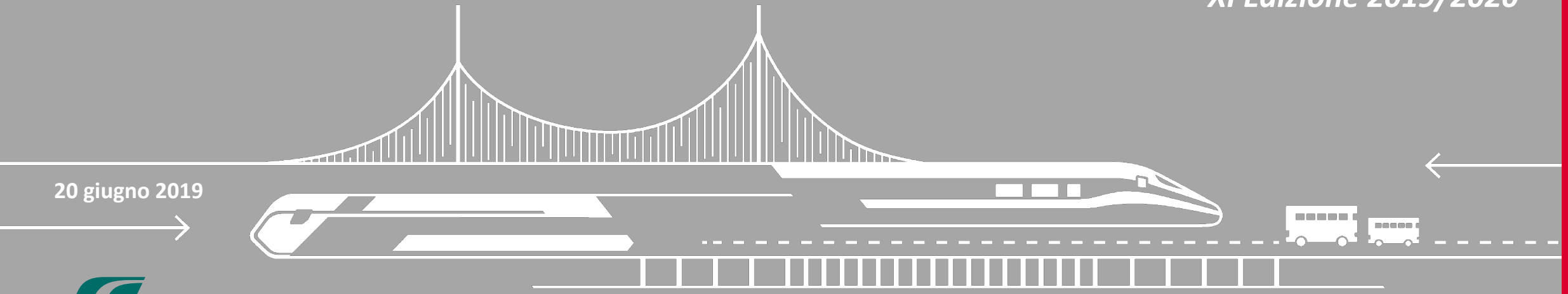
La Cyber Security nel Gruppo FS

Cyber Security e Sicurezza Nazionale

Master Homeland Security
XI Edizione 2019/2020



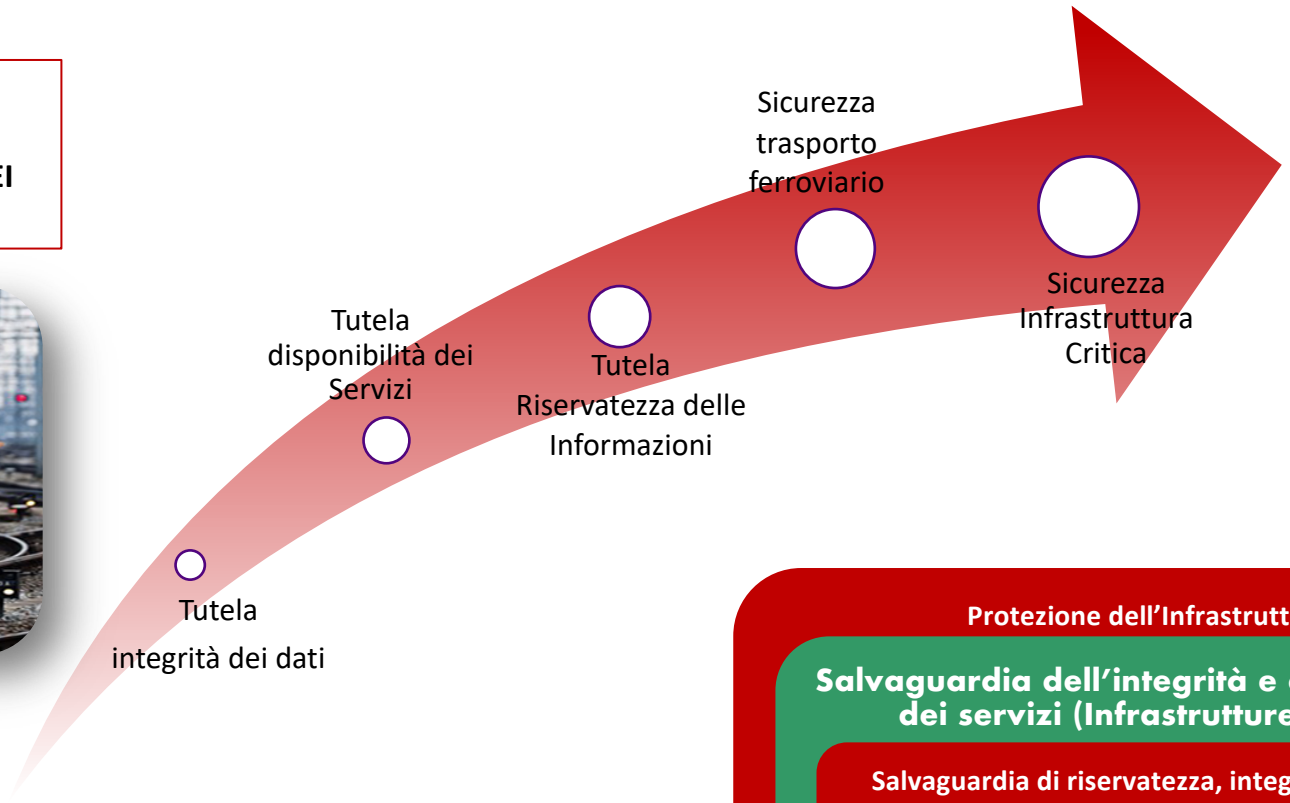
20 giugno 2019

FERROVIE DELLO STATO ITALIANE

Il sistema ferroviario come Infrastruttura Critica

La tutela delle infrastrutture critiche attraverso la protezione delle informazioni

LA **TUTELA DELLE INFRASTRUTTURE CRITICHE** PASSA ATTRAVERSO LA **PROTEZIONE DELLE INFORMAZIONI E DEI SISTEMI INFORMATIVI**



Protezione dell'Infrastruttura Critica

Salvaguardia dell'integrità e della disponibilità dei servizi (Infrastrutture e Trasporti)

Salvaguardia di riservatezza, integrità e disponibilità delle informazioni

Sicurezza informatica (*Cyber Security*)

Contesto Normativo

D.Lgs. del 18 maggio 2018 n. 65 - Attuazione Direttiva NIS 2016/1148

Obiettivo: Definire le misure necessarie a conseguire un elevato livello di sicurezza delle reti e dei sistemi informativi degli Operatori di Servizi Essenziali (OSE) e dei Fornitori di Servizi Digitali (FSD).

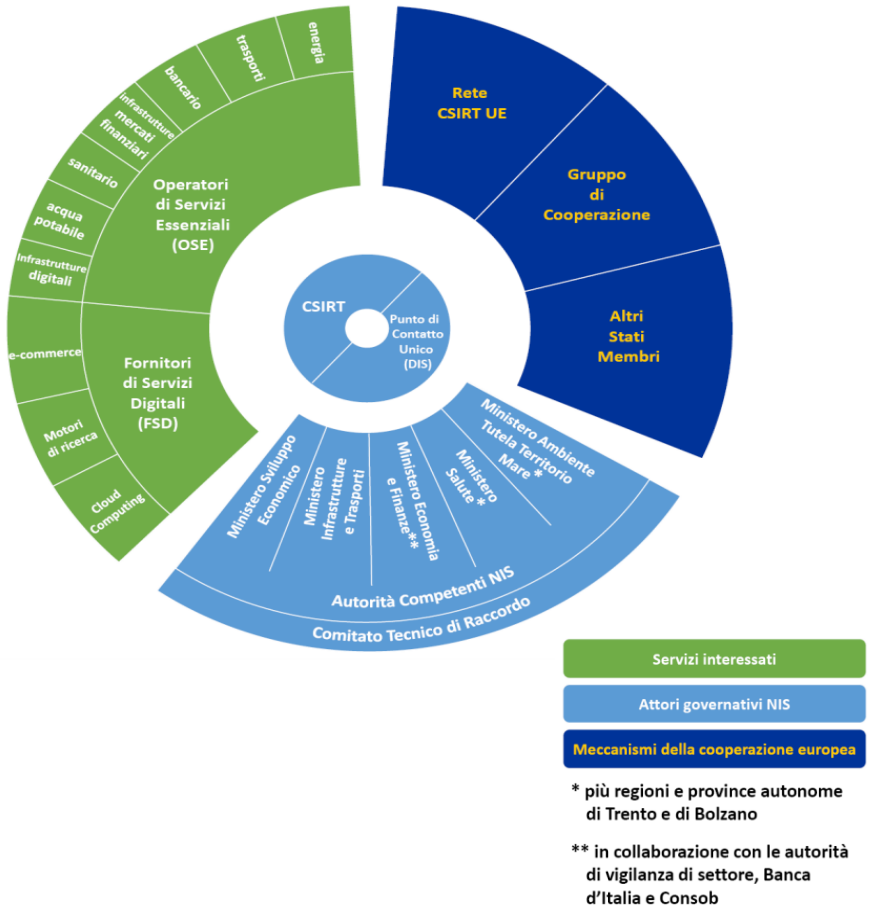
Gli OSE sono i soggetti, pubblici o privati, che forniscono servizi essenziali per la società e l'economia nei settori sanitario, dell'energia, dei trasporti, bancario, delle infrastrutture dei mercati finanziari, della fornitura e distribuzione di acqua potabile e delle infrastrutture digitali

