05-06 dicembre 2024 Roma
10° SEMINARIO NAZIONALE SISTEMA TRAM
Giornate di Studio
"20 anni di esperienze, per traguardare il futuro"
METRAM RENO

Cyber minacce nei sistemi a guida vincolata

Luca Cancelliere / Matteo Morazzoni
Netservice SpA

Coordinato da:
MINISTERO DELLE INFRASTRUTTURE E DEI TRASPORTI

Organizzato da:
in qualità di Provider asstra service
in collaborazione con ASSOCIAZIONE ITALIANA per l'INGEGNERIA del TRAFFICO e dei TRASPORTI AIIT, asstra IMPRESE IN MOVIMENTO, CIFI COLLEGIO INGEGNERI FERROVIARI ITALIANI

L'evoluzione del trasporto pubblico tra rischi ed opportunità

La digitalizzazione ha trasformato profondamente il settore a guida vincolata, migliorando l'efficienza operativa e l'esperienza dei passeggeri grazie a tecnologie come la bigliettazione elettronica, i sistemi di gestione avanzata del traffico e il monitoraggio in tempo reale. Sistemi fondamentali come il CBTC e SCADA oltre a diverse classi di sensori interconnessi, rappresentano il cuore delle operazioni moderne, offrendo automazione e connettività senza precedenti.

Tuttavia questa trasformazione ha esposto le infrastrutture critiche a nuove minacce. L'integrazione tra IT e OT ha ampliato la superficie d'attacco, rendendo questi sistemi vulnerabili a ransomware, sabotaggi e attacchi alla supply chain. Garantire la sicurezza è quindi una priorità per assicurare la continuità e la resilienza delle operazioni dei sistemi a guida vincolata.

L'evoluzione del trasporto pubblico e rischi associati

- **Digitalizzazione**
  - Biglietteria elettronica.
  - Sistemi di gestione del traffico e automazione (CBTC, SCADA)
- **Connessione costante:**
  - IoT nei treni e metropolitane.
  - Comunicazione (sistemi e infrastrutture critiche)
- **Minacce correlate:**
  - Attacchi ransomware ai sistemi del business
  - Attacchi DoS (Denial of Service)
  - Furto dei dati dei passeggeri
  - Sabotaggi mirati ai sistemi di sicurezza (es. controllo del traffico, frenata d'emergenza).
  - Attacchi rivolti ai clienti finali (ss. Phishing/Smishing/Quishing)

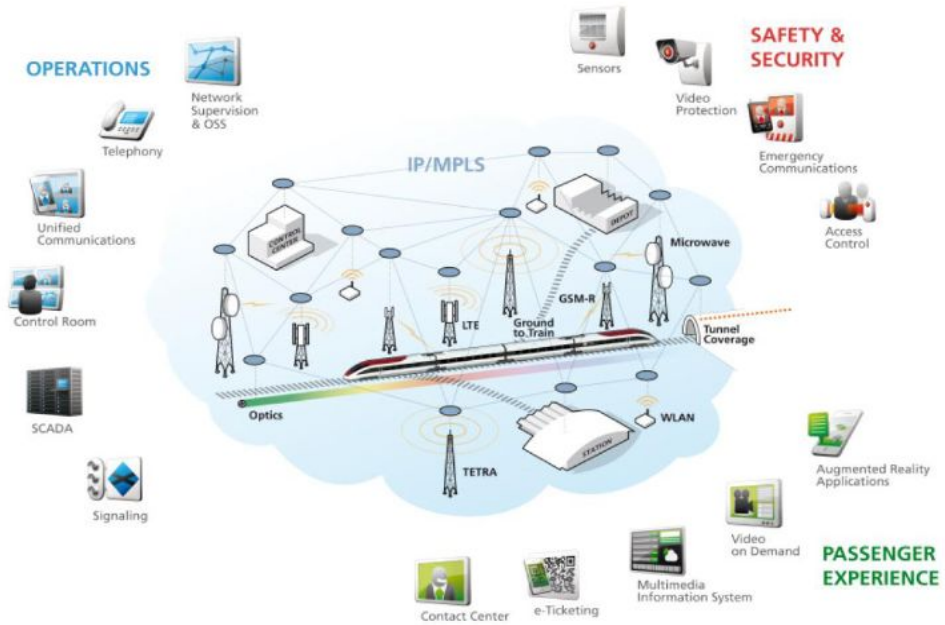


Figure 1 - Railway system scheme

Convergenza tra IT e OT nei Sistemi a guida vincolata

La convergenza tra IT e OT nel settore dei trasporti a guida vincolata ha trasformato il modo in cui le reti operano, consentendo una maggiore efficienza, interoperabilità ed automazione. Questa integrazione comporta però anche sfide significative in termini di sicurezza informatica.

Convergenza tra IT e OT nei Sistemi a guida vincolata: Benefici della convergenza IT-OT

- **Automazione e controllo avanzati**
  - L'adozione di sistemi come CBTC (Communication-Based Train Control) e SCADA permette un controllo centralizzato e in tempo reale delle operazioni ferroviarie.

- **Efficienza operativa**
  - La digitalizzazione dei processi operativi riduce i tempi di risposta e migliora la puntualità dei servizi.

- **Manutenzione predittiva**
  - Sensori IoT e analisi dei dati consentono di anticipare guasti e ottimizzare la manutenzione delle infrastrutture.

Convergenza tra IT e OT nei Sistemi a guida vincolata: Rischi associati alla convergenza

- **Superficie di attacco più ampia**
  - L'interconnessione tra IT e OT espone le reti ferroviarie a nuove vulnerabilità, poiché i sistemi OT tradizionalmente isolati sono ora accessibili tramite reti IT.

- **Minacce agli asset critici**
  - Attacchi mirati possono compromettere i sistemi di segnalazione, il controllo del traffico e altri componenti vitali, mettendo a rischio la sicurezza dei passeggeri.

- **Mancanza di standardizzazione**
  - I sistemi OT spesso utilizzano tecnologie proprietarie e non standardizzate, complicando l'implementazione di misure di sicurezza unificate.

Convergenza tra IT e OT nei Sistemi a guida vincolata: Sfide per la sicurezza

- **Sistemi Legacy e obsolescenza**
  - Molti sistemi OT sono progettati senza sicurezza intrinseca, rendendo difficoltosa la loro protezione contro minacce moderne.

- **Interoperabilità**
  - Garantire la compatibilità tra sistemi IT e OT senza compromettere la sicurezza è una delle principali sfide dal punto di vista della cybersecurity.

- **Impatto sui sistemi critici**
  - Attacchi alle infrastrutture di segnalazione o controllo possono portare ad eventi catastrofici.

- **Interconnessione IT/OT**
  - Amplificazione delle dipendenze critiche e potenziali vulnerabilità.

Equilibrio tra opportunità e rischi

Opportunità:

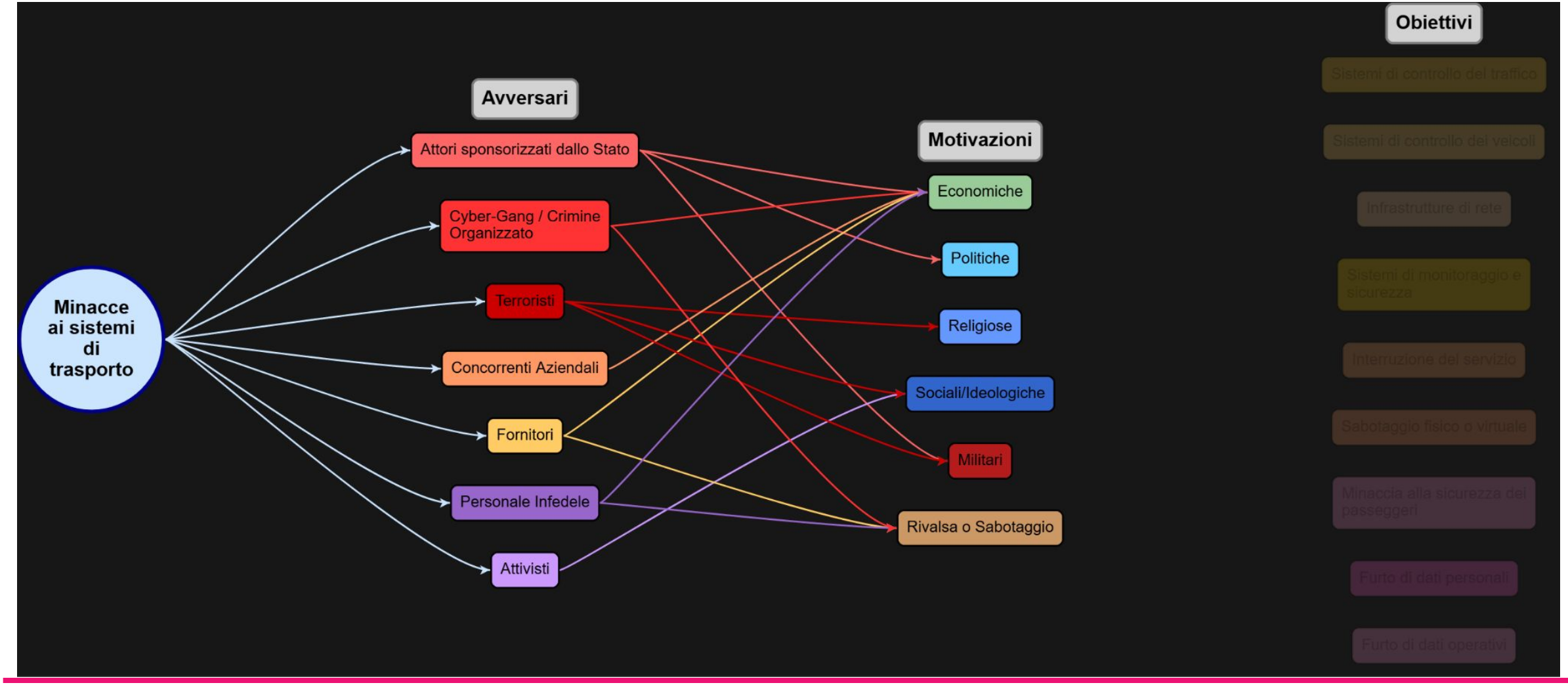
- Efficienza operativa
  - gestione avanzata del traffico e automazione dei sistemi.
- Esperienza del passeggero
  - bigliettazione elettronica e informazioni in tempo reale.
- Riduzione dei costi
  - manutenzione predittiva e ottimizzazione delle risorse.

Rischi:

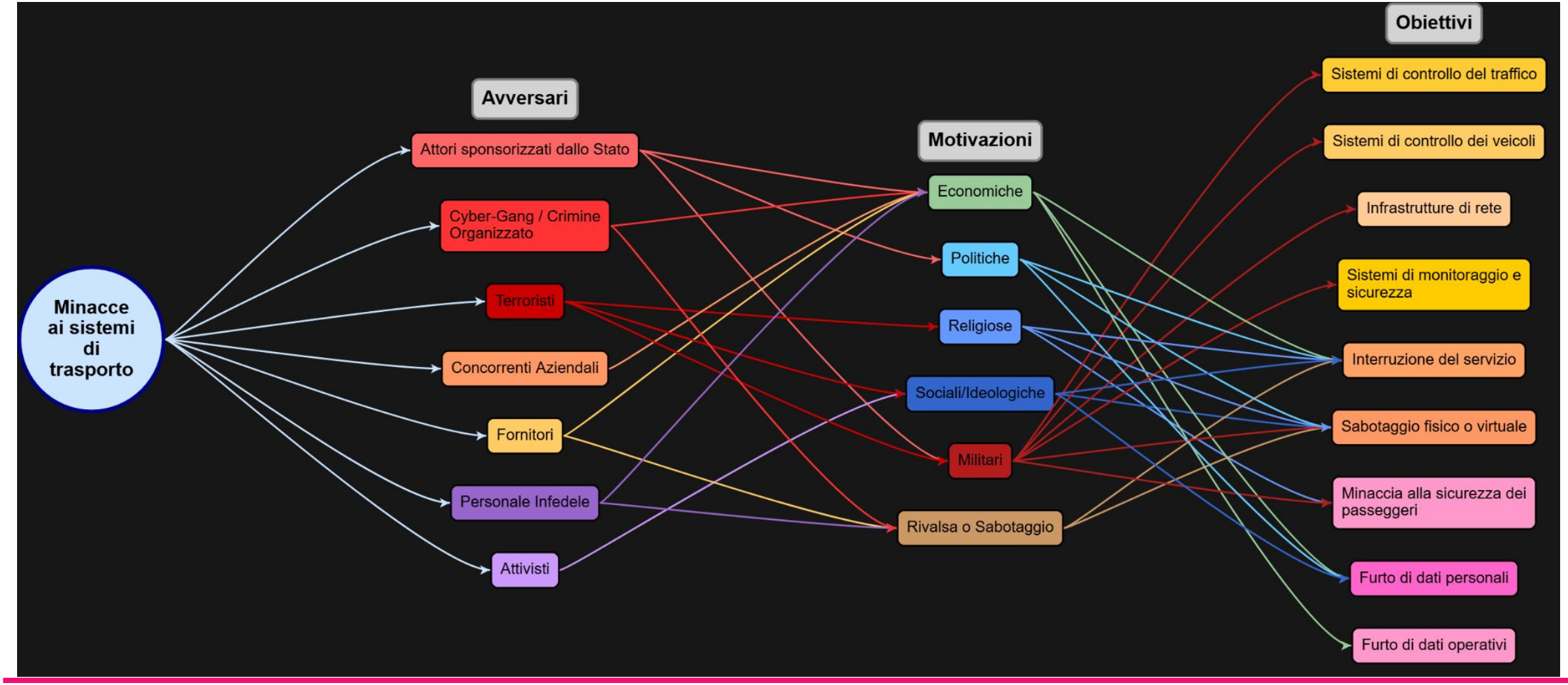
- Cybersecurity
  - esposizione ad attacchi ransomware, phishing o sabotaggi mirati.
- Impatto sui sistemi critici
  - attacchi alle infrastrutture di segnalazione o controllo.
- Interconnessione IT/OT
  - amplificazione delle dipendenze critiche e potenziali vulnerabilità.

Panoramica delle minacce

Panoramica delle minacce



Panoramica delle minacce



Anatomia dell'avversario: State-Sponsored Actors

- **Capacità**: Hanno accesso a risorse avanzate, team altamente qualificati e strumenti personalizzati (APT - Advanced Persistent Threats).
  Gli attacchi possono essere pianificati ed eseguiti su archi temporali estesi (da 6 mesi a 2 o più anni)

- **Obiettivi**: Spionaggio strategico, sabotaggio di infrastrutture critiche, destabilizzazione geopolitica.

Anatomia dell'avversario: Attivisti (Hacktivist)

- **Capacità:** Utilizzano strumenti open-source e tecniche di social engineering; attacchi spesso identificabili come DDoS o defacement di siti web.

- **Obiettivi:** Promuovere cause ideologiche o politiche, attirare l'attenzione su questioni sociali o economiche.

Anatomia dell'avversario: Terroristi

- **Capacità:** Limitate rispetto agli attori statali, ma possono utilizzare strumenti disponibili al pubblico; sfruttano vulnerabilità non monitorate.

- **Obiettivi:** Causare panico e interruzioni, danneggiare infrastrutture chiave per massimizzare l'impatto psicologico.

Anatomia dell’avversario: Cyber-Gang / Crimine Organizzato

- **Capacità:** Esperti nell'uso di ransomware, frodi finanziarie e attacchi alla supply chain; collaborano spesso con insider.

- **Obiettivi:** Profitto economico tramite estorsioni (es. ransomware) o furto di dati sensibili per rivenderli nel dark web.

Anatomia dell'avversario: Business Competitors

- **Capacità:** Vengono ingaggiati team specializzati per attacchi mirati volti al furto di proprietà intellettuale o per acquisire vantaggi competitivi (es. Dati del business, occupazione delle tratte, etc.)

- **Obiettivi:** Sottrarre dati sensibili o strategici, sabotare i sistemi del concorrente per ottenere vantaggi di mercato.

Anatomia dell'avversario: Personale Infedele (Insider Threats)

- **Capacità:** Accesso diretto a sistemi e dati sensibili, sfruttano privilegi interni o mancanze nei controlli.

- **Obiettivi:** Vendetta personale, guadagno economico (vendita di dati), supporto a campagne di attacco esterne.

Anatomia dell'avversario: Fornitori (Supply Chain Threats)

- **Capacità:** Duplici. Possono diventare inconsapevoli vettori di attacco attraverso software compromessi o accesso alle reti o essere loro stessi gli attori malevoli, fornendo sistemi o software aventi funzionalità nascoste (es. introduzione errori o spegnimenti alla scadenza del contratto commerciale)

- **Obiettivi:** Nel caso di attori inconsapevoli, i medesimi dei reali attaccanti. Nel secondo caso per lo più economiche o di rivalsa.

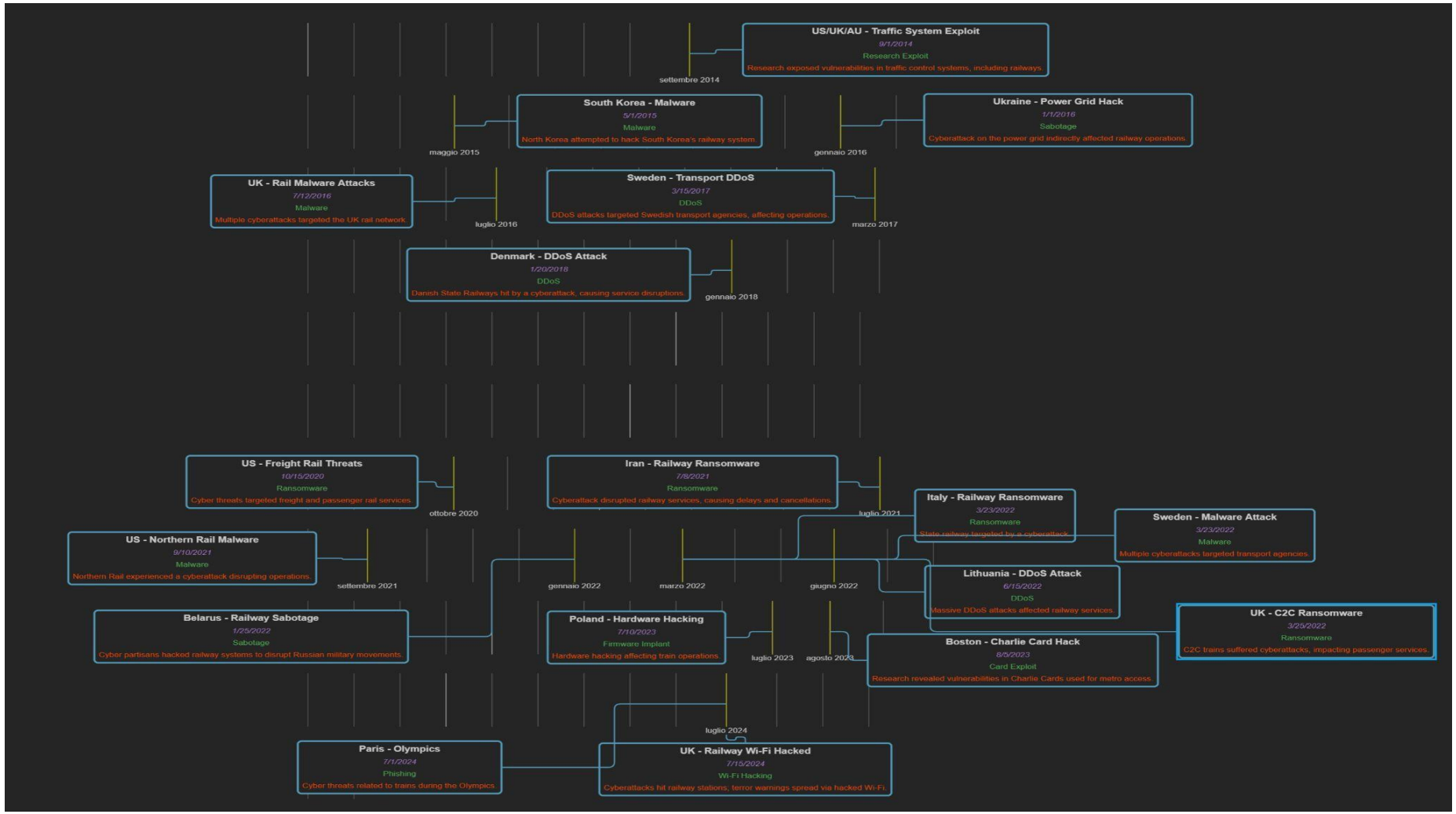
Superficie d'attacco

- Società erogatrici
  - Attacchi mirati ai sistemi o dipendenti aziendali

- Operational Systems (Sistemi & Servizi Digitali)
  - **Sistemi IT**
  - **Sistemi OT**
  - **Sistemi di comunicazione**

- Utenti finali
- Fornitori (Supply-Chain)

Cronologia degli attacchi ai sistemi a guida vincolata
(2014-2024)

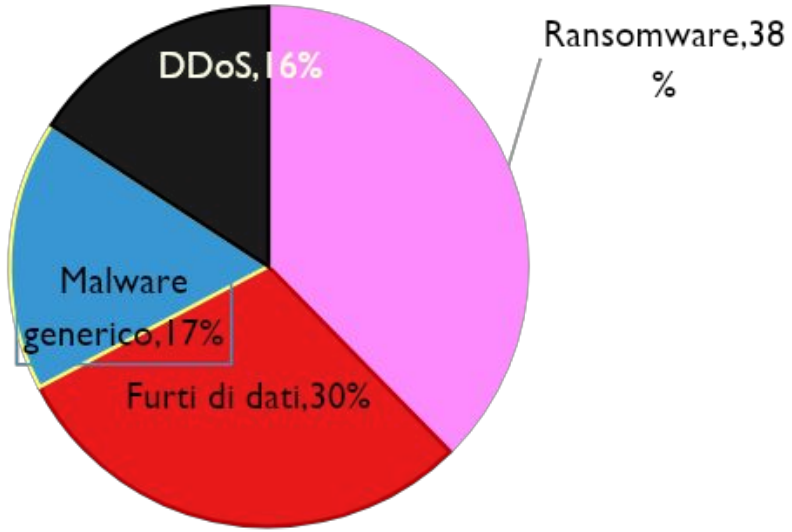


Statistiche Cyber nel Settore a guida vincolata

Aumento degli attacchi

- (2019-2021) **+175%**
- (2022-2024) **+220%**

Tipologia di attacchi principali (2021-2022)



Minacce Emergenti

Il 54% degli attacchi è attribuito a cybercriminali, mentre il 23% a hacktivisti motivati da cause ideologiche

Le principali vulnerabilità riguardano sistemi legacy e mancanza di patching (CBTC, SCADA)

Caso di studio - Attacco Wi-Fi

Il 25 settembre 2024, le reti Wi-Fi pubbliche del Regno Unito sono state compromesse, mostrando messaggi allarmanti relativi ad attacchi terroristi delle principali stazioni ferroviarie i in Europa. Le stazioni coinvolte includevano London Euston, Manchester Piccadilly e Birmingham

- **Causa dell'incidente**
  L'attacco è stato attribuito a una modifica non autorizzata delle pagine di accesso al Wi-Fi, effettuata tramite un account amministrativo legittimo. Ciò ha permesso agli aggressori di alterare i contenuti visualizzati dagli utenti al momento della connessione.
- **Attori coinvolti**
  Un dipendente di Global Reach Technology, l'azienda responsabile della fornitura del servizio Wi-Fi, è stato arrestato con l'accusa di aver abusato dei propri privilegi per diffondere contenuti islamofobi.
- **Lesson Learned**
  Questo incidente evidenzia la vulnerabilità delle infrastrutture digitali nei trasporti pubblici e sottolinea l'importanza di controlli rigorosi sugli accessi amministrativi per prevenire abusi interni.

Caso di studio - Sabotaggio

Il 26 luglio 2024, a poche ore dalla cerimonia di apertura delle Olimpiadi di Parigi, la rete ferroviaria francese è stata colpita da atti di sabotaggio coordinati che hanno paralizzato i treni ad alta velocità (TGV) su tre delle quattro principali linee: Atlantica, Nord ed Est. Questi atti dolosi hanno causato disagi a circa 800.000 passeggeri, molti dei quali diretti alla capitale per l'evento inaugurale.

- **Causa dell'incidente**
  Gli attacchi hanno coinvolto incendi dolosi che hanno danneggiato infrastrutture critiche della rete ferroviaria, tra cui cavi in fibra ottica e quadri elettrici, compromettendo la circolazione dei treni.
- **Causa dell'incidente**
  Sebbene nessun gruppo abbia rivendicato la responsabilità, le autorità sospettano l'implicazione di gruppi estremisti interni. Le indagini sono tutt'ora in corso per identificare i responsabili.
- **Implicazioni**
  Questo incidente sottolinea la vulnerabilità delle infrastrutture critiche durante eventi di grande portata e l'importanza di misure di sicurezza proattive per prevenire tali attacchi.

Caso di studio - Supply-Chain

Nel 2022, la compagnia ferroviaria polacca ha riscontrato guasti inspiegabili su diverse mezzi di un particolare modello fornito da un unico costrutture. Nonostante le procedure di manutenzione fossero state eseguite correttamente da una officina terza, i mezzi risultavano inoperativi, con i sistemi che indicavano falsi errori e impedivano l'avvio dei motori.

- **Causa dell'incidente**
  Un'analisi condotta dal gruppo di hacker etici ha rivelato che il software dei treni conteneva codice progettato per bloccare il funzionamento dei veicoli se rilevava che la manutenzione era stata effettuata da officine non autorizzate dal produttore. In particolare, il sistema utilizzava dati GPS per determinare la posizione del treno e, se questa corrispondeva a quella di un manutentore indipendente, il software impediva l'avvio del treno.
- **Attori coinvolti**
  l Produttore dei treni, accusato di aver inserito intenzionalmente nel software dei veicoli meccanismi che ne impedivano il funzionamento dopo manutenzioni effettuate da terzi non autorizzati. Il produttore ha negato tali accuse e le indagini sono tutt'ora in corso
- **Implicazioni**
  Questo caso evidenzia i rischi associati all'integrazione di software proprietario nelle infrastrutture critiche e solleva questioni etiche riguardo alle pratiche dei produttori che limitano le riparazioni da parte di terzi, influenzando la concorrenza e la sicurezza operativa.

Caso di studio - Disservizi legati ad attacchi

Svezia - Attacco Malware

Nel 2022, la compagnia ferroviaria polacca ha riscontrato guasti inspiegabili su diversi mezzi di un particolare modello fornito da un unico costrutture. Nonostante le procedure di manutenzione fossero state eseguite correttamente da una officina terza, i mezzi risultavano inoperativi, con i sistemi che indicavano falsi errori e impedivano l'avvio dei motori.

- **Impatto**
  Rallentamenti nei servizi ferroviari e aumento delle misure di sicurezza.

Italia - Attacco Ransomware

Nel mese di Marzo 2022 le ferrovie dello Stato italiane sono state prese di mira da un ransomware che ha bloccato i sistemi di bigliettazione e gestione delle operazioni

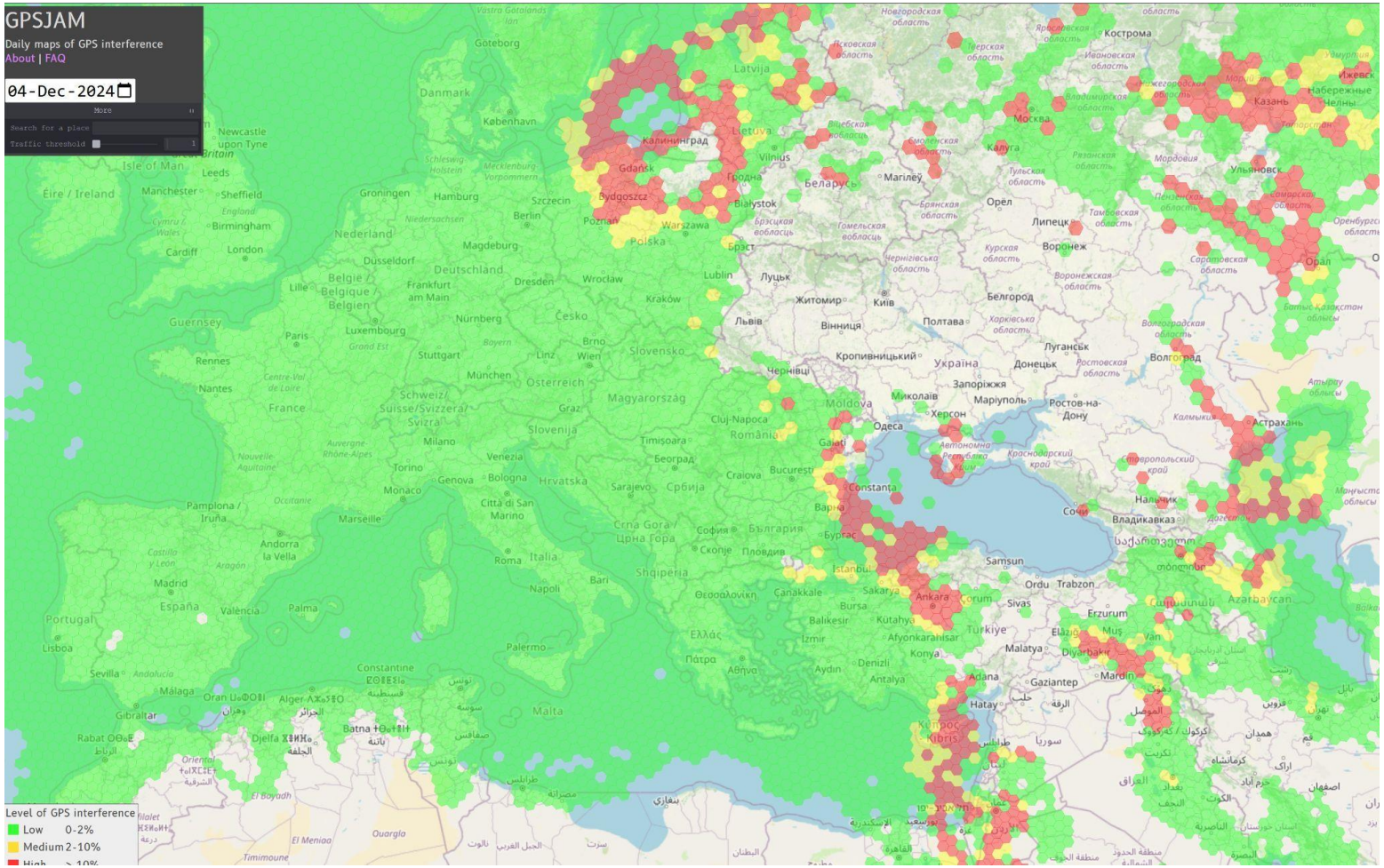
- **Impatto**
  Servizi temporaneamente sospesi e perdita di dati sensibili.

UK - Attacco Ransomware

Sempre nel Marzo 2022 la linea ferroviaria C2C nel Regno Unito ha subito un attacco ransomware che ha bloccato i sistemi di prenotazione e informazioni per i passeggeri

- **Impatto**
  Servizi temporaneamente sospesi e perdita di dati sensibili.

Caso di studio - Electronic Warfare



GPS Signal Jamming

Attacchi elettronici su larga scala stanno interferendo nel traffico aeronavale, in particolare nei paesi baltici.

