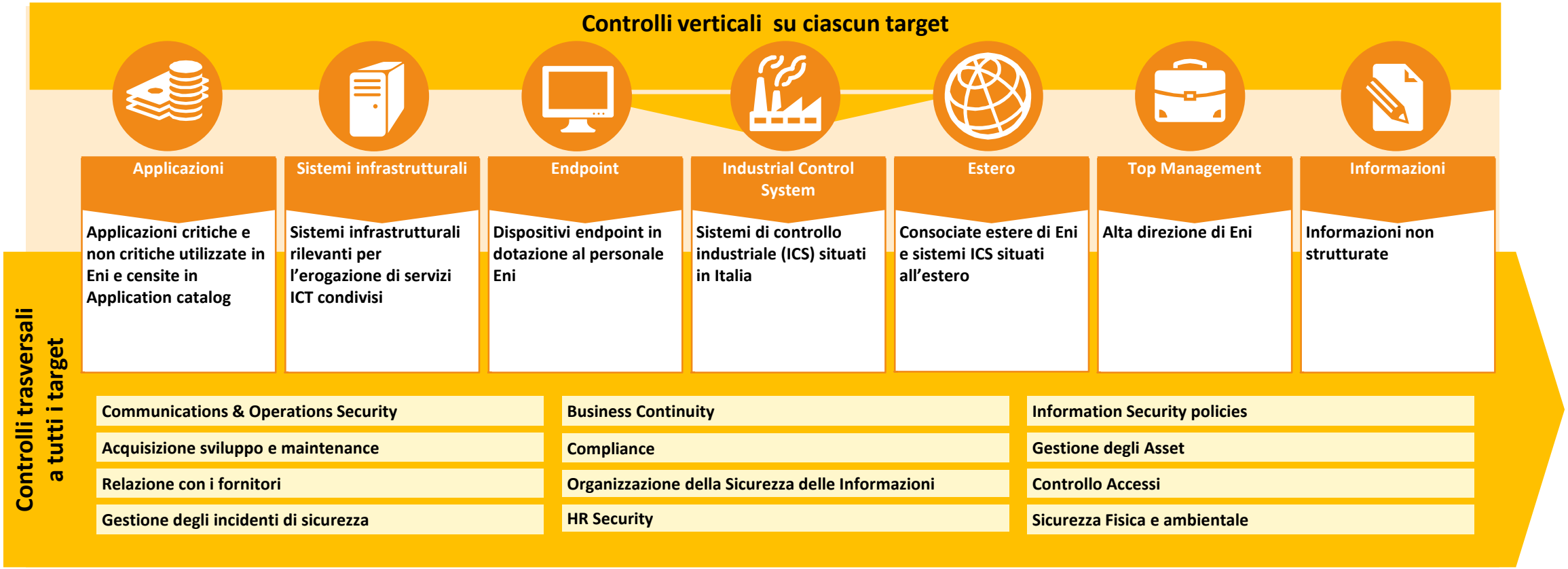
Riferimento a **best practices** e **Standard** Internazionali

Integra la dimensione "**People**" nella valutazione

Evoluzione verso una **valutazione quantitativa** del Rischio Cyber business oriented

