

Poste Italiane

Impegno nella Cyber Security

Sicurezza delle Informazioni

Ing. Rocco Mammoliti

Agenda

1

Gruppo Poste Italiane

2

Ecosistema di Cyber Security di PI

2.1

Cyber Security Innovation Lab

2.2

CERT di Poste

2.3

Distretto di Cyber Security

3

CERT REGIONALE

4

Poste per la collaborazione Pubblico - Privato



230 mila pacchi movimentati giornalmente

540 articolati
5 aerei

38.000 mezzi
3.800 corrieri

Primo Operatore Postale in Italia
con oltre 15 mln di lettere
movimentate giornalmente



Posteitaliane

13.000 Uffici postali
7.000 ATM
700 Chioschi multimediali



**400 mld € di Risparmio degli Italiani
gestito**

2 mln di conti on line



50 mln di operazioni al giorno

19 mln di Carte di pagamento
di cui 12 mln prepagate
Postepay prima carta Prepagata in Europa



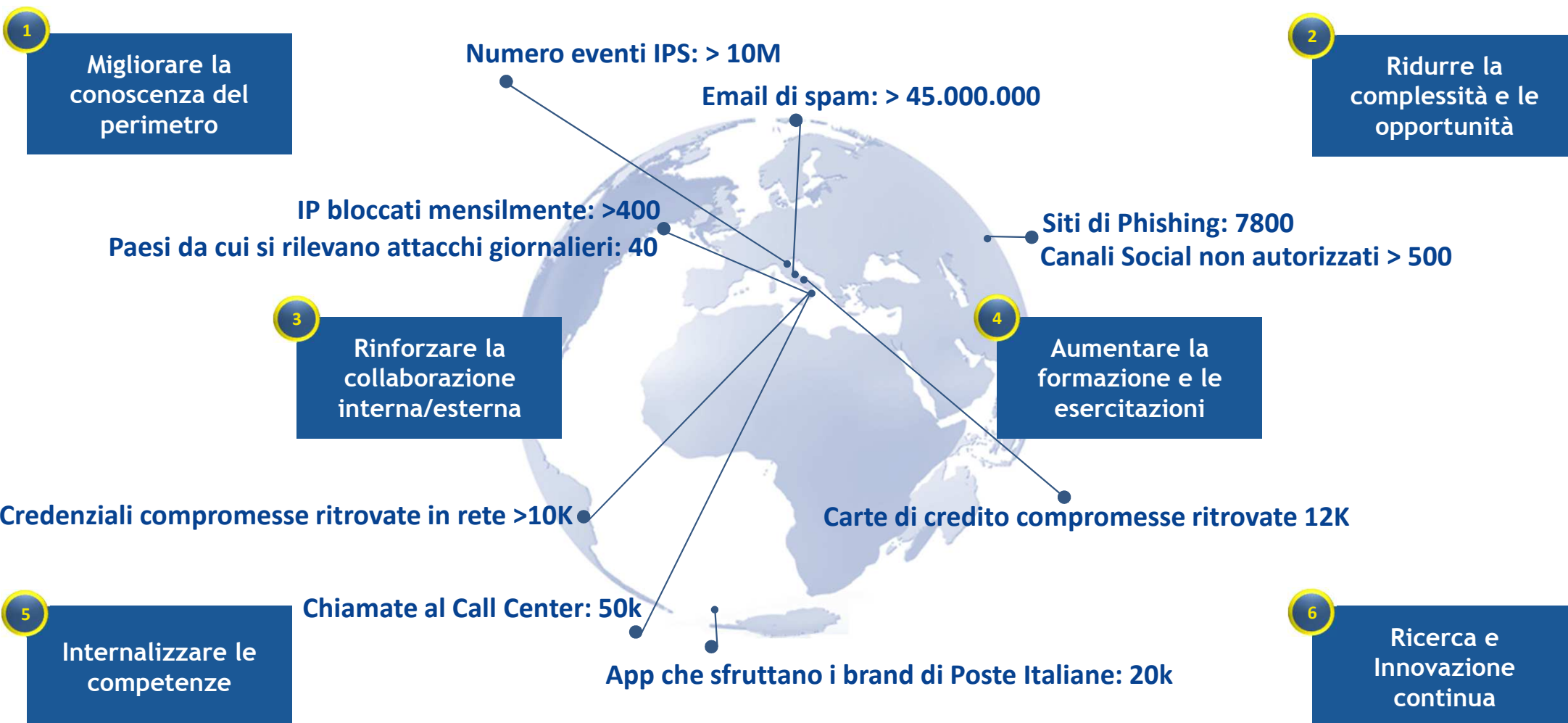
**Ai vertici del mercato Vita in Italia
con 13,2 mld € di Premi Vita raccolti
nel 2013**