- Fenomeno correlato agli attuali scenari di guerra (Russo-Ucraina)
- In continua evoluzione in termini di intensità ed estensione geografica
- Le attuali tecnologie difensive risultano estremamente costose e limitate nell'efficacia

Panoramica sintetica delle strategie di difesa

- Standard di sicurezza: NIST, ISO/IEC 27001, IEC 62443 e le direttiva TSA
- Risk Assessment: IEC 62443, CLC/TS 50701 e linee guida ENISA
- Cyber Security Strategy
- Vulnerability Management, Penetration Test e Red Teaming
- Piani e procedure di Patching, Incident Response, Comunicazione pubblica
- Formazione e sensibilizzazione di tutto il personale
- Attenta gestione delle terze parti
- Monitoraggio e audit continui
- Continuo aggiornamento delle procedure
- Ricerca e innovazione

Strategie di Difesa: Benefici di Audit e Pentest Continuativi - perché sono fondamentali

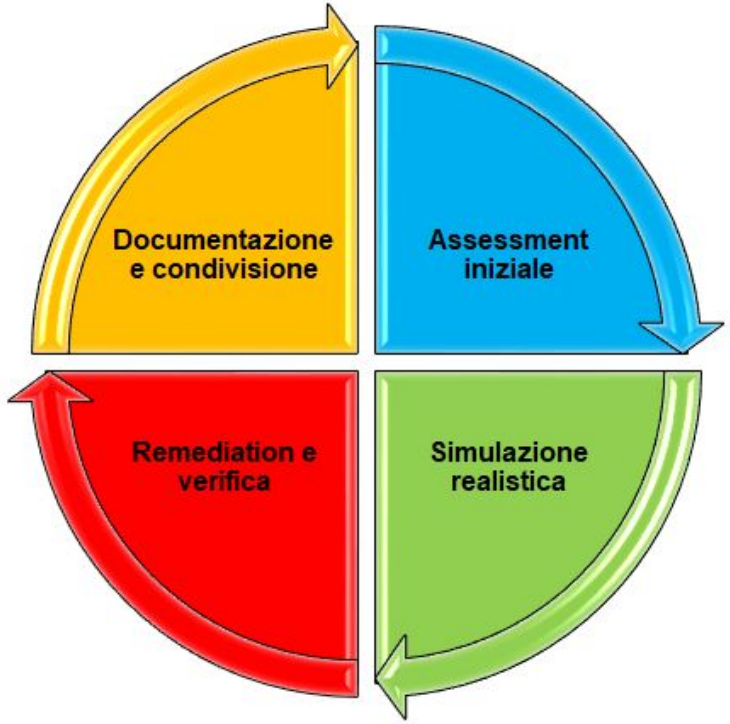
- **Identificazione precoce delle vulnerabilità**
  - Gli audit periodici permettono di scoprire configurazioni errate, vulnerabilità sconosciute e falle nei sistemi.
  - Pentest e attività di red-teaming simulano attacchi reali per identificare scenari di rischio specifici.
- **Adattamento alle minacce emergenti**
  - Gli scenari di attacco evolvono rapidamente: un approccio continuativo consente di aggiornare costantemente le difese.
- **Miglioramento continuo**
  - Le raccomandazioni risultanti da queste attività aiutano a perfezionare i processi di sicurezza, migliorando la resilienza complessiva.
- **Validazione delle misure di sicurezza**
  - Test periodici assicurano che le patch, i sistemi e le configurazioni implementate siano effettivamente efficaci.

Strategie di Difesa: Benefici di Audit e Pentest Continuativi - Benefici tangibili

- **Riduzione del rischio**
  - diminuzione della probabilità di incidenti gravi e loro impatto.
- **Conformità normativa**
  - molte regolamentazioni (es. ISO/IEC 27001, NIS Directive) impongono audit periodici.
- **Risparmio economico**
  - prevenire un attacco costa molto meno che gestirne le conseguenze.
- **Miglioramento della reputazione:**
  - dimostrare un impegno continuo nella sicurezza aumenta la fiducia di clienti e stakeholder.

Strategie di Difesa: Benefici di Audit e Pentest Continuativi - Ciclo continuo di miglioramento

- **Assessment iniziale:**
  - Identificazione delle aree critiche e definizione del perimetro d'azione.
- **Simulazione realistica:**
  - Attività di red-teaming focalizzate su asset critici.
- **Remediation e verifica:**
  - Implementazione delle raccomandazioni e verifica del loro successo tramite follow-up audit.
- **Documentazione e condivisione:**
  - Report chiari per stakeholder e management, per guidare decisioni strategiche.



✶Grazie per la cortese attenzione ✶

Luca Cancelliere	*CyberSecurity & Ethical Hacking*	*Netservice SpA*	
Matteo Morazzoni	*Cybersecurity & Risk Management*		

Per approfondimenti: info@flosslab.com

Coordinato da:

MINISTERO DELLE INFRASTRUTTURE E DEI TRASPORTI

Organizzato da:

in qualità di Provider

asstra service

in collaborazione con

ASSOCIAZIONE ITALIANA per l'INGEGNERIA del TRAFFICO e dei TRASPORTI AIIT

asstra IMPRESE IN MOVIMENTO

CIFI COLLEGIO INGEGNERI FERROVIARI ITALIANI