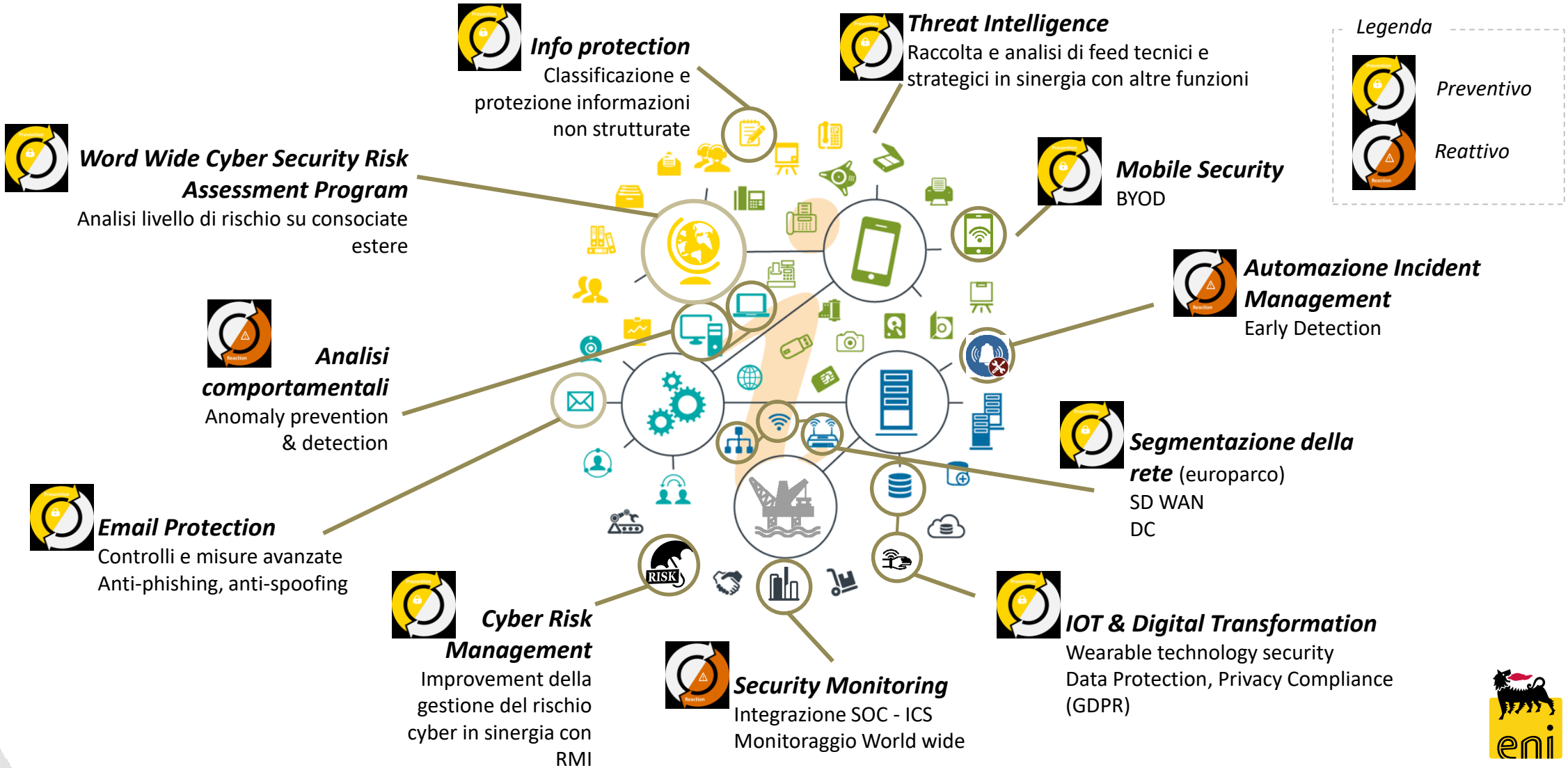
Il Sistema di Gestione della Sicurezza delle Informazioni di Eni

*Il **Sistema di Gestione della Sicurezza delle Informazioni** (SGSI) adottato da Eni consente di **implementare un approccio risk-based** per la gestione delle iniziative in ambito ICT Security*



Il Piano di Gestione della Sicurezza in Eni – Processi e Tecnologie

*Eni indirizza i **rischi** individuati attraverso diversi **interventi di processo** e **tecnologici***