Postevita

Posteitaliane

Il contesto tecnologico e di sicurezza di Poste Italiane è caratterizzato da complessità, dimensioni elevate, forte variabilità tecnologica.

Risposta: «Attuazione dei Principi Generali per una corretta Governance della Sicurezza delle Informazioni»



Il Cyber Security Innovation Lab nasce dalla collaborazione tra Poste Italiane e l'ecosistema di Trento per costruire un centro di eccellenza per lo sviluppo di innovazione scientifica e tecnologica



Data inizio Progetto: 01/01/2014



Laboratorio e risorse condivise PI - Trento

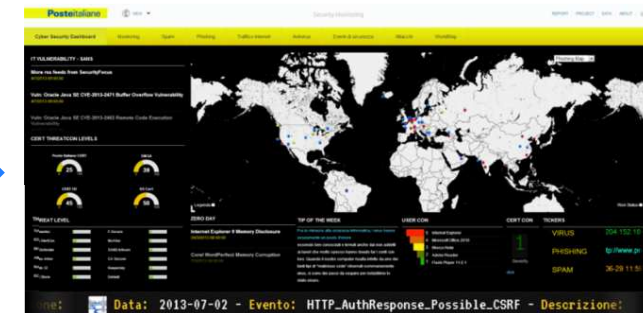
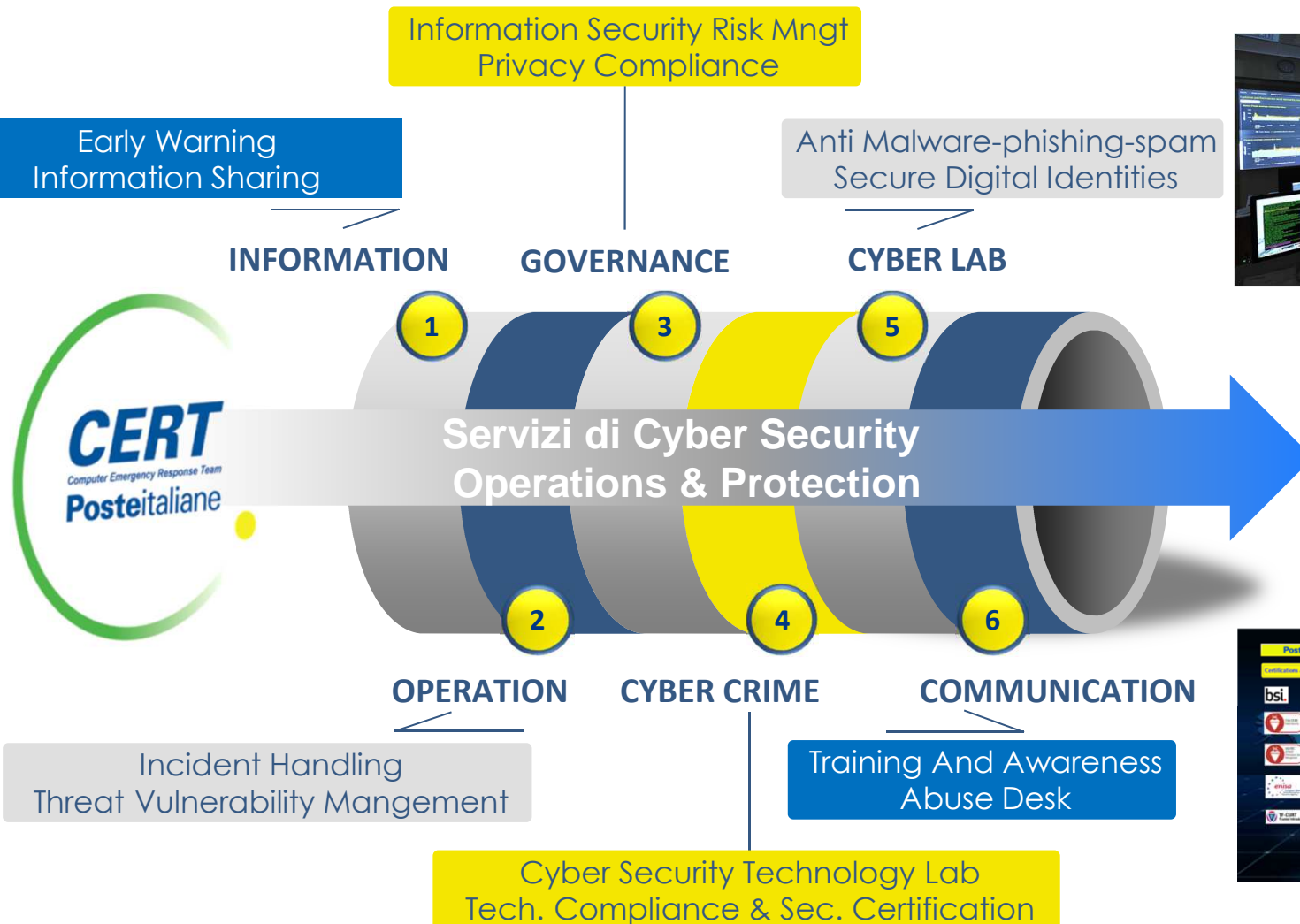


