FEDERMACCHINE

Cybersecurity e beni strumentali: una partita da giocare (e vincere)

Organizzazione della cybersecurity in un’azienda manifatturiera

23 Febbraio 2023

SACMI

Francesca Merighi
Cybersecurity Officer, SACMI Group

Metodologia e standard di riferimento per la Cybersecurity

1. Qual'è l'**impatto** di un incidente di sicurezza sul business? → Business Impact Analysis

   Perdite finanziarie, di mercato, danni reputazionali, danni alla salute delle persone, ecc.

2. Qual'è la **probabilità accettabile** che un incidente di sicurezza causi l'impatto?
   → **Da chi mi voglio difendere?**

3. Come mi posso difendere?

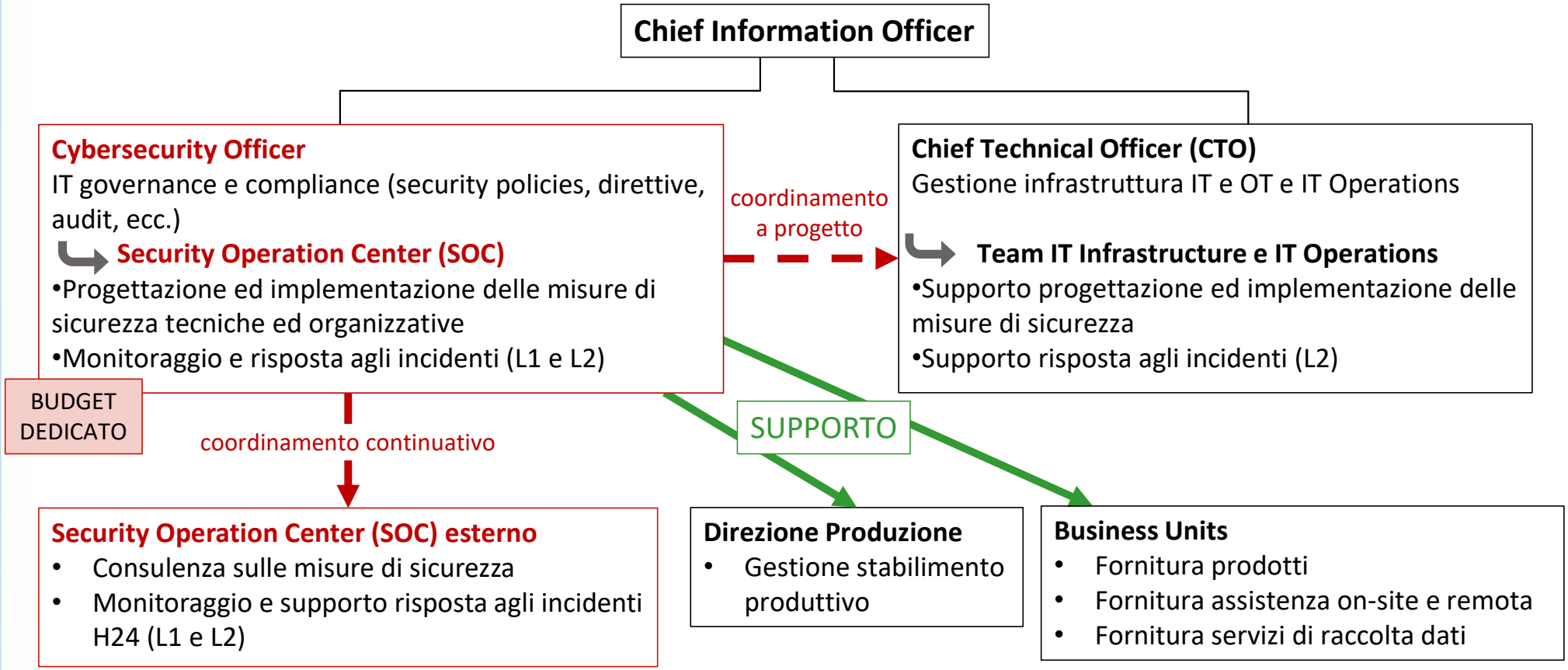
   Con **misure e controlli adatti al Security Level Target (SL-T) stabilito**

   - Misure di sicurezza organizzative — *Standard **ISO 27001***
   - Misure di sicurezza tecniche — *Standard **IEC 62443***

IEC 62443 - Security Levels (SL)		
SL 0	nessun requisito di security specifico	
SL 1	protezione contro una violazione casuale	
SL 2	**protezione contro violazione intenzionale avvenuta con metodi semplici e poche risorse**	Target tipico per le aziende manifatturiere
SL 3	protezione contro violazione intenzionale avvenuta con metodi sofisticati e risorse moderate	Target tipico per produttori di generi alimentari e medicali
SL 4	protezione contro violazione intenzionale avvenuta con metodi sofisticati e risorse estese	Target tipico per fornitori servizi critici (energia, acqua, gas, ecc.)