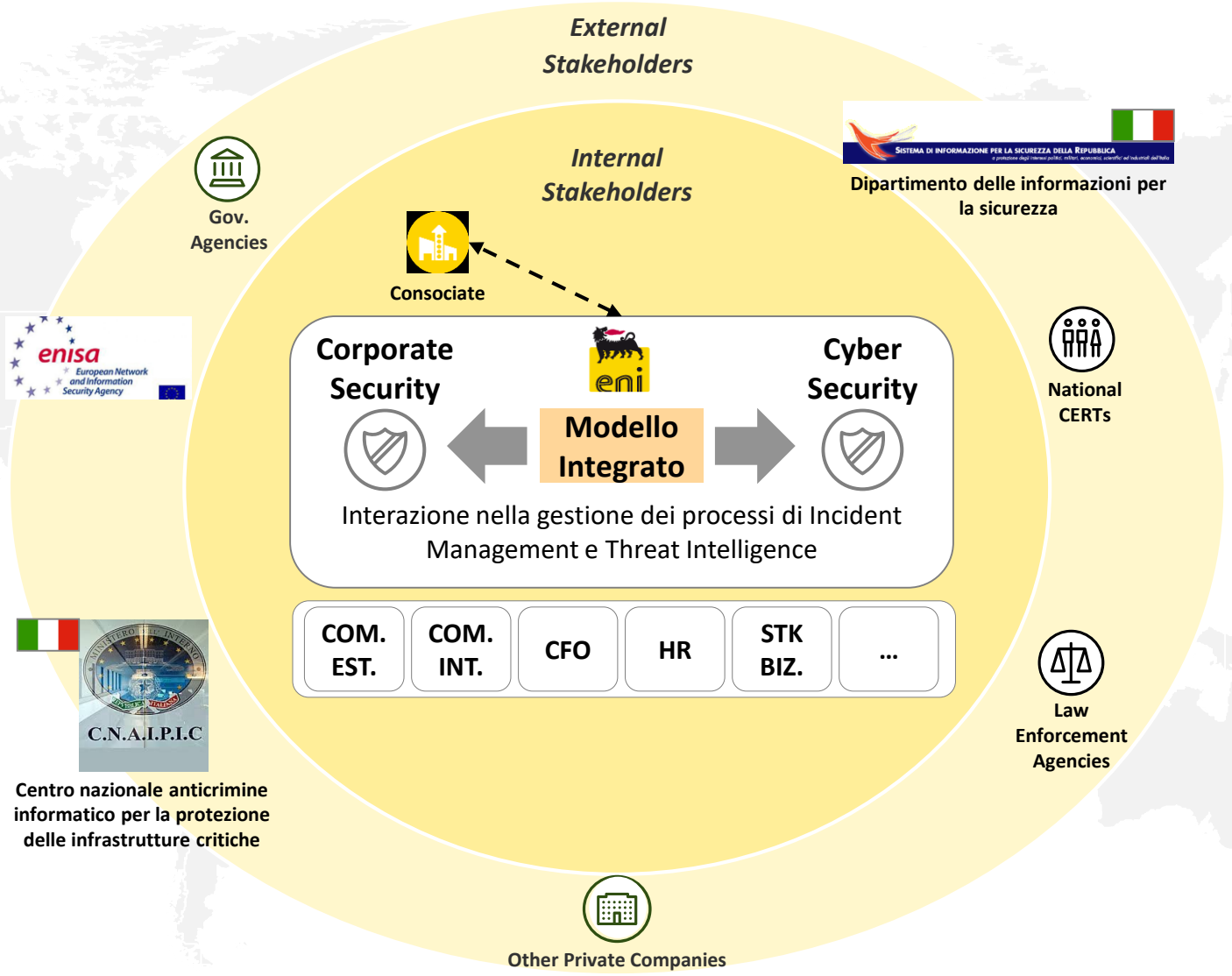
Gli interventi in ambito Operational Technology (OT)

*In particolare Eni interviene con **iniziative** focalizzate al **rafforzamento** della **Cyber Security** all'interno degli **impianti industriali***

Driver	Contesto	Principali interventi di Cyber Security
Enterprise Business Site Business Zone	**Servizi a supporto** del corporate business e delle persone	• **Servizi di monitoraggio preventivo e gestione degli incidenti** da parte del Security Operation Center • **Policy e procedure** i processi corporate business • Campagne di **sensibilizzazione al rischio cyber** specifiche per il mondo industriale
Interazioni Esterne	**Servizi condivisi** (email, Internet, Cloud…)	• Disaccoppiamento dei sistemi che risiedono in ambienti diversi per **evitare le connessioni dirette dal mondo esterno**
Sistemi di Fabbrica Supervisione sistemi OT Normative Nazionali	**Gestione e conduzione** dei **processi di produzione industriale**	• **Enforcing di sicurezza informatica delle workstation** presenti nelle reti industriali per evitare l'infezione da malware • **Gestione delle identità e degli accessi** in accordo con il principio di segregation of duties e need to know • Processo di interazione tra il Security Operation Center – Operational Control Room • **Monitoraggio Passivo del traffico di rete** a supporto dei sistemi di detection e correlazione • **Policy e procedure** specifiche per i processi che potrebbero esporre al rischio cyber gli ICS