**Mobile Security, Future CERT,
Secure Digital Identity, E2E Encryption**

Benefici

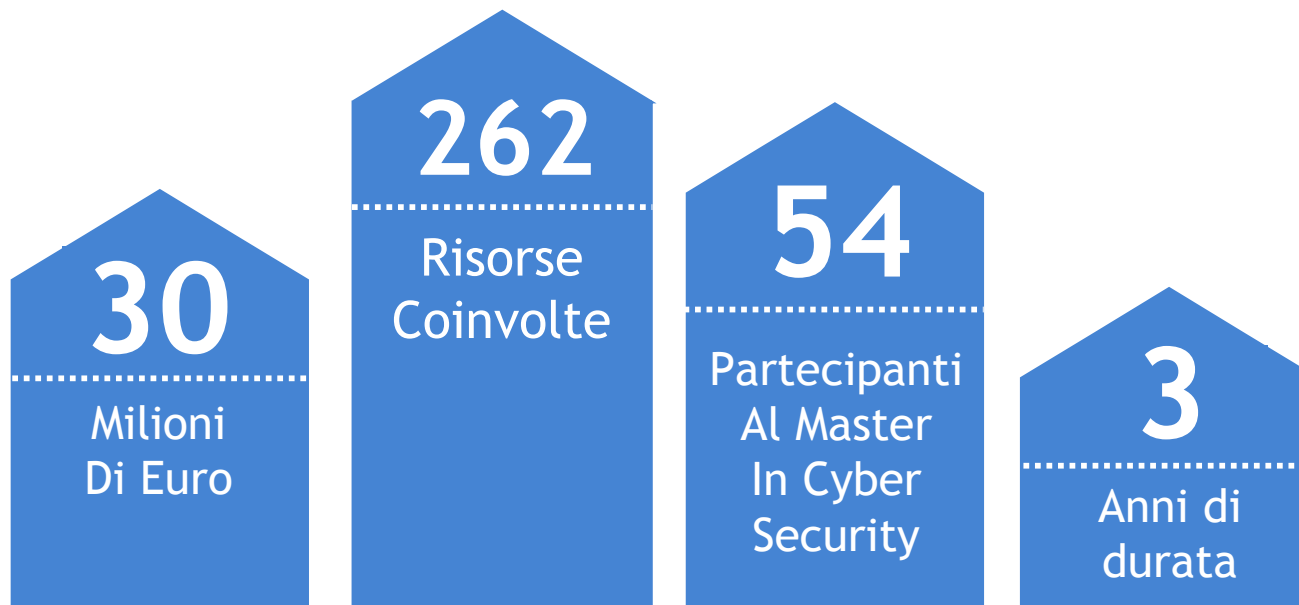
- ☑ Ricerca e innovazione applicata in ambito mobile security e gestione sicura delle identità digitali
- ☑ Partecipazione a programmi locali, nazionali ed europei per il finanziamento della ricerca
- ☑ Partecipazione al programma Horizon 2020
- ☑ Recupero di investimenti e costi per la realizzazione di soluzioni innovative di Cyber Security