COSTO

Ruoli e responsabilità nell'ambito della Cybersecurity



Misure di sicurezza in ambito IT

PRIORITÀ

- RISERVATEZZA
- INTEGRITÀ
- DISPONIBILITÀ

TEMPO DI VITA 2-3 ANNI

DISPOSITIVI CHE OPERANO ANCHE IN **MOBILITÀ**

SICUREZZA DEI DISPOSITIVI

1. **Aggiornamenti di sicurezza** frequenti
2. Rilevazione, prevenzione delle minacce e risposta agli incidenti da remoto con **antivirus di ultima generazione**
3. Controllo del software installato e dei processi in esecuzione

CONTROLLO DEL TRAFFICO DI RETE

1. **Controllo** e limitazione del **traffico internet** anche per i dispositivi in mobilità
2. **Controllo** e limitazione del **traffico di rete locale**

PROTEZIONE IDENTITA'

1. **Monitoraggio** dei log di accesso e delle attività degli account
2. **Autenticazione a più fattori** (MFA) per gli accessi a rischio

PROTEZIONE E-MAIL

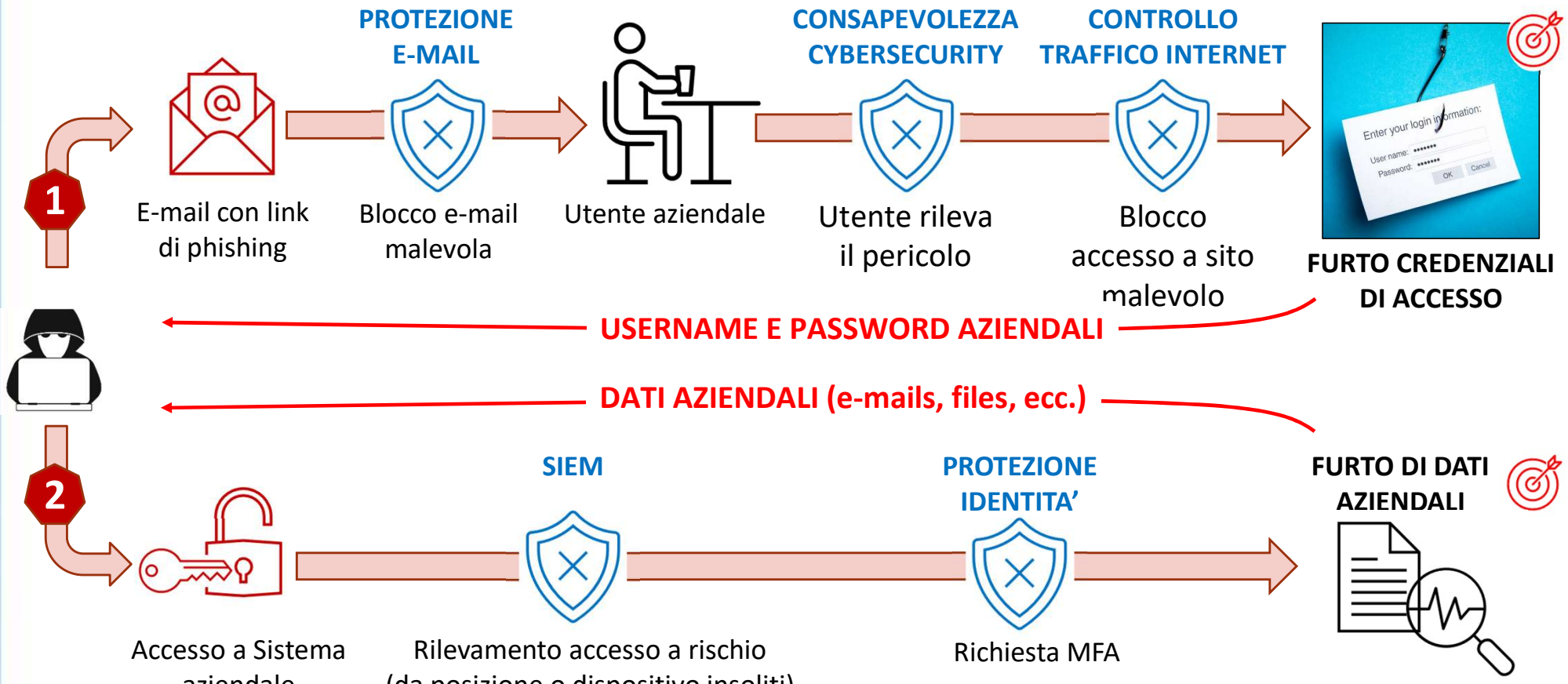
Prevenzione di phishing e infezioni malware attraverso controllo