Il modello integrato della Cyber Security ed il rapporto con le Istituzioni

*La **Cyber Security** in Eni ricopre un ruolo **cruciale** per la **sicurezza** degli **asset** e dei **dipendenti** in tutti i paesi in cui l'azienda opera*



Il Programma di Cyber Security Culture Eni

*La Cyber culture è uno dei **fattori chiave della strategia** di sicurezza informatica, l'obiettivo è **diffondere i giusti comportamenti** e le **azioni** a tutta la popolazione Eni*

Corsi On-line e Workshop dedicati

- 12.000 partecipanti in Italia, 1.700 corsi erogati all'estero
- Sessioni in aula rivolte a specifiche famiglie aziendali

Awareness per Top Management

Campagne di awareness e sessioni per assistenti

Cyber Tips & Alert intranet Eni

Uscite mensili con 4/5 topic di sicurezza ciascuno, più rassegna stampa

Esercitazioni di phishing

Campagne di Phishing periodiche

Security Week per consociate estere

Security Week con ICT Manager provenienti dalla maggior parte dei paesi in cui opera Eni

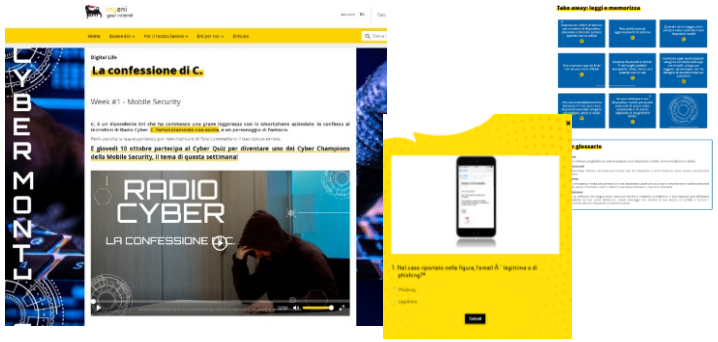
Cyber Security Month

Mese intero rivolto ad iniziative a tema Cyber Security

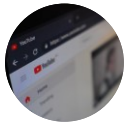
Cyber Security 4 Kids

Cyber Security Culture Program

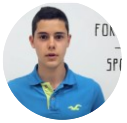
Cyber Security Month – Ottobre 2019



Cyber Security 4 Kids



Scalabilità



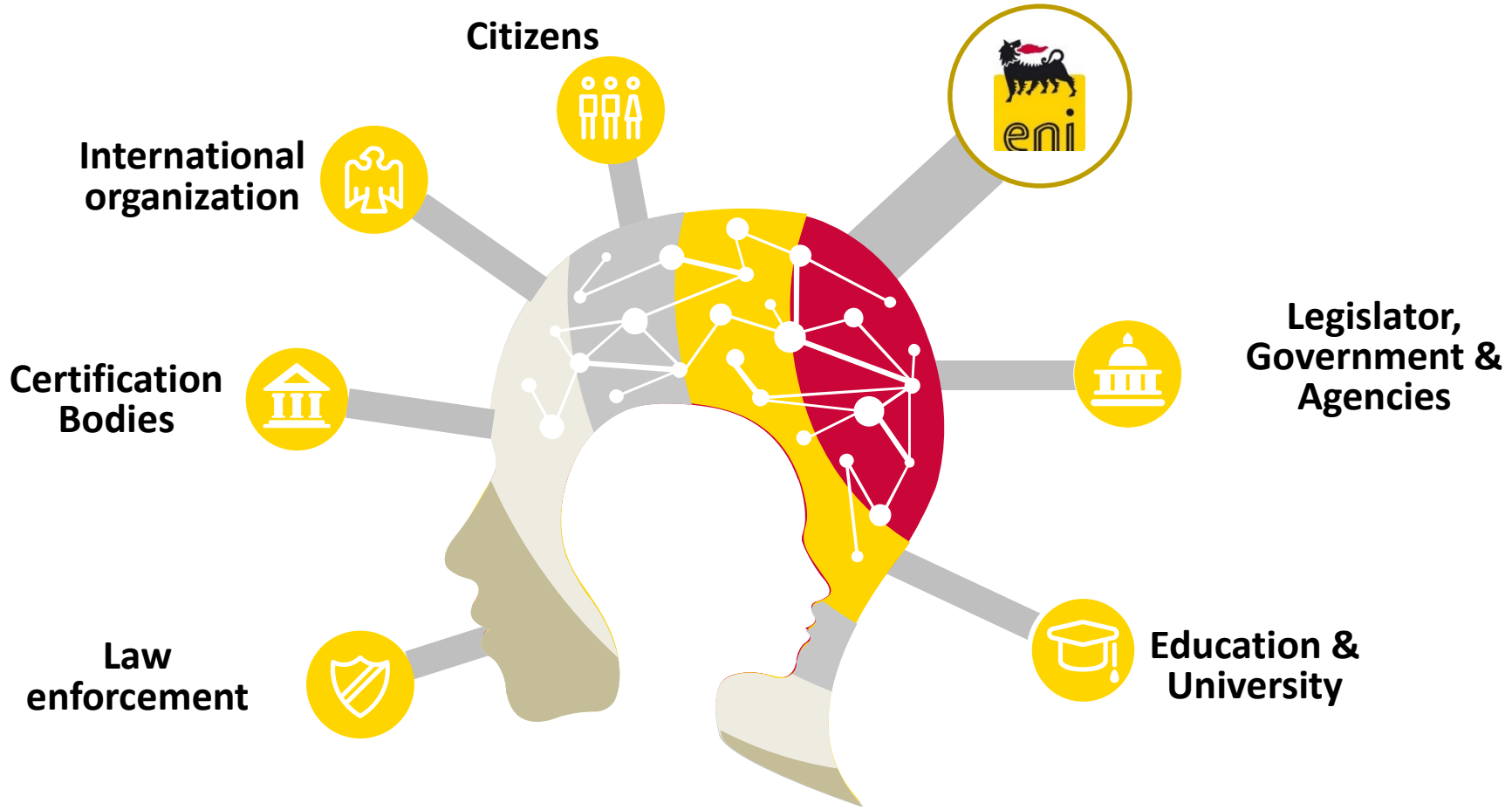
Engagement

Efficacia

*Promuovere la **cultura digitale sicura** e **consapevole** in coerenza con altre iniziative **Eni** su **sostenibilità** ed **impegno sociale***

L’importanza degli stakeholder per Eni

*Eni **collabora** attivamente con diversi **stakeholder pubblici** e **privati** nel corso delle proprie **attività di business***