Il CERT di Poste Italiane è organizzato su 6 macro stream di servizi di sicurezza, collaborando con molteplici realtà ed organizzazione in ambito sicurezza. Tra le attività di scambio informazioni si evidenzia l'accreditamento con il **FIRST**, la collaborazione con **ENISA** e con la **Task Force Trusted Introducer**, oltre a iniziative quali **OF2CEN** e **EECTF**.





L'obiettivo del Distretto Tecnologico è quello di creare una piattaforma territoriale localizzata in Calabria, nell'Area di Cosenza, e specializzata nell'ambito della Cyber Security, contribuendo così allo sviluppo e all'aumento della competitività delle imprese del Distretto e, più in generale, del sistema economico calabrese e nazionale.



Posteitaliane

NTT DATA



UNIVERSITÀ
DELLA CALABRIA

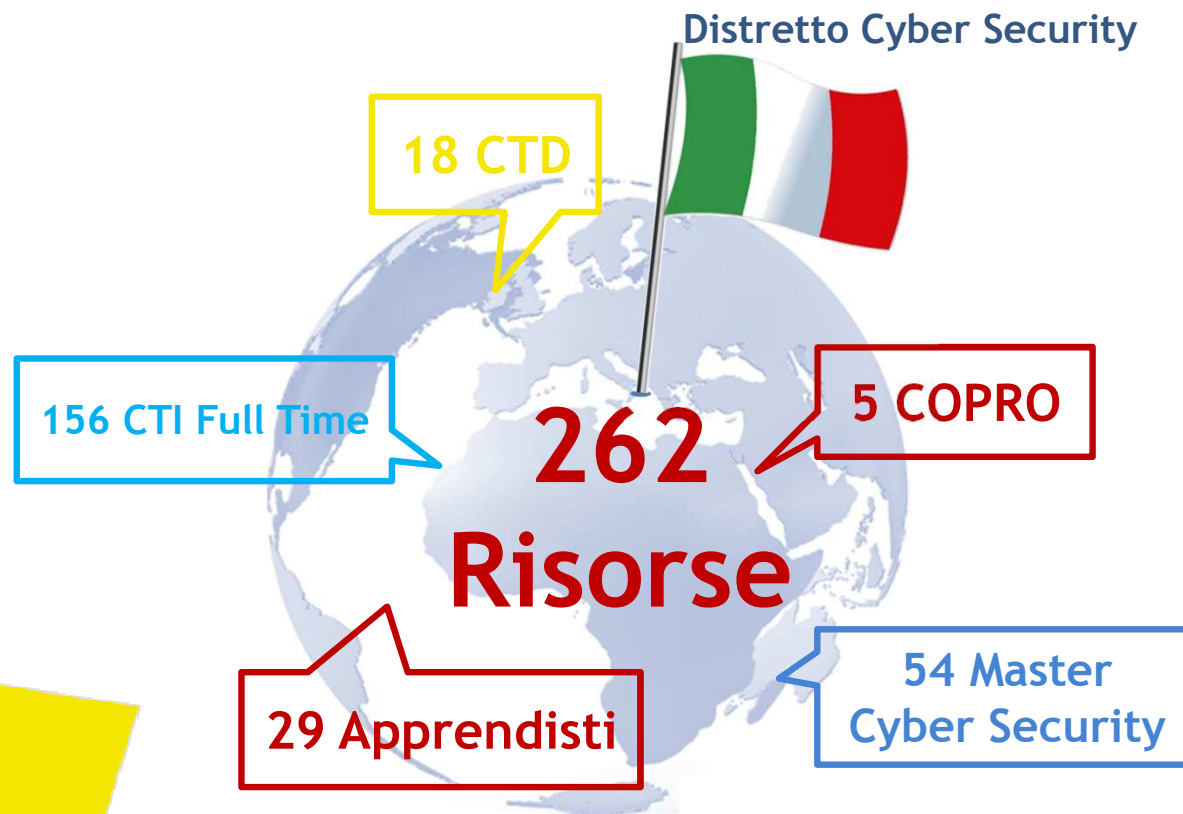


Università degli Studi
Mediterranea
di Reggio Calabria



Distretto di Cyber Security

« Una opportunità di sviluppo tecnologico, cultura, economico e sociale a livello territoriale nazionale »



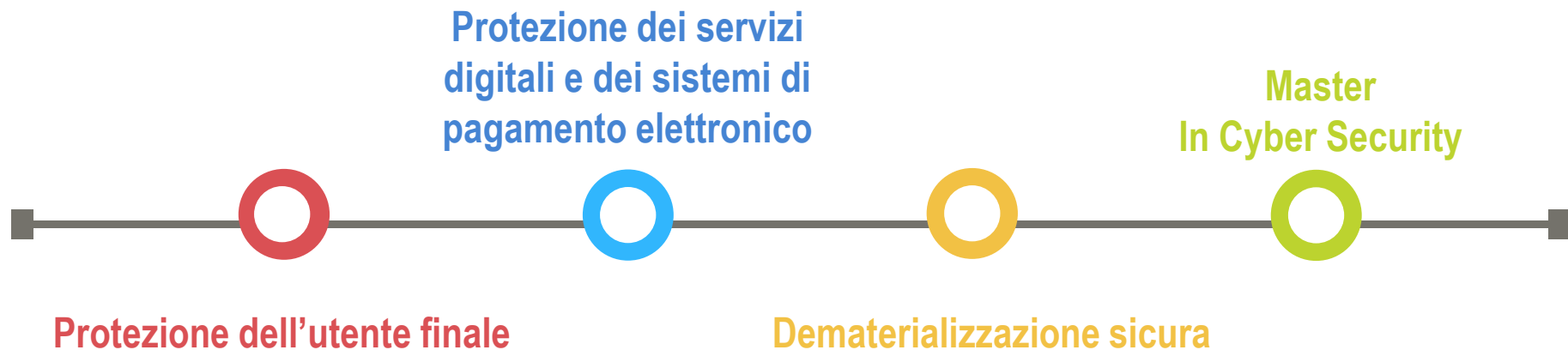
Impatti sul sistema economico territoriale 1

2 Sviluppo complessivo del Know how sul territorio

3 Benefici sul cliente finale pubblico e privato

4 Impatti sulle imprese partner dell'iniziativa

Sviluppo Industriale, Innovazione, Ricerca e Formazione per costruire il Futuro



