SS4SP
safety and security for
smart production

Safety e Security for Smart Production

SOLUZIONI PROCEDURALI E TECNOLOGICHE INNOVATIVE PER MIGLIORARE LA SICUREZZA INFORMATICA, LA CONTINUITÀ OPERATIVA E LA SAFETY DEGLI IMPIANTI DELL'INDUSTRIA 4.0

21 Luglio 2022

I partners del progetto

END USERS

IMA SPA

imola informatica

SACMI

COLLABORAZIONI

bi-rex
Big Data Innovation & Research Excellence

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Università degli Studi di Ferrara

UNIMORE
UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA

TECHNOLOGY SERVICE PROVIDERS (TSP)

Alascom

SIEMENS

SS4SP
safety and security for smart production

Speakers

Coordinatrice del progetto e moderatrice

- Francesca Merighi, *Cybersecurity Officer, SACMI Group*

End users

- Filippo Bosi, *Chief Executive Officer, Imola Informatica*
- Gildo Bosi, *Automation R&D manager, SACMI Group*
- Pier Luigi Vanti, *ICT Corporate Director, IMA*

Referente scientifico

- Michele Colajanni, *Professore ordinario Università degli Studi di Bologna*

Collaboratori

- Carlo Giannelli, *Professore associato Università degli Studi di Ferrara*
- Mirco Marchetti, *Professore associato Università degli Studi di Modena e Reggio Emilia*
- Vincenzo Mucciante, *Assegnista di ricerca, Università degli Studi di Bologna*
- Giorgio Valenziano Santangelo, *Assegnista di ricerca, Università degli Studi di Modena e Reggio Emilia*

SS4SP
safety and security for smart production

SS4SP
safety and security for smart production

Introduzione

A cura di

Michele Colajanni

Filippo Bosi

Gildo Bosi

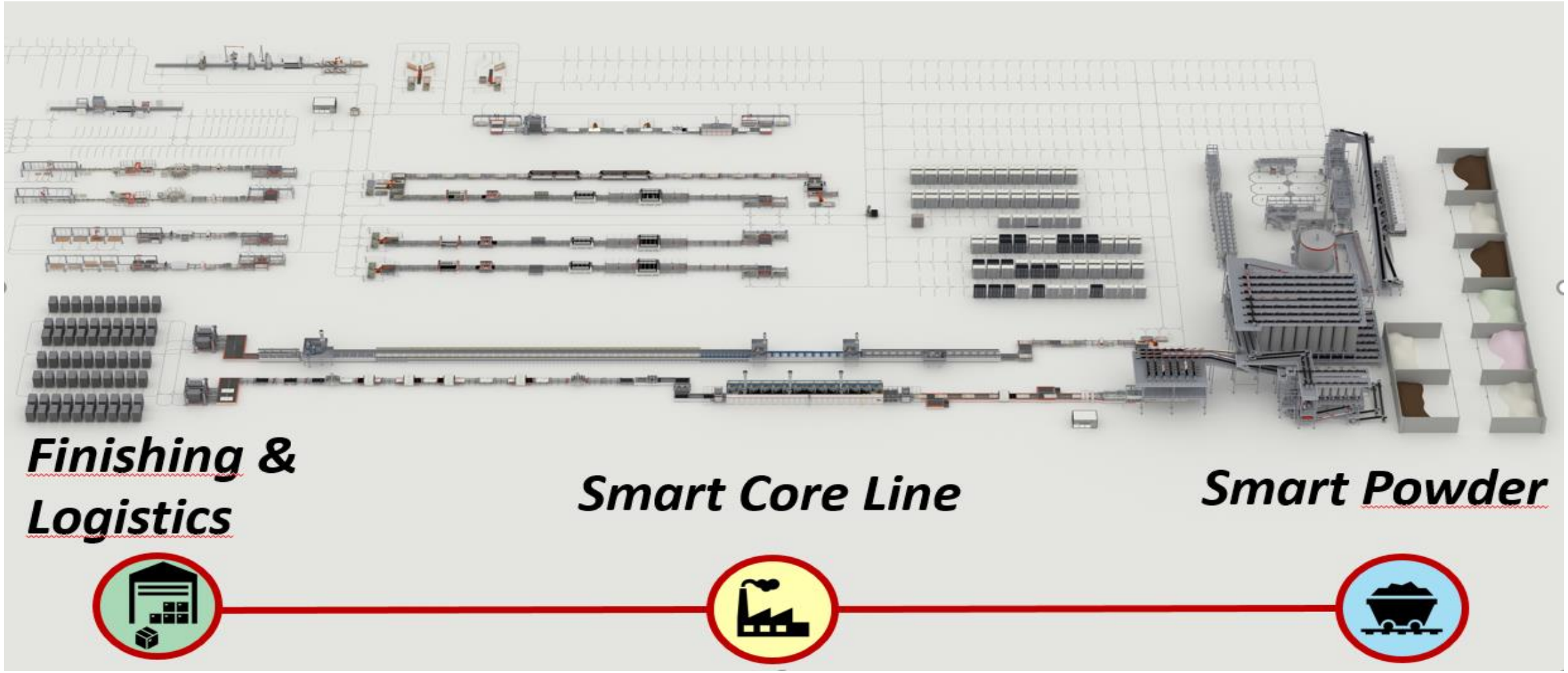
Francesca Merighi

Pier Luigi Vanti

Contenuti

- Origini e finalità del progetto
- Lo use case SACMI
- Lo use case BI-REX/IMA
- Obiettivi realizzativi del progetto

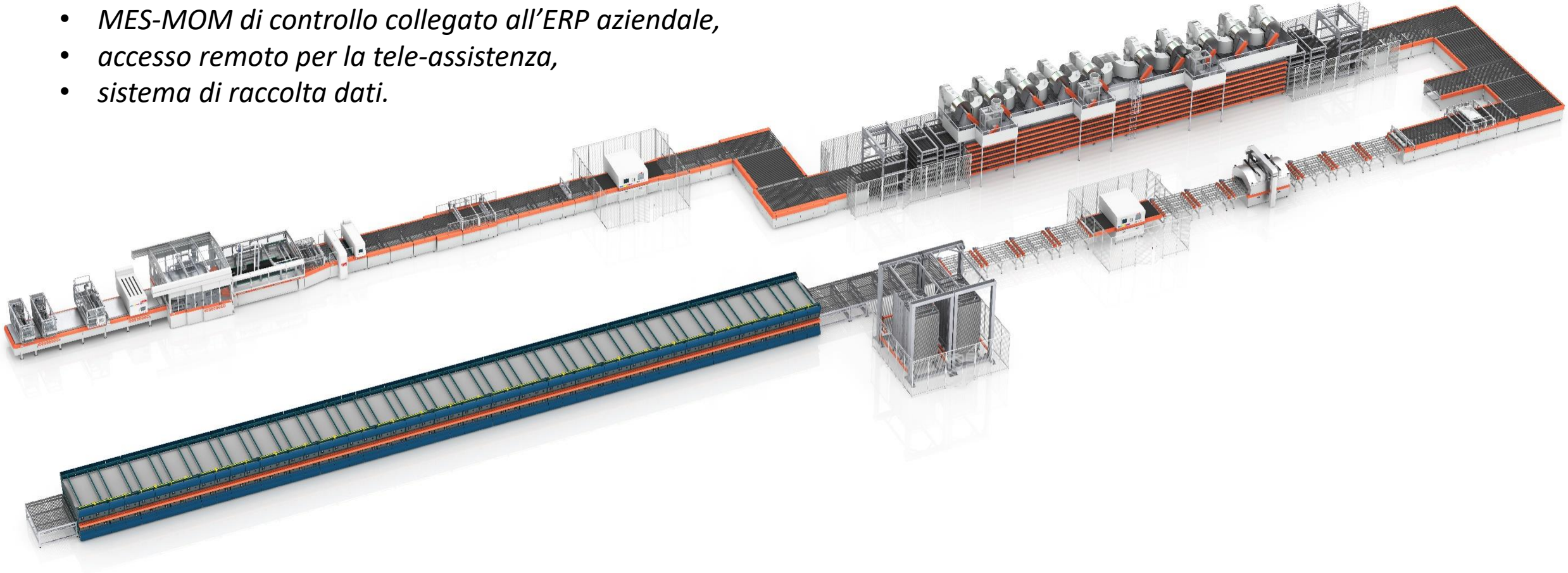
Use case SACMI – Tiles Plant



Use case SACMI – Tiles Lab – Linea Continua

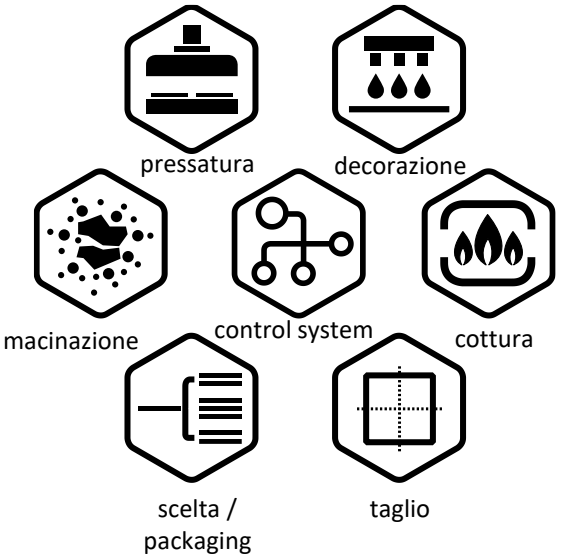
Linea produttiva ceramica di 28 macchine che comprende:

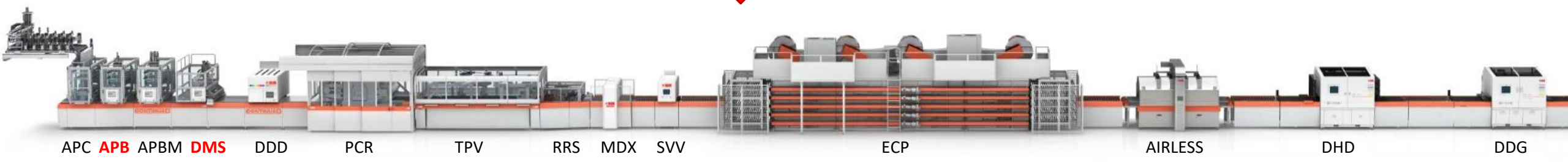
- *MES-MOM di controllo collegato all'ERP aziendale,*
- *accesso remoto per la tele-assistenza,*
- *sistema di raccolta dati.*



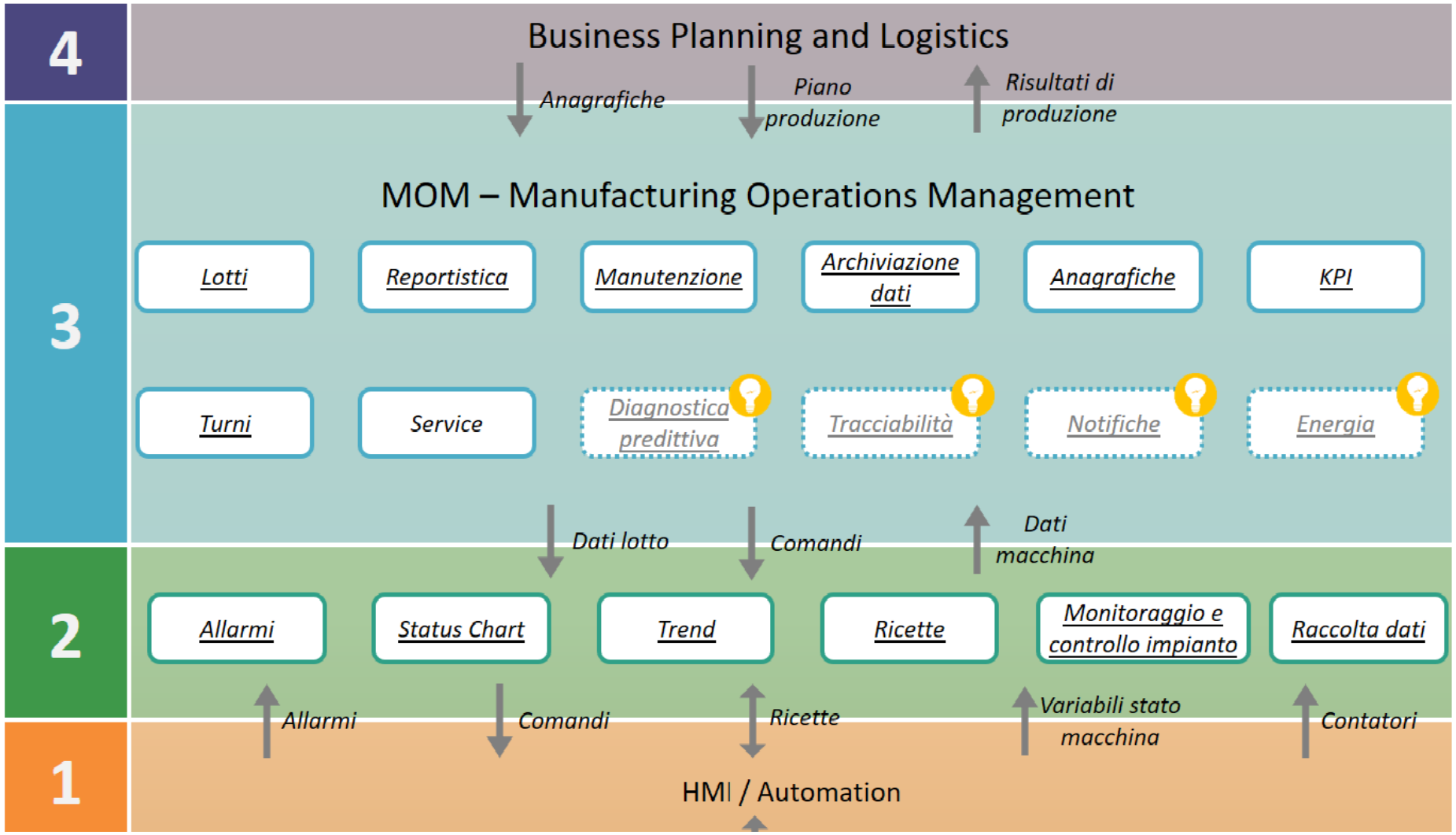
Use case SACMI – Tiles Lab – Linea Continua

here
Human Expertise
for Reactive Engineering





Use case SACMI – Tiles Lab



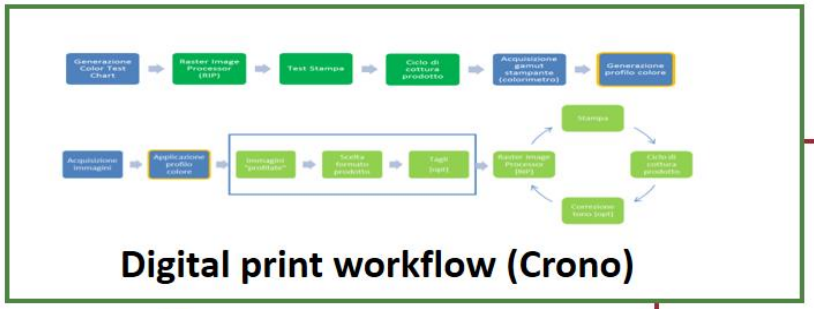
Use case SACMI – Digital print workflow

1

Architetto:
Progetto
ambiente

Studio Grafico Ceramico:
Progetto prodotto

2



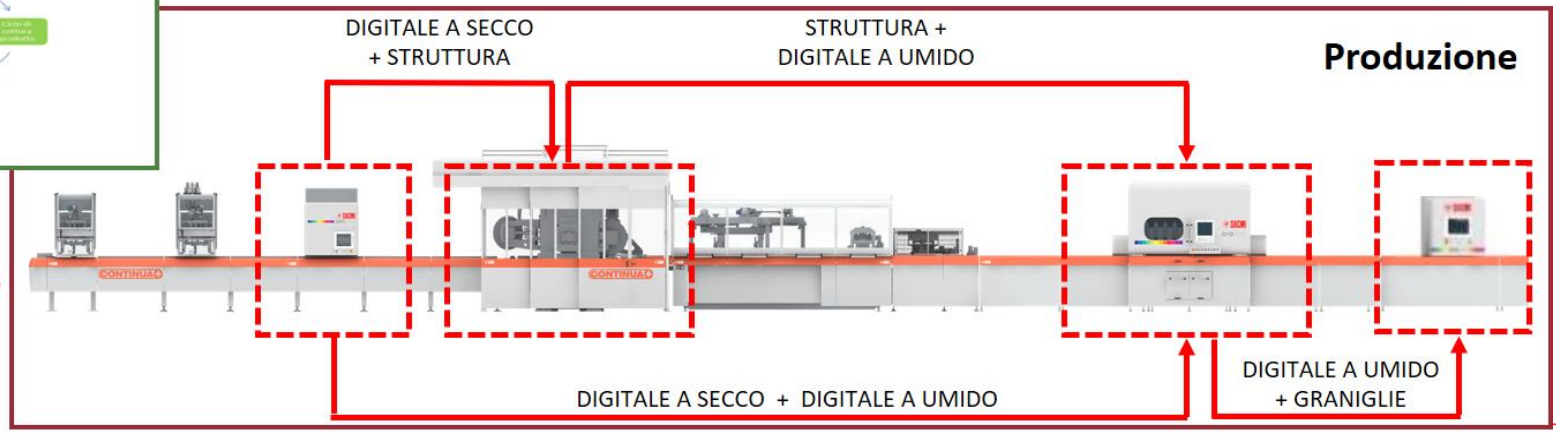
Retroazione qualità
prodotto (machine
learning)

4

here
Human Expertise
for Reactive Engineering

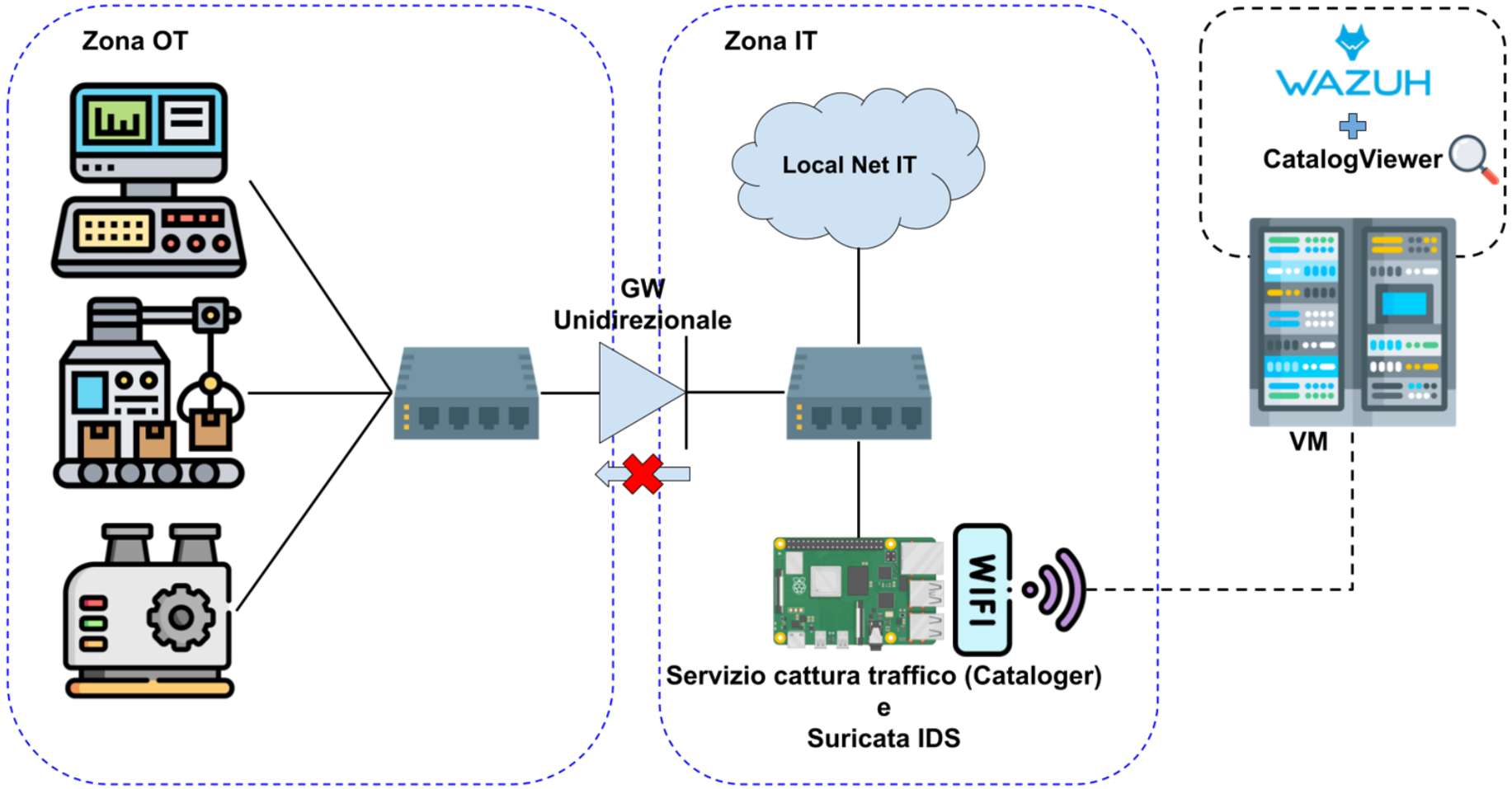
3

Impianto ceramico:
Cicli di lavorazione, gestione lotti



SS4SP
safety and security for
smart production

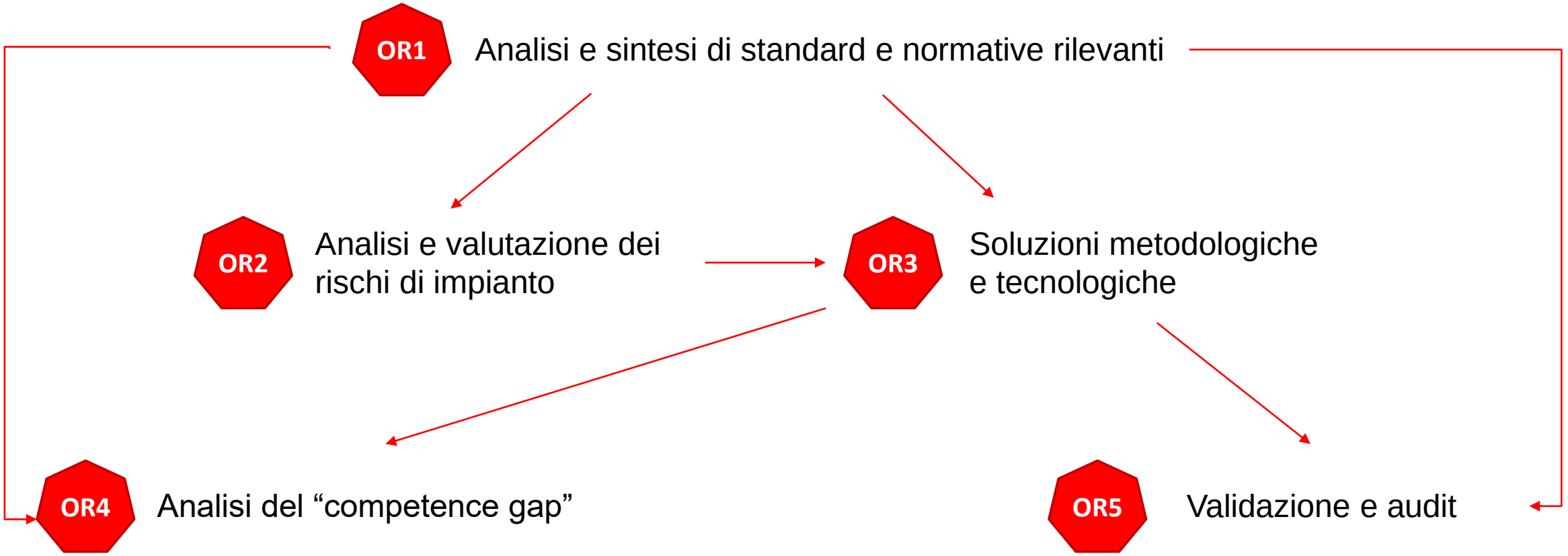
Use case BI-REX/IMA - Architettura



Use case BI-REX/IMA - Gateway IoT

- Tramite software IoT edge raccoglie i dati dai componenti delle macchine presenti nella zona OT

Obiettivi realizzativi del progetto



SS4SP
safety and security for
smart production

Presentazioni

Contenuti

1. Standard di sicurezza informatica applicabili in ambito industriale
2. Analisi e valutazione dei rischi informatici di impianto
3. Introduzione alle soluzioni metodologiche e tecnologiche a mitigazione dei rischi informatici di impianto
4. Monitoraggio del traffico di rete in ambito industriale
5. Implementazione della segregazione delle reti industriali
6. Verifica della mitigazione dei rischi