1. della provenienza delle e-mail
2. del testo della e-mail
3. Controllo di link ed allegati

GOVERNANCE

1. **Raccolta e correlazione di tutti gli eventi di sicurezza** (SIEM), risposta automatica ad alcuni eventi (SOAR)
2. Programma continuativo **di sensibilizzazione (Awareness) del personale** sulla Cybersecurity
3. **Assicurazione Cyber**

Esempio: furto di identità e dati aziendali



Sicurezza dei dispositivi OT

PRIORITÀ

DISPONIBILITÀ

INTEGRITÀ

RISERVATEZZA

TEMPO DI VITA
15-20 ANNI

PROCESSI DI PROTEZIONE DALLE MINACCE → Possono **interferire con i processi produttivi**

MODIFICHE HARDWARE → Se eseguite quando la macchina è in produzione, possono richiedere

- **interruzione della Produzione**
- riesecuzione di **FAT/SAT** o **ricertificazione** della macchina

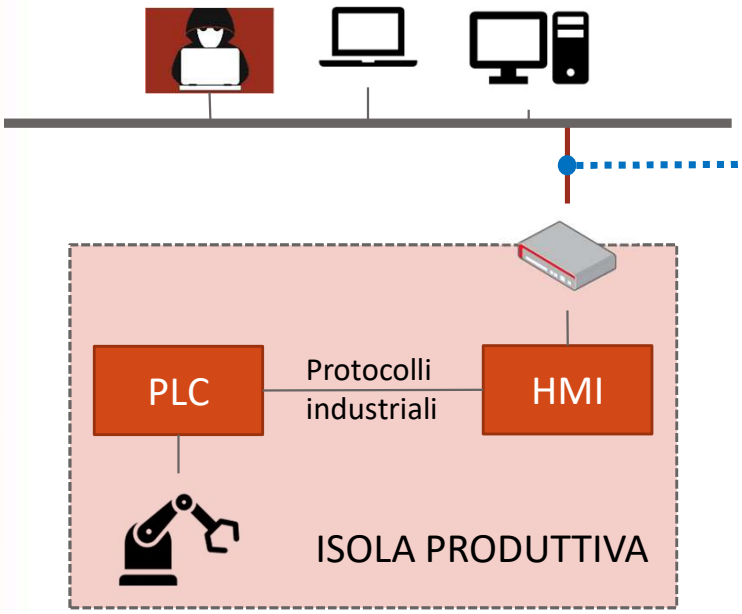
Es. Estensione di RAM e HD per rendere più performante il dispositivo

MODIFICHE SOFTWARE

- Installazione programmi
- Aggiornamenti software (sistema operativo e programmi)
- Cambiamenti di configurazione (abilitazione/disabilitazione servizi, impostazione Windows Firewall, ecc.)

COSTI

Controllo di rete in ambito OT



Intrusion Detection System (IDS)

Security Operation Center (H 24)

Monitoraggio passivo del traffico di rete non altera il funzionamento della strumentazione OT

Dispositivi

che generano traffico di rete (IP, MAC Address, sistemi operativi, porte aperte, servizi attivi, ecc.)

⚠ Alert: dispositivi sconosciuti, non conformità nella configurazione dei dispositive (sistemi operativi obsoleti, ecc.)

Flussi di dati

generati dai dispositivi (sorgente e destinazione, protocolli, contenuto dei messaggi, ecc.)

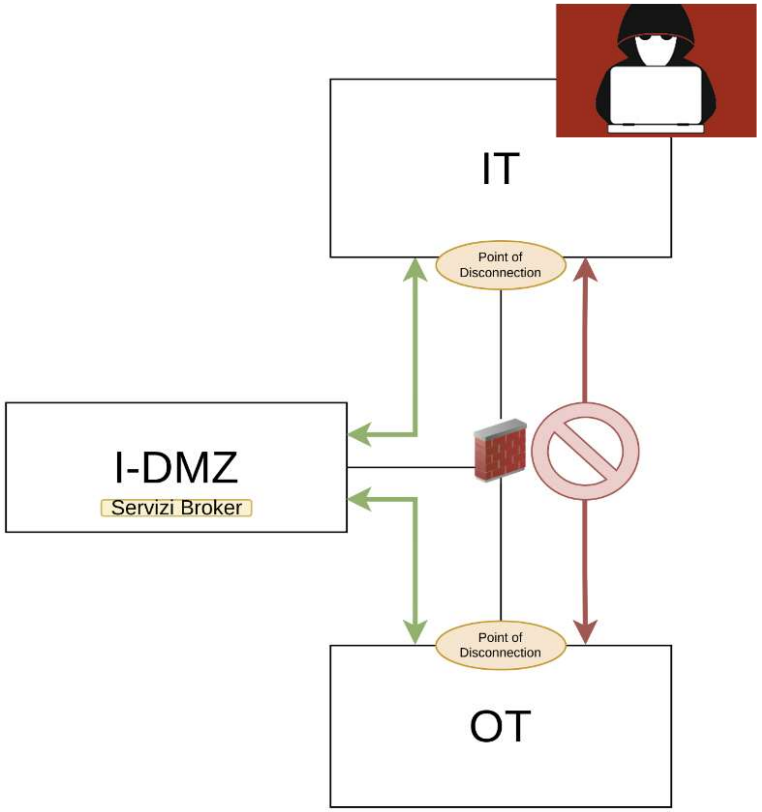
⚠ Alert: comunicazioni insolite, dal contenuto palesemente malevolo o semplici non-conformità (protocolli obsoleti, ecc.)

Segregazione di rete IT/OT e Industrial DMZ

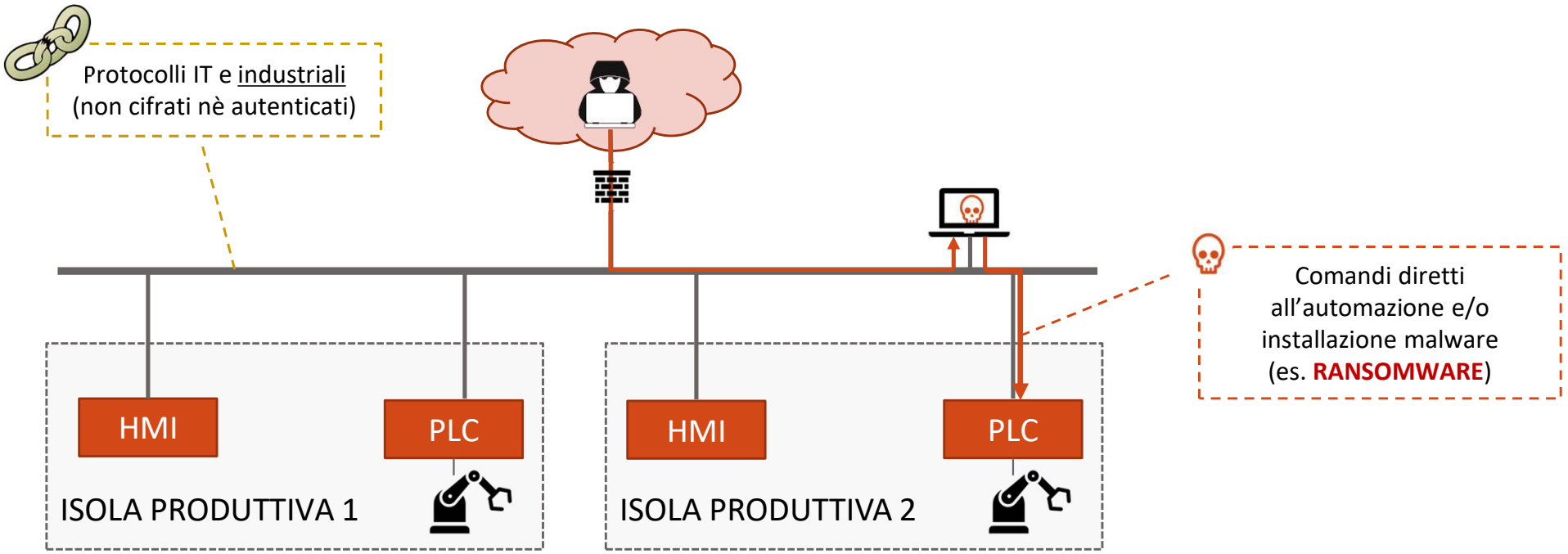
Livello di sicurezza addizionale tra la rete Corporate (IT) e la rete industriale (OT).

Principi

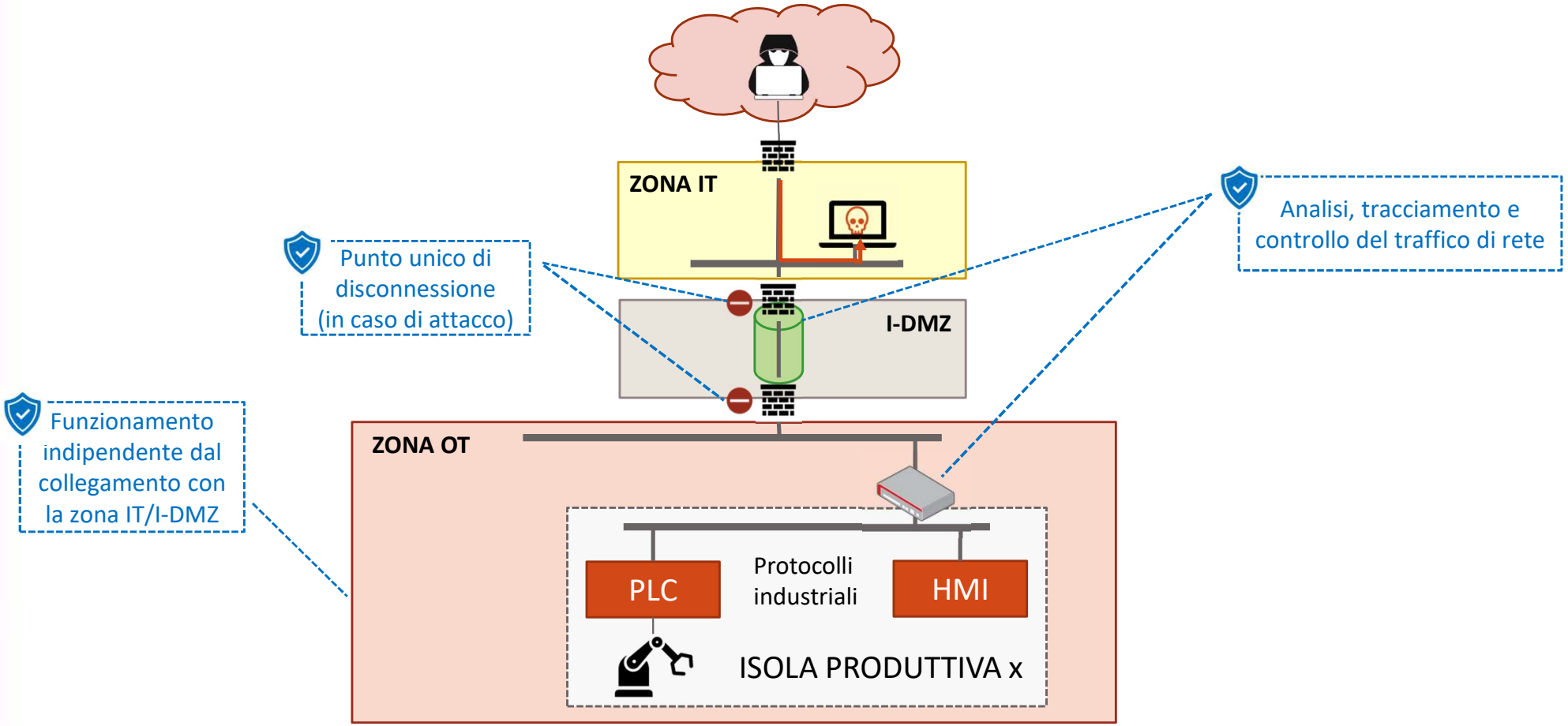
- La rete IT è considerata non affidabile: nessuna connessione diretta consentita tra rete IT e OT;
- Comunicazioni con protocolli di rete industriali confinati nella rete OT;
- Almeno un Single Point of Disconnection tra la rete IT e la rete OT.



Architettura industriale vulnerabile



Segregazione di rete IT/OT e Industrial DMZ



FEDERMACCHINE

Grazie per l'attenzione, per informazioni

SACMI

Francesca Merighi | CyberSecurity Officer

SACMI Group | Via Selice Prov.le, 17/a | 40026 Imola (BO) |Italy

T +39 - 0542 – 607896 | M +39 342 7648233

francesca.merighi@sacmigroup.com |www.sacmi.com