L'Indirizzo Operativo 5 al punto 5.1 c prevede di favorire la creazione di CERT Regionali con il compito di supportare le Pubbliche Amministrazioni Locali del territorio e di implementare regole e modelli organizzativi nazionali

Indirizzi Operativi del Piano Nazionale

- 1 Potenziamento delle capacità di intelligence, di polizia e di difesa civile e militare
- 2 Potenziamento dell'organizzazione e delle modalità di coordinamento e di interazione a livello nazionale
- 3 Promozione e diffusione della cultura della sicurezza informatica. Formazione e Addestramento
- 4 Cooperazione internazionale ed esercitazioni
- 5 Operatività del CERT nazionale, del CERT-PA e dei CERT dicasteriali
- 6 Interventi legislativi e compliance con obblighi internazionali
- 7 Compliance a standard e protocolli di sicurezza
- 8 Supporto allo sviluppo industriale e tecnologico
- 9 Comunicazione strategica
- 10 Risorse
- 11 Information Risk Management Nazionale

Il sistema di protezione civile si basa sul principio di sussidiarietà. «Prima risposta» all'emergenza deve essere garantita a livello locale. Quando un evento non può essere fronteggiato con i mezzi a disposizione del comune, si mobilitano i livelli superiori attraverso un'azione integrata: Provincia, Prefettura, Regione, Stato.