Eni crede pertanto nella **collaborazione con** le diverse **Istituzioni** ed **aziende** finalizzata anche a **costruire un ecosistema informatico realizzabile** e **sostenibile**

Possibili spunti di miglioramento per la Community

*Un **ruolo** sempre più **centrale** delle **Istituzioni** per **supportare** la **crescita nazionale** in materia di **Cyber Security***

1. **Sviluppo** delle capabilities nazionali, anche attraverso la promozione e **incentivazione** dell'**industria** Cyber **italiana**

2. **A**dozione diffusa di **soluzioni innovative** e applicazione del principio di **security by design**

3. Crescita della **maturità** cyber delle **imprese**, delle infrastrutture critiche e dei **cittadini**

ANNEX

Le leggi (inter)nazionali in ambito Cyber

*La gestione di un **panorama** di **minaccia complesso** richiede un **approccio «risk-based»** alla Cyber Security che tenga in considerazione anche i diversi **vincoli normativi***

I D.lgs. n. 231/2001 disciplina in alcuni articoli specifici le responsabilità per le società relativamente a "Delitti informatici e trattamento illecito di dati"

Il **Nuovo Regolamento sulla protezione dei dati personali** definisce i **principi** e le **regole** da seguire per la corretta gestione dei dati personali

Attuazione della Direttiva NIS (Network and Information Security) riguardante la sicurezza dei sistemi, delle reti e informazioni

Cybersecurity Act: rafforzare la resilienza dell'Unione agli attacchi informatici, a creare un mercato unico della sicurezza cibernetica in termini di prodotti, servizi e processi

Legge **n. 133 del 18 novembre 2019:** Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica