La Cyber Security nel Gruppo FS Italiane

RICCARDO BARRILE
CHIEF INFORMATION SECURITY OFFICER
Gruppo Ferrovie dello Stato Italiane

29 giugno 2021

FERROVIE DELLO STATO ITALIANE

Informazione ad uso interno

L’ecosistema del Gruppo FSI in Italia

16.700 km di line ferroviarie

1.400 km di linee Alta velocità

1.380 km di gallerie

530 km di ponti e sovrapassi

26.000 km di strade

2.200 stazioni ferroviarie

800 treni merci al giorno

50 milioni di tonnellate di merci trasportate ogni anno

8.000 treni al giorno

15 navi traghetto

600 millioni di passeggeri anno

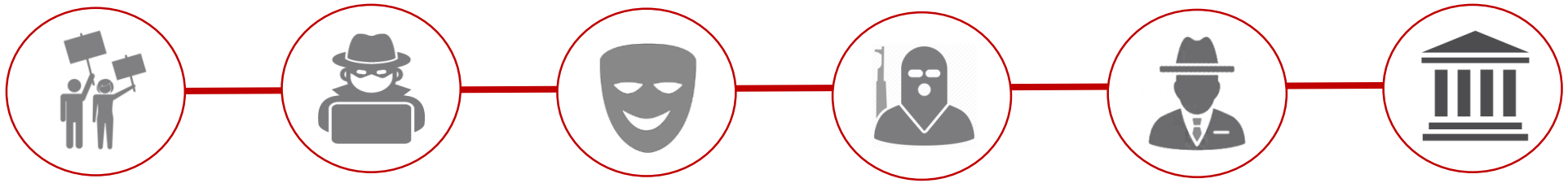
83.000 dipendenti

Le minacce alla sicurezza del trasporto ferroviario

Diverse minacce alla sicurezza del trasporto ferroviario possono manifestarsi attraverso la compromissione delle informazioni e dei sistemi informativi

Vento
Frane
Interruzione di servizi
Vandalismo
Frodi
Ostacoli lungo linea
Furto materiali
Azionamento freno di emergenza
Rapine
Attentati alla sicurezza dei trasporti
Eventi sismici
Neve
Irregolarità di viaggio
Accessi non autorizzati
Furti ai clienti
Rimborsi fraudolenti
Incendi dolosi
Spionaggio
Sabotaggio
Aggressioni al personale
Aggressioni ai clienti
Attività abusive
Incendi boschivi
Corruzione di dati
Graffiti
Infedeltà dipendenti
Lancio sassi
Terrorismo
Furto di dati
Occupazioni abusive
Inondazioni

Cyber Security nel settore dei Trasporti



CHI ATTACCA E PERCHÈ?

- HACKTIVISM
- CYBER-CRIMINE
- INSIDER
- TERRORISMO
- SPIONAGGIO
- WARFARE

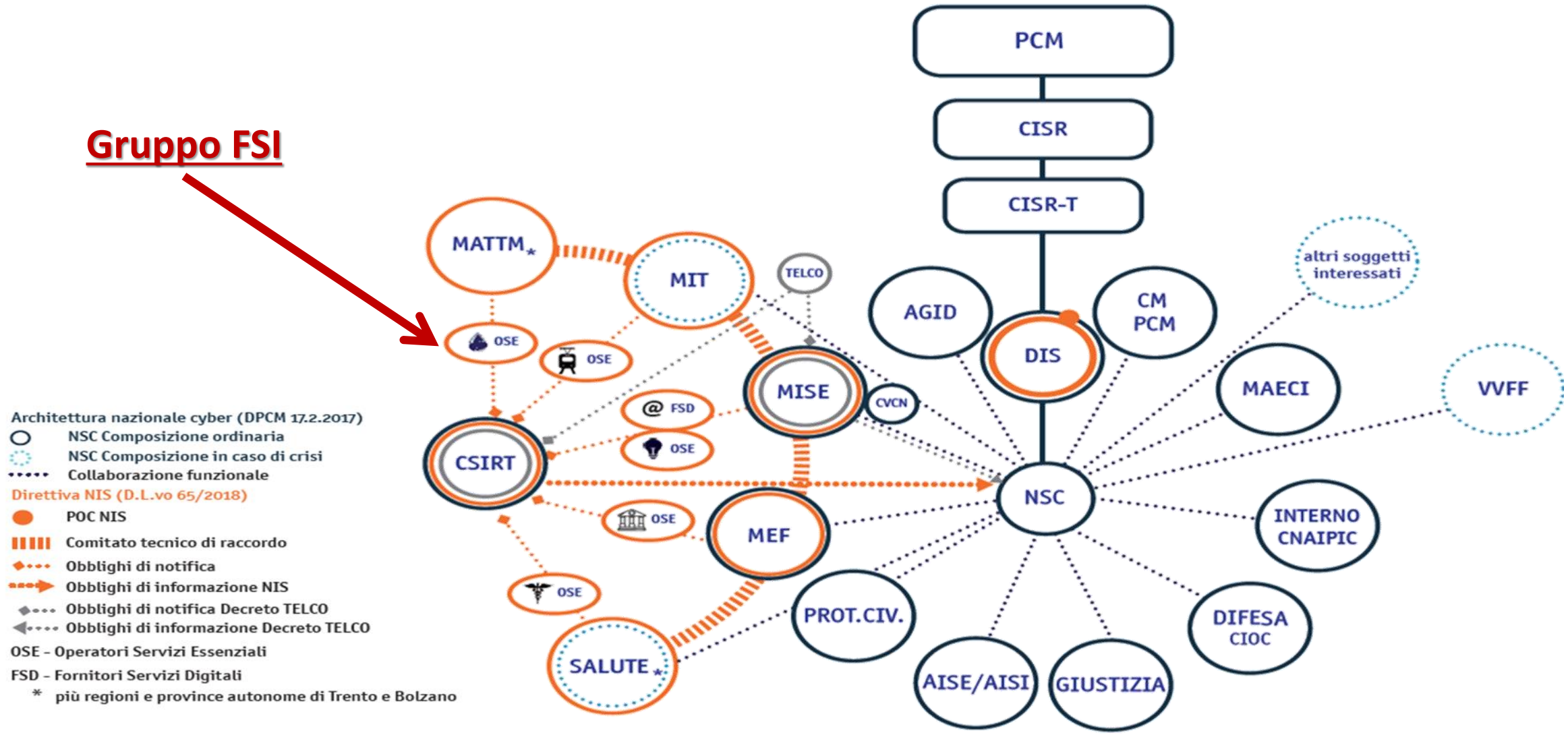
TIPOLOGIA DI MINACCE

- DDOS
- PHISHING
- MALWARE
- SQL INJECTION
- DEFACEMENT
- SOCIAL ENGINEERING

IMPATTI

- MALFUNZIONAMENTO O DANNEGGIAMENTO DELL'INFRASTRUTTURA
- MANCATA EROGAZIONE DI SERVIZI ESSENZIALI DI TRASPORTO
- FURTO DI DATI
- DANNI REPUTAZIONALI
- MANCATO RISPETTO DEGLI OBBLIGHI DI LEGGE (ES. PRIVACY)
- SPIONAGGIO INDUSTRIALE

Il Gruppo FS nell'ecosistema Cyber in Italia



Direttiva 1148/2016 Network and Information Security (NIS)

Obiettivo: migliorare il livello di sicurezza dei sistemi, delle reti e dell'informazione all'interno dell'UE attraverso:

- l'istituzione di un gruppo di cooperazione (Art. 10)
- l'istituzione di una rete di CSIRT (*Computer Security Incident Response Team*) (Art. 11)
- l'obbligo di notifica degli incidenti di sicurezza al CSIRT nazionale (Art. 12)
- l'implementazione di misure organizzative e di sicurezza adeguate (Art. 12)

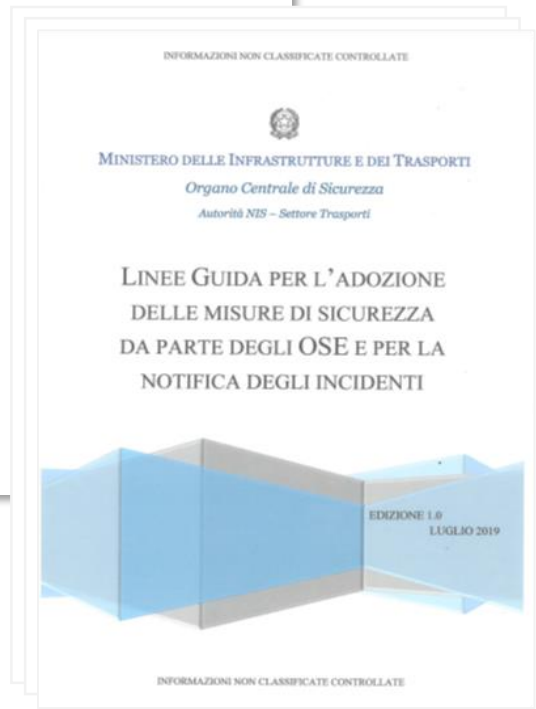
- ✓ Individuazione e nomina degli operatori pubblici e privati che erogano servizi essenziali (OSE).
- ✓ Condivisione dell'assetto della funzione di Cyber Security.
- ✓ Condivisione delle procedure di gestione degli incidenti di sicurezza.
- ✓ Definizione e implementazione e verifica delle misure da adottare per la gestione dei rischi

D. Lgs.65/2018 attuazione Direttiva NIS (UE 2016/1148)

Il **31 luglio 2019** l'Autorità NIS – Settore Trasporti ha approvato la pubblicazione delle

«Linee guida per l'adozione delle misure di sicurezza da parte degli OSE e per la notifica degli incidenti».

Attività
✓ Avvio del processo di trasmissione delle notifiche di incidenti all'Autorità NIS ✓ Comunicazione degli assetti organizzativi atti ad assicurare gli adempimenti preposti.
✓ Mappatura del profilo attuale delle misure tecniche e organizzative di sicurezza ✓ Self-assessment del rischio cyber, comprensiva delle matrici di rischio sulle applicazioni ✓ Politiche di sicurezza
✓ Attuazione misure di sicurezza che servono per raggiungere un livello minimo consentito di maturità. ✓ Trasmissione all'autorità NIS delle evidenze di attuazione secondo la Mappatura indicata nelle Linee Guida
✓ Identificazione e comunicazione all'Autorità NIS del Responsabile delle segnalazioni di incidenti.


INFORMAZIONI NON CLASSIFICATE CONTROLLATE

MINISTERO DELLE INFRASTRUTTURE E DEI TRASPORTI

Organo Centrale di Sicurezza

Autorità NIS – Settore Trasporti

LINEE GUIDA PER L'ADOZIONE DELLE MISURE DI SICUREZZA DA PARTE DEGLI OSE E PER LA NOTIFICA DEGLI INCIDENTI

EDIZIONE 1.0
LUGLIO 2019

INFORMAZIONI NON CLASSIFICATE CONTROLLATE

D. Lgs.105/2019 Perimetro di Sicurezza Nazionale Cibernetica

Con la Legge n. 133 del 18 novembre 2019 è convertito in legge il Decreto-Legge n.105 del 21 settembre 2019 che istituisce il Perimetro di sicurezza nazionale cibernetica. La legge prevede la pubblicazione dei seguenti DPCM

DPCM 131/2020
"Regolamento in materia di perimetro di sicurezza nazionale cibernetica"

- Modalità e i criteri per l'individuazione dei soggetti da includere nel perimetro
- Criteri per la predisposizione e aggiornamento dell'elenco delle reti, dei sistemi informativi e dei servizi informatici.

DPCM 81/2021
"Regolamento di notifica degli incidenti e delle misure di sicurezza"

- Procedure di notifica degli incidenti al CSIRT nazionale
- Misure di sicurezza che i soggetti devono implementare
- Procedure, modalità e termini per l'affidamento di forniture di beni, sistemi e servizi ICT al Centro di Valutazione e Certificazione Nazionale (CVCN)

SANZIONI

- **Ammende fino a 1,8 mln per**
  - ✓ inadempimenti sulla predisposizione e aggiornamento degli elenchi reti, sistemi e servizi IT
  - ✓ Inosservanza delle misure di sicurezza
  - ✓ mancata comunicazione degli affidamenti al CVCN
  - ✓ violazione delle condizione imposte dal CVCN sull'utilizzo di prodotti e servizi
- **Cessazione dei contratti non ottemperanti le condizioni imposte dal CVCN**
- **Incapacità di assumere incarichi di direzione, amministrazione e controllo per 3 anni**
- **Reclusione da 1 a 3 anni per**
  - ✓ ostacolo o condizionamento delle attività ispettive e di vigilanza
  - ✓ omissione di comunicazione nei termini prescritti

Perimetro di Sicurezza Nazionale Cibernetica

DPCM n.81 del 11/06/2021

GAZZETTA UFFICIALE
DELLA REPUBBLICA ITALIANA

Il regolamento stabilisce le regole e le modalità di notifica degli incidenti al CSIRT nazionale

Notifica degli Incidenti
(Obbligatoria da gennaio 2022)

Entro 1 ora
(All. A, Tab 2)

- *Inibizione Funzioni*
- *Compromissione Processi*
- *Disservizi*

Entro 6 ore
(All. A, Tab1)

- *Infezione (malware)*
- *Guasto (degrado; perdita dati)*
- *Privilege Escalation*
- *Establish Persistence*
- *Movimenti laterali*
- *Raccolta, Esfiltrazione*

FERROVIE DELLO STATO ITALIANE

Perimetro di Sicurezza Nazionale Cibernetica

DPCM n.81 del 11/06/2021

GAZZETTA UFFICIALE
DELLA REPUBBLICA ITALIANA

Il regolamento stabilisce le misure di sicurezza da implementare

Misure di sicurezza

All. B, Categoria A: entro 6 mesi dalla trasmissione beni ICT
(più organizzative)

- *Identity Asset Management*
- *Governance*
- *Risk Assessment*
- *Risk Management*
- *Supply Change*
- *Awareness and Training*
- *Process Detection*
- *Response Plan*
- *Communication*
- *Analysis*
- *Response and Recover*

All. B, Categoria B: entro 30 mesi dalla trasmissione beni ICT
(più tecniche)

- *Supply Change*
- *Access Control*
- *Data Security*
- *Information Protect*
- *Maintenance*
- *Protection Technology*
- *Event Detection*
- *Continuous Monitoring*
- *Mitigation*

All. C: entro 60 giorni dalla trasmissione beni ICT
(misure minime di sicurezza)

- *Sicurezza fisica e documentale*
- *Ausilio di strumenti elettronici*

FERROVIE DELLO STATO ITALIANE

Informazione ad uso interno

Convenzioni e partenariato

Accordo con la 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

AZIONI: 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.

Convenzioni e partenariato

Accordo con la Polizia di Stato - CNAIPIC

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.

464 bollettini di segnalazione vulnerabilità, malware e campagne di phishing durante il 2021

FORMAZIONE IN AMBITO CYBER SECURITY SVOLTA DAL CNAIP

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

PROGRAMMA

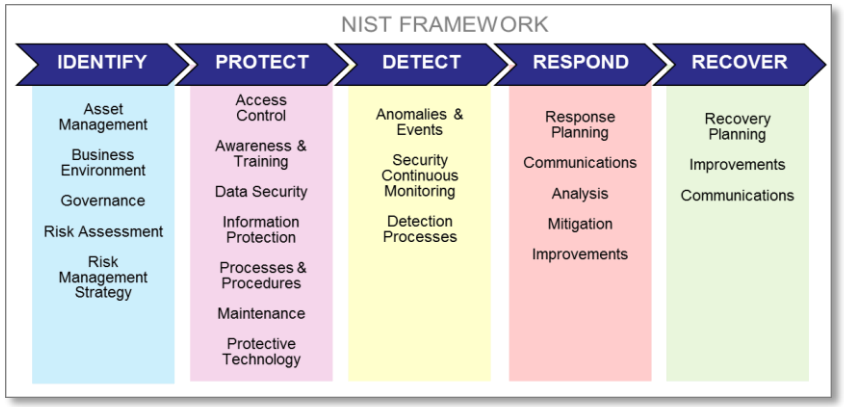
- Criminalità informatica: *ransomware*, *credit card fraud*, *skimming,* etc.
- Comuni email di *spam* e *unsolicited advertising*
- Come riconoscere e prevenire la minaccia

PRINCIPALI AZIONI

- ✓ Incontri formativi con il Top Management tenuti dala Polizia Postale sul quadro normativo sulla cyber Security e criminalità informatica
- ✓ Supporto nella definizione dei contenuti per la realizzazione di pillole formative sulla Cyber Security per tutti i dipendenti

Struttura organizzativa e modello funzionale di Cyber Security in FS

Il Gruppo Ferrovie dello Stato Italiane, in qualità di **Operatore di Servizi Essenziali**, ha ridefinito il modello organizzativo della Cyber Security ed adottato un approccio basato sul framework internazionale «NIST» (*National Institute of Standards and Technology of US*).



DIREZIONE CENTRALE PROTEZIONE AZIENDALE

CYBER SECURITY

- INFOSHARING & COMPLIANCE
- ENGINEERING & SERVICE MANAGEMENT
- CYBER SECURITY OPERATIONS
- PROJECT & PROGRAM MANAGEMENT

Identification → **Protection** → **Detection** → **Respond** → **Recover**

Analisi I° livello — ***Analisi II° livello*** — ***CSIRT***

Tecnologie e servizi di Cyber Security

IACS
Security Assessment, analisi e correlazione eventi

Operational Intelligence
Tecnologie di analisi di sicurezza e *compliance* dei sistemi e degli apparati di rete.

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

Threat Intelligence (analisi OSINT e CLOSINT)
Servizio di analisi delle fontiaperte e chiuse

CSIRT (Computer Security Incident Response Team)
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)
Servizi e misure di sicurezza perimetrale contro attacchi DDoS volumetrici e applicativi

***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

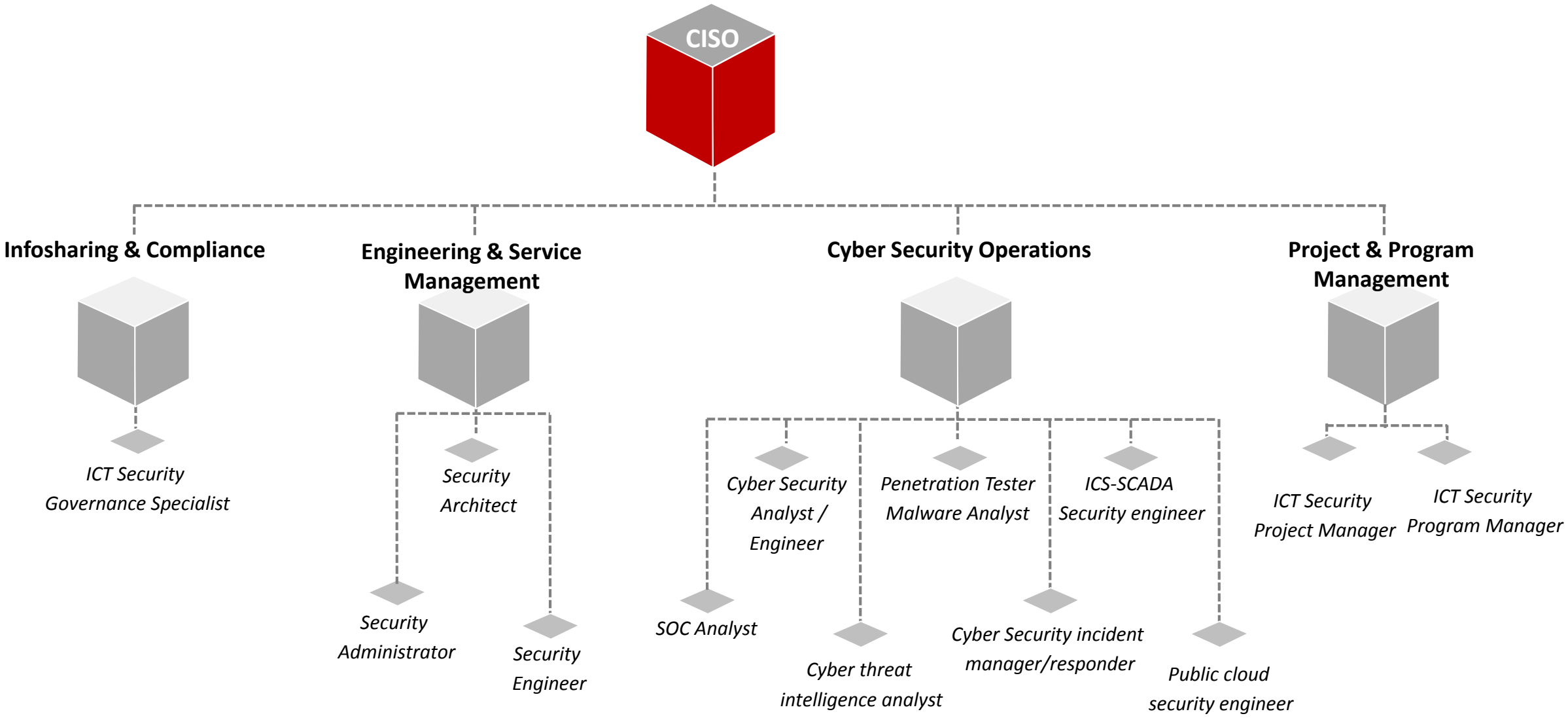
Malware Protection
Sistema per la protezione in tempo reale contro gli attacchi malware APT e 0DAY

Web Application Security
Application firewall per applicazioni critiche HTTP

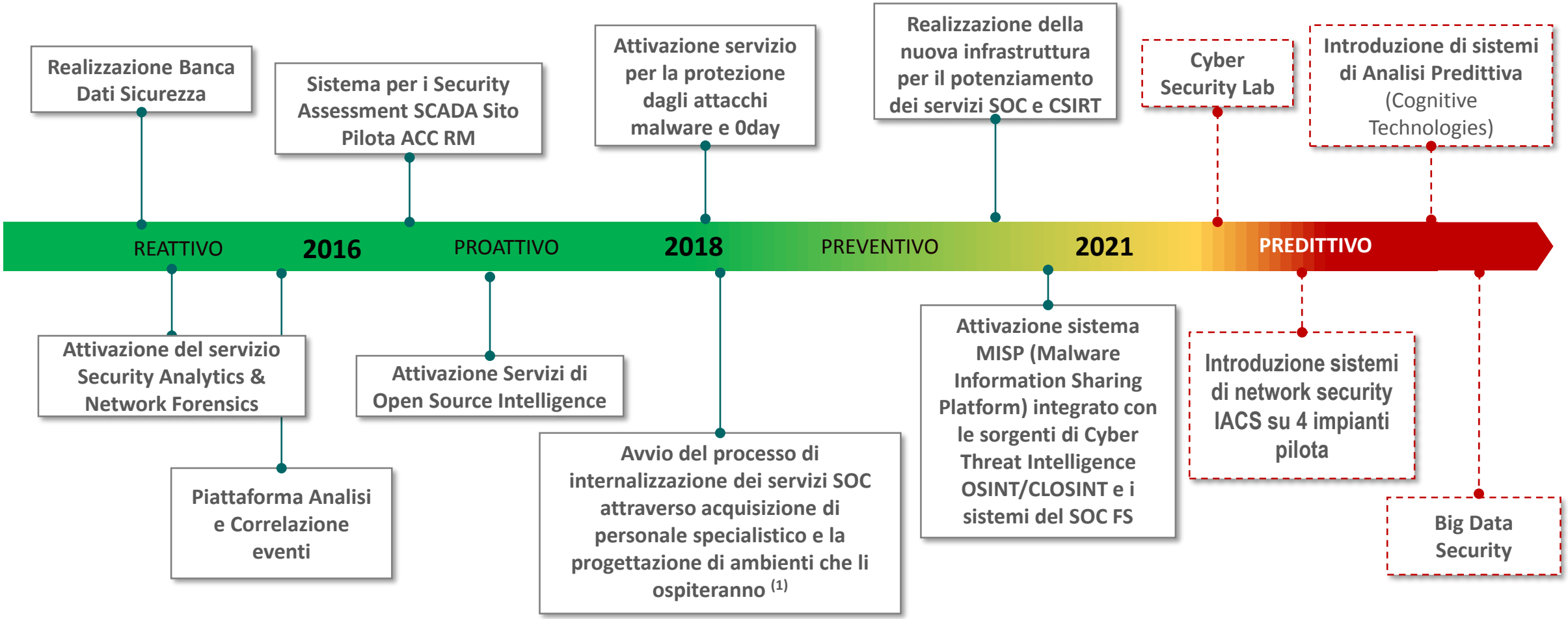
Email Protection
Antispam, live malware analysis, malicious link e rilevamento di downloads da parte degli utenti

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

Ruoli e competenze



Il Cyber Security Operation Center del Gruppo FS



La gestione degli attacchi informatici

Fase 1 - Rilevazione attacco informatico o attività anomale	• Identificazione dell'Incidente di Sicurezza. • Integrazione con le procedure di Incident Management.
Fase 2 - Prima analisi e registrazione	• Esame Knowledge Base in base ai dati contenuti nella rilevazione. • Analisi del contesto e apertura Incidente di Sicurezza Logica.
Fase 3 - Classificazione dell'Incident e analisi	• Identificazione degli elementi caratterizzanti l'incidente. • Determinazione del livello di criticità.
Fase 4 - Notifica ed eventuale «escalation»	• Condivisione informazioni con i soggetti interessati/autorizzati in funzione del fenomeno osservato.
Fase 5 - Contenimento e contrasto	• Applicazione della contromisura e individuazione eventuali ulteriori azioni di contenimento o a supporto dell'analisi.
Fase 6 - Recovery	• Verifica efficacia contromisura e analisi dell'evoluzione dello scenario d'attacco nel tempo.
Fase 7 - Follow-Up & Incident Report	• Raccolta delle evidenze e predisposizione del Security Incident Report. • Notifiche di chiusura.

Lo stato della Cyber Security

Raccolta, analisi e correlazione eventi di sicurezza

800+ NETWORK SECURITY DEVICES

5000+ SERVER

40000+ WORKSTATIONS/LAPTOPS/MOBILE CLIENTS MONITORATI IN REAL TIME

↓

OLTRE 5 MILIARDI DI LOGS RACCOLTI A SETTIMANA

↓

MIGLIAIA DI ALERTS A SETTIMANA

↓

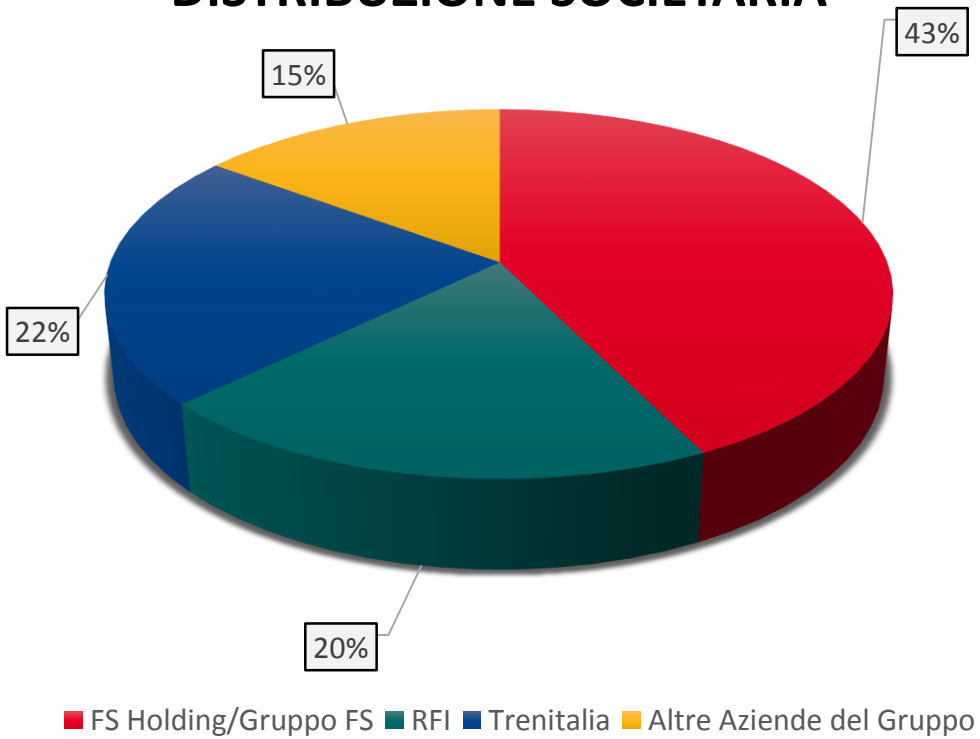
2051 INCIDENTI DI SICUREZZA GESTITI NEL PERIODO GENNAIO-MAGGIO 2021

Lo stato della Cyber Security (gennaio - maggio 2021)

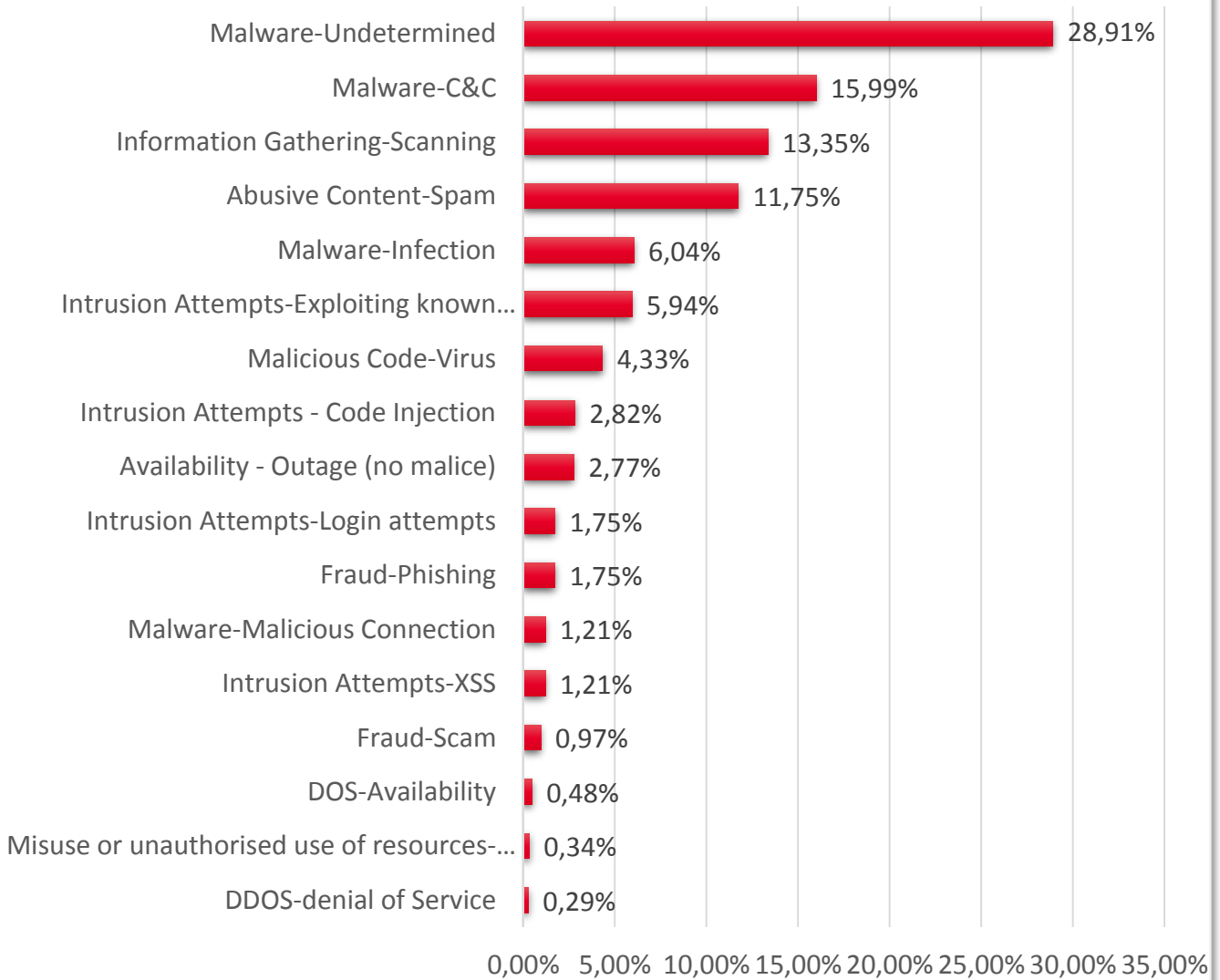
Gli attacchi cyber gestiti

2.051 i tentativi di attacco rilevati e neutralizzati

DISTRIBUZIONE SOCIETARIA

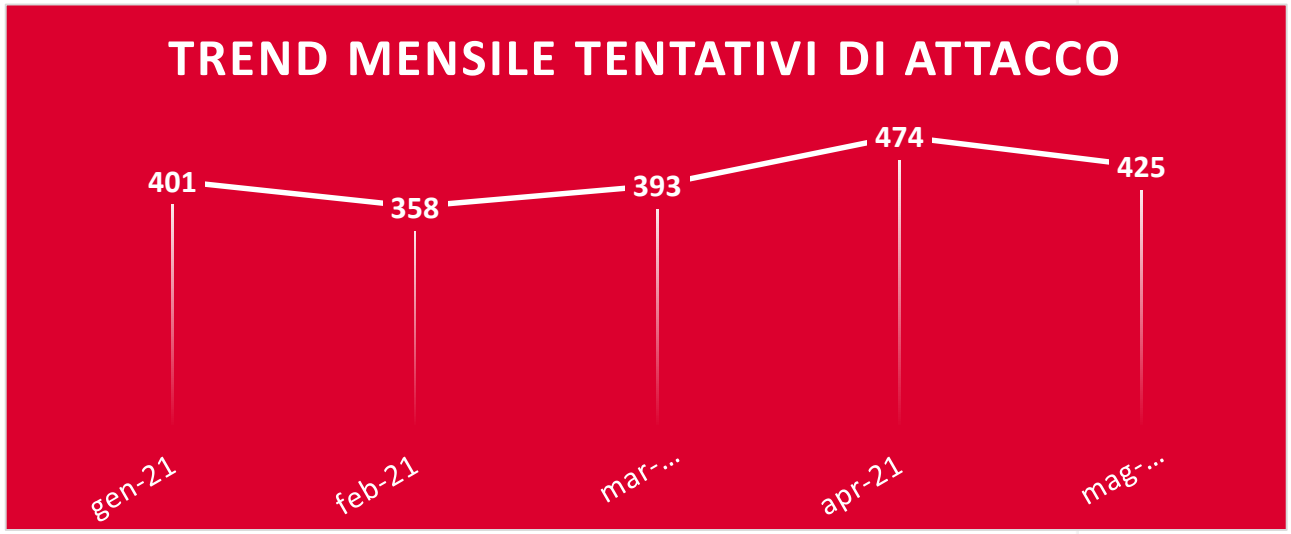


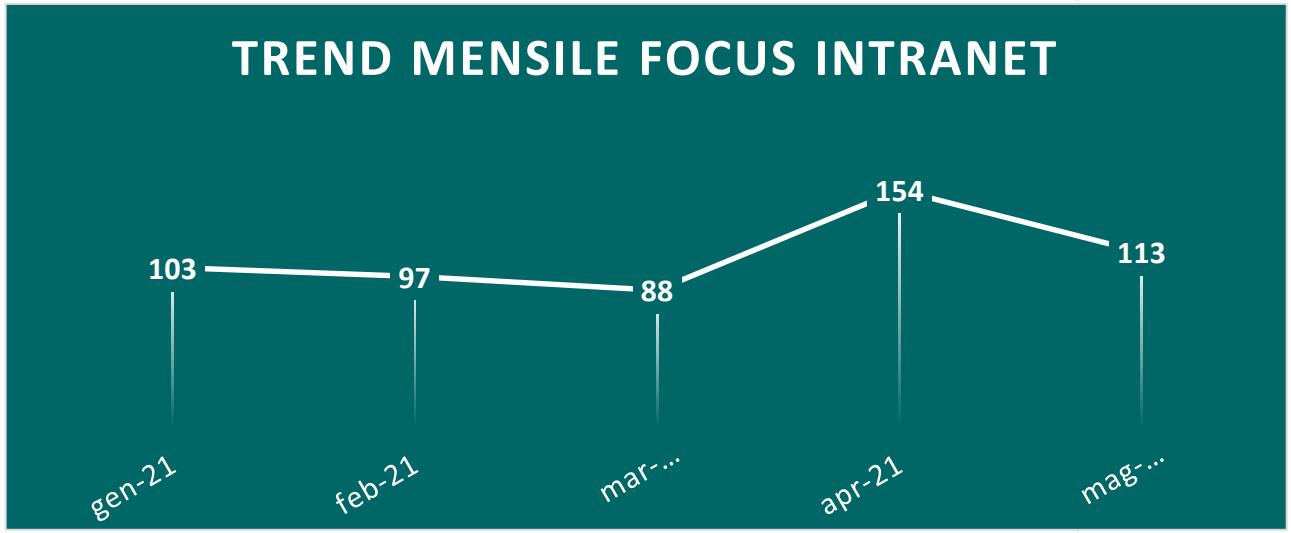
TIPOLOGIA TENTATIVI DI ATTACCO

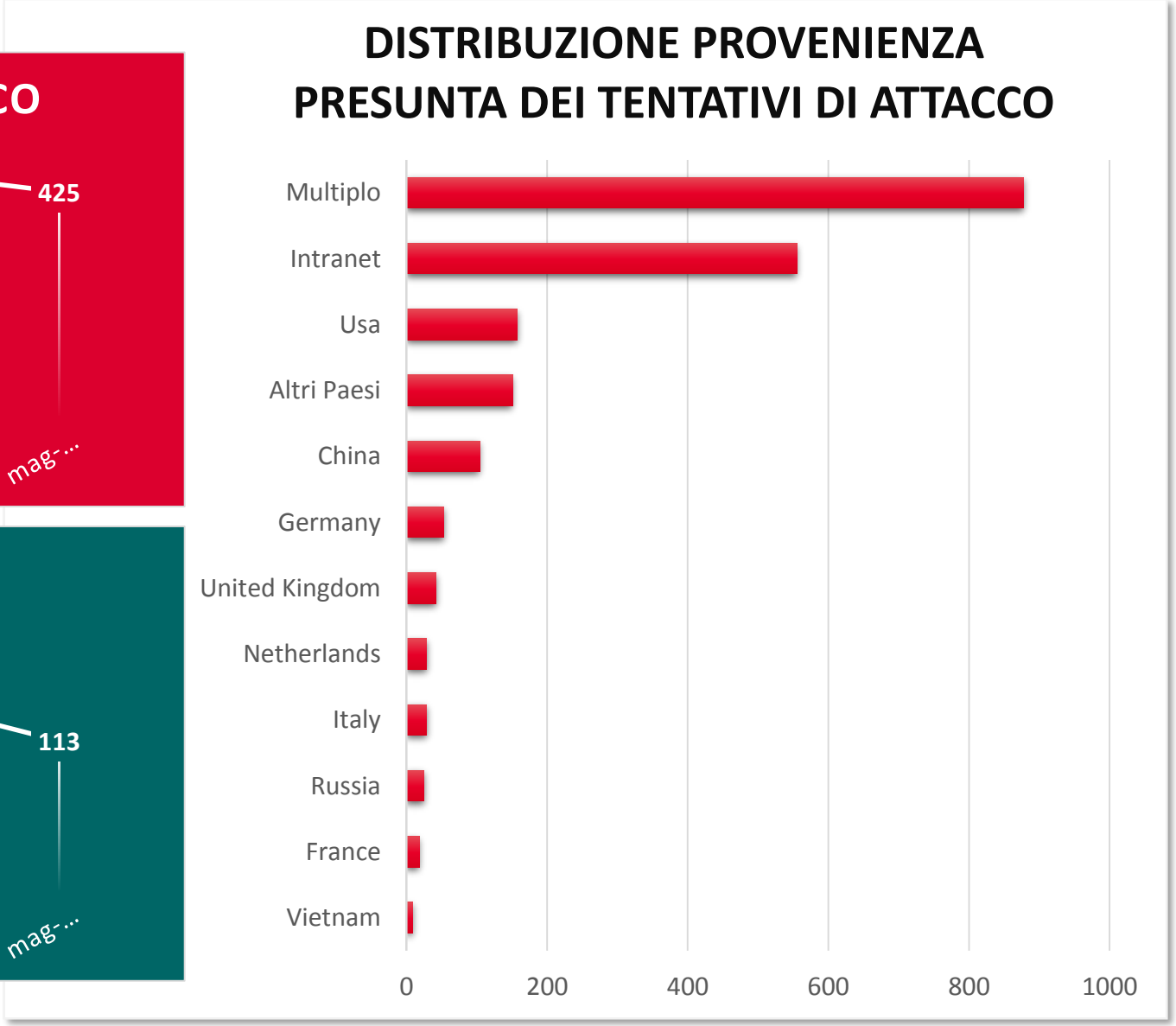


Lo stato della Cyber Security (gennaio - maggio 2021)

Provenienza degli attacchi e trend mensile





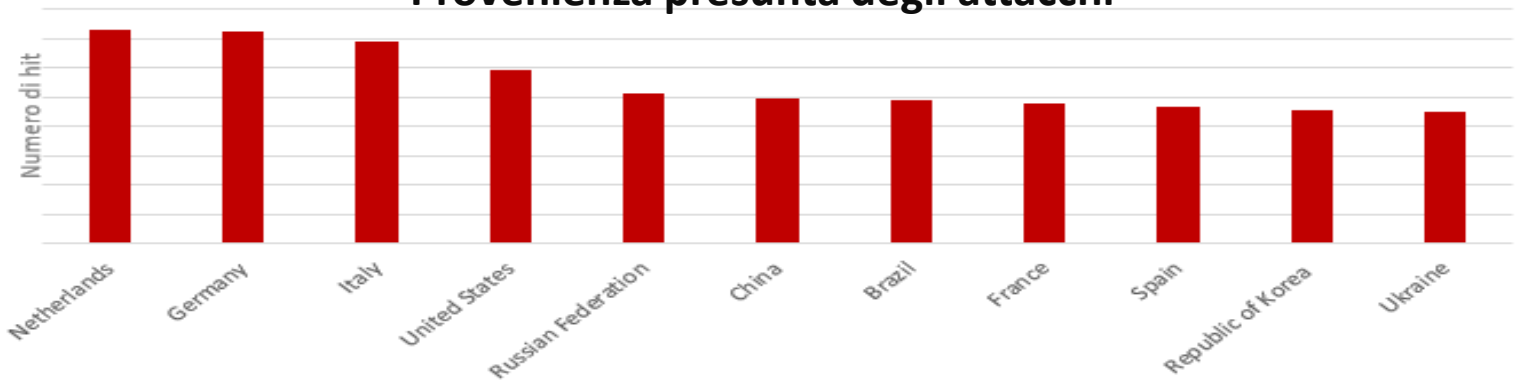


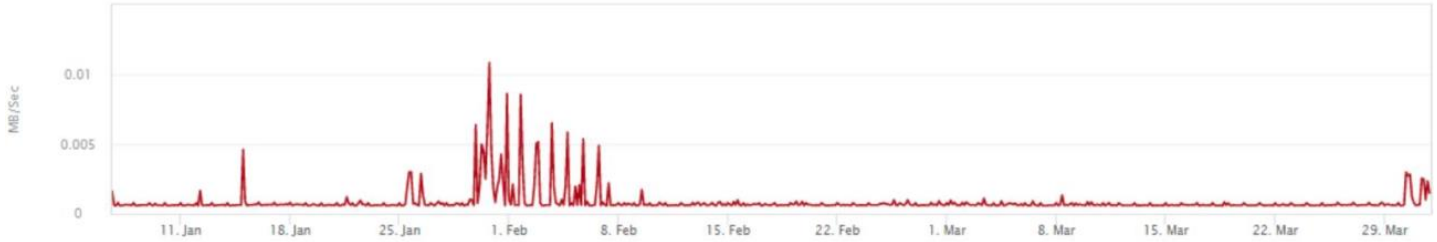
Lo stato della Cyber Security (gennaio - maggio 2021)

Akamai – Attacchi DOS rilevati

642.2GB su 335 TB Traffico ricevuto e classificato come DOS

Provenienza presunta degli attacchi





Trend di attacco DOS gennaio-marzo 2021

Trend di attacco DOS aprile-maggio 2021

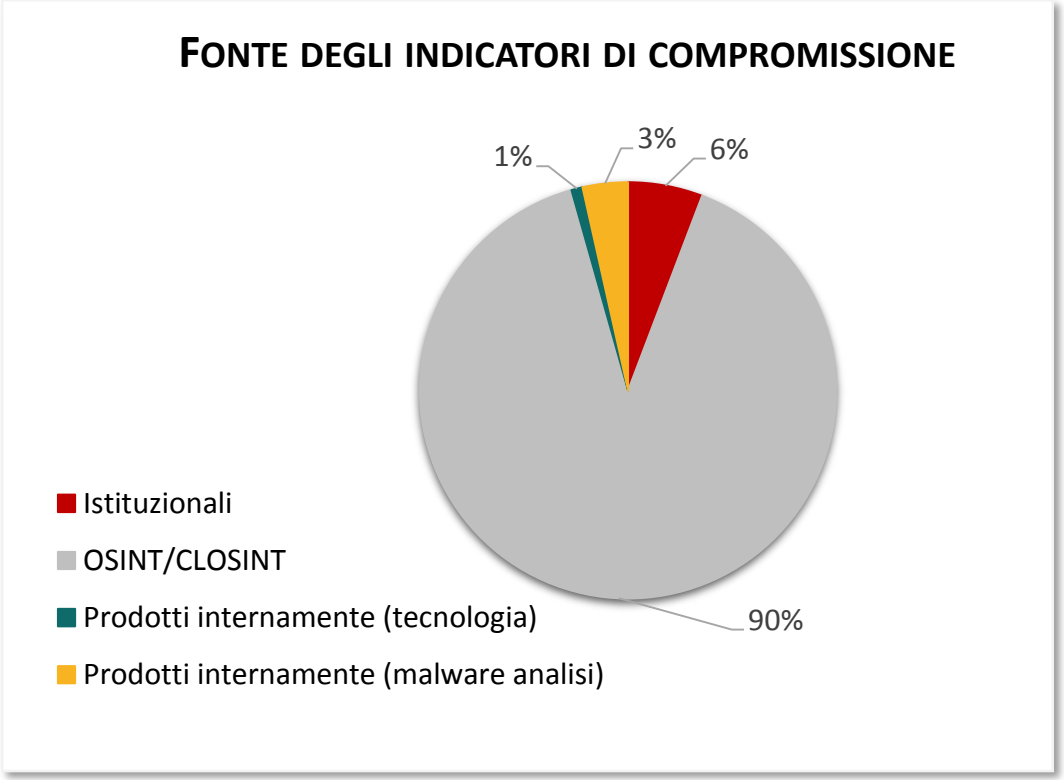
Lo stato della Cyber Security

Attività di Threat Intelligence (gennaio - maggio 2021)

464 bollettini istituzionali (CNAIPIC)

Oltre **28.000** indicatori di compromissione (IoC)

Principali minacce bloccate preventivamente (APT e BotNet)
Current Events to Widespread Campaigns: Pivoting from Samples to Identify Activity
Exploits in the Wild for Citrix Vulnerability
Necurs Out Of Ideas
Campagna di Attacco TrickBot
New Variant of TrickBot Being Spread by Word Document

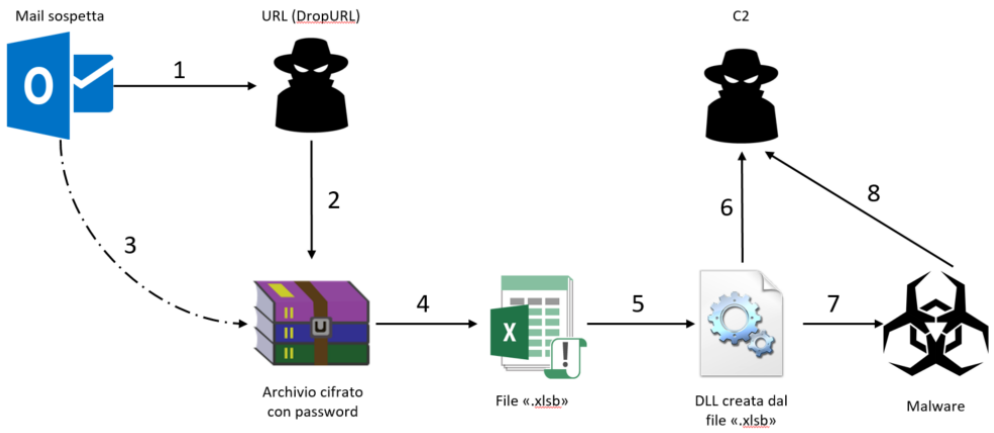


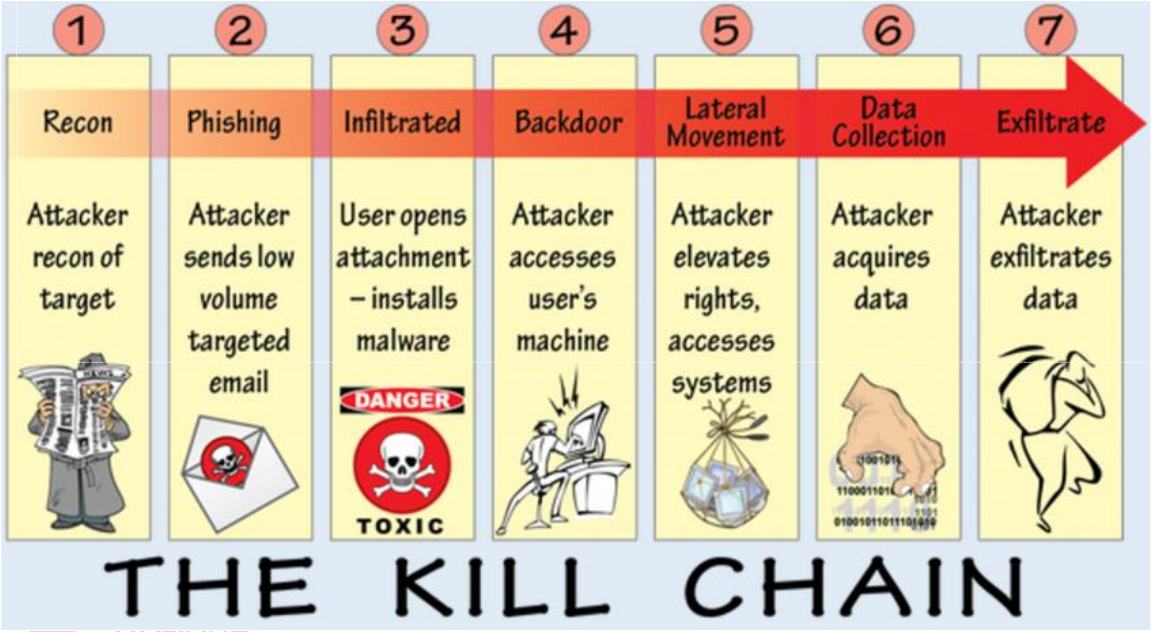
Campoloader: una nuova variante scoperta dal SOC di FS

Le istruzioni di protezione sono state condivise con il CNAIPIC della Polizia di Stato

Attacco

- La mail sospetta non viene riconosciuta dai sistemi di protezione
- E' presente un allegato office cifrato protetto da password inviata in chiaro
- Il malware si attiva all'apertura del file, si diffonde nella rete e attiva un canale di comunicazione esterno per trasferire informazioni.





Azioni di contrasto

- Analisi del comportamento in un ambiente isolato
- Individuazione degli Indicatori di Compromissione (IoC)
- Creazione delle istruzioni di protezione
- Segnalazione al CNAIPIC e ai vendor

Iniziative di Awareness

Cyber Security Learning Pills

Non diffondere informazioni aziendali

Utilizzo sicuro dei dispositivi mobili

Protezione delle reti domestiche

Accesso ai locali tecnologici

Vademecum Cyber Security in Smart Working

Dispositivi aziendali e personali

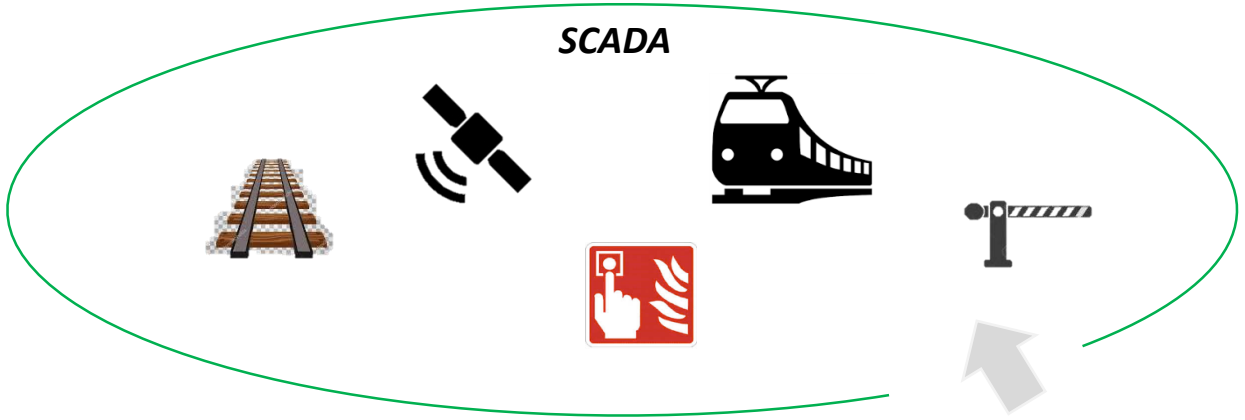
Reti domestiche e router

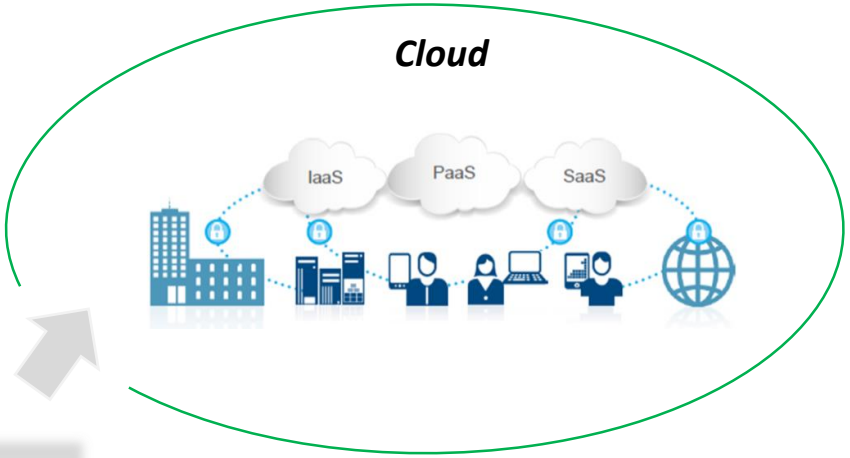
Gestione e condivisione dei dati aziendali

Digital workspace e videoconferenze

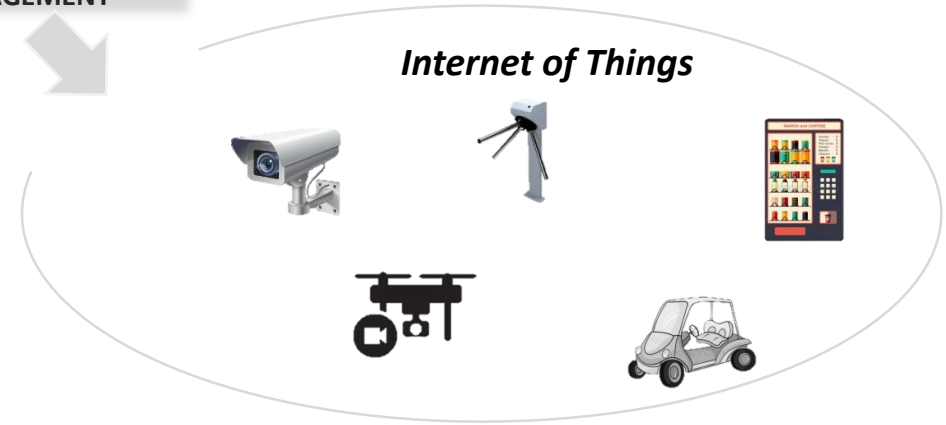
Scenari evolutivi del C-SOC

Integrazione dei perimetri SCADA, Cloud e Internet of Things





- ASSESSMENT
- POLICY
- LOG
- INCIDENT MANAGEMENT



Attività avviata — Attività da avviare

Scenari evolutivi del C-SOC

Cognitive & Big Data Security

COGNITIVE SECURITY

L'intelligenza artificiale applicata tramite tecnologie con capacità cognitive consente di implementare meccanismi di apprendimento automatico al fine di individuare, interpretare e integrare una vasta quantità di dati, imparando dopo ogni interazione e agendo in modo proattivo alle minacce.
Con l'intelligenza artificiale gli analisti di sicurezza, possono rispondere alle minacce con maggiore attendibilità e velocità.

Strumenti come IBM Watson for Cyber Security supportano le indagini e le analisi di sicurezza collegando automaticamente le anomalie di sicurezza che si manifestano sul perimetro aziendale a dati ed informazioni esterne evidenziando le condizioni di maggiore criticità potenziale.

BIG DATA SECURITY

I Big Data, intesi come patrimonio di informazioni ad alto volume, ad alta velocità e/o alta varietà richiedono nuove forme di analisi per migliorare la sicurezza delle reti di dati aziendali.

PRINCIPALI SFIDE

1. **Volume**: aumento della quantità di dati (dai *terabyte* agli *zettabyte)*
2. **Velocità**: aumento della velocità dei dati (in ingresso e in uscita)
3. **Varietà**: diverse tipologie e fonti dati
4. **Valore** dei dati nel contesto