Sistema Italia PA



Poste Italiane



CERT operativo ed accreditato a livello internazionale, unica realtà italiana;



Presenza capillare su tutto il territorio nazionale



Capacità di erogare servizi digitali e servizi di e-government per la PA, più in generale per il sistema paese, per i quali è una ritenuta terza parte di fiducia



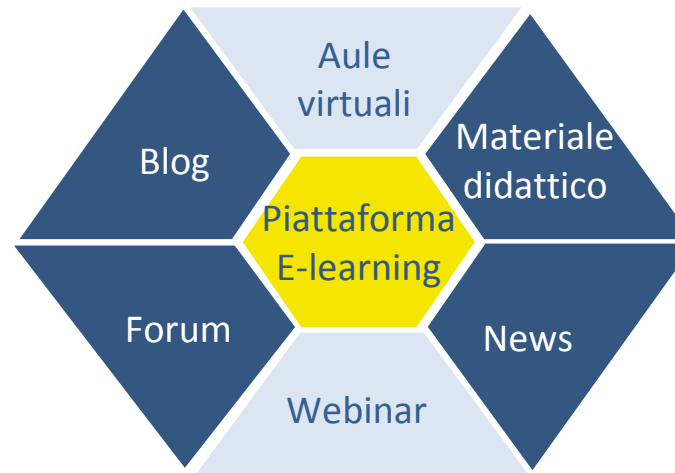
Infrastrutture materiali e immateriali, know how e personale altamente qualificato

Knowledge Skill Ability Assessment module



- 2 modelli di valutazione:
 - Modulo light per i cittadini
 - Modulo evolution basato sul NIST per i professionisti
- Possibilità di analisi statistiche in termini di
 - Età/sex
 - Formazione
 - ...
- Domande multi-livello con assegnazione di ranking personale o di gruppo
- 5 categorie di domande per i cittadini (Social network, Email, E-payment, Smartphone, Internet)
- Più di 2.300 domande basate sui 780 KSA del NICE per i professionisti nella versione evolution

Knowledge Skill Ability Continuous Enhancement module



- Piattaforma a supporto dell'erogazione di:
 - Master di formazione sulla cyber security
 - Corsi di formazione generali sulla cyber security
 - Corsi basati sul modello NICE
 - Possibilità di lavorare su progetti di formazione e ricerca congiunti con altri partner
 - Completa di strumenti per la virtualizzazione totale di una classe di formazione

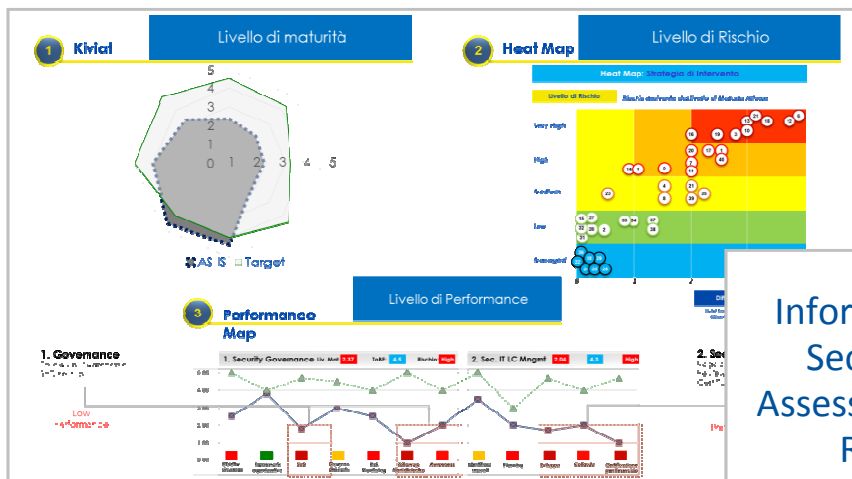
Simulation & Exercise module



- Replica di servizi digitali attraverso la riproduzione della catena tecnologica a supporto
- Possibilità di esercitazioni di attacco e difesa sui servizi replicati (es. Sistemi di pagamento, infrastruttura aziendale,...)
- Possibilità di esercitazioni su servizi interconnessi
- Test bed per nuove tecnologie