SS4SP
safety and security for
smart production

Standard di sicurezza informatica applicabili in ambito industriale

A cura di

Vincenzo Mucciante

Contenuti

- Stato dell'arte
- Standard safety
- Standard security
- Bridging documents

Metodologia integrata per safety e security

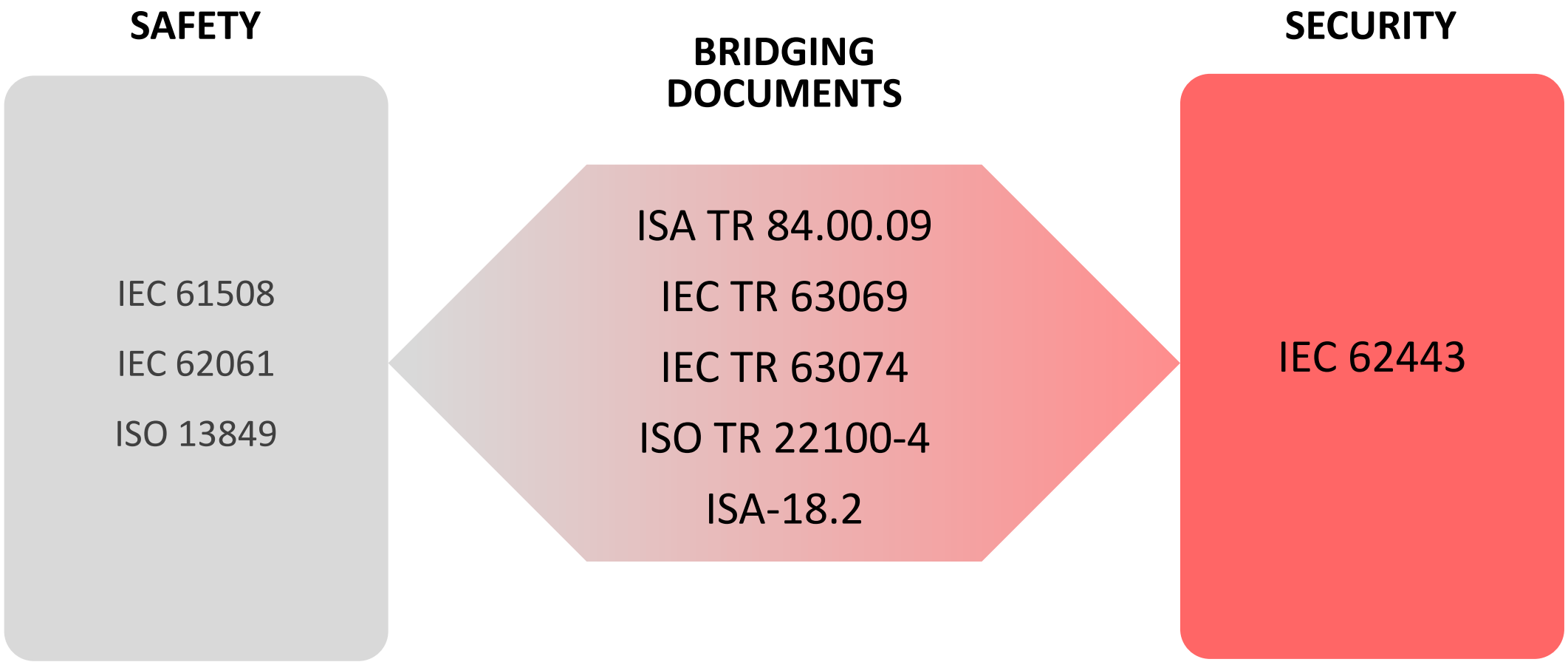
Scenario attuale

- Safety lifecycle e cybersecurity lifecycle sono due metodologie distinte
- In ambienti convergenti IT/OT, ciò comporta dei problemi
  - Scarsa efficacia nella comunicazione tra personale IT e OT
  - Differente percezione del rischio
  - Documentazione dispersiva
  - Ridotta efficacia delle soluzioni di sicurezza

Scenario desiderabile

- Integrazione dei due approcci

Panoramica degli standard rilevanti



Standard per la safety

- **IEC 61508 (Functional safety of electrical/electronic/programmable electronic safety-related systems)**
  - Definizione delle varie fasi del lifecycle di un sistema safety-related E/E/P Electrical/Electronic/Programmable Electronic)
  - Definizioni e documentazione di alto livello sugli hazard e risk analysis e requisiti di safety
- **IEC 62061 (Safety of machinery – Functional safety of safety- related electrical, electronic, and programmable electronic control systems)**
  - Standard di più basso livello, incentrato sulla functional safety dei macchinari industriali
- **ISO 13849 (Safety of machinery)**
  - Uno degli standard principali per la safety. Obiettivi di safety da raggiungere, concetto di Performance Level (PL) e Performance Level Required (PLr)

Standard per la security: IEC 62443

IEC 62443: Security for industrial automation and control systems

- Famiglia di standard per la *cybersecurity* per sistemi di controllo industriali (ICS)
- Parti essenziali dello standard

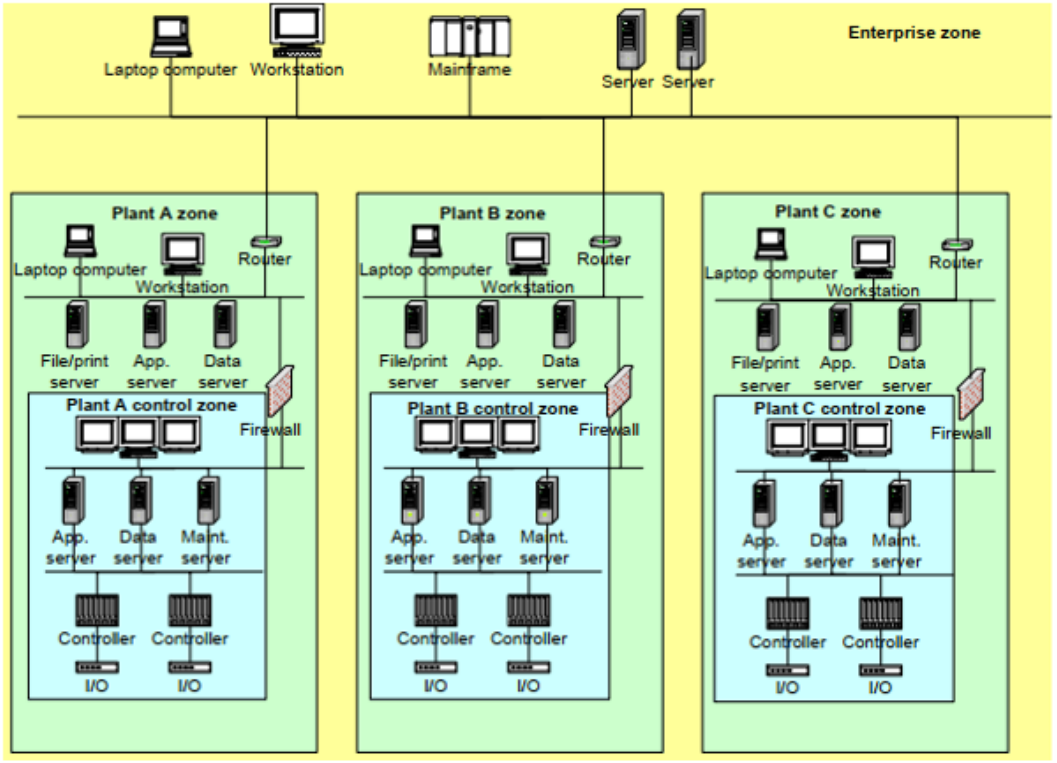
1-1	terminologia e concetti generali
3-2	suddivisione in zone e conduit, risk analysis
3-3	requisiti di sistema e Security Levels
4-1	ciclo di vita per lo sviluppo sicuro
4-2	requisiti per il singolo componente

Definizione Zone & Conduits: Zone

Entità che rappresentano il partizionamento del sistema, definite in base alle caratteristiche che si vogliono raggruppare

Ogni zona è caratterizzata da:

1. Policy di sicurezza
2. Inventario degli asset
3. Requisiti di accesso e controllo
4. Threat e vulnerabilità
5. Conseguenze di un security breach
6. Tecnologie utilizzabili in base alle policy di sicurezza
7. Change management process



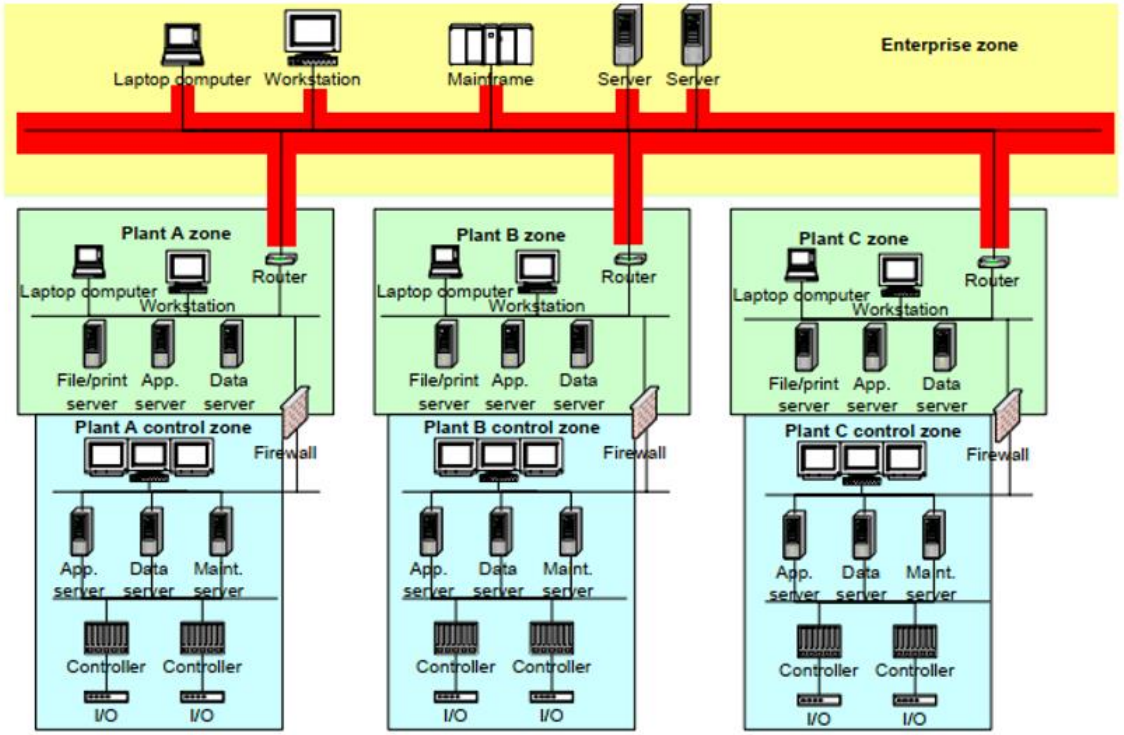
Esempio raggruppamento zone

Definizione Zone & Conduits: Conduits

Raggruppamento logico di canali di comunicazione che collegano due o più zone e condividono requisiti di security

Ogni conduit è caratterizzato da:

1. Policy di sicurezza
2. Requisiti di accesso e controllo
3. Threat e vulnerabilità
4. Conseguenze di un security breach
5. Tecnologie permesse
6. Change management process
7. Zone connesse



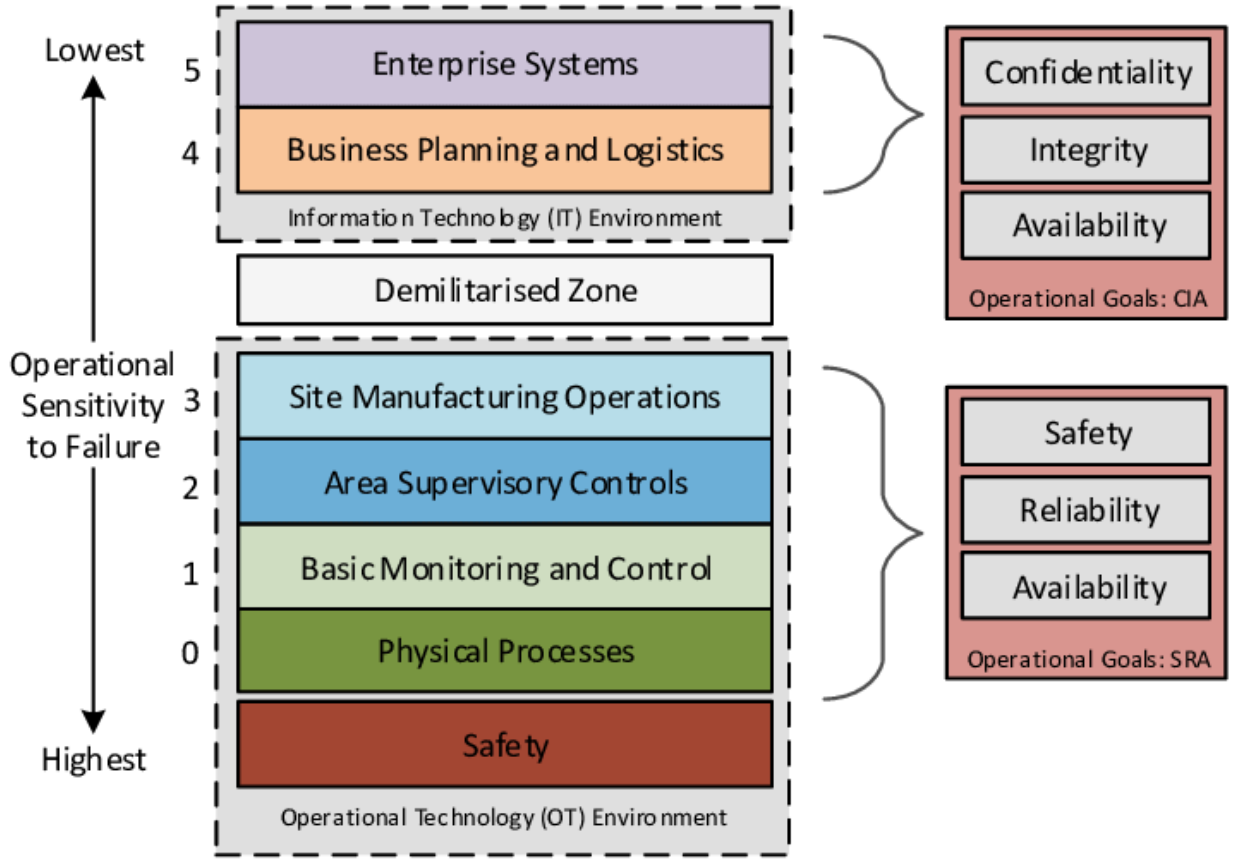
Esempio conduit

Purdue Reference Model – Zona IT e OT

Modello concettuale per la segmentazione delle reti ICS.

Mostra interconnessioni e interdipendenze di tutti i componenti principali dividendo l'architettura ICS in due zone principali

- Information Technology (IT)
- Operational Technology (OT)



Purdue Reference Model - 6 livelli

0: componenti fisici -> motori, pompe, sensori, valvole, ecc.

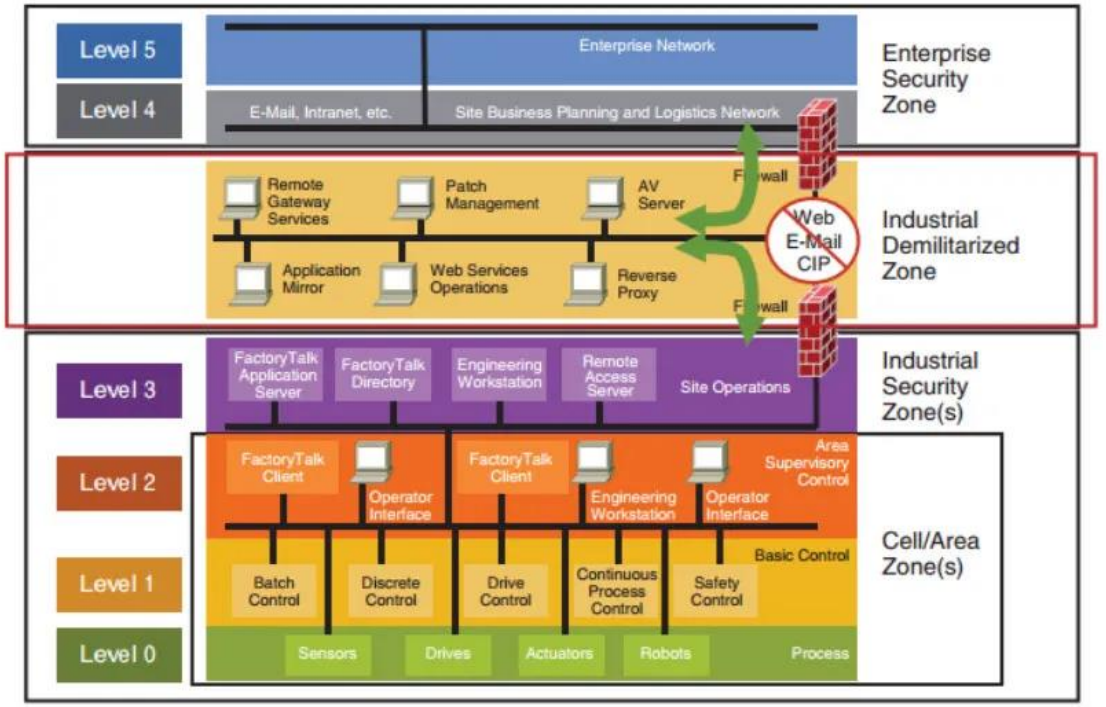
1: sistemi che monitorano e inviano comandi ai dispositivi di livello 0 -> PLC, RTU, IED

2: dispositivi che controllano i processi complessivi all'interno del sistema -> HMI e SCADA software

3: gestione dei flussi di lavoro di produzione -> Batch management, data historians etc.

3.5: Industrial DMZ (iDMZ): barriera tra le reti IT e OT.

4: sistemi di gestione della produzione, delle comunicazioni e dell' archiviazione dei dati



Purdue Reference Model

5: rete aziendale, raccoglie dati dai sistemi ICS per le decisioni aziendali

IEC 62443 - Security Lifecycle

Tre fasi principali relative al Security Lifecycle

1) Assessment Phase

- Identificare chiaramente il SuC (System under Consideration)
- Effettuare il partizionamento del SuC in zone e conduit
- Eseguire un cyber security risk assessment del SuC

2) Design Phase

- (ri)valutazione di zone e conduits
- Lista di interfacce software di terze parti identificate durante il processo
- Lista di contromisure necessarie per rispettare il SL-Target e garantire la risk reduction richiesta
- Se il livello di rischio risulta accettabile, si può procedere alla fase di design dettagliata del processo

3) Operate & Maintain Phase

- L'impianto viene esposto a potenziali attacchi cyber
- Segue una valutazione delle minacce e relativi interventi
- Gestione delle attività di manutenzione e modifica delle contromisure esistenti

IEC 62443 - Security Levels (1)

- Approccio qualitativo per la valutazione della security di zone e conduits
- Applicabili sia alle end user companies, che ai fornitori di IACS e prodotti di security
- Utilizzati per selezionare i dispositivi e le contromisure IACS da utilizzare all'interno di una zona ed identificare e confrontare la sicurezza delle zone
- Definiti in cinque livelli

Security Levels (SL)	
SL 0	nessun requisito di security specifico
SL 1	protezione contro una violazione casuale
SL 2	protezione contro violazione intensionale avvenuta con metodi semplici e poche risorse
SL 3	protezione contro violazione intenzionale avvenuta con metodi sofisticati e risorse moderate
SL 4	protezione contro violazione intenzionale avvenuta con metodi sofisticati e risorse estese

IEC 62443 - Security Levels (2)

Acronimo	Security Level	Descrizione
SL-T	Security Level **Target**	**Livello di security desiderato** per un particolare sistema. Solitamente determinato nella fase di risk assessment
SL-A	Security Level **Achived**	**Attuale livello di security** di un sistema. Dipende dalla proprietà di security e/o dalle contromisure adottate per prevenire problemi di security
SL-C	Security Level **Capability**	**Livello di security che i componenti o il sistema possono realizzare** quando opportunamente configurati. È definito per le contromisure e le proprietà di sicurezza che possono essere applicabili

L'obiettivo è assicurare che in qualsiasi momento il SL-A di una zona/conduit sia maggiore o uguale al suo SL-T

IEC 62443 - Foundational Requirements

	Titolo	Descrizione
FR 1	**Identification and authentication control (IAC)**	Identificare e autenticare in modo affidabile tutti gli utenti che tentano di accedere all'ICS
FR 2	**Use Control (UC)**	Applicare e monitorare l'uso dei privilegi assegnati a un utente autenticato per eseguire l'azione richiesta sul sistema o sulle risorse
FR 3	**System Integrity (SI)**	Garantire l'integrità dell'IACS per prevenire manipolazioni non autorizzate
FR 4	**Data Confidentiality (DC)**	Garantire la riservatezza delle informazioni sui canali di comunicazione e negli archivi di dati, impedendone la divulgazione non autorizzata
FR 5	**Restricted Data Flow (RDF)**	Segmentare il sistema tramite zone e conduit per limitare il flusso di dati non necessari
FR 6	**Time Response to Events (TRE)**	Rispondere in presenza di problemi di security e adottare soluzioni correttive
FR 7	**Resource Availability (RA)**	Garantire la disponibilità del sistema di controllo

A seconda del Security Level in considerazione, ogni FR ha più condizioni che devono essere soddisfatte

Bridging documents

- **ISA TR 84.00.09 (Cybersecurity Related To The Functional Safety Lifecycle)**
  - Contiene indicazioni per lo sviluppo di una metodologia che integri safety e security
  - Sviluppato da un working group composto da membri di ISA84 (autori di IEC 61511) e ISA99 (autori di IEC 62443)

- **ISA TR 63069 (Industrial-process measurement, control and automation Framework for functional safety and security)**
  - Chiarisce l'uso di vocaboli simili, ma con diverso significato, in IEC 61508 e IEC 62443

- **ISA TR 63074 (Security aspects related to functional safety of safety-related control systems)**
  - Descrive come le vulnerabilità di security possono impattare sulla safety

SS4SP
safety and security for smart production

Analisi e valutazione dei rischi informatici di impianto

A cura di

Mirco Marchetti

Giorgio Valenziano Santangelo

Contenuti

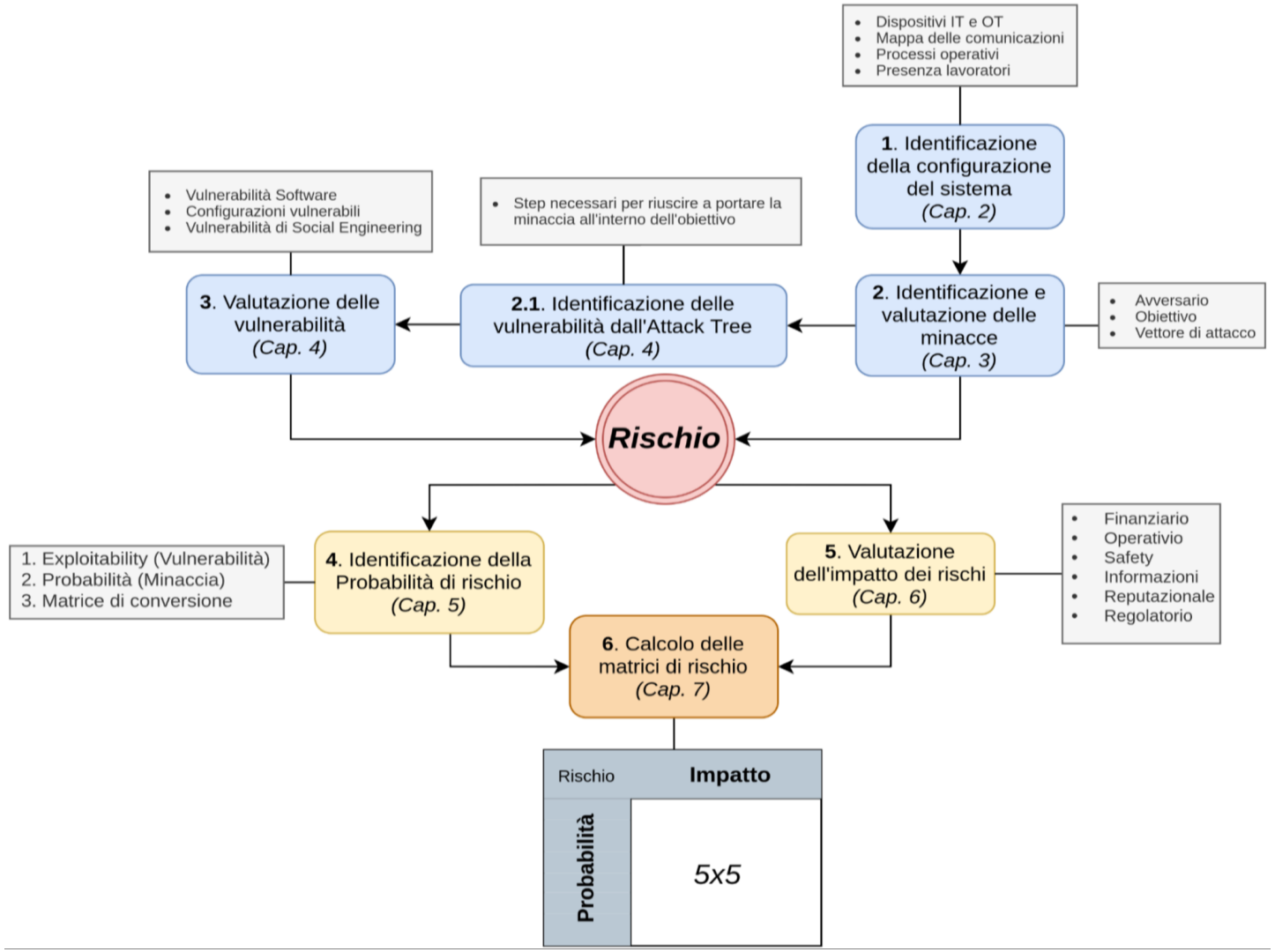
- Metodologia di analisi del rischio
- Valutazione dei rischi sugli Use Case
- Penetration test prima dell'implementazione delle misure di sicurezza

Metodologia di analisi del rischio (1)

- Metodologia di analisi e valutazione dei rischi che parte dai **rischi cyber** e che integra **safety** e **operation**.

- Motivazioni:
  - La maggior parte delle minacce inizia o **passa dall'IT** per poi arrivare al **blocco dell'operatività**;
  - Le metodologie OT orientate a minacce non intenzionali (guasti, malfunzionamenti, incuria);
  - **Cyber risk management** IT orientato a **minacce umane intenzionali**.

Metodologia di analisi del rischio (2)



Metodologia di analisi del rischio
Identificazione Attaccanti

- Considerando l'azienda, i suoi obiettivi e il settore produttivo in cui essa si colloca, bisogna identificare i possibili attaccanti.

