



CONVEGNO • DIGITAL FORENSICS

Digital Forensics e Incident Response in un'infrastruttura energetica critica IT/OT: analisi di un cyberattacco



A cura di Fabrizio Giuliani



ONIF GENOVA • 16 OTTOBRE 2026



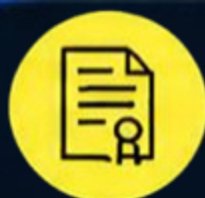
CHI SONO



Laureato in Ingegneria Meccanica presso l'Università La Sapienza di Roma



Consulente Informatico Forense per privati, aziende ed Autorità Giudiziarie



Iscritto Albo CTU Nazionale



Perito ed Esperto C.C.I.I.A. di Roma



Socio Ordinario ONIF Osservatorio Nazionale Informatica Forense



Socio AIP Associazione Informatici Professionisti



IT — INFORMATION TECHNOLOGY



IDENTITÀ E ACCESSI



VPN / CLOUD



SISTEMI ERP



WORKSTATION
E SERVER

CONVERGENZA IT/OT



IIoT



ENGINEERING
WORKSTATION



DATI DI
PROCESSO

OT — OPERATIONAL TECHNOLOGY



SCADA / HMI



PLC / RTU / IED



RETE INDUSTRIALE



SENSORI E
ATTUATORI



IT: CONFIDENZIALITÀ E INTEGRITÀ



OT: DISPONIBILITÀ E SAFETY



DFIR: CORRELAZIONE IT → OT → PROCESSO

LIVELLI 5 & 4 (IT - RETE AZIENDALE)

Dominio IT, Server Email, ERP, Workstation
Impiegati. Accesso Internet.

LIVELLO 3.5 (DMZ - ZONA DEMILITARIZZATA)

Zona Cuscinetto, Proxy Server, Jump Host,
Historian, Gateway VPN.

LIVELLO 3 (OT - GESTIONE OPERAZIONI)

Server SCADA, Workstation Ingegneria (EWS),
Domain Controller OT.

LIVELLO 2 (OT - CONTROLLO SUPERVISORE)