Poste Italiane ha sviluppato piattaforme innovative per la protezione del proprio business che sono di assoluto valore aggiunto anche ad altri stakeholder pubblici e privati quali ad esempio i CERT Regionali

Information Security Assessment & Risk Mgmt



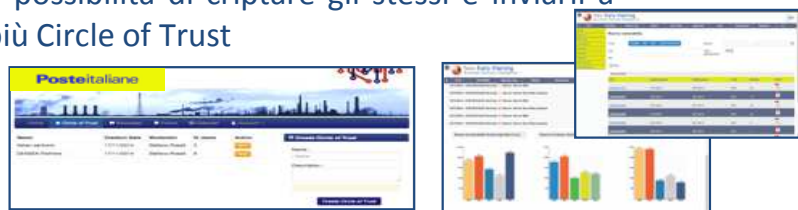
Formazione ed esercitazione

Piattaforma per le simulazioni (serious game) per testare le reali competenze delle risorse attraverso ambienti simulati virtuali, valutare il dimensionamento dei team di security e svilupparne le competenze



Early Warning, Information Sharing

Early Warning associa automaticamente minacce e vulnerabilità agli asset e ne valuta la criticità ed i livelli di alerting. Piattaforma per Info sharing condivide le informazioni, con codifica dei messaggi (TLP) e possibilità di criptare gli stessi e inviarli a più Circle of Trust



Information Security Assessment & Risk Management

Capability Development

Early Warning Information Sharing

Formazione Awareness

Sensibilizzazione del cittadino

Web app e Demo in grado di testare le conoscenze di sicurezza informatica sia di semplici cittadini





PRIMO IT CONTEXT ITALIANO DI CYBER SECURITY
ITA CYBER RANGE

3 GIORNI
DI FULL IMMERSION IN AMBIENTI REAL-LIKE

SOC CERT
CSIRT CYBERSECURITY CAPABILITIES CHALLENGER

SALITE SUL PODIO
DEI TALENTUOSI

PREMI PER I PRIMI 3 CLASSIFICATI

INFO & REGISTRAZIONI
[HTTP://CYBERRANGE.IT](http://cyberrange.it)

Il Context permette di misurare e perfezionare le proprie competenze in un ambiente sicuro, etico/legale e realistico, proponendo esercitazioni real-like derivanti da attività reali di sicurezza. Per ogni ambito saranno proposti scenari a difficoltà crescente. Le tipologie di esercitazioni e interazioni con il Cyber Range sono aderenti al framework dello United States - National Initiative for Cybersecurity Education orientato a classificare i compiti tipici e le competenze richieste dagli addetti IT in diverse macro aree in ambito sicurezza informatica.

INCIDENT ANALYSIS
MALWARE ARTIFACT
PENETRATION TESTING
MOBILE SECURITY
FORENSIC ANALYSIS

Partners:

Des Distretto Cyber Security, Posteitaliane, GLOBAL CYBER SECURITY CENTER, UNIVERSITÀ DELLA CALABRIA, CERT, ICTfirst, trentorise, CIS SAPIENZA

WISH : First Italian CyberSecurity Incubator

Credere e supportare nuove idee ed iniziative per una «secure humanity»



Technology Based Incubator

Wish è il primo acceleratore di cyber-sicurezza italiano, con sede nel Distretto Cyber Security di Cosenza.

Crossroad of Innovation

Wish supporta l'avvio di imprese che sviluppino prodotti e servizi tecnologici di sicurezza attraverso servizi logistici, di accelerazione e supporto al mercato.

Call for Action

GRAZIE!

Ing. Rocco Mammoliti

Responsabile Sicurezza delle Informazioni

Poste Italiane S.p.A.

mammoliti.rocco@posteitaliane.it