Attaccanti	Obiettivi	Threat vector	Probabilità
Criminale non competente	Ricatto mediante crittografia e minaccia di divulgazione dei dati aziendali	Common malware e Ransomware	Molto alta
Crime-as-a-Service	Ricatto mediante crittografia e minaccia di divulgazione dei dati aziendali	Malware e ransomware as-a-service	Alta
Criminale competente	Furto dati e ricatto mediante sabotaggio e/o minaccia di divulgazione dei dati aziendali riservati	Targeted Malware e Ransomware. Hijacking 2FA.	Media

Metodologia di analisi del rischio
Valutazione delle vulnerabilità

- Identificazione delle vulnerabilità

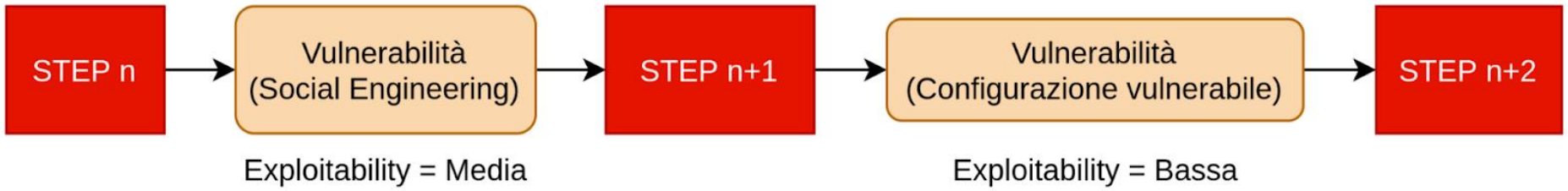
- Si distinguono tre tipologie di vulnerabilità:
  - **Vulnerabilità Software**, basate sul Exploitability score CVSS.
  - **Configurazioni vulnerabili**, basate sulla facilità di sfruttamento.
  - **Vulnerabilità di Social Engineering**, basate sui controlli di sicurezza, sulla consapevolezza e sul training del personale.

Metodologia di analisi del rischio
Exploitability complessiva

- L'exploitability complessiva è data dalla combinazione delle exploitability di ogni vulnerabilità che deve essere sfruttata per portare a termine l'attacco.

$$Exploitability_{complessiva} = min(Exploitability_1, Exploitability_2, ...)$$

- Esempio:



$$Exploitability_{complessiva} = min(Media, Bassa, ...) = Bassa$$

Metodologia di analisi del rischio
Probabilità di rischio

La **Probabilità di rischio** deriva dalla combinazione di:

- Probabilità di incorrere in un tentativo di attacco;
- Exploitability complessiva delle vulnerabilità.

Probabilità della minaccia	5 – Quasi certa	5 - Media	10 - Alta	15 - Alta	20 - Quasi certa	25 – Quasi Certa
	4 - Alta	4 – Bassa	8 - Media	12 - Alta	16 - Alta	20 – Quasi certa
	3 - Media	3 – Bassa	6 - Media	9 - Media	12 - Alta	15 - Alta
	2 - Bassa	2 – Bassa	4 - Bassa	6 - Media	8 - Media	10 -Alta
	1 – Molto bassa	1 – Molto bassa	2 - Bassa	3 - Bassa	4 - Bassa	5 -Media
		1 – Molto bassa	2 - Bassa	3 - Media	4 - Alta	5 – Quasi certa

Sfruttabilità dell'attacco

Metodologia di analisi del rischio

Valutazione dell'impatto dei rischi

- L'impatto complessivo è dato dalla combinazione di più impatti appartenenti a diverse **categorie**:

  - **Finanziario;**
  - **Operativo;**
  - **Furto di Informazioni**;
  - **Reputazionale**;
  - **Regolatorio;**
  - **Safety lavoratori;**
  - **Safety consumatori**;
  - **Safety sociale**.

- Si distinguono i seguenti livelli di impatto: Trascurabile*, Basso, Medio, Alto, Estremo.*

- Considerando il caso peggiore (tutte le metodologie di analisi e valutazione del rischio tendono ad adottare una *worst case analysis*), l'impatto complessivo è uguale al **massimo** tra gli impatti nelle diverse categorie.

$$Impatto_{complessivo} = max(Finanziario, Operativo, ..., Safety)$$

Metodologia di analisi del rischio

Calcolo dell' entità di rischio

- Il rischio da calcolare è il rischio complessivo di incorrere in un determinato attacco che sfrutta determinate vulnerabilità.
- Una volta calcolata la probabilità di accadimento con il relativo impatto, è possibile collocare il rischio all'interno della matrice di rischio.

Impatto					
5 - Estremo	5 - Medio	10 - Alto	15 - Alto	20 -Estremo	25 - Estremo
4 - Alto	4 - Basso	8 - Medio	12 - Alto	16 - Alto	20 - Estremo
3 - Medio	3 - Basso	6 - Medio	9 - Medio	12 - Alto	15 - Alto
2 - Basso	2 - Basso	4 - Basso	6 - Medio	8 - Medio	10 -Alto
1 - Trascura-bile	1 - Trascurabile	2 - Basso	3 - Basso	4 - Basso	5 -Medio
	1 – Molto bassa	2 - Bassa	3 - Media	4 - Alta	5 – Quasi certa

Probabilità

Metodologia di analisi del rischio

SL-T e soglia di accettabilità del rischio

- SL - T = 4: rischio accettabile 1
- SL - T = 3: rischio accettabile <= 4
- **SL - T = 2: rischio accettabile <= 9**
- SL - T = 1: rischio accettabile <= 16
- SL - T = 0: tutti i rischi sono accettabili

In funzione dei potenziali danni di una compromissione della zona OT, per gli use case si sceglie SL-T tipico delle aziende manufatturiere

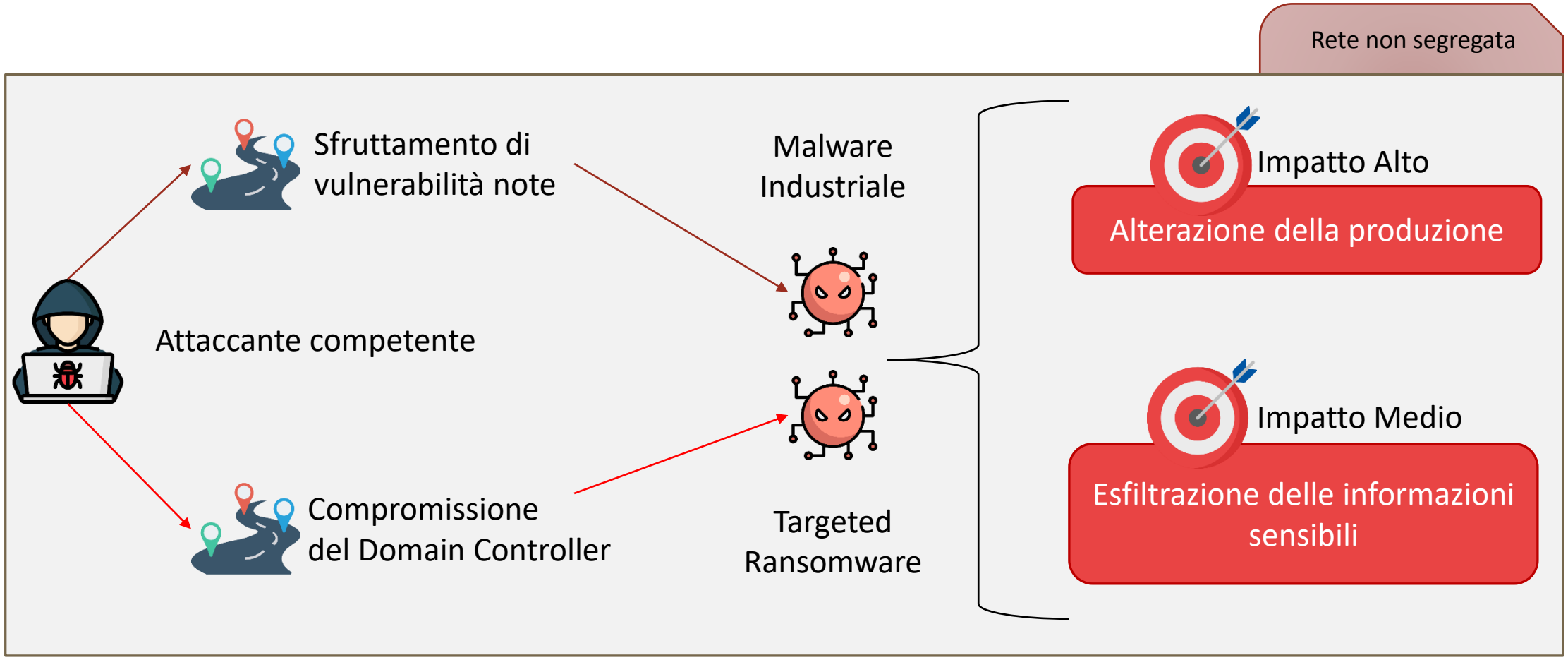
Impatto						
5 - Estremo	5 - Medio	10 - Alto	15 - Alto	20 -Estremo	25 - Estremo
4 - Alto	4 - Basso	8 - Medio	12 - Alto	16 - Alto	20 - Estremo
3 - Medio	3 - Basso	6 - Medio	9 - Medio	12 - Alto	15 - Alto
2 - Basso	2 - Basso	4 - Basso	6 - Medio	8 - Medio	10 -Alto
1 - Trascura-bile	1 - Trascura-bile	2 - Basso	3 - Basso	4 - Basso	5 -Medio
	1 – Molto bassa	2 - Bassa	3 - Media	4 - Alta	5 – Quasi certa
			Probabilità		

SL-T = 2 → protezione contro violazione intensionale avvenuta con metodi semplici e poche risorse

Valutazione dei rischi sugli Use Cases

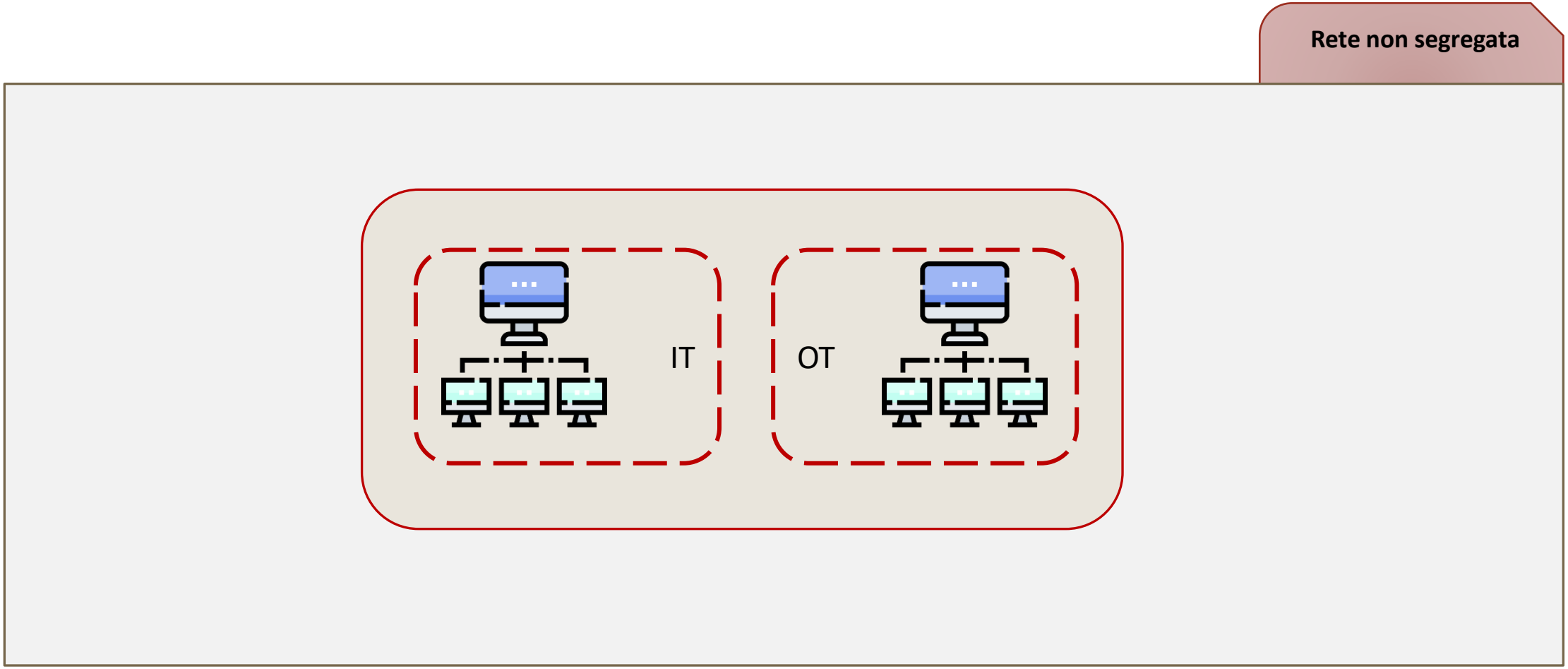
- Considerazioni fatte:
  - Non si consideri il vettore di attacco con cui l'attaccante ha ottenuto l'accesso alla rete IT;
  - Sono state fatte delle assunzioni riguardo la presenza di vulnerabilità in base alla conoscenza pregressa sui dispositivi presenti all'interno degli Use Cases.
  - In base agli impatti che si possono generare si considera per gli Use Case in esame un Security Level Target (SL-T) pari a 2. Quindi, la soglia di accettazione del rischio è <= Medio (9).
- System under Consideration:
  - Scenario di rete non segregata

Valutazione dei rischi sugli Use Cases
Pattern di attacco

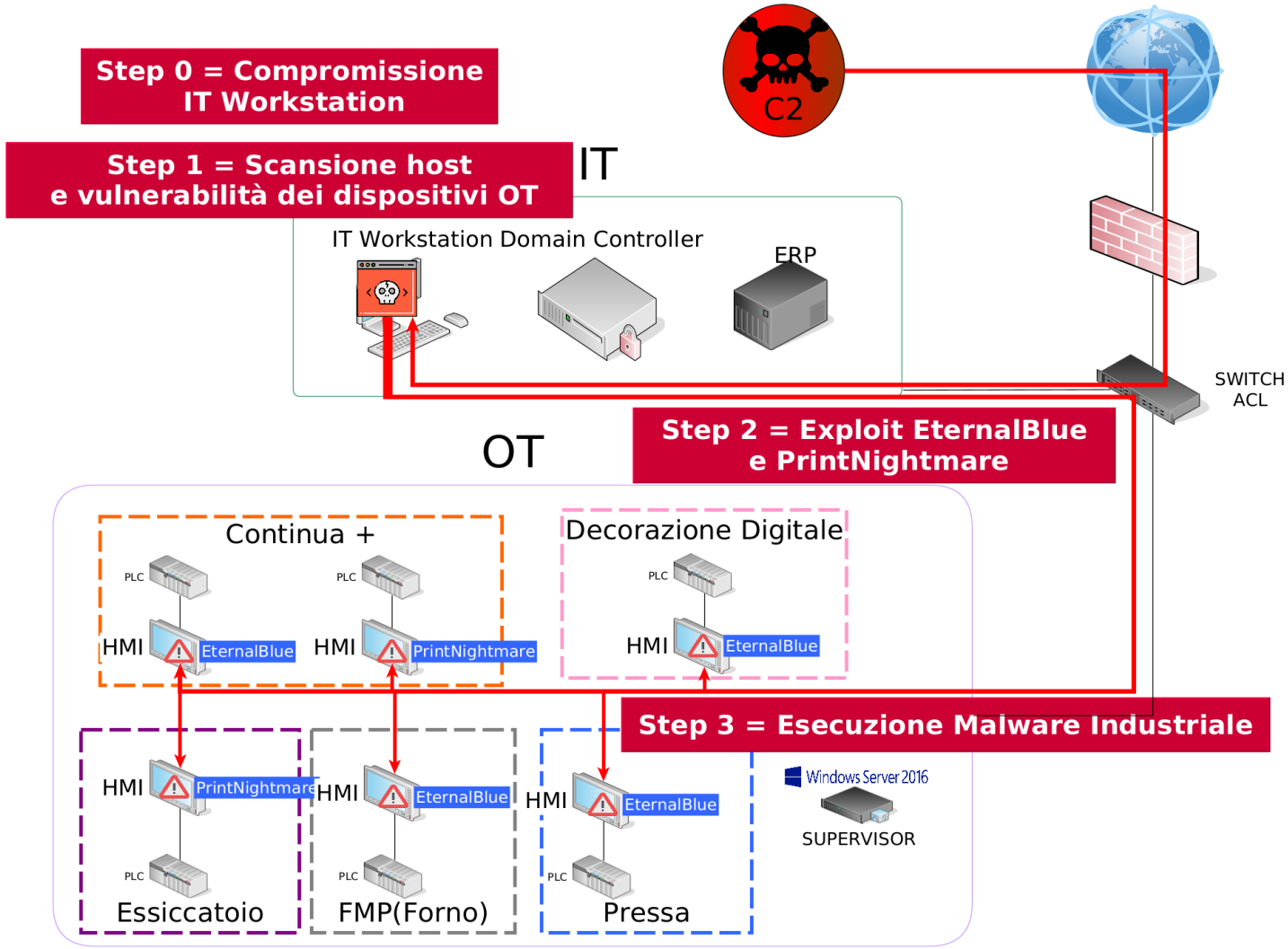


Valutazione dei rischi sugli Use Cases

Assenza di contromisure



Valutazione dei rischi sugli Use Cases

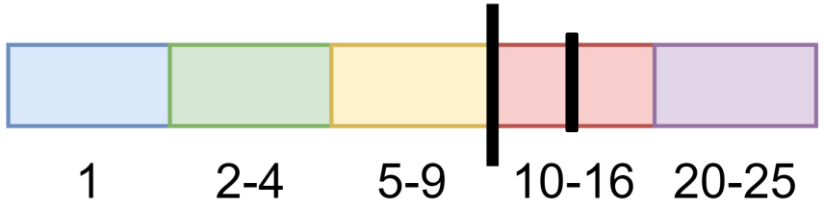


Sfruttamento di vulnerabilità note

Scenario	Casi	Impatto	Probabilità di rischio	Rischio
Rete non segregata	EternalBlue	Alto	Alta	16 - Alto
	PrintNightmare	Alto	Alta	16 - Alto

Risultati

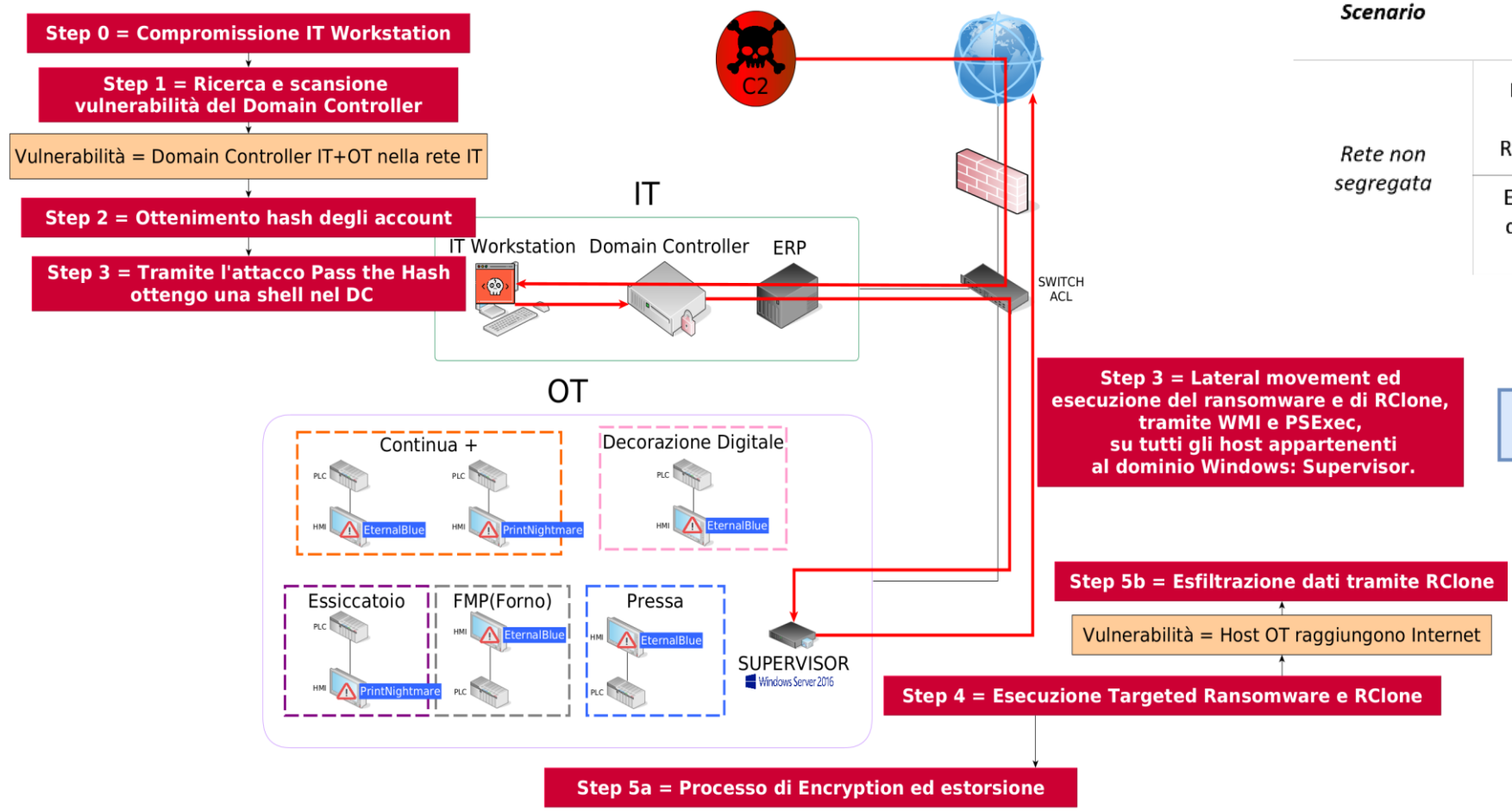
Il Rischio non è accettabile per SL-T 2



SS4SP
safety and security for smart production

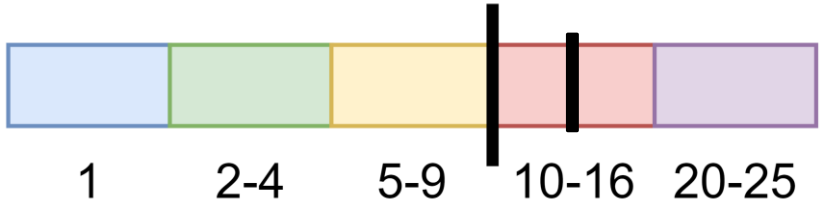
Valutazione dei rischi sugli Use Cases

Compromissione del Domain Controller



Scenario	Casi	Impatto	Probabilità di rischio	Rischio
Rete non segregata	Esecuzione Targeted Ransomware	Alto	Alta	16 - Alto
	Esfiltrazione dati tramite RClone	Medio	Alta	16 - Alto

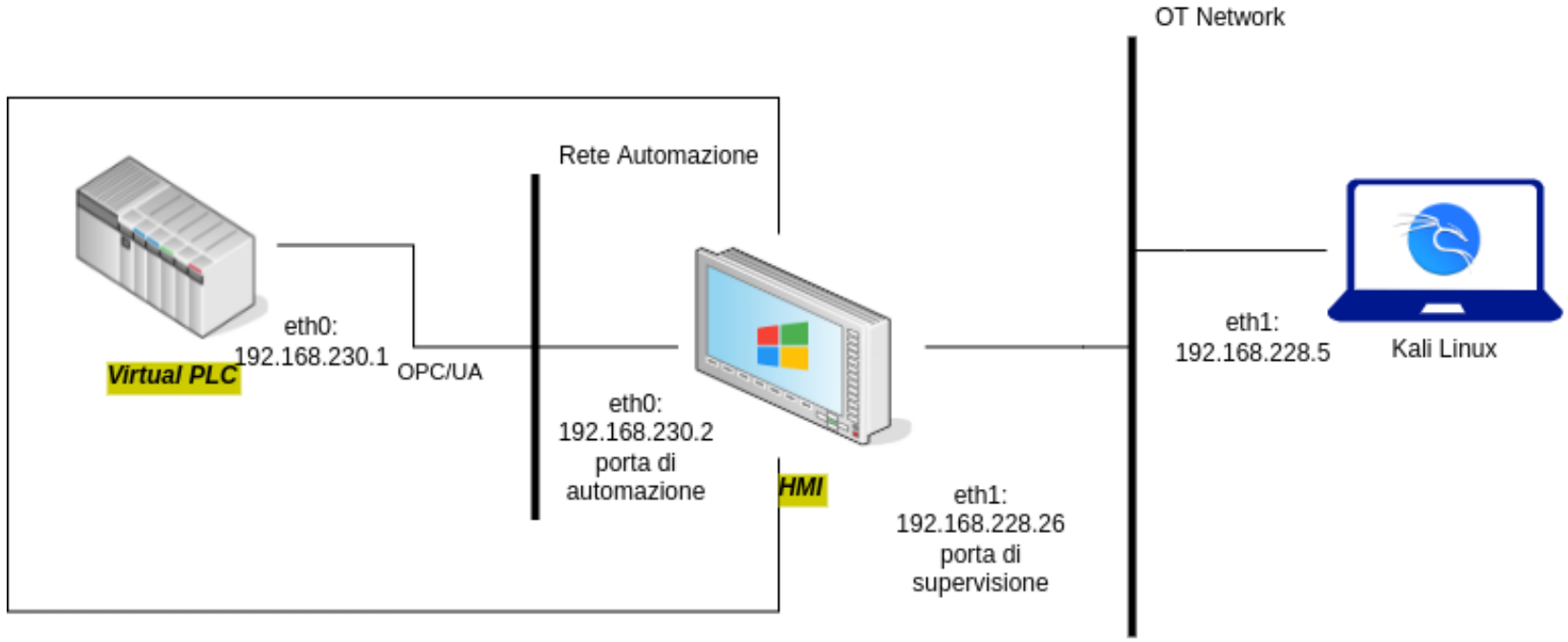
Risultati



Il Rischio non è accettabile per SL-T 2

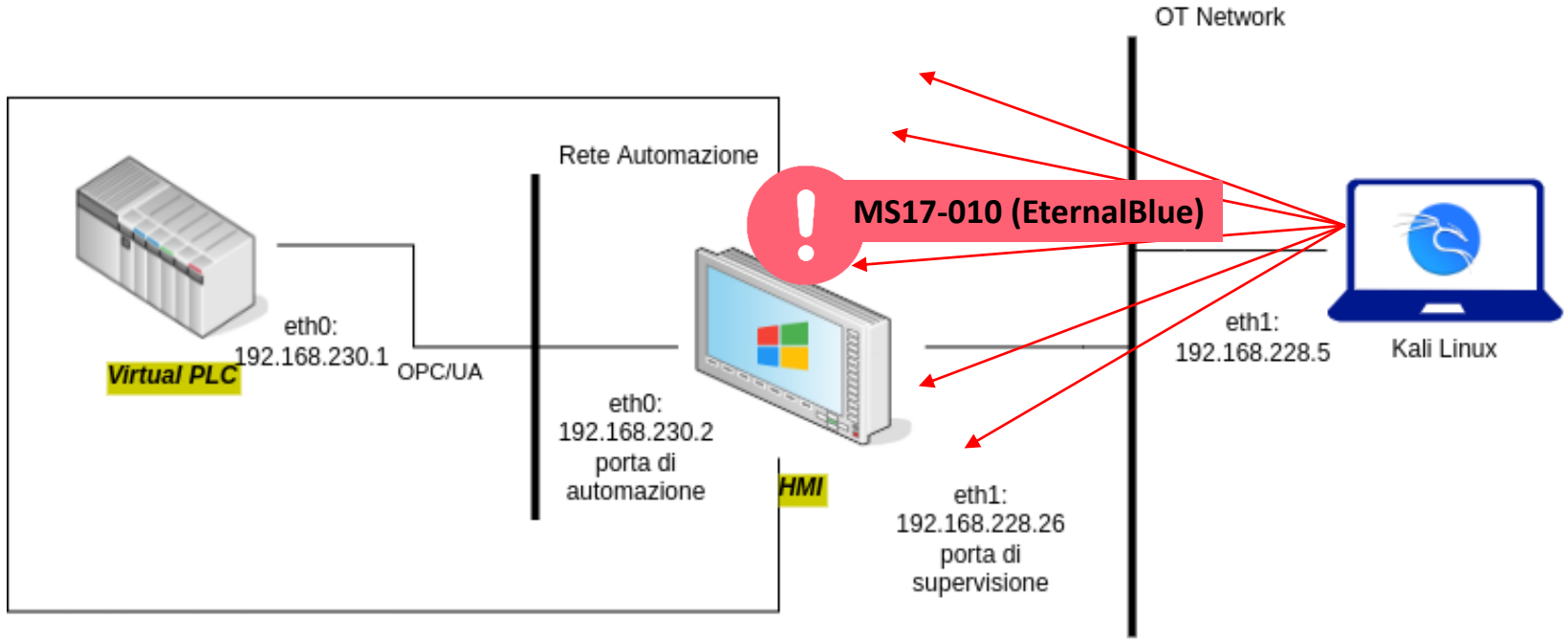
Penetration Test Scenario di rete non segregata

- Scenario di rete semplificato, intenzionalmente vulnerabile:



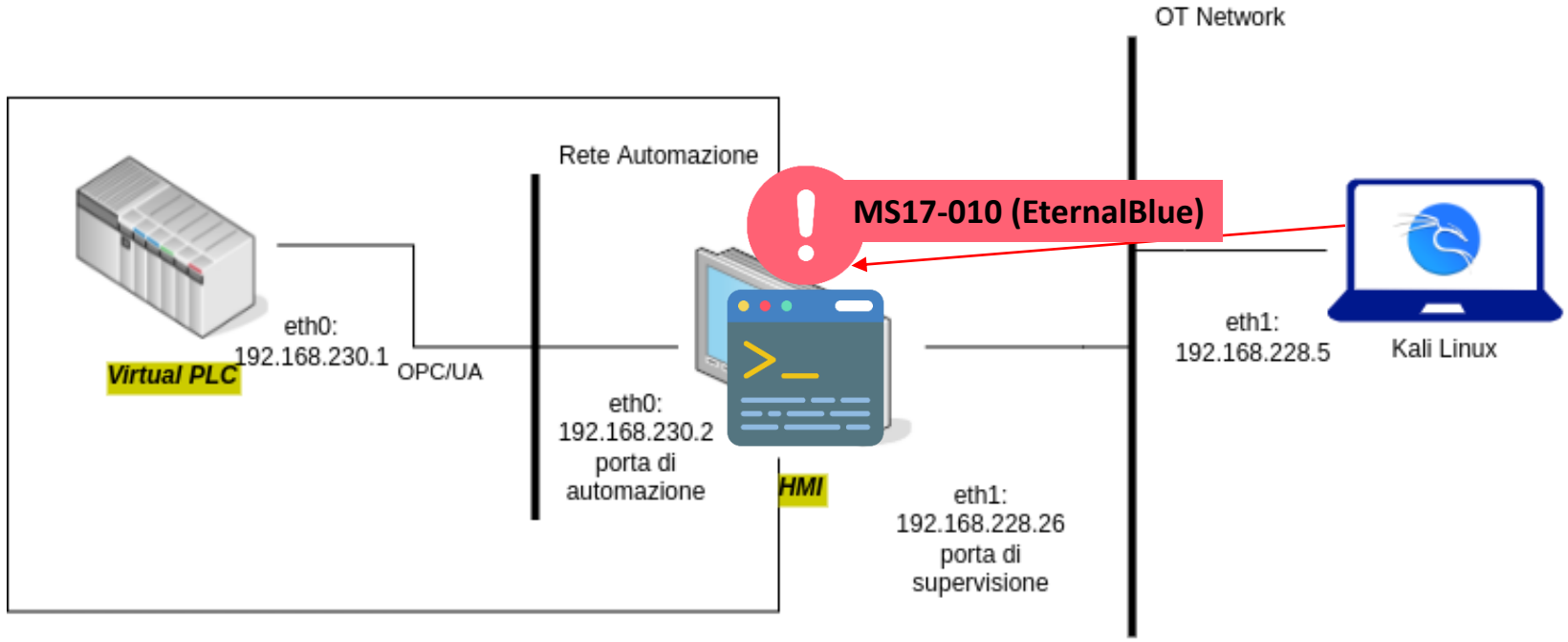
Penetration Test di rete non segregata
Reconnaissance

- Scansione della rete e Vulnerability Scan



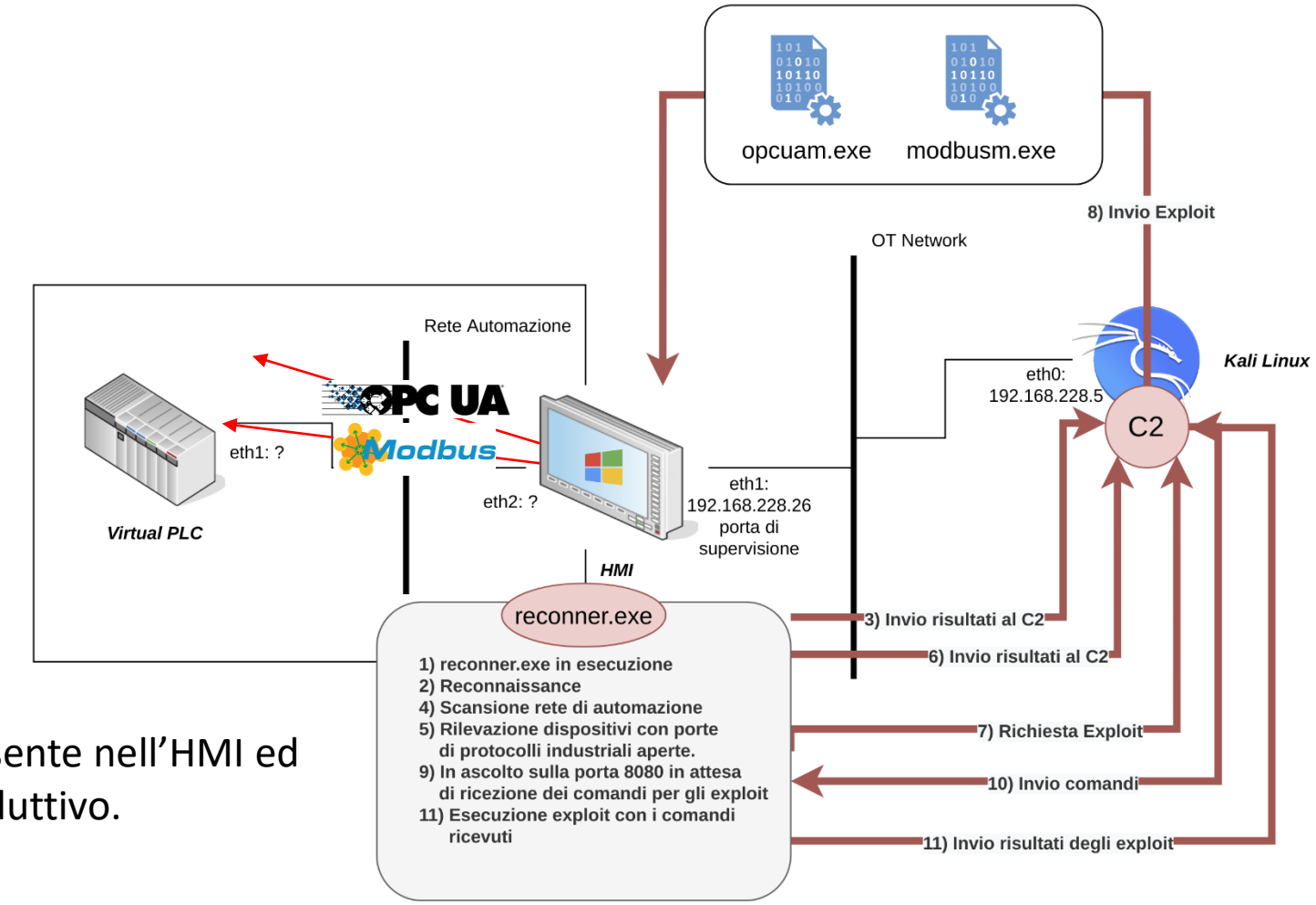
Penetration Test sullo Use Case SACMI
Exploit

- Sfruttamento vulnerabilità MS17-010 (EternalBlue) al fine di ottenere il controllo con i massimi privilegi sull'HMI



Penetration Test di rete non segregata
Delivery and Installation, Command and Control ed Action on Objectives

- Invio ed esecuzione del malware, esfiltrazione dati e richiesta al C2 dei payload specifici;
- Ricezione delle informazioni dell'host infetto ed invio comandi.
- Interpretazione dei comandi ed esecuzione dei payload per alterare il processo produttivo.



Risultato: Esfiltrazione della ricetta presente nell'HMI ed alterazione del processo produttivo.

<u>Il rischio è stato confermato</u>

SS4SP
safety and security for smart production

Introduzione alle soluzioni metodologiche e tecnologiche a mitigazione dei rischi informatici di impianto

A cura di

Francesca Merighi

Contenuti

- Endpoint security
- Monitoraggio di rete e Intrusion Detection System (IDS)
- SIEM
- Segregazione di rete e Industrial DMZ
- Politiche di sicurezza

Misure di sicurezza in ambito IT

PRIORITÀ

RISERVATEZZA

INTEGRITÀ

DISPONIBILITÀ

DISPOSITIVI CHE OPERANO ANCHE IN **MOBILITÀ**

TEMPO DI VITA 2-3 ANNI

ENDPOINT SECURITY 1

1. **Aggiornamenti di sicurezza** frequenti
2. Rilevazione e prevenzione delle minacce a “signature” -> richiede l’aggiornamento periodico delle signature
3. Rilevazione e prevenzione delle minacce con AI -> richiede solitamente la comunicazione con il cloud
4. Controllo del software installato e dei processi in esecuzione

CONTROLLO DEL TRAFFICO DI RETE 2

1. Controllo e limitazione del traffico internet
2. Analisi del traffico il rete locale

Endpoint security OT (1)

PRIORITÀ

DISPONIBILITÀ

INTEGRITÀ

RISERVATEZZA

TEMPO DI VITA 15-20 ANNI

MODIFICHE HARDWARE

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

MODIFICHE SOFTWARE

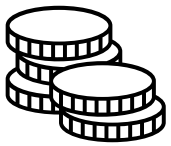
- Installazione programmi
- Aggiornamenti software (sistema operativo e applicazioni)
- Cambiamenti di configurazione (abilitazione/disabilitazione servizi, impostazioni di sicurezza quali ad esempio Windows Firewall, ecc.)
- Ecc.

PROCESSI DI PROTEZIONE DALLE MINACCE

possono interferire con quelli produttivi

Se eseguite quando la macchine è in Produzione, possono richiedere

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



COSTI

Endpoint security OT (2)

PRIMA DEL COLLAUDO DELLA MACCHINA

SYSTEM HARDENING COLLAUDATO

1. Disabilitazione servizi non necessari,
2. Configurazione impostazioni di sicurezza quali ad esempio Windows Firewall, policy del Sistema operativo, ecc.
3. Installazione di programmi di rilevazione e prevenzione delle minacce specifici per gli endpoint OT

PERIODICAMENTE, solo per le aziende con **SL-T 3 e 4** (farmaceutiche, alimentari, facility, ecc.)

AGGIORNAMENTO TECNOLOGICO

1. Aggiornamento del sistema operativo e dei programmi
2. Aggiornamento hardware per supportare nuovi software e processi
3. Installazione nuovi software di protezione

Monitoraggio di rete e IDS

Soluzione che effettua **monitoraggio passivo del traffico di rete** non alterando il funzionamento della strumentazione OT

Dispositivi che generano traffico di rete ← Registra → **Flussi di dati** generati dai dispositivi e le loro caratteristiche (sorgente e destinazione, protocolli, contenuto dei messaggi, ecc.)

Caratteristiche dei dispositivi (sistemi operativi, porte aperte, servizi attivi, ecc.) ← Individua → **Baseline delle comunicazioni** attraverso Machine Learning

Non-conformità e vulnerabilità dei dispositivi ← Rileva → Anomalie e **comunicazioni malevole**

Blacklist: i messaggi che corrispondono ad un certo pattern sono una minaccia

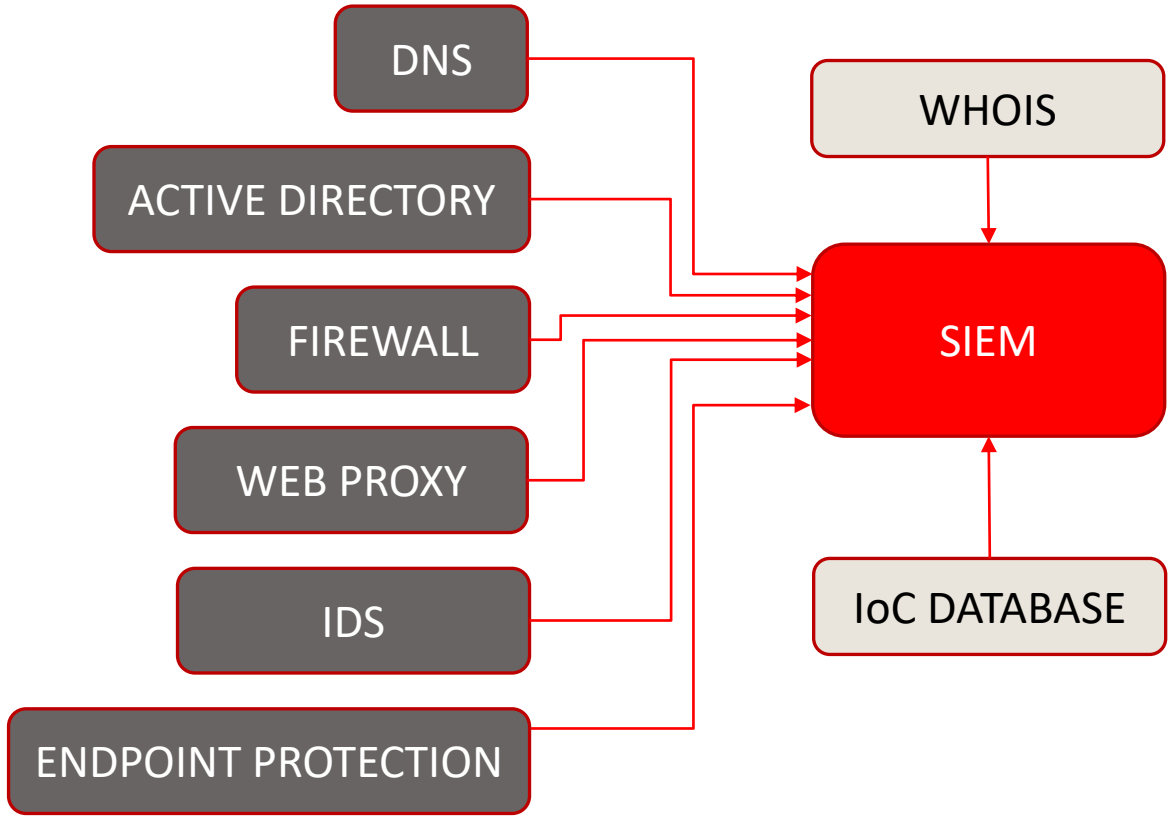
Whitelist: ciò che si discosta dalla baseline è un'anomalia

SS4SP
safety and security for smart production

SIEM

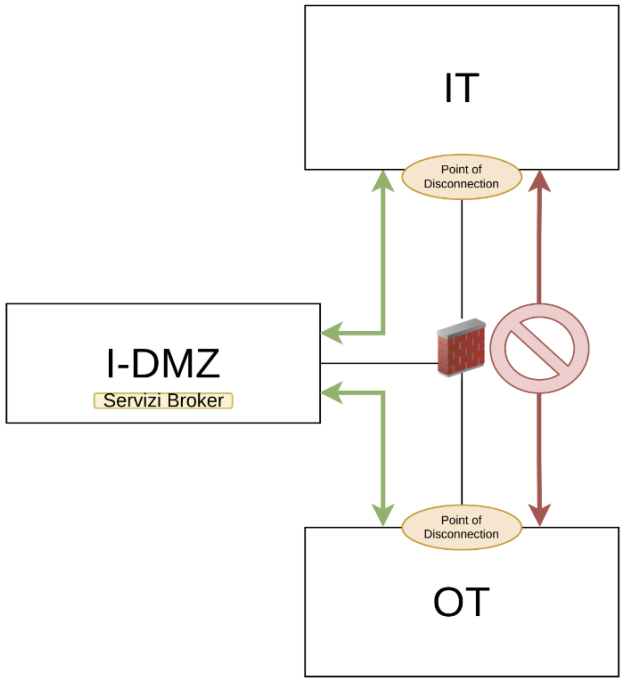
Security Information Management (SIM)
Archiviazione a lungo termine, **analisi** e **presentazione** delle informazioni raccolte

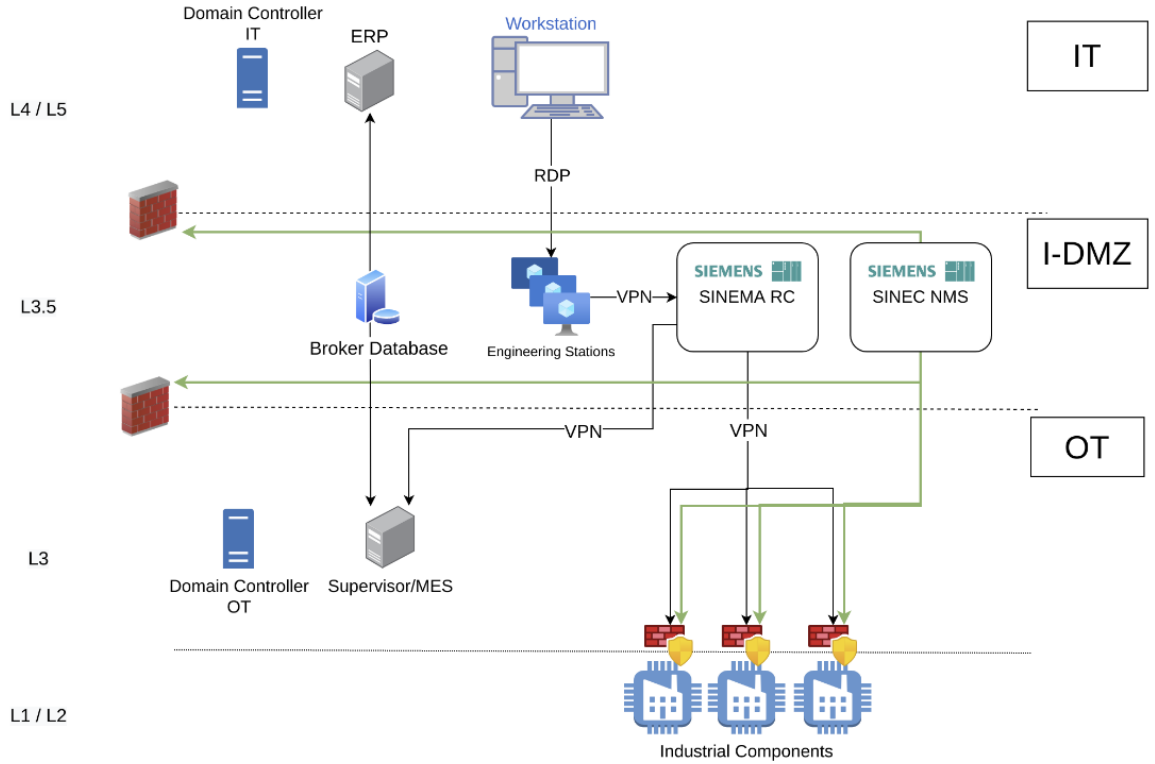
Security Event Management (SEM)
Monitoraggio in tempo reale e **correlazione** delle informazioni **in eventi**, **notifiche** e visualizzazioni aggregate



- **Aggregazione dei dati**
- **Correlazione di eventi**
- **Generazione di alert**
- **Visualizzazione**
- **Conformità**

Industrial DMZ





Politiche di sicurezza per la zona OT

Foundational Requirement		Politiche di sicurezza
FR 1	**Identification and authentication control (IAC)**	Politiche di gestione e amministrazione delle utenze, delle password, dei diritti di accesso
FR 2	**Use Control (UC)**	Politiche di gestione ed Amministrazione dei privilegi
FR 3	**System Integrity (SI)**	Politiche per la verifica dell'integrità dei sistemi
FR 4	**Data Confidentiality (DC)**	Politiche di classificazione e riservatezza delle informazioni
FR 5	**Restricted Data Flow (RDF)**	Politiche di utilizzo dei supporti removibili
FR 6	**Time Response to Events (TRE)**	Politiche di incident response
FR 7	**Resource Availability (RA)**	Politiche di backup e disaster recovery

SS4SP
safety and security for smart production

Monitoraggio del traffico di rete in ambito industriale

A cura di

Carlo Giannelli

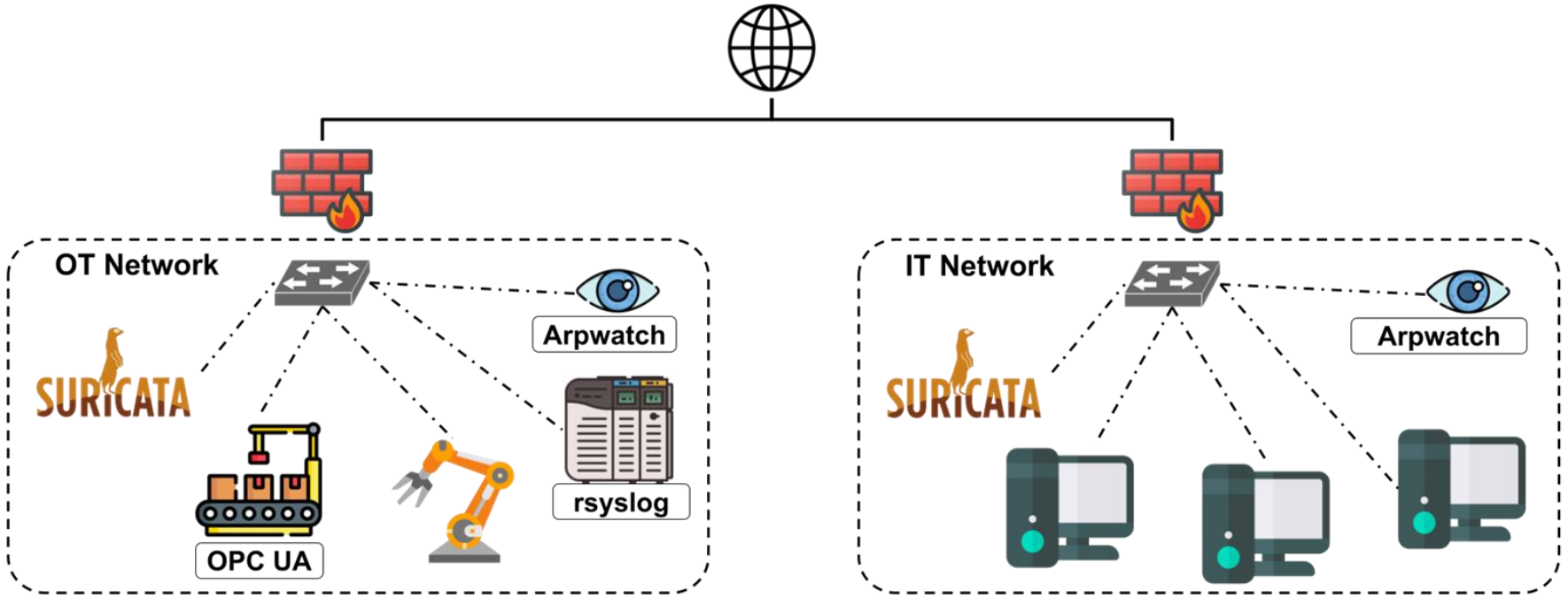
Francesca Merighi

Contenuti

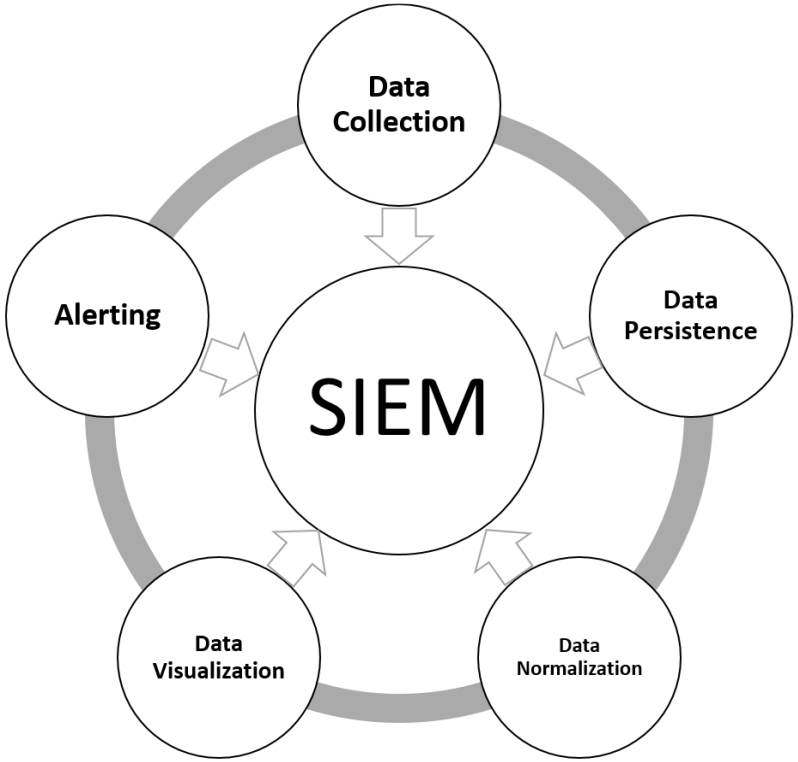
- Soluzioni open source per il monitoraggio delle minacce
- Soluzioni commerciali per il monitoraggio delle minacce

Monitoraggio integrato IT/OT

- Nodi eterogenei: HMI/PLC, macchine server, nodi edge
- Protocolli eterogenei: industriali, Web, proprietari
- Informazioni non confinate a singolo nodo/rete



SIEM: Wazuh



Security Information and Event Management (SIEM) per fornire visione globale:

- **aggregazione eventi**
- **normalizzazione log**
- generazione di alert e risposta attiva

Wazuh:

- **Security Analytics** → analisi log per rilevare anomalie, intrusioni e minacce
- **Vulnerability Detection** → database di Common Vulnerabilities and Exposures (CVE) per individuare vulnerabilità note

WAZUH

IDS: Suricata

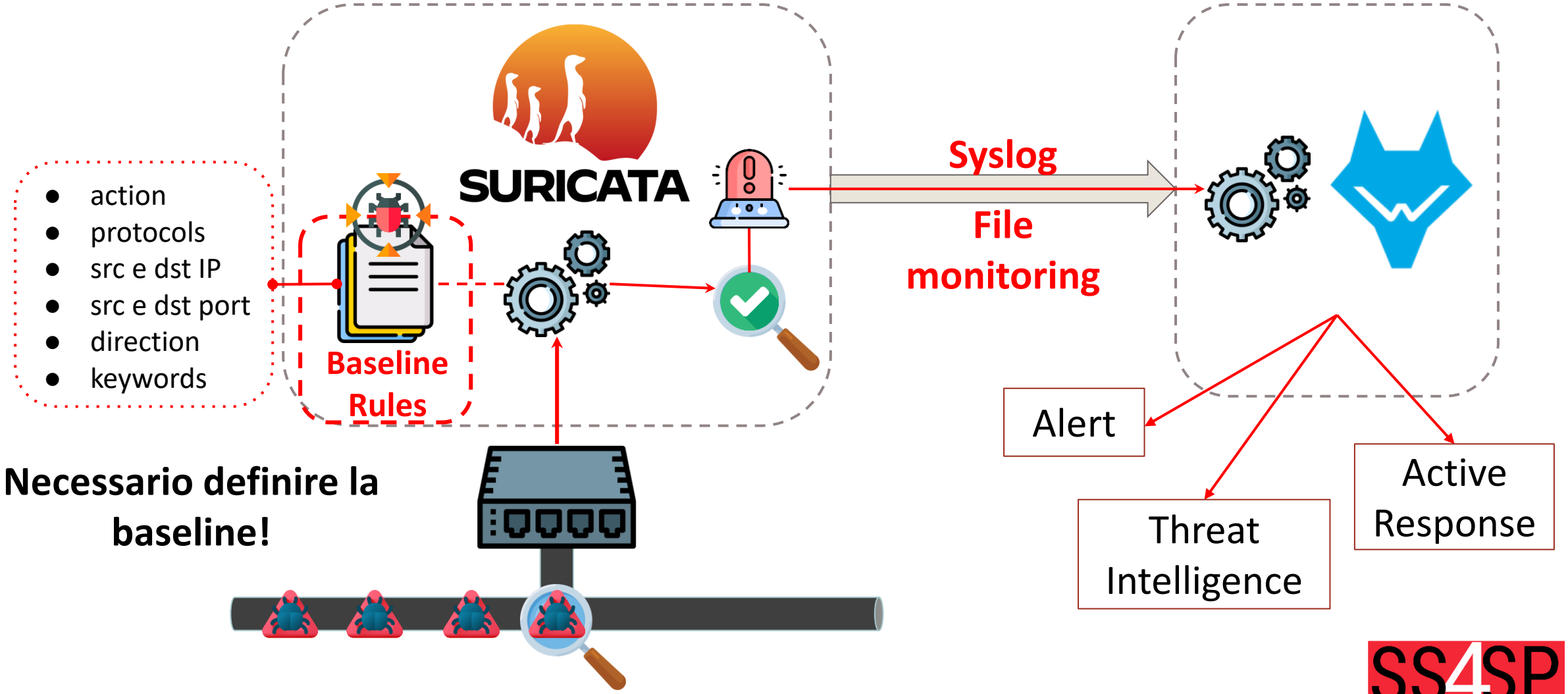
Intrusion Detection System (IDS) per:

- **sniffing del traffico** utilizzando logger PCAP
- **analisi off line** di file PCAP
- integrazione avanzata con Linux Netfilter firewalling

Protocol parser:

- packet decoding of: IPv4, IPv6, TCP, UDP, SCTP, ICMPv4, ICMPv6, GRE, Ethernet…
- App layer: HTTP, HTTP/2, SSL, TLS, SMB, DCERPC, SMTP, FTP, SSH, DNS, **Modbus**, ENIP/CIP, **DNP3**, NFS, NTP, DHCP, **SIP**, SNMP, **MQTT**…

Pipeline di monitoraggio

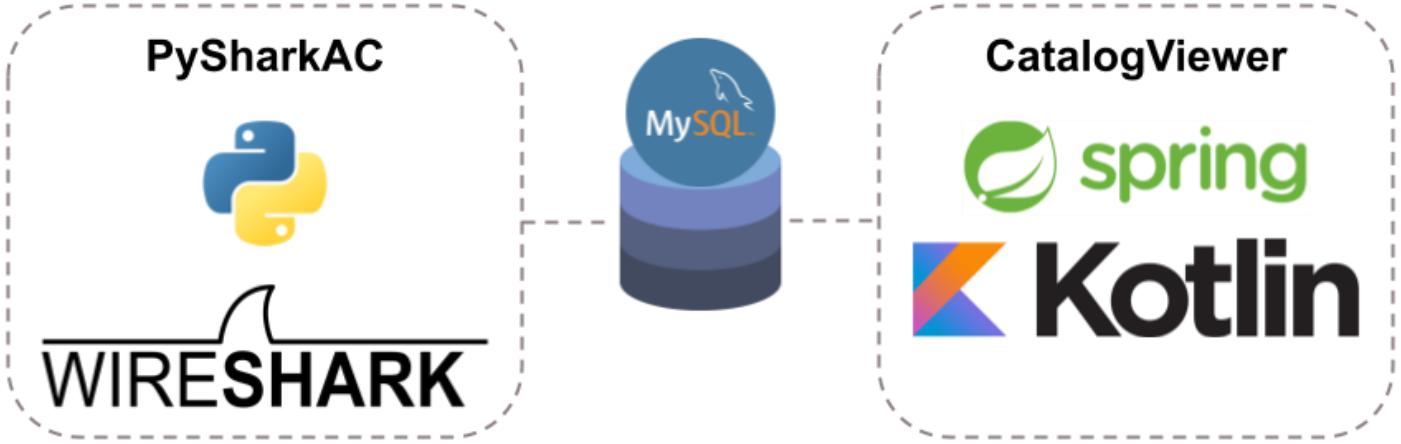


Definizione Baseline - Catalogazione traffico

Obiettivo: implementazione strumento per **asset discovery/inventory** e catalogazione del traffico (flusso, protocollo, indirizzo):

- **sniffing passivo del traffico** e catalogazione delle comunicazioni
- implementazione interfaccia di visualizzazione del catalogo

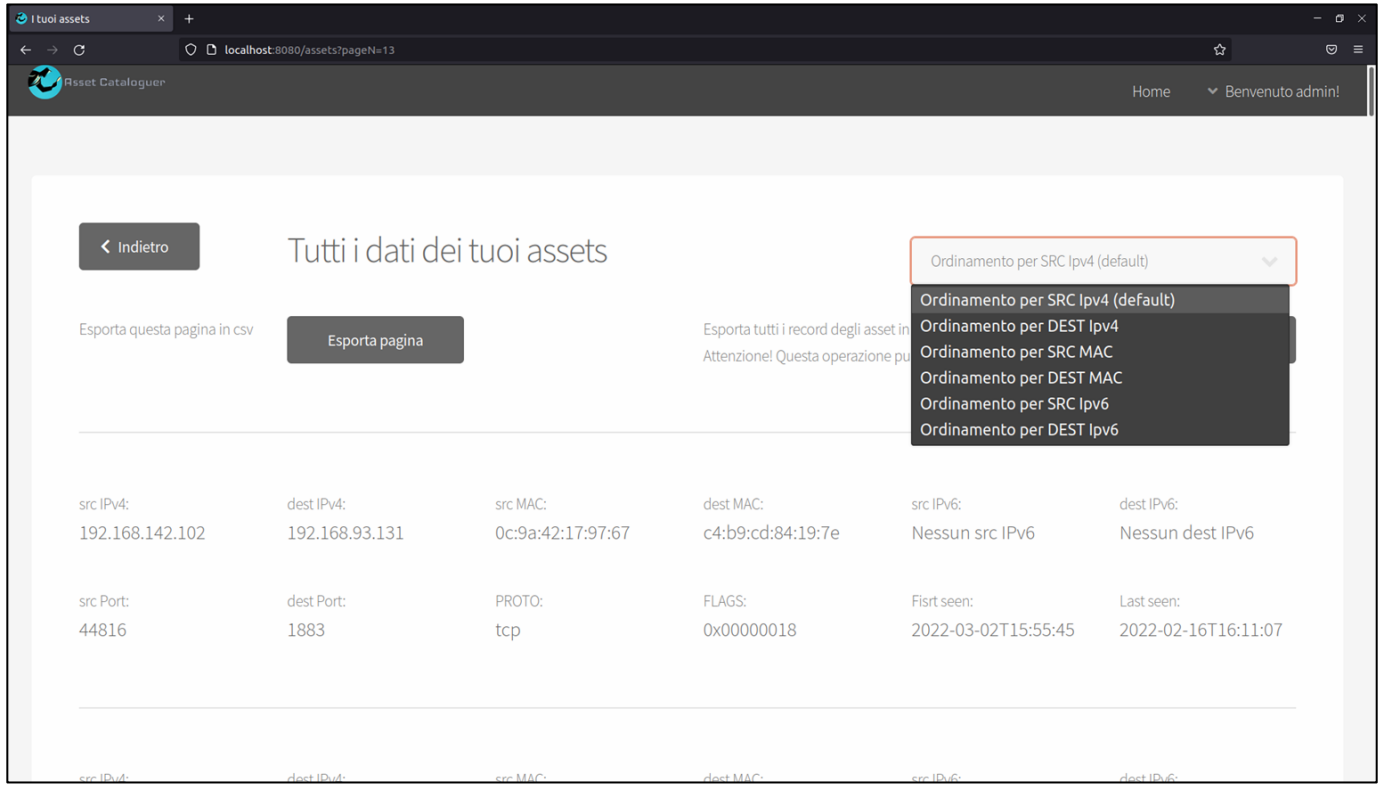
Output: traffico catalogato di supporto al rilevamento delle anomalie



Use Case SACMI
Lab. Ceramico

Definizione Baseline - Analisi traffico catalogato

- 8 M pacchetti → ~4 K comunicazioni distinte
- Rilevati ~40 protocolli
  - TCP, UDP, HTTP, DNS…
  - Modbus, MQTT, GVCP…
  - SMB, DCE/RPC, LLMNR…
- Rilevati ~100 dispositivi distinti
  - ~65% interni, 35% esterni



Definizione Baseline - Generazione regole (1)

Traffico interno

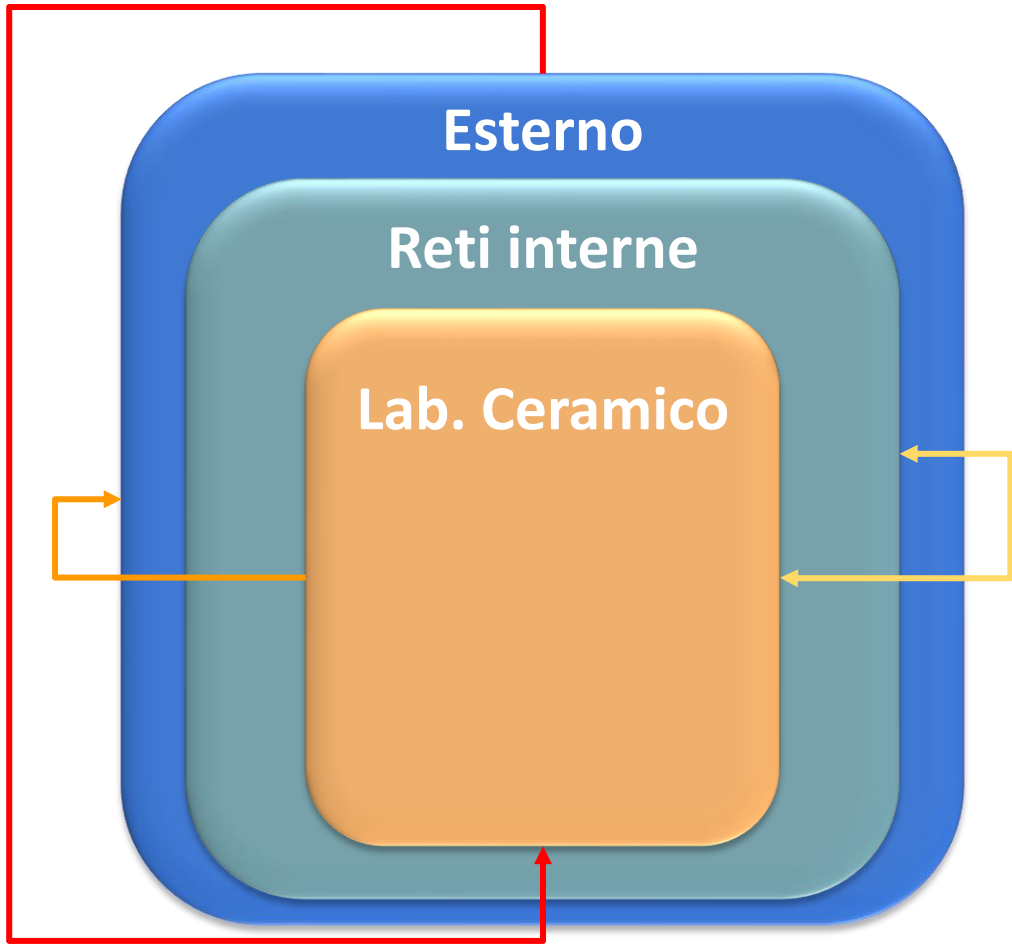
- **regole create sulla base di indicazioni di SACMI** e in base ai risultati di catalogazione
- script Python per generazione automatica regole in base alle indicazioni

```
alert tcp $PLC_MICRON_SCAGLIE ![80, 81] <> any any (msg:"Comunicazione tcp
    ↪  non prevista fra PLC_MICRON_SCAGLIE e any"; sid: 5000000;)
alert tcp $PLC_MICRON_SCAGLIE ![11159, 11169] <> any any (msg:"
    ↪ Comunicazione tcp non prevista fra PLC_MICRON_SCAGLIE e any"; sid:
    ↪ 4999999;)
alert udp $PLC_MICRON_SCAGLIE ![11159, 11169] <> any any (msg:"
    ↪ Comunicazione udp non prevista fra PLC_MICRON_SCAGLIE e any"; sid:
    ↪ 4999998;)
alert tcp $PLC_STRATO_SOFFICE ![80, 81] <> any any (msg:"Comunicazione tcp
    ↪  non prevista fra PLC_STRATO_SOFFICE e any"; sid: 4999997;)
alert tcp $PLC_STRATO_SOFFICE ![11159, 11169] <> any any (msg:"
    ↪ Comunicazione tcp non prevista fra PLC_STRATO_SOFFICE e any"; sid:
    ↪ 4999996;)
alert udp $PLC_STRATO_SOFFICE ![11159, 11169] <> any any (msg:"
    ↪ Comunicazione udp non prevista fra PLC_STRATO_SOFFICE e any"; sid:
    ↪ 4999995;)
```

Definizione Baseline - Generazione regole (2)

Traffico esterno

Da	A	Gravità
Esterno	Lab. ceramico	Grave
Lab. ceramico	Esterno	Media
Reti interne	Lab. ceramico	Bassa
Lab. ceramico	Reti interne	Bassa



Emerging Threat Rules

Set di **regole di alerting** open source realizzato da community di esperti:

- Attack-Response Rules
- BotCC Rules
- DOS Rules
- Exploit Rules
- Inappropriate Rules
- Malware Rules
- Scan Rules
- Web Rules
- Web-SQL-Injection Rules
- …

Risultati ottenuti

Suricata: Alert - Rilevata connessione INBOUND da reti locali verso Lab. Ceramico
Suricata: Alert - ET WEB_SERVER Possible CVE-2014-6271 Attempt
Suricata: Alert - ET EXPLOIT Apache log4j RCE Attempt (tcp ldap) (CVE-2021-44228)
Suricata: Alert - ET EXPLOIT Apache log4j RCE Attempt - lower/upper TCP Bypass M2 (CVE-2021-44228)
Suricata: Alert - GPL NETBIOS SMB-DS IPC$ share access
Suricata: Alert - SCADA_IDS: Modbus TCP - Illegal Packet Size, Possible DOS Attack
Suricata: Alert - ET EXPLOIT ETERNALBLUE Exploit M2 MS17-010

Interfacciamento con dispositivi Siemens

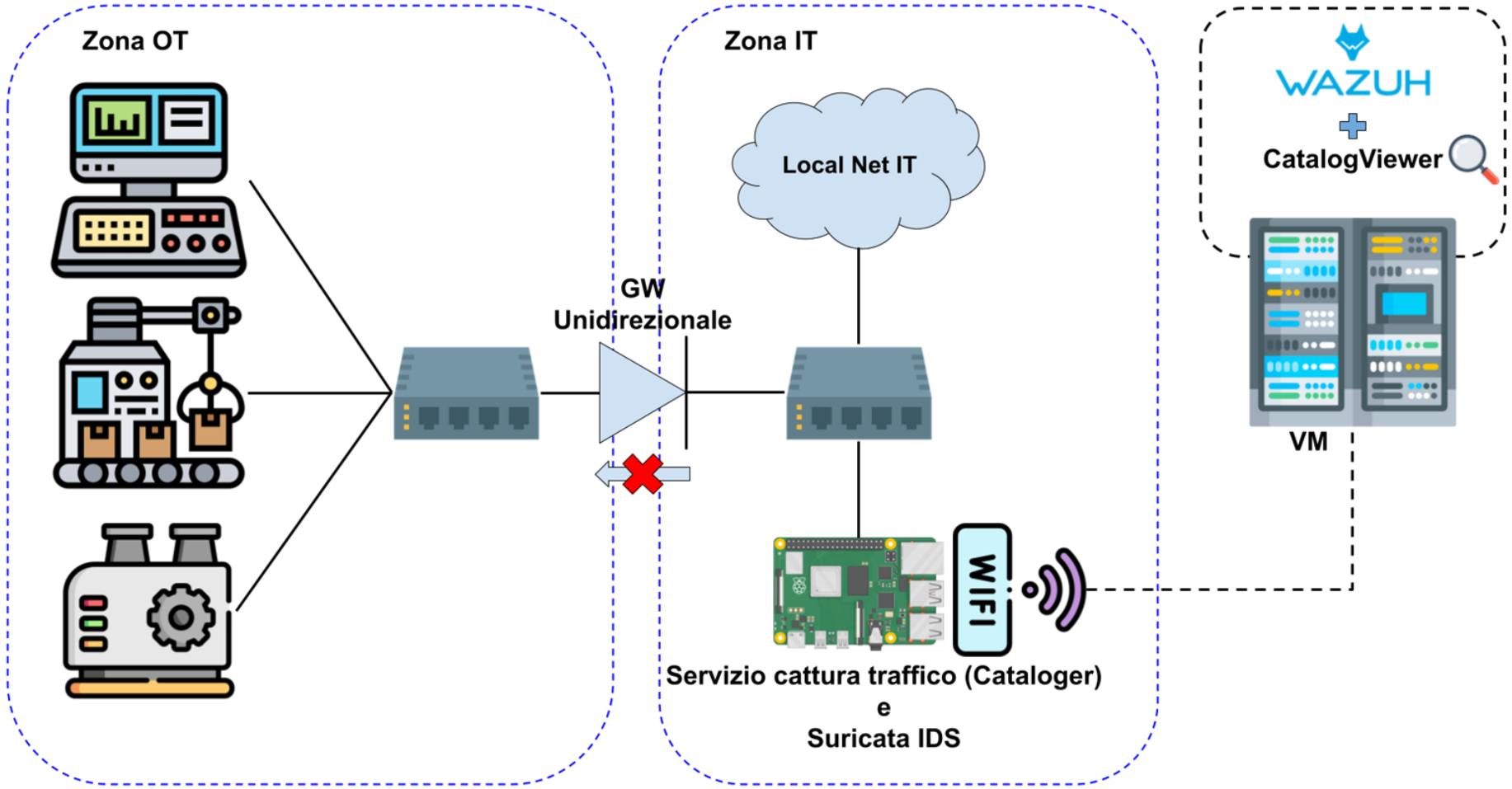
Obiettivo: monitorare azioni di blocco e reject

- **Siemens Scalance:** firewall frontend/backend
  - implementazione di un parser scritto in Python per normalizzare i log ricevuti
  - predisposizione di apposite regole di Wazuh
    → **alert in caso di azioni REJECT o DROP**

- **Sinema RC:** jumping station, gestisce connessioni VPN
  - predisposizione di decoder e regole per log di interesse
  - **alert in caso di (molteplici) login falliti** (credenziali errate, utente inesistente, tentativo di bruteforce, etc)

Use Case IMA
Linea Pilota BI-REX

Architettura di alto livello



a4GATE - Gateway IoT Unidirezionale

- Tramite software IoT edge raccoglie i dati dai componenti delle macchine presenti nella zona OT
- Uso del software Kepware come “concentratore di dati” con 150 driver di comunicazione a disposizione
- Dati trasmessi in tempo reale alla parte connessa alla rete esterna (zona IT)

Esempio traffico catalogato

src IPv4:	dest IPv4:	src MAC:	dest MAC:	src IPv6:	dest IPv6:
192.168.111.1	192.168.111.31	34:48:ed:43:89:bf	00:60:e9:29:f0:ed	Nessun src IPv6	Nessun dest IPv6
src Port:	**dest Port:**	**PROTO:**	**FLAGS:**	**Fisrt seen:**	**Last seen:**
61933	4840	opcua	0x00000018	2022-06-24T08:12:40	2022-06-24T10:13:4
src IPv4:	**dest IPv4:**	**src MAC:**	**dest MAC:**	**src IPv6:**	**dest IPv6:**
192.168.111.31	192.168.111.1	00:60:e9:29:f0:ed	34:48:ed:43:89:bf	Nessun src IPv6	Nessun dest IPv6
src Port:	**dest Port:**	**PROTO:**	**FLAGS:**	**Fisrt seen:**	**Last seen:**
4840	61933	opcua	0x00000018	2022-06-24T08:12:40	2022-06-24T10:13:4

Comunicazioni esterne rilevate

Da una prima analisi del traffico è emerso che il dispositivo comunica con diversi indirizzi IP esterni:

- **IMA Spa via Emilia:** abilitazione teleassistenza
- **Microsoft:** comunicazione gateway Azure IoT Edge
- **Snapcraft:** servizio di gestione pacchetti snap
- **Canonical:** interrogazioni repository Ubuntu

Tali comunicazioni possono essere eliminate disabilitando servizi non strettamente necessari

Baseline implementata

Le regole inserite per svolgere i seguenti controlli:

- segnalare **comunicazioni che non rientrino tra quelle note**, con particolare attenzione ad indirizzi IP pubblici
- segnalare comunicazioni **OPC-UA non cifrate**

Jun 28, 2022 @ 18:29:34.616	p319-ss4sp	Suricata: Alert - Comunicazione non prevista
Jun 28, 2022 @ 18:29:34.616	p319-ss4sp	Suricata: Alert - Traffico OPC-UA non cifrato (MSG)

Conclusioni

- **Soluzioni opensource validi supporti in ambito IT e OT**, alternative a soluzioni commerciali che potrebbero non essere alla portata delle PMI
- **Soluzioni opensource estensibili e personalizzabili** grazie ad API
- **Soluzioni opensource richiedono configurazioni manuali** e implementazione di script ad-hoc, strumenti commerciali compiono molte azioni in modo automatico → **soluzioni opensource necessitano di personale competente**

Soluzioni commerciali: Nozomi Guardian

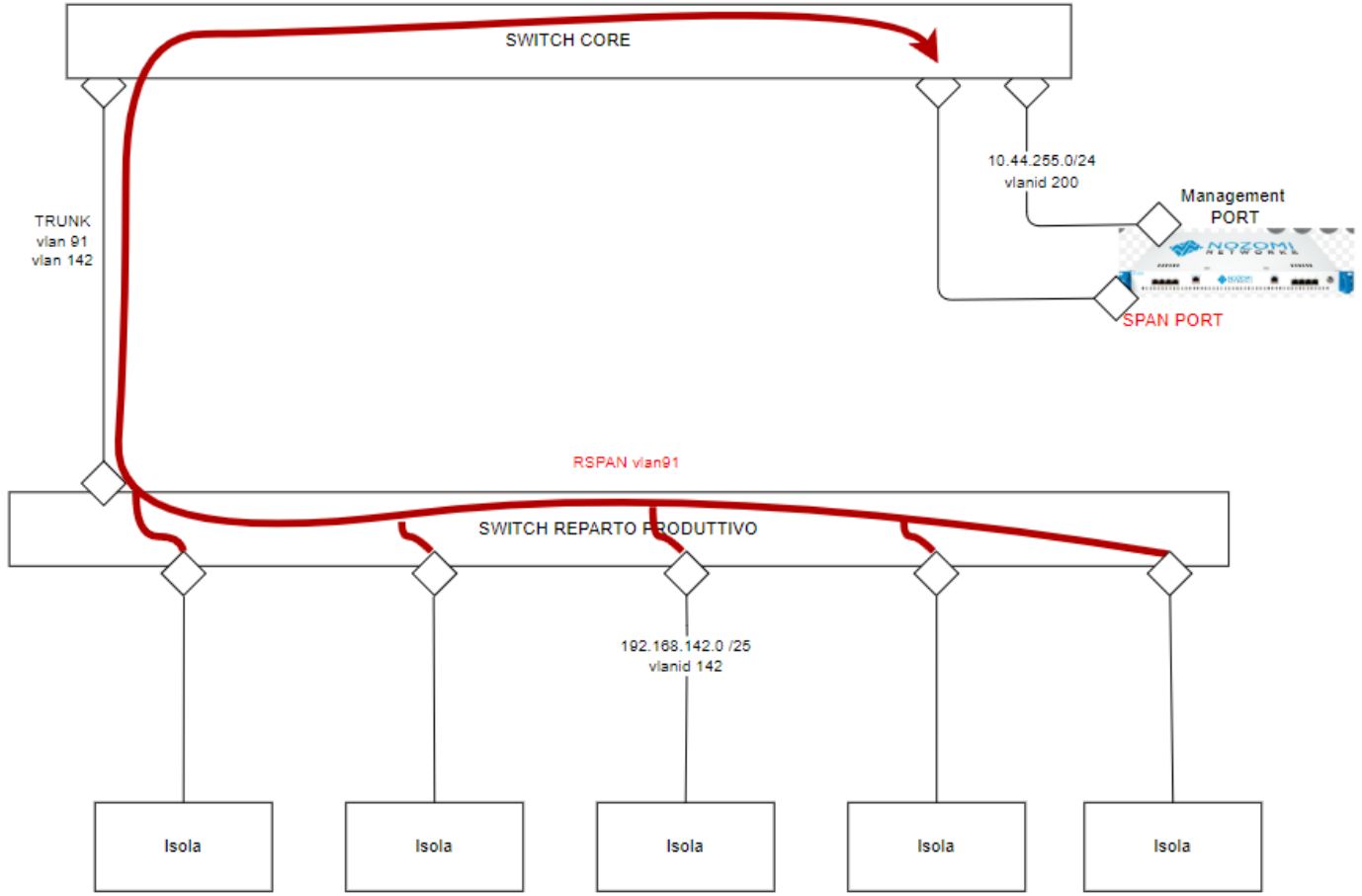
Appliance di monitoraggio di rete che fornisce visibilità sugli asset OT, IoT, IT con funzioni di:

1. Device discovery → individua tutti i dispositivi che generano traffico di rete e le relative caratteristiche (sistema operativo, servizi attivi, ecc.)
2. Network visualization → genera una mappa dell'architettura di rete, personalizzabile anche secondo il modello Purdue
3. Vulnerability assessment → monitorando passivamente il traffico rileva le vulnerabilità degli host connessi in rete (es. utilizzo di protocolli insicuri)
4. Risk monitoring and cyber threat detection → rileva traffico malevolo applicando pattern noti oppure identificando le comunicazioni che si discostano dalla baseline

Nozomi Guardian: Deployment Use Case SACMI

La **sonda** Nozomi Guardian è stata installata come **Macchina Virtuale nel Datacenter SACMI**.

Sia sullo switch core, centro stella della rete SACMI che sugli switch periferici sono state configurate **SPAN port per inviare il traffico da analizzare alla sonda**.



SS4SP
safety and security for
smart production

Nozomi Guardian: funzionalità utilizzate

Appliance di monitoraggio di rete che fornisce visibilità sugli asset OT, IoT, IT con funzioni di:

1. Device discovery → utilizzata per verificare ed arricchire l'inventario degli asset per ogni zona
2. Network visualization → utilizzata per verificare ed arricchire le informazioni sui conduits
3. Vulnerability assessment → utilizzata come input di alto livello per l'analisi dei rischi
4. Risk monitoring and cyber threat detection → utilizzata durante il penetration test per valutare l'effettiva visibilità delle minacce

Soluzioni open source vs commerciali

Soluzioni	PRO	CONTRO
OPENSOURCE	**No costi di licenza**; estensibili e personalizzabili	Necessitano di **specifico know-how** per l'installazione e configurazione; generalmente **no supporto e consulenza tecnica**
COMMERCIALI	Disponibili interfacce pronte e user-friendly; disponibile **supporto e consulenza tecnica**	**Costi di licenza**; limiti di integrazione, personalizzazione ed estensione.

SS4SP
safety and security for smart production

Implementazione della segregazione delle reti industriali

A cura di

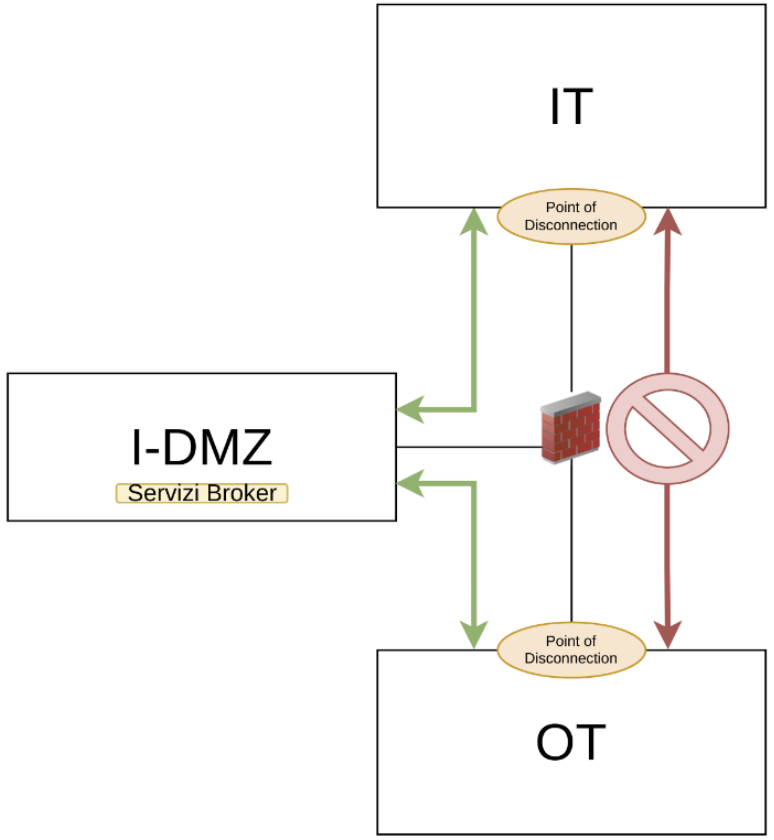
Giorgio Valenziano Santangelo

Contenuti

- Principi di progettazione dell'industrial DMZ
- Tecnologie per l'implementazione dell'industrial DMZ
- Implementazione dell'IDMZ nello Use Case SACMI
- Implementazione del Data-Diode nello Use Case BI-REX/IMA

Principi di progettazione dell'I-DMZ

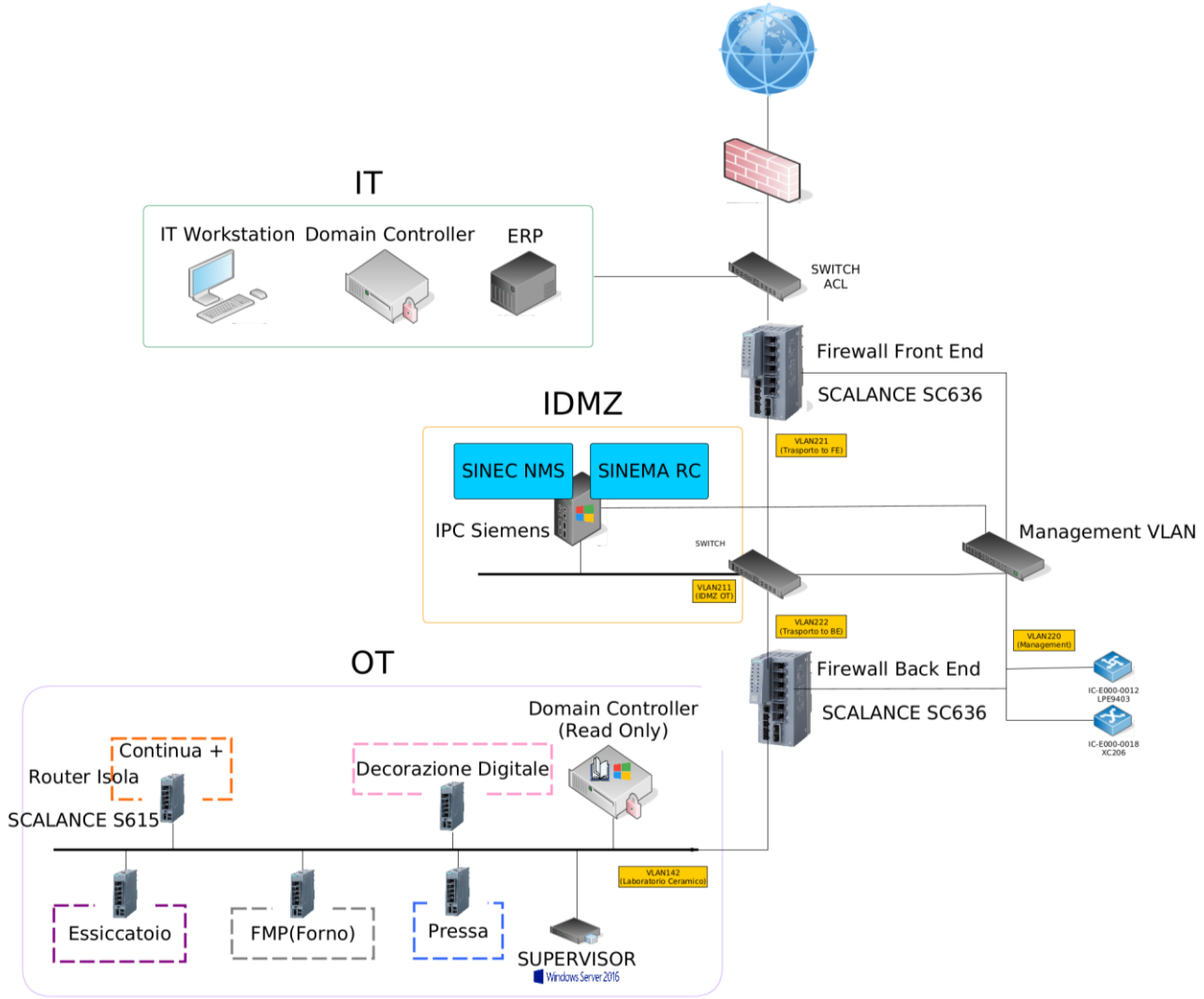
- L'Industrial DMZ è un livello di sicurezza addizionale tra la rete Corporate (IT) e la rete di Automazione (OT).
- Essa intermedia le comunicazioni tra le due reti:
  - Nessuna connessione dovrebbe attraversare l'I-DMZ;
  - I protocolli di rete industriali devono rimanere confinati nell'OT;
  - I Servizi primari non devono risiedere nella I-DMZ;
  - I dati sono transitori;
  - Servizi Broker segmentati e segregati dal resto della I-DMZ;
  - Single Point of Disconnection.



Tecnologie per l’implementazione dell’industrial DMZ

- **Siemens Scalance**:
  - **S615**, LAN-Router, appliance che fornisce protezione per i dispositivi e le reti di automazione e per le comunicazioni industriali tramite VPN e Firewall.
  - **SC-636**, un Industrial Security Appliance per la protezione di apparecchi e reti nella produzione discreta e nell'industria di processo.
- **SINEMA RC**: applicazione Server che permette di gestire le connessioni (tunnel) VPN tra le sedi, i tecnici dell’assistenza, le macchine e gli impianti;
- **SINEC NMS**: un Network Management System (NMS) usato per monitorare, gestire e configurare in maniera centralizzata le reti industriali;
- **Engineering Stations**: host che permettono l’accesso alla rete OT con a bordo tutti i software necessari alla configurazione e manutenzione dei device industriali (PLC, HMI, ecc.);

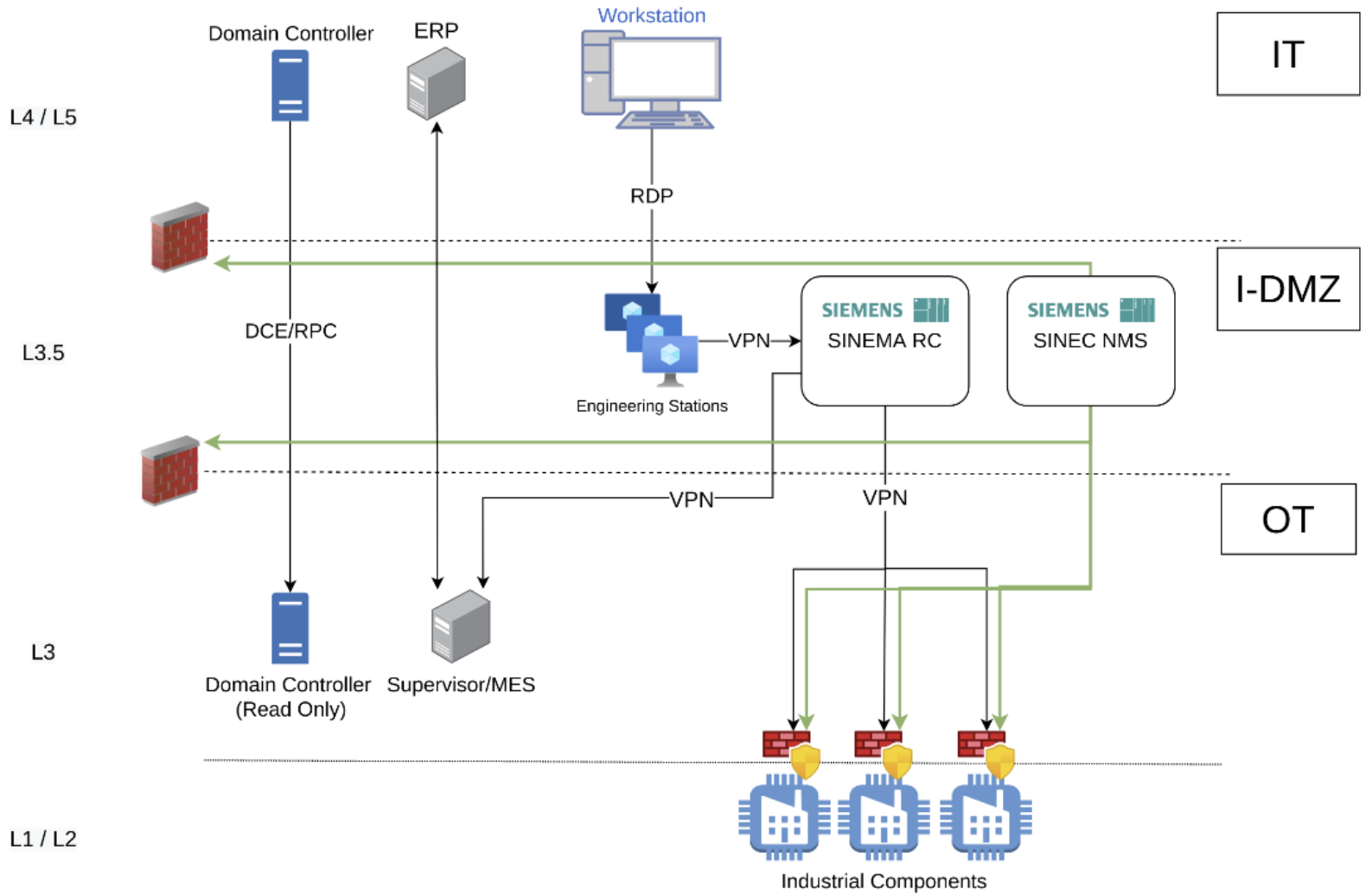
Implementazione IDMZ Use Case SACMI



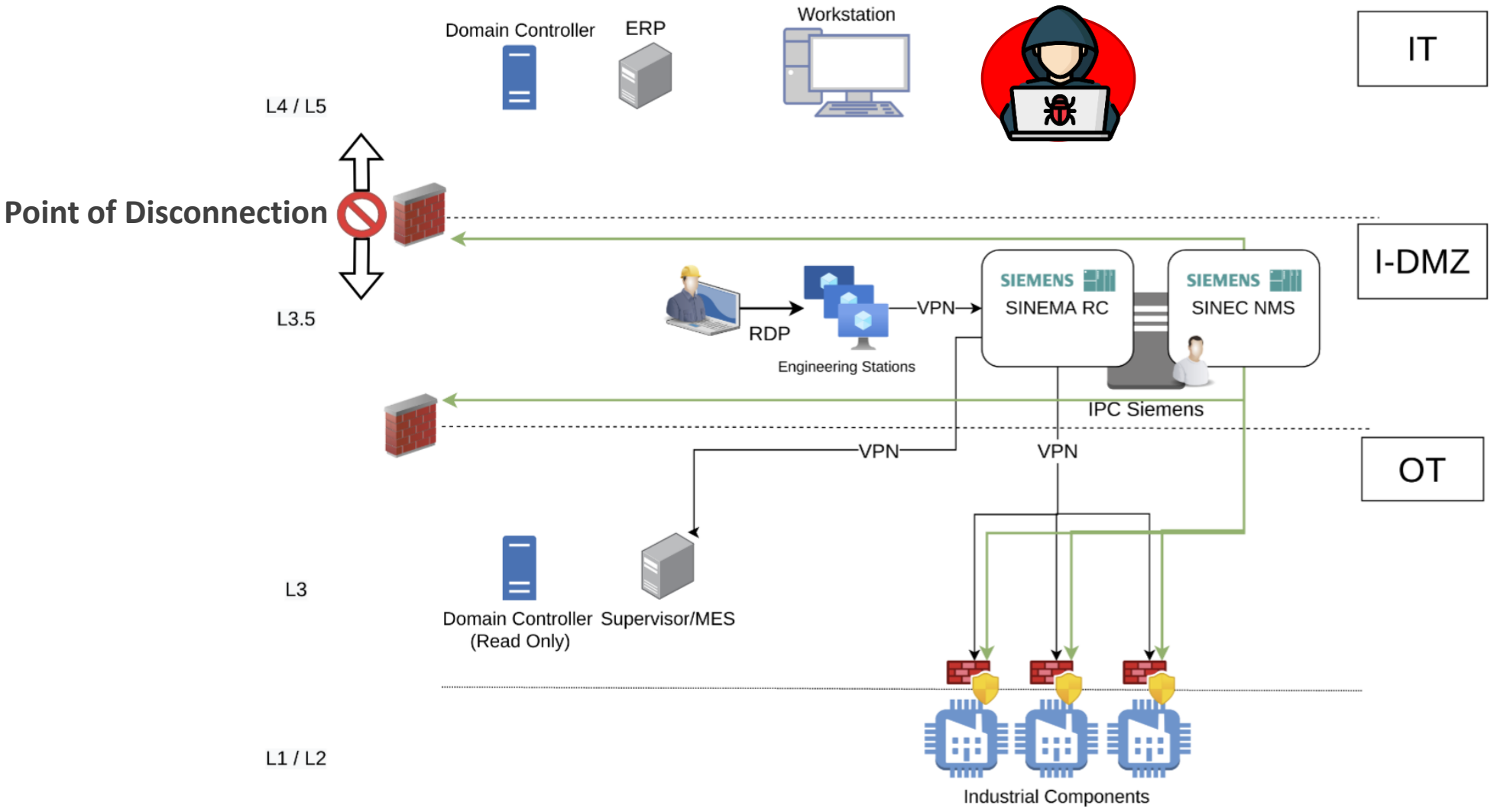
- Firewall di Front End
- Firewall di Back End
- IDMZ:
  - SINEMA RC
  - SINEC NMS
  - Engineering Workstations
- Rete OT:
  - Supervisor;
  - Read Only Domain Controller;
  - Processi produttivi
    - Segmentati e segregati tramite Scalance.
- Rete di Management

SS4SP
safety and security for smart production

Implementazione IDMZ Use Case SACMI
Data Flow IDMZ

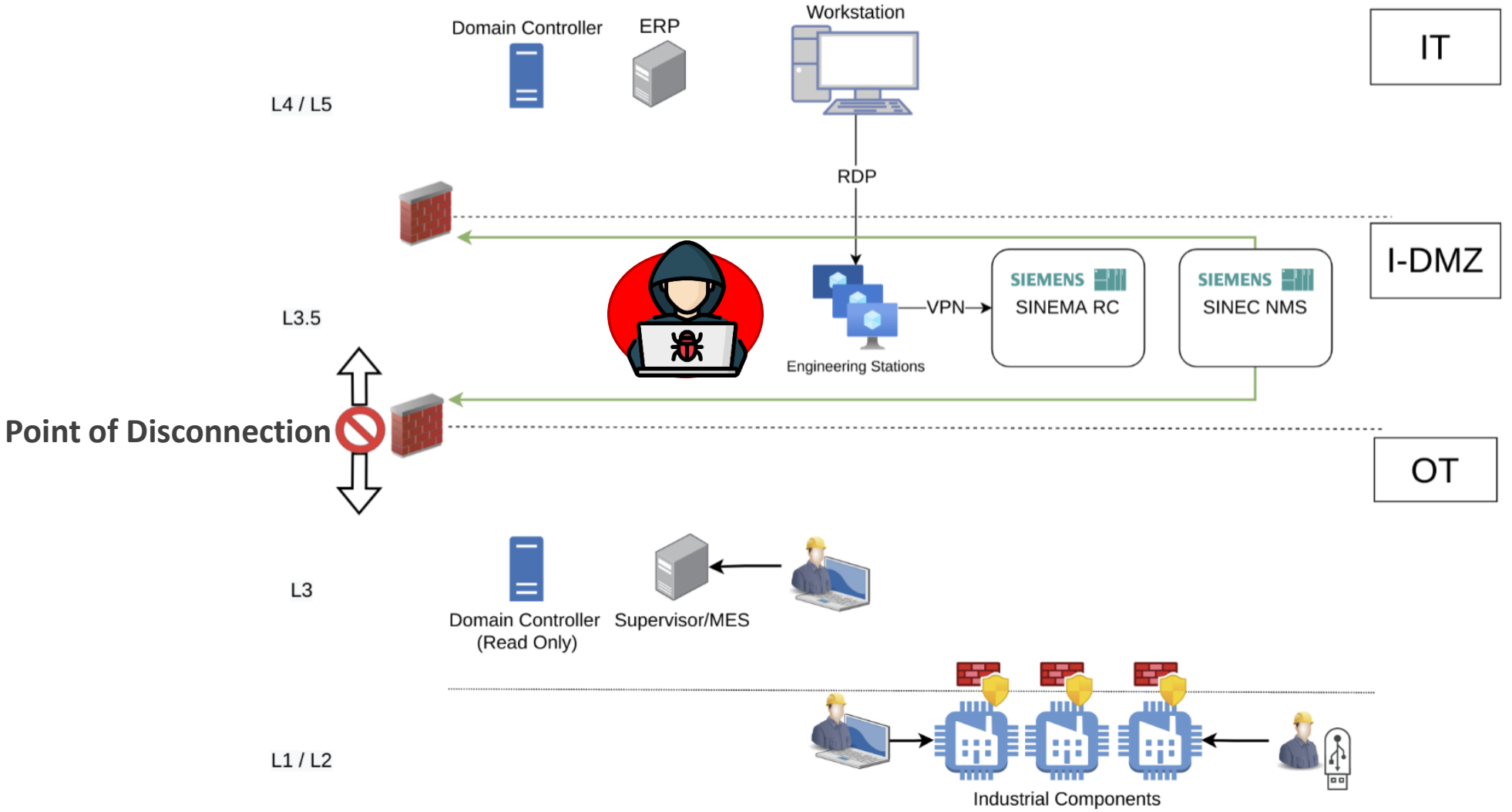


Implementazione IDMZ Use Case SACMI
Point of Disconnection (1)



Implementazione IDMZ

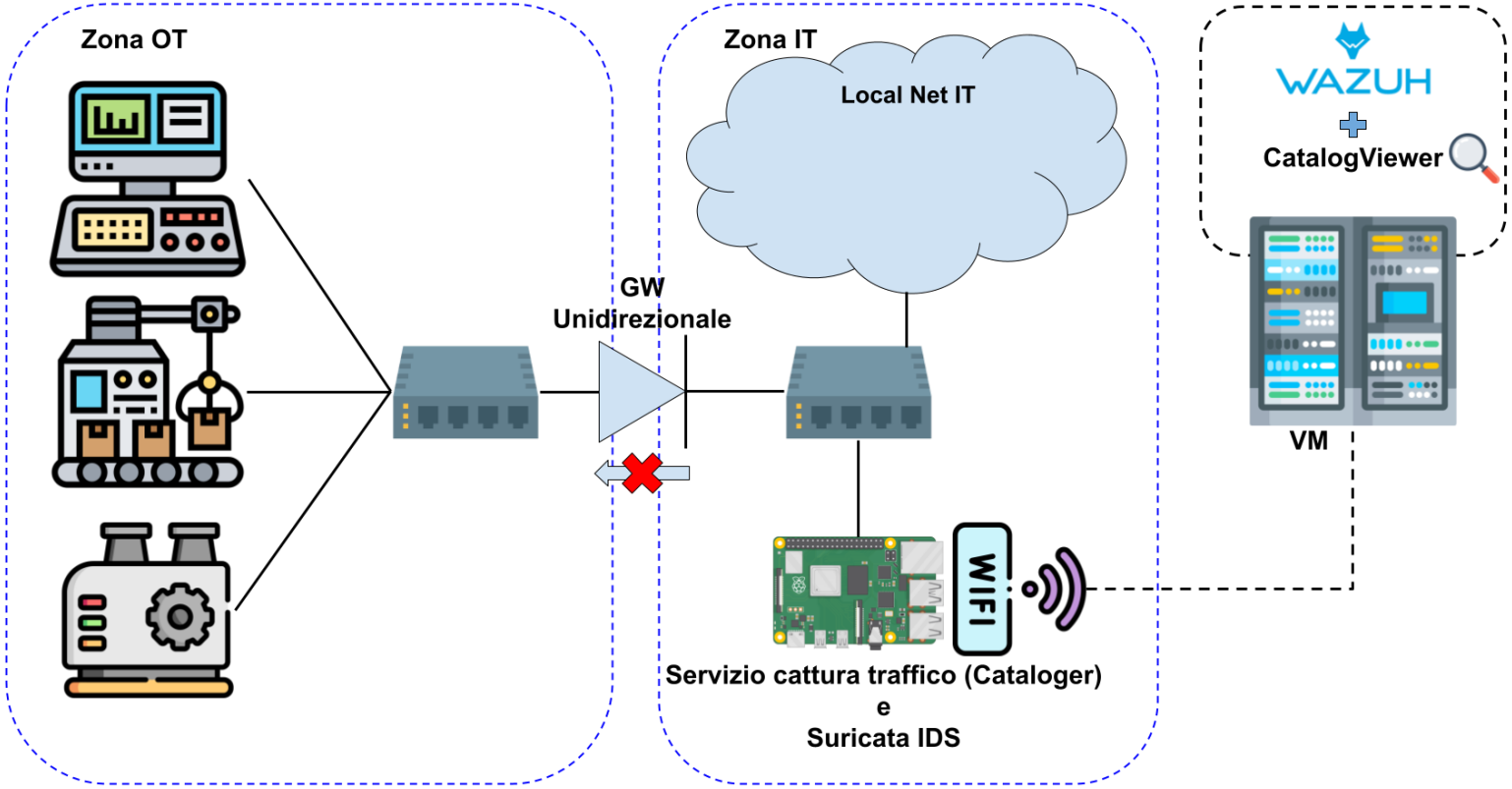
Use Case SACMI - *Point of Disconnection (2)*



A4Gate Unidirectional Gateway

Use Case BI-Rex / IMA

- Traffico consentito da Rete OT a Rete IT per telemetria;
- La bidirezionalità è consentita su richiesta per attività di configurazione e manutenzione della strumentazione di automazione.



SS4SP
safety and security for smart production

Verifica della mitigazione dei rischi

A cura di

Mirco Marchetti

Giorgio Valenziano Santangelo

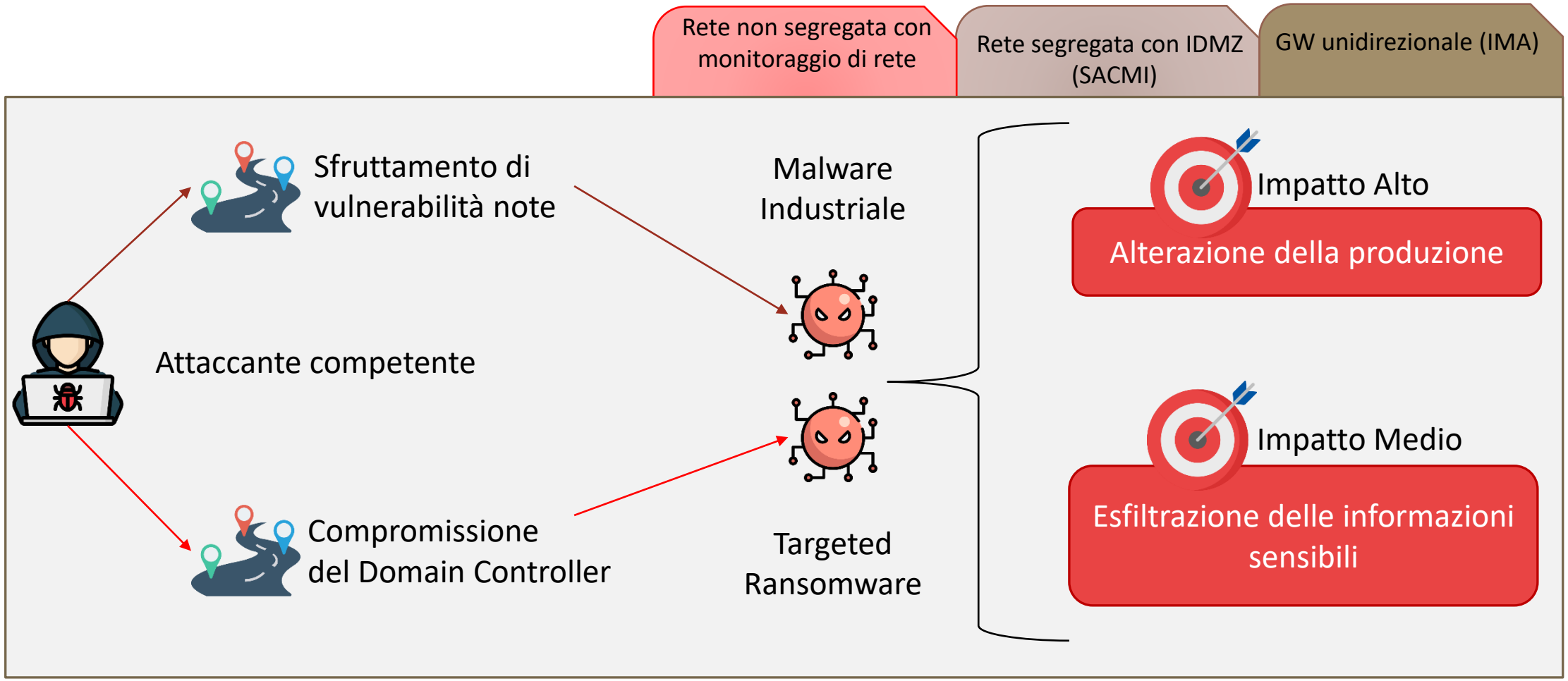
Contenuti

- Penetration test a seguito dell'applicazione delle misura di sicurezza
- Valutazione del rischio a seguito dell'applicazione di ogni misura di sicurezza
- Calcolo del rischio residuo

Valutazione dei rischi sugli Use Cases

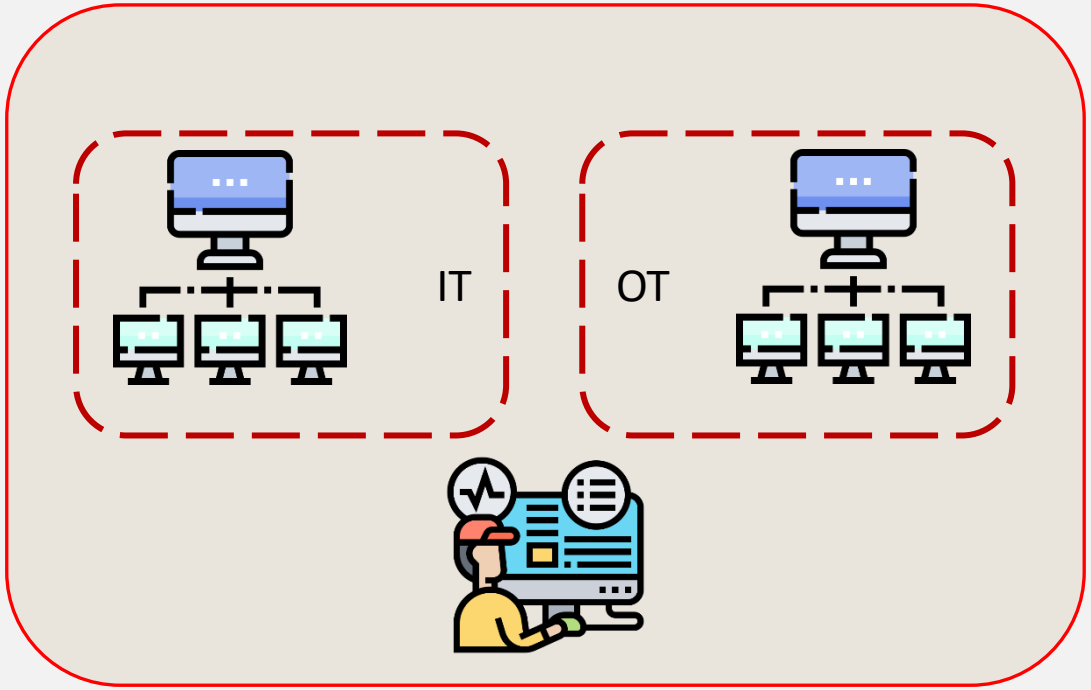
- Considerazioni fatte:
  - Non si consideri il vettore di attacco con cui l'attaccante ha ottenuto l'accesso alla rete IT;
  - Sono state fatte delle assunzioni riguardo la presenza di vulnerabilità in base alla conoscenza pregressa sui dispositivi presenti all'interno degli Use Cases;
  - In base agli impatti che si possono generare si considera per gli Use Case in esame un Security Level Target (SL-T) pari a 2. Quindi, la soglia di accettazione del rischio è <= Medio (9).
- System under Consideration:
  - Scenario di rete non segregata con monitoraggio di rete;
  - Scenario di rete segregata con Industrial DMZ (Use Case Laboratorio Ceramico SACMI);
  - Scenario di rete segregata con Unidirectional Gateway (Use Case IMA-BI-Rex).

Valutazione dei rischi sugli Use Cases

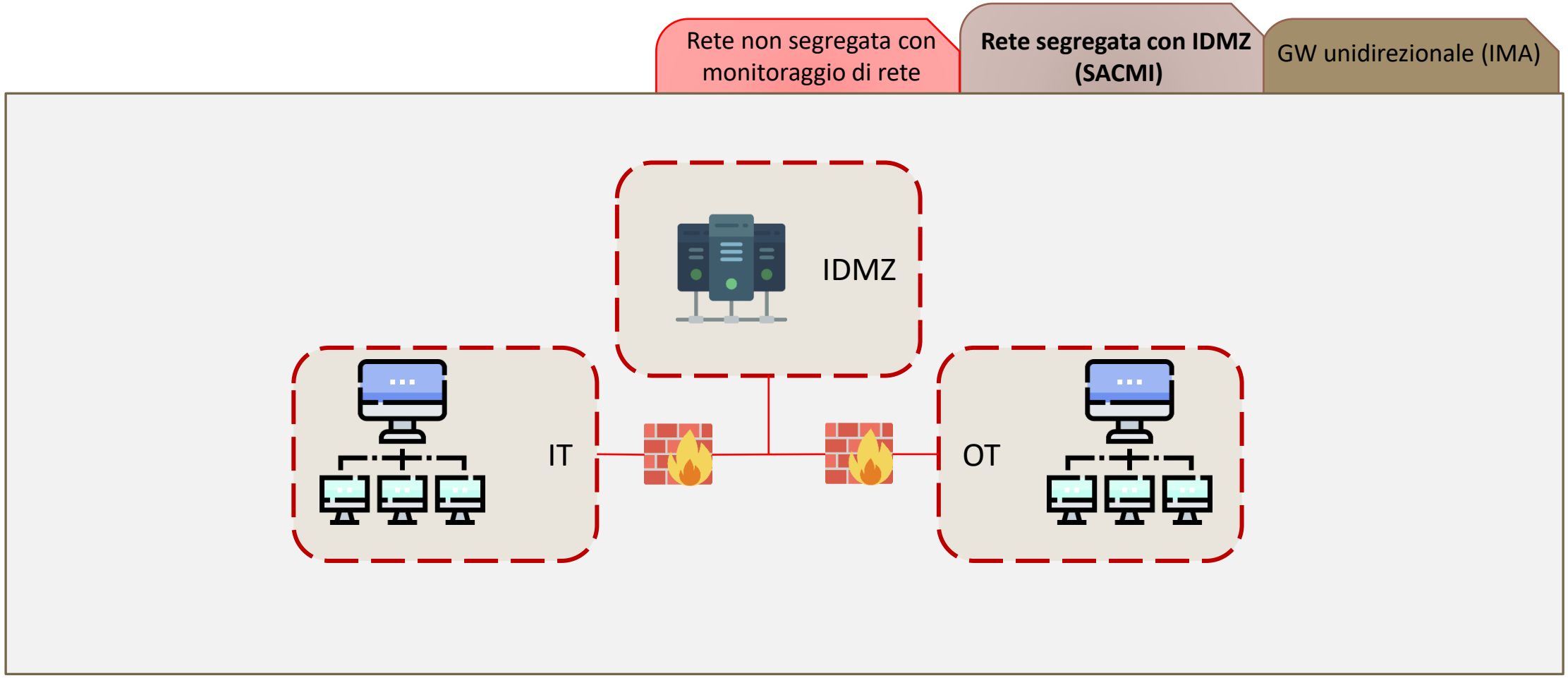


Valutazione dei rischi sugli Use Cases

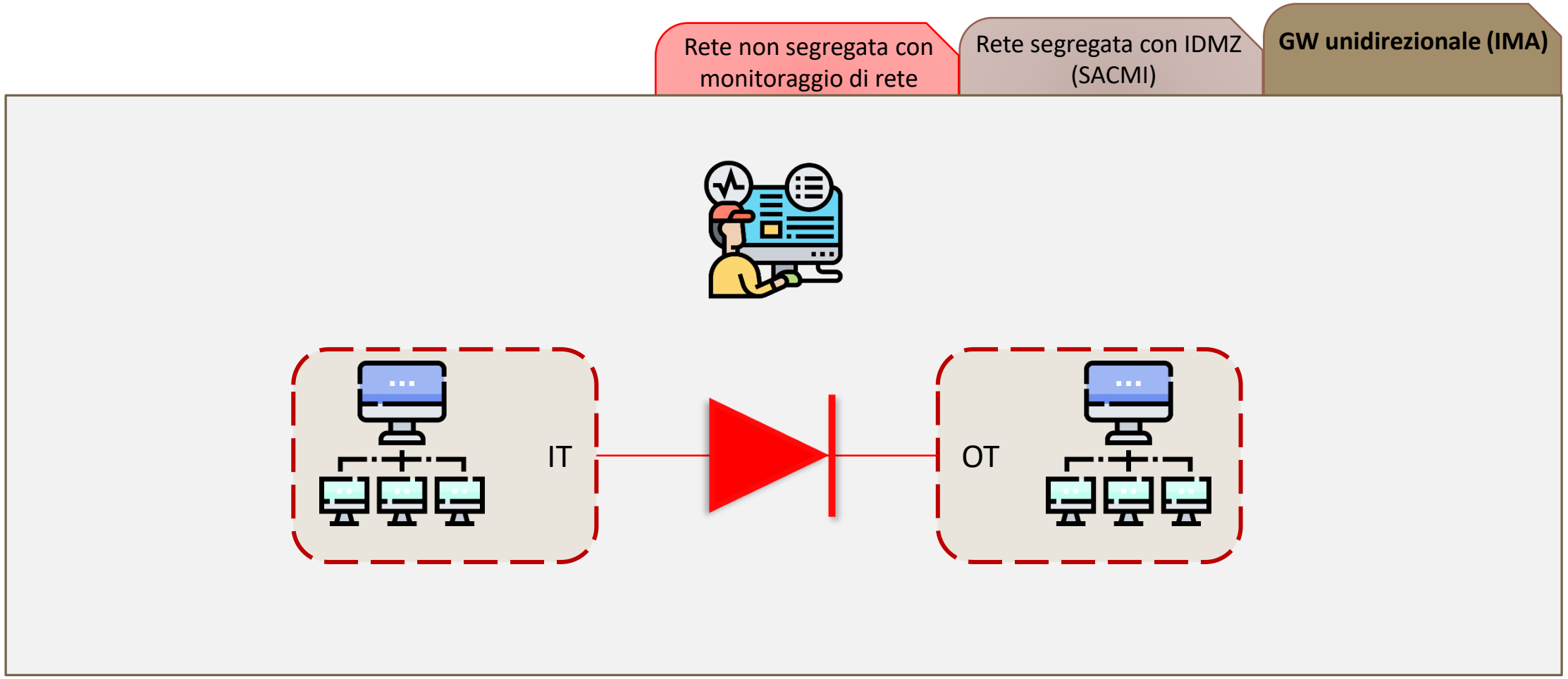
Rete non segregata con monitoraggio di rete | Rete segregata con IDMZ (SACMI) | GW unidirezionale (IMA)



Valutazione dei rischi sullo Use Cases

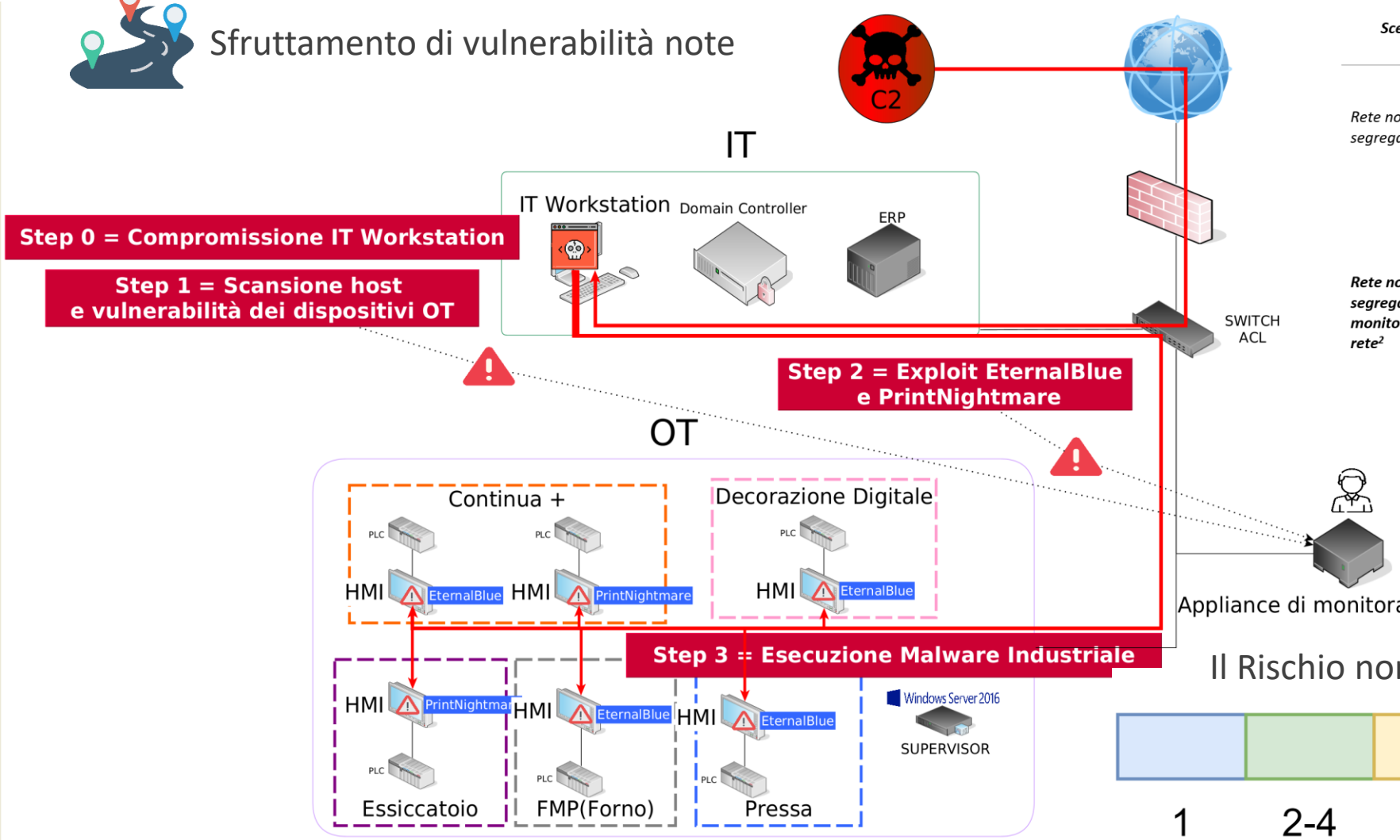


Valutazione dei rischi sullo Use Cases



Valutazione dei rischi sugli Use Cases

Sfruttamento di vulnerabilità note

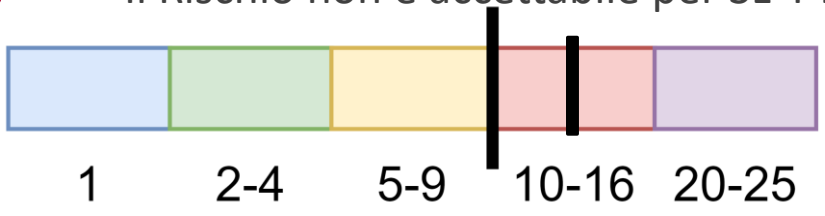


Scenario	Casi	Impatto	Probabilità di rischio	Rischio
Rete non segregata	EternalBlue	Alto	Alta	16 - Alto
	PrintNightmare	Alto	Alta	16 - Alto
Rete non segregata con monitoraggio di rete[2]	EternalBlue	Alto	Media	12- Alto
	PrintNightmare	Alto	Media	12 - Alto

Risultati

NB: Probabilità di mancata interruzione dell'attacco considerata = Bassa. 30 min < f < 2h

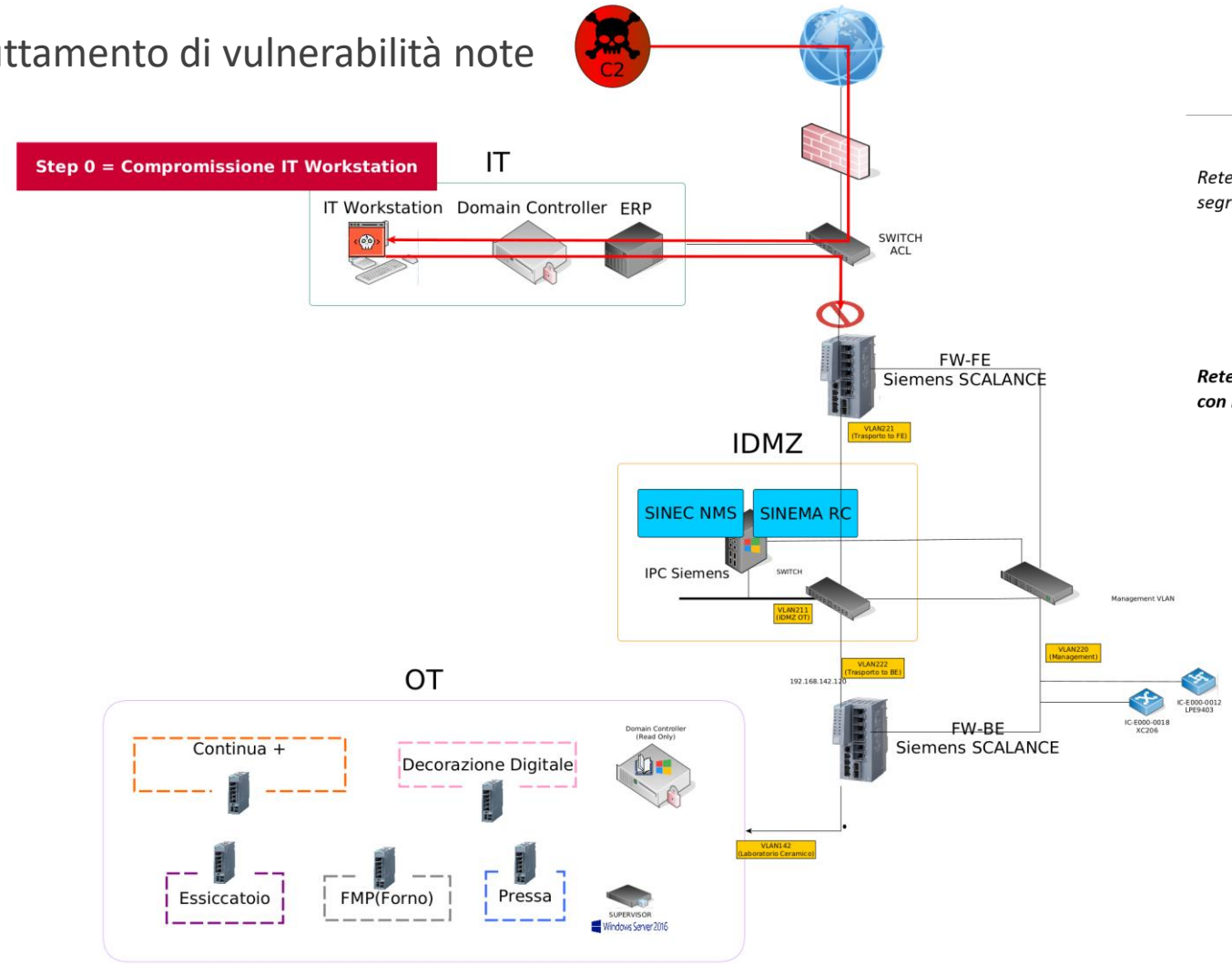
Il Rischio non è accettabile per SL-T 2



SS4SP safety and security for smart production

Valutazione dei rischi sugli Use Cases

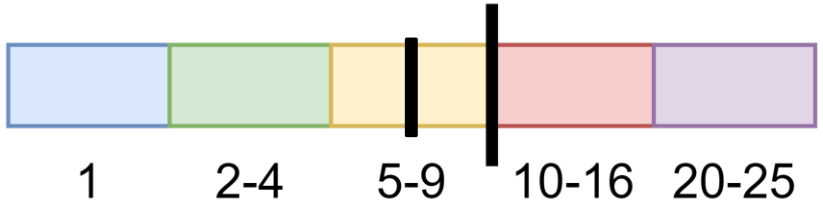
Sfruttamento di vulnerabilità note



Scenario	Casi	Impatto	Probabilità di rischio	Rischio
Rete non segregata	EternalBlue	Alto	Alta	16 - Alto
	PrintNightmare	Alto	Alta	16 - Alto
Rete segregata con I-DMZ	EternalBlue	Alto	Bassa	8 - Medio
	PrintNightmare	Alto	Bassa	8 - Medio

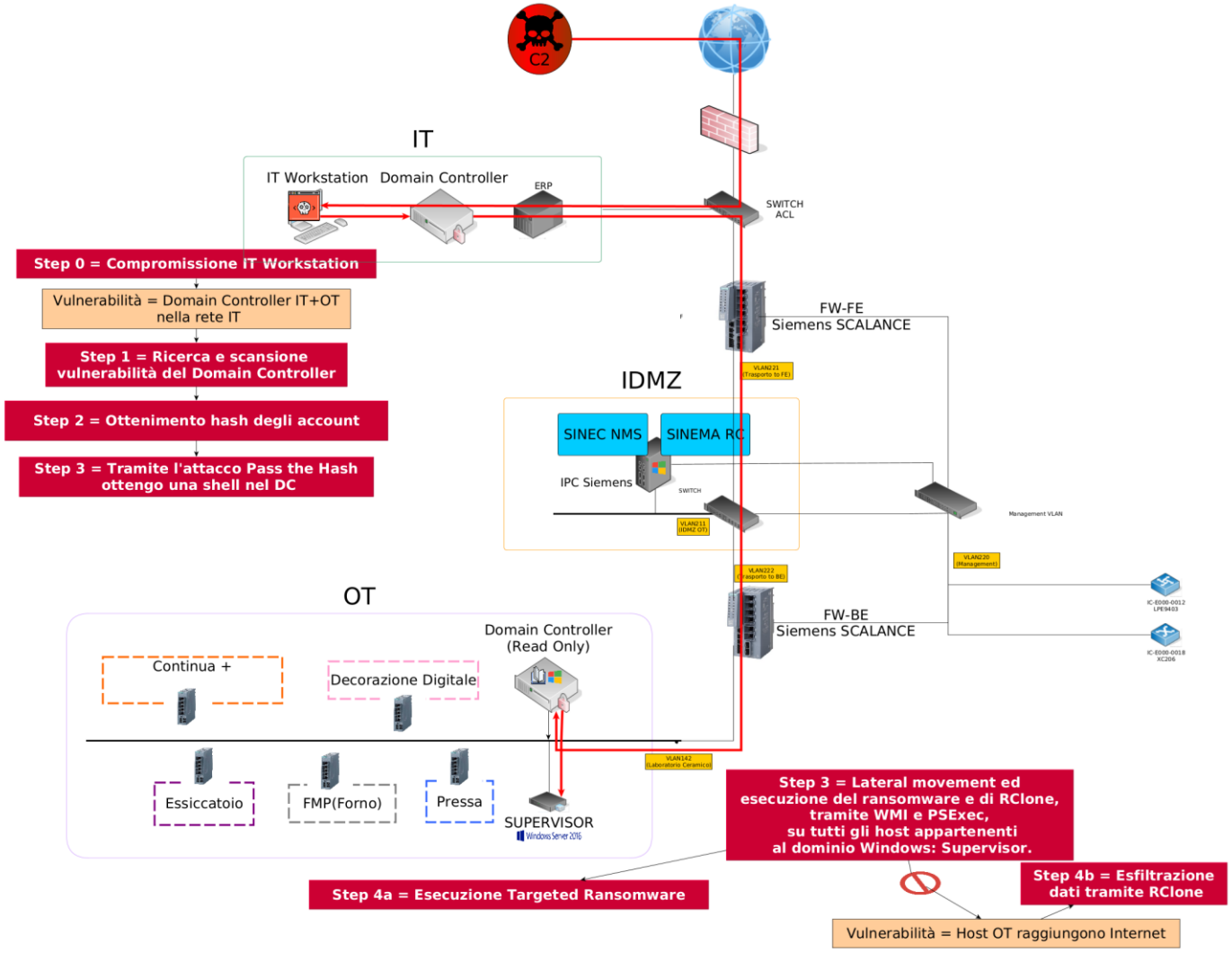
Risultati

Il Rischio è accettabile per SL-T 2



SS4SP
safety and security for smart production

Valutazione dei rischi sullo Use Case SACMI

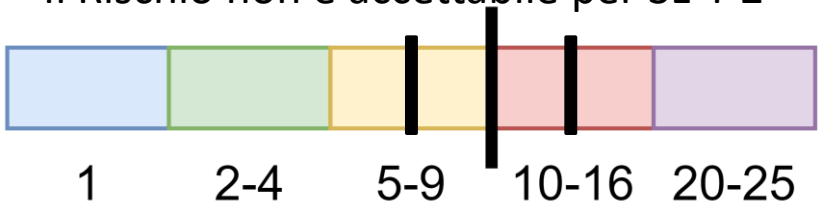


Compromissione del Domain Controller

Risultati

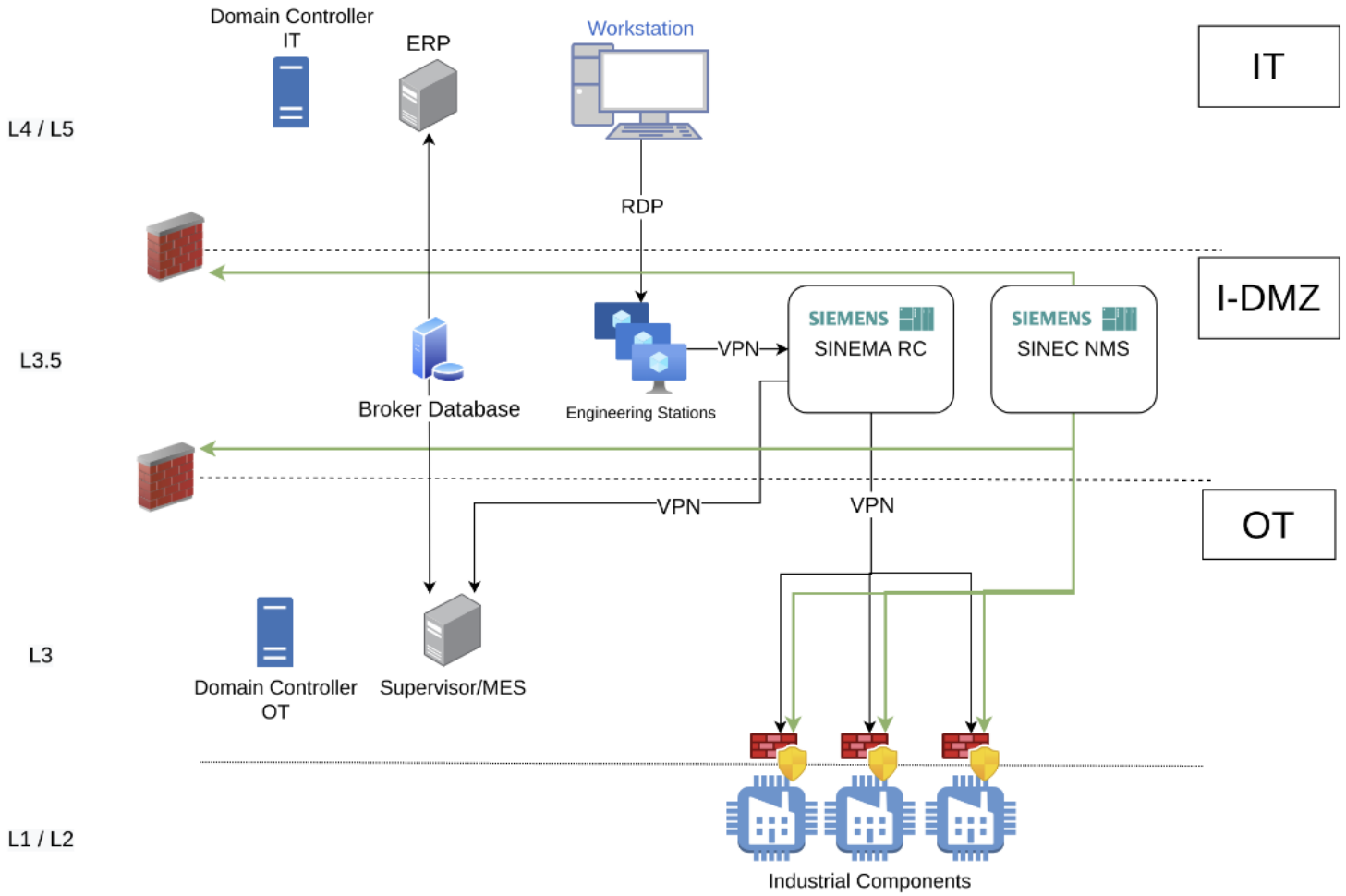
Scenario	Casi	Impatto	Probabilità di rischio	Rischio
Rete non segregata	Esecuzione Targeted Ransomware	Alto	Alta	16 - Alto
	Esfiltrazione dati tramite RClone	Medio	Alta	16 - Alto
Rete segregata con I-DMZ	Esecuzione Targeted Ransomware	Alto	Alta	16 - Alto
	Esfiltrazione dati tramite RClone	Medio	Bassa	6 - Medio

Il Rischio non è accettabile per SL-T 2



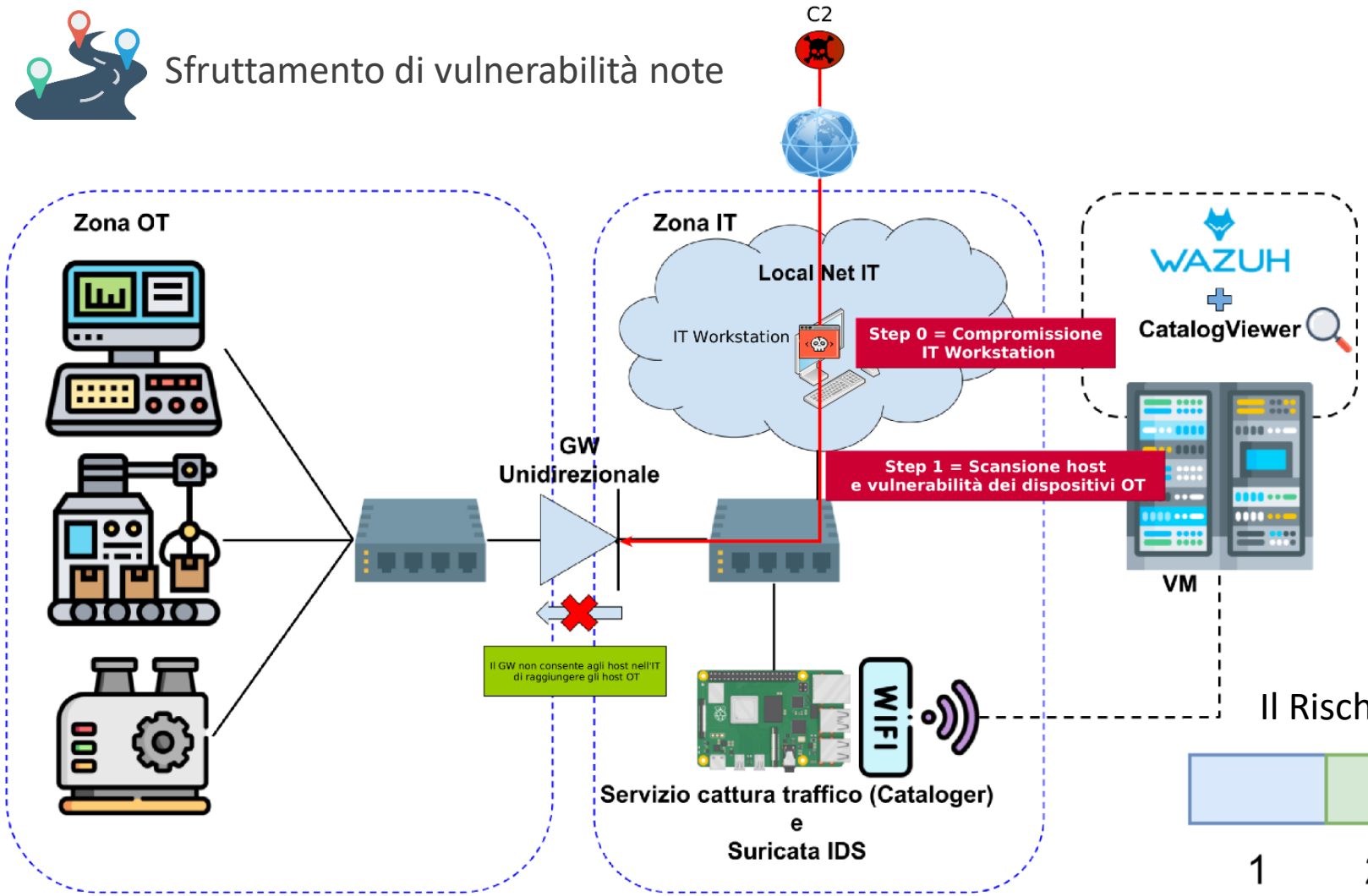
SS4SP
safety and security for smart production

Architettura finale Use Case SACMI



Valutazione dei rischi sullo Use Case BI-Rex / IMA

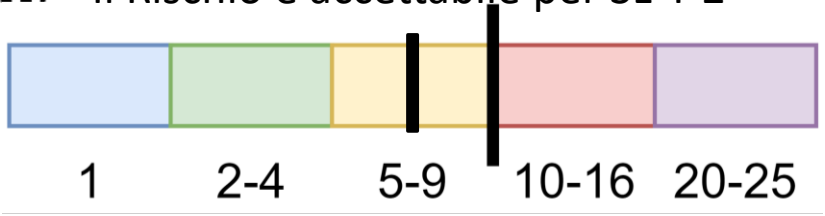
Sfruttamento di vulnerabilità note



Scenario	Casi	Impatto	Probabilità di rischio	Rischio
Rete non segregata	EternalBlue	Alto	Alta	16 - Alto
	PrintNightmare	Alto	Alta	16 - Alto
Rete segregata con Unidirectional Gateway	EternalBlue	Alto	Bassa	8 - Medio
	PrintNightmare	Alto	Bassa	8 - Medio

Risultati

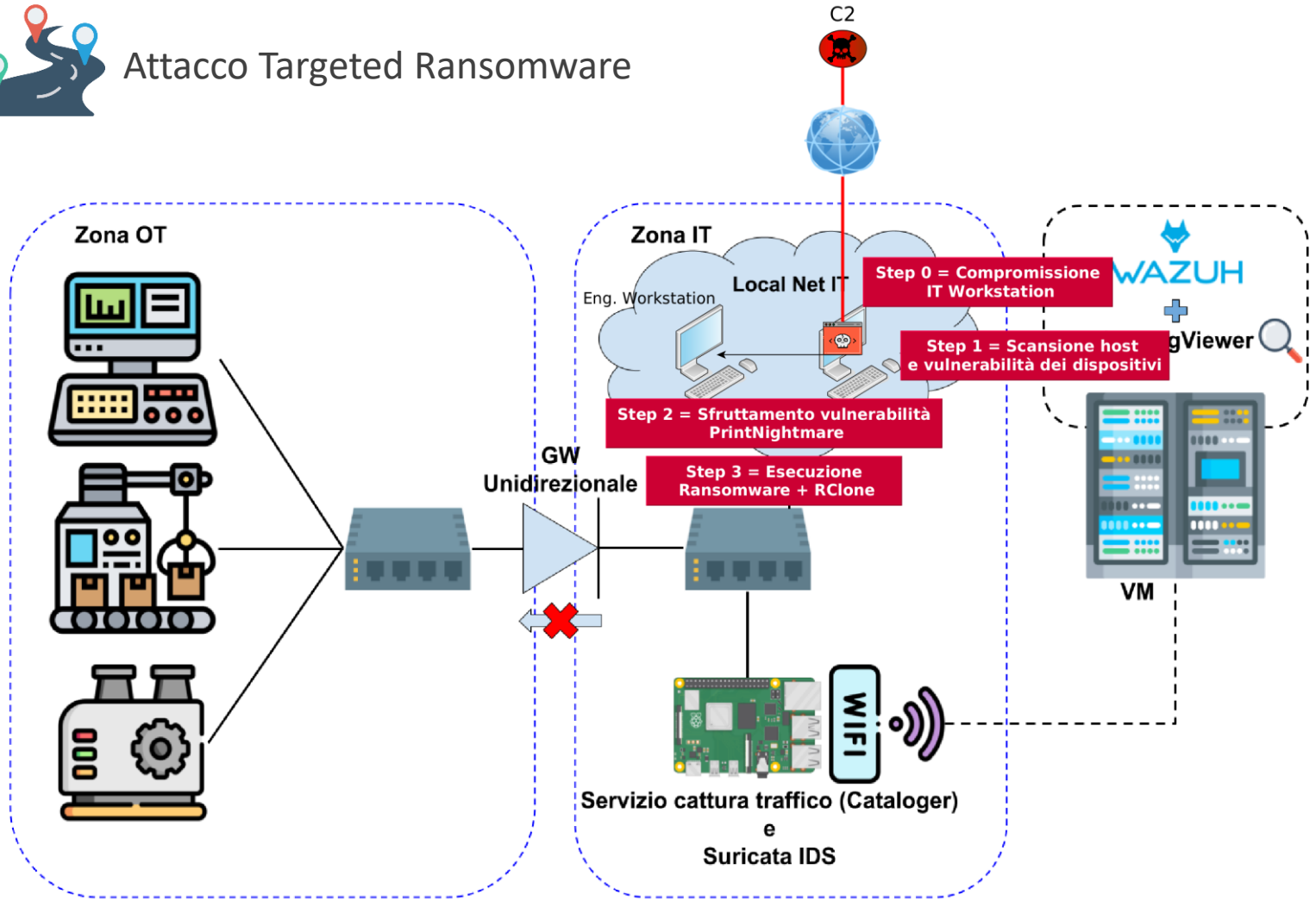
Il Rischio è accettabile per SL-T 2



SS4SP
safety and security for smart production

Valutazione dei rischi sullo Use Case BI-Rex / IMA

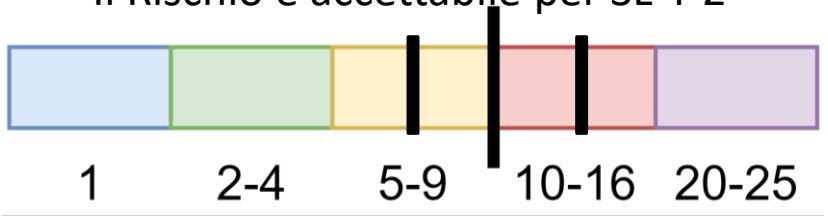
Attacco Targeted Ransomware



Scenario	Casi	Impatto	Probabilità di rischio	Rischio
Rete segregata con Unidirectional Gateway	Esecuzione Targeted Ransomware	Basso	Alta	8 - Medio
	Esfiltrazione dati tramite RClone	Medio	Alta	12 - Alto

Risultati

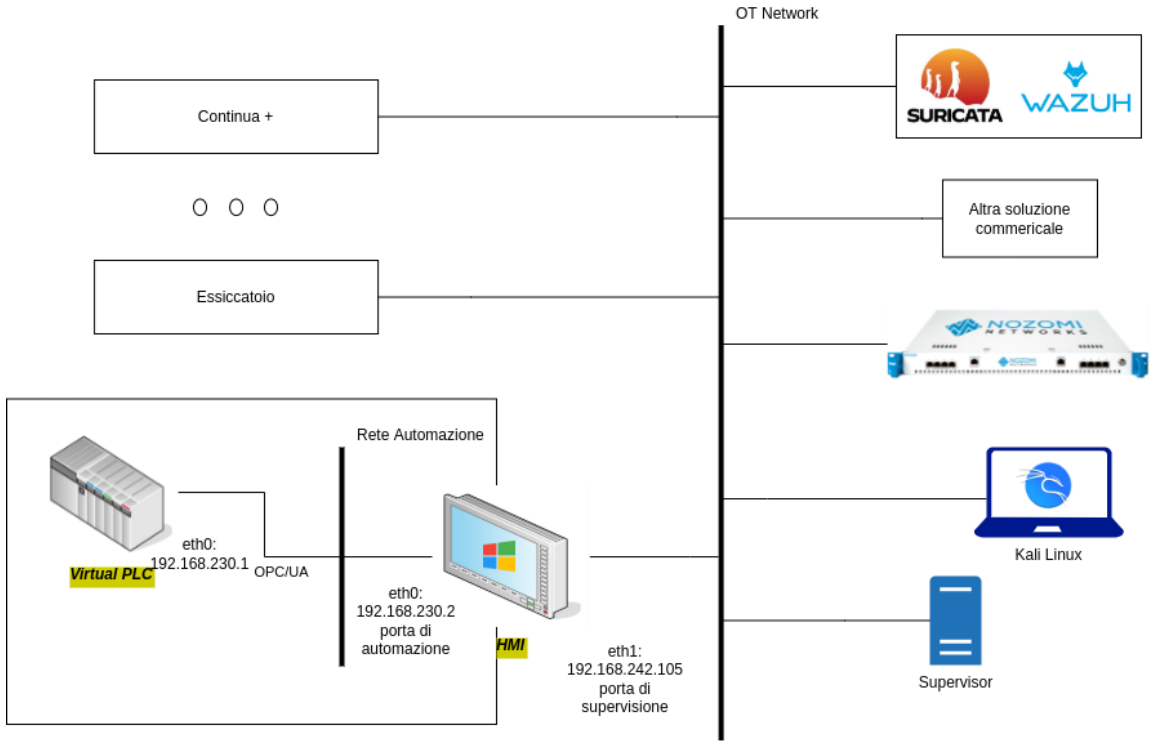
Il Rischio è accettabile per SL-T 2



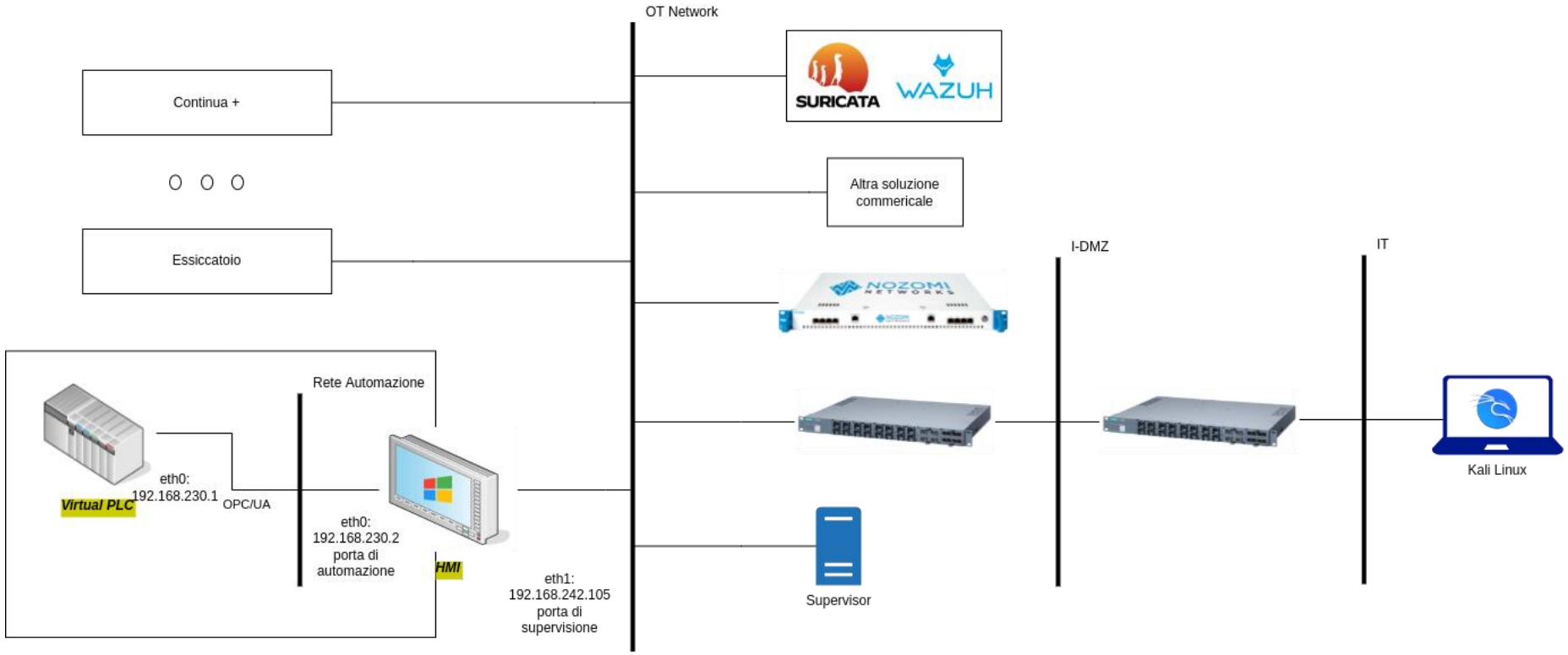
SS4SP
safety and security for smart production

Penetration Test sugli Use Cases

- Scenario di rete con la presenza di appliance di monitoraggio di rete.
- **Obiettivo**: valutare la capacità delle sonde di monitoraggio di rilevare le attività malevole svolte dagli attaccanti:
  - Reconnaissance;
  - Exploit.
- **Risultato**: replicando le attività precedentemente descritte, tutte le sonde sono in grado di produrre i relativi alert che consentirebbero ad un operatore di intraprendere le azioni più consone al caso.



Penetration Test sullo Use Case SACMI



- **Obiettivo**: verificare la capacità dell'Industrial DMZ di bloccare l'attacco nelle sue fasi iniziali.
- **Risultato**: fase di reconnaissance bloccata con conseguente impossibilità di replicare le azioni malevole svolte in precedenza

Rischio residuo sugli Use Cases

Rischio	Entità di rischio iniziale	Contromisura	Entità di rischio residuo	Rischio accettabile o non accettabile (per SL-T = 2)
Un malware Industriale proveniente dalla zona IT altera la produzione e/o esfiltra dati dalla zona OT	ALTO (16)	Monitoraggio	ALTO (12)	**Non Accettabile**
		Unidirectional Gateway	MEDIO (8)	**Accettabile**
		IDMZ	MEDIO (8)	**Accettabile**
Attacco con ingresso il Domain Controller IT che esfiltra dati dalla zona OT	ALTO (16)	IDMZ	MEDIO (6)	**Accettabile**
		IDMZ + Domain Controller OT	BASSO (4)	**Accettabile**
Attacco con ingresso il Domain Controller IT che inietta un ransomware nella zona OT	ALTO (16)	IDMZ	ALTO (16)	**Non Accettabile**
		IDMZ + Domain Controller OT	BASSO (4)	**Accettabile**

Conclusioni

- Dallo **Use Case SACMI**
  - L'industrial DMZ riduce il rischio che un malware proveniente dalla zona IT comprometta la zona OT: non riduce il rischio in presenza di un unico Dominio IT/OT.
  - L'industrial DMZ e un Dominio indipendente e dedicato alla zona OT riducono il rischio sotto la soglia di accettabilità.
- Dallo **Use Case BI-Rex / IMA**
  - L'Unidirectional Gateway riduce il rischio che un malware proveniente dalla zona IT comprometta la zona OT sotto la soglia di accettabilità.