Tanto gli OSE che gli FSD:

- sono chiamati ad adottare misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi e a prevenire e minimizzare l'impatto degli incidenti a carico della sicurezza delle reti e dei sistemi informativi, al fine di assicurare la continuità del servizio;
- hanno l'obbligo di notificare, senza ingiustificato ritardo, gli incidenti che hanno un impatto rilevante, rispettivamente sulla continuità e sulla fornitura del servizio, al *Computer Security Incident Response Team* (CSIRT) italiano, informandone anche l'Autorità competente NIS di riferimento.

IL **GRUPPO FS** È STATO IDENTIFICATO DALLE AUTORITÀ COMPETENTI TRA GLI **OPERATORI DI SERVIZI ESSENZIALI** (OSE)

Attori

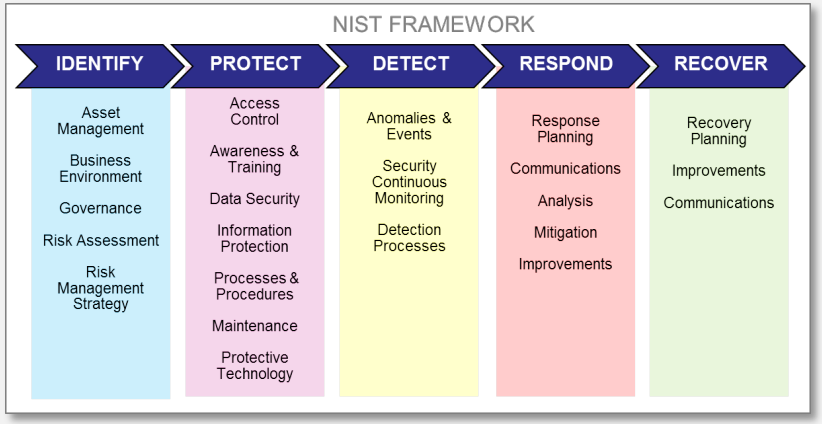


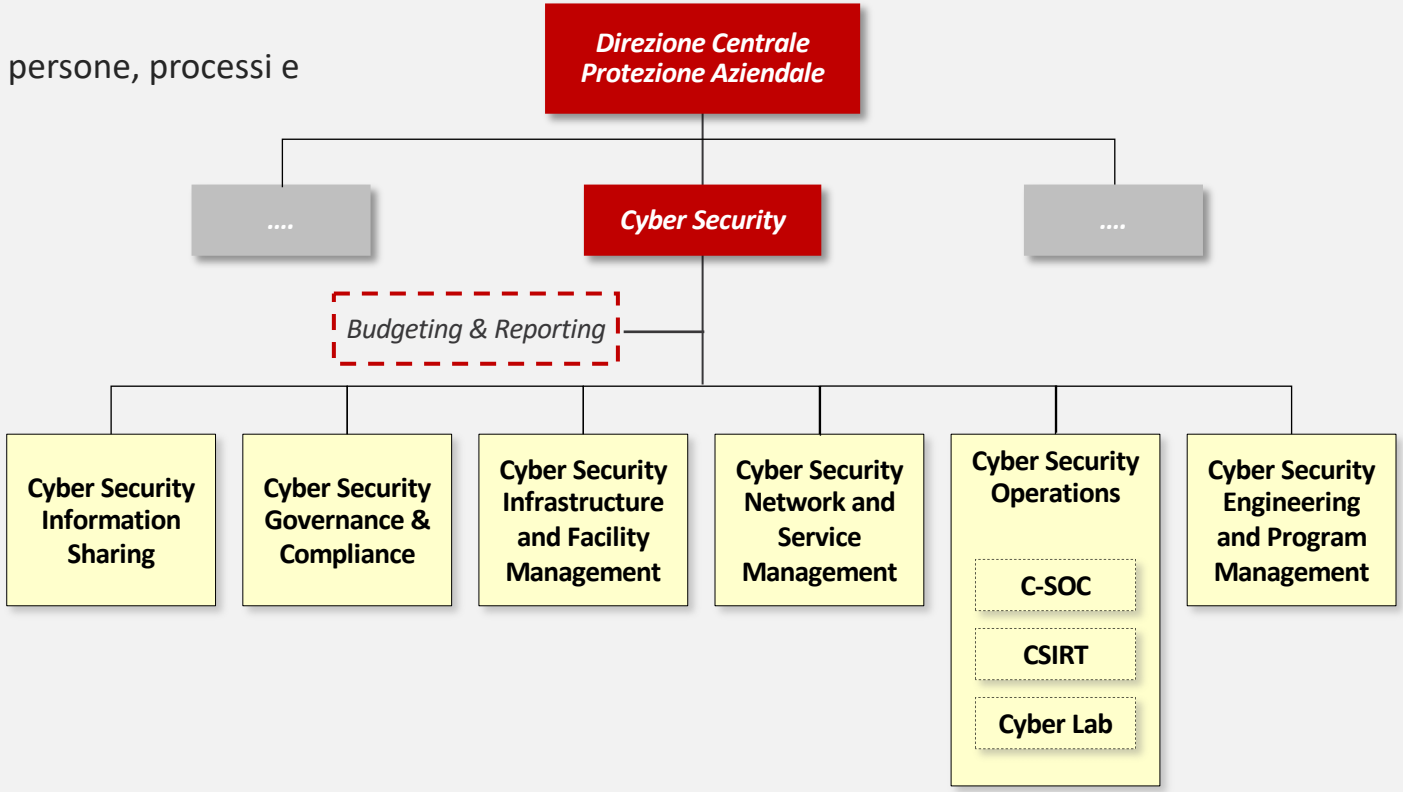
Approccio Cyber Security Gruppo FSI

Struttura Organizzativa

Di seguito è rappresentata la struttura odierna di Cyber Security all'interno della Direzione Centrale Protezione Aziendale (DCPA) basata sul framework NIST (National Institute of Standards and Technology of US) e opera:

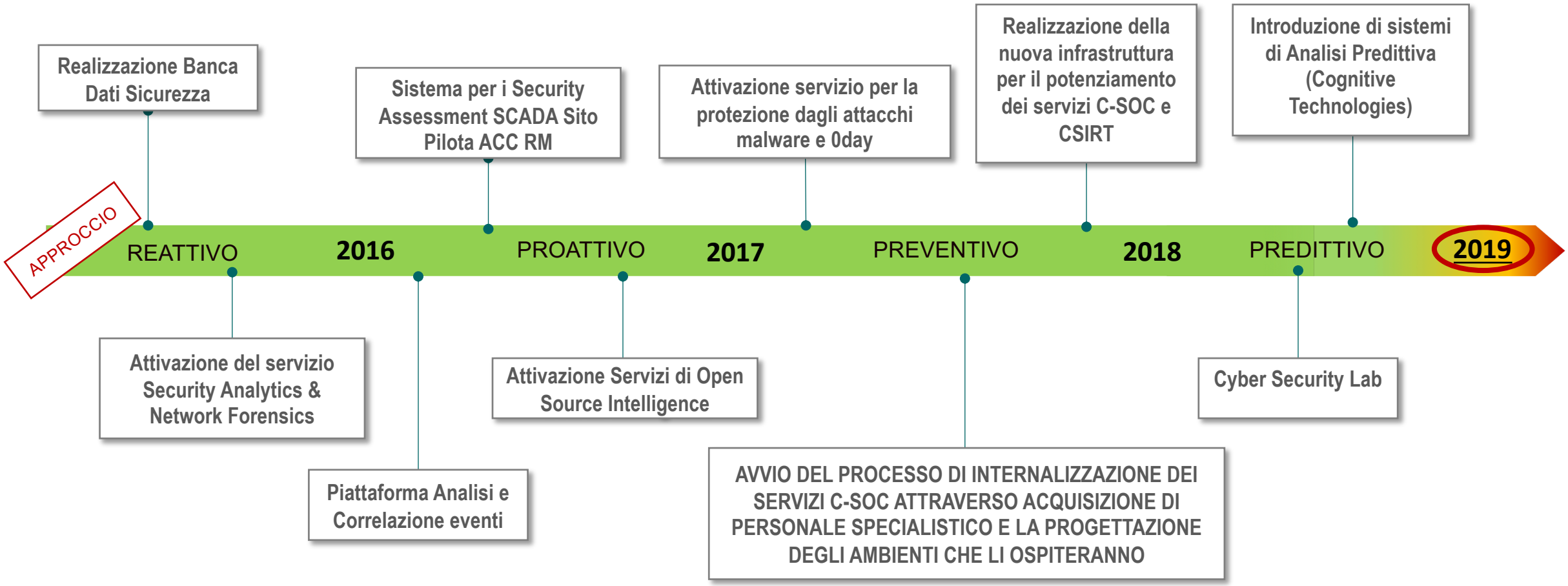
- ✓ sulle funzioni considerate essenziali nella gestione del rischio cibernetico (Identificare, Proteggere, Rilevare, Rispondere, Recuperare);
- ✓ attraverso le macro-attività declinate in termini di persone, processi e tecnologie dedicate.





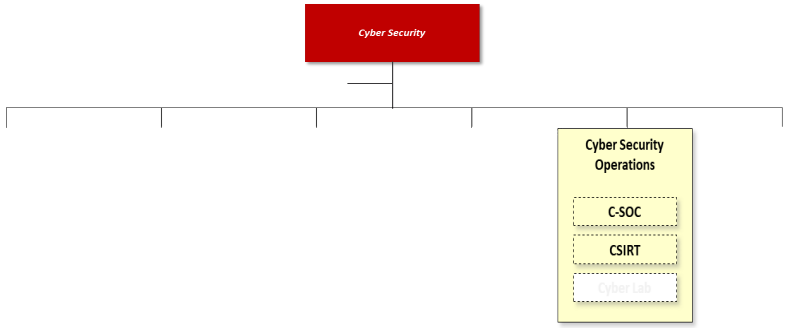
Approccio Cyber Security Gruppo FSI

Evoluzione



Approccio Cyber Security Gruppo FSI

Approccio operativo al CSIRT



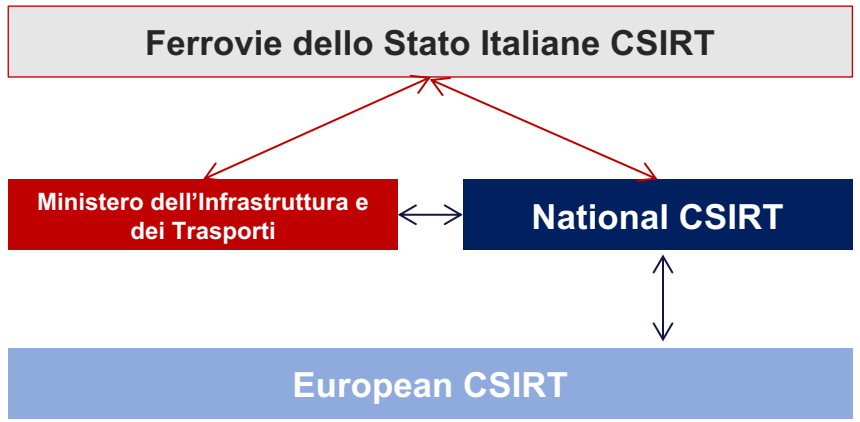
La funzione di Cyber Security nella sua componente di **Cyber Security Operations** (di seguito anche CS Operations) si compone di due sub-funzioni che hanno natura operativa, quali:

- **C-SOC (*Cyber Security Operations Center*):** assicura l'acquisizione, l'analisi e la correlazione degli eventi di sicurezza provenienti dai dispositivi di sicurezza perimetrale e dai sistemi del Gruppo che al suo interno. Il C-SOC si compone di due livelli, quali:
  - ✓ Analisi di I° livello;
  - ✓ Analisi di II° livello.
- **CSIRT (*Cyber Security Incident Response Team*):** assicura la gestione degli incidenti di sicurezza attraverso l'individuazione di soluzioni operative/ tecniche di risposta e il monitoraggio del processo fino alla loro risoluzione e supporta il Responsabile della Struttura Cyber Security nella cooperazione con organizzazioni e istituzioni di riferimento.

NIS DIRECTIVE (UE) – 6 JULY 2016

Art. 12 comma 5

Gli operatori di servizi essenziali notificano al CSIRT italiano e, per conoscenza, all'autorità competente NIS, senza ingiustificato ritardo, gli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali forniti.



CYBER SECURITY OPERATIONS CENTER (C-SOC)

Il C-SOC è un' infrastruttura centralizzata per il monitoraggio dello stato della sicurezza logica di Gruppo a protezione del business e delle piattaforme di intermodalità.

Tra le principali aree di intervento figurano:

- **Gestione degli incidenti di sicurezza;**
- **Analisi avanzata delle minacce cyber sui sistemi IT, OT (SCADA/ICS) e Internet of Things (IoT);**
- **Realizzazione del nodo di collegamento con le istituzioni preposte.**

FERROVIE DELLO STATO ITALIANE

Approccio Cyber Security Gruppo FSI

Convenzioni FS con Presidenza del Consiglio dei Ministri

L'ACCORDO CON LA PRESIDENZA DEL CONSIGLIO (DIS)

Il 15 maggio 2013 è stata firmata la convenzione tra la Presidenza del Consiglio dei Ministri - Dipartimento delle Informazioni per la Sicurezza (DIS) e il Gruppo Ferrovie dello Stato Italiane.

L' obiettivo della convenzione è sviluppare forme di collaborazione utili per lo svolgimento, da parte del DIS, dei propri compiti istituzionali attraverso un:

- **collegamento telematico dedicato e sincrono tra le strutture della Presidenza del Consiglio e quelle del Gruppo**
- **istituzione di una rete di CSIRT (Computer Security Incident Response Team)**
- **accesso diretto su specifici archivi informatici del Gruppo FSI.**

- Attivazione di un canale per l'accesso ai sistemi del Security Operation Center (SOC)
- Implementazione della piattaforma di *Info Sharing* tra le istituzioni e le infrastrutture critiche nazionali

FORMAZIONE IN AMBITO CYBER SECURITY SVOLTA DAL DIS

OBIETTIVO: Programma di ***AWARENESS*** sulla sicurezza logica al fine di far maturare la consapevolezza nell'utilizzo sicuro degli strumenti IT a disposizione nella quotidiana attività aziendale.

SESSIONE: giugno 2017 incontro con la Presidenza del Consiglio dei Ministri, sul tema cyber.

Approccio Cyber Security Gruppo FSI

Convenzioni FS con Polizia di Stato

L'ACCORDO CON LA POLIZIA DI STATO

Il 16 gennaio 2019 è stata rinnovata la convenzione tra la Polizia Postale – Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC) e il Gruppo Ferrovie dello Stato Italiane.

L' obiettivo dell'accordo è sviluppare procedure di collaborazione utili a prevenire e reprimere attacchi informatici verso i sistemi informativi che gestiscono la sicurezza e la regolarità del trasporto ferroviario, attraverso la predisposizione di un canale diretto per segnalare eventi di natura criminosa ai danni del Gruppo FSI.

FORMAZIONE IN AMBITO CYBER SECURITY SVOLTA DAL CNAIPIC

OBIETTIVO: Programma di ***AWARENESS*** sulla sicurezza logica al fine di accrescere la consapevolezza nell'utilizzo sicuro degli strumenti IT a disposizione nella quotidiana attività aziendale.

PROGRAMMA

- Nuovo quadro normativo in materia di dati personali (GDPR)
- Criminalità informatica: *ransomware*, *credit card fraud*, *skimming,* etc.
- Comuni email di *spam* e *unsolicited advertising*
- Come riconoscere e prevenire la minaccia

SESSIONE: gennaio 2018 incontro con la Polizia Postale sul nuovo quadro normativo in materia di dati personali e criminalità informatica.

Awareness and training

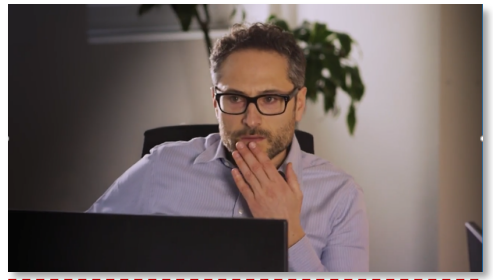
Cyber Security Learning Pills per i dipendenti

Mese della Cyber Security: pubblicazione di una fiction settimanale di 4 puntate su come difendersi dalle più comuni minacce informatiche

Non cedere / condividere le proprie password aziendali.

Non utilizzare indirizzi di posta aziendali per la creazione di profili social.

Non condividere informazioni riservate con strumenti di file sharing commerciali.



Non inoltrare e-mail ricevute sull'indirizzo di posta aziendale su un indirizzo di posta privata o viceversa.

Pillola 1

Awareness and training

Comitato per la Sicurezza delle Informazioni e Sistemi Informativi

Il Comitato è un organo consultivo istituito dal Gruppo Ferrovie dello Stato Italiane, nel novembre del 2013, con il compito di monitorare tutte le iniziative riguardanti i sistemi di sicurezza delle informazioni.

MEMBRI

- Comprende le funzioni del Gruppo coinvolte nei processi critici di gestione del rischio IT
- La sua organizzazione è modellata sulle esigenze specifiche del Gruppo

OBIETTIVO

Il Comitato per la sicurezza dei sistemi informativi e informatici gestisce tutte le principali questioni di gestione del rischio IT sollevate dal Gruppo e le parti interessate, al fine di garantire un adeguato livello di sicurezza delle informazioni.

Approccio Cyber Security Gruppo FSI

Le principali iniziative in ambito Cyber Security

SCADA

Security Assessment, analisi e correlazione eventi

Operational Intelligence

Potenziamento delle tecnologie di analisi di sicurezza e *compliance* dei sistemi e degli apparati di rete.

SOC – Railway

Realizzazione del Security Operation Center di Gruppo per il monitoraggio dello stato della sicurezza logica di Gruppo a protezione del business e delle piattaforme di intermodalità

OSINT (Open Source Intelligence)

Servizio di analisi delle fonti aperte

CSIRT (Computer Security Incident Response Team)

Realizzazione del nodo di collegamento con i CSIRT istituzionali e delle infrastrutture critiche nazionali ed internazionali per la rilevazione e condivisione di minacce/ vulnerabilità e per la gestione degli incidenti di sicurezza

Anti-DDoS (Denial of Services)

Potenziamento delle misure di sicurezza perimetrale contro attacchi DDoS

***Cyber Security* Lab**

Laboratorio per la ricerca di nuove minacce informatiche non pubblicamente note

Network and Host Protection

Firewall, VPN and virtualization network access, network forensics e sistemi di intrusion prevention, end point protection and antivirus

Malware Protection

Attivazione del sistema per la protezione in tempo reale contro gli attacchi malware APT e 0DAY

Web Application Security

Application firewall per applicazioni critiche HTTP

Email Protection

Antispam, live malware analysis, malicious link e rilevamento di downloads da parte degli utenti

Internet access protection

Web content filtering, in-line network sandbox, malware callback detection

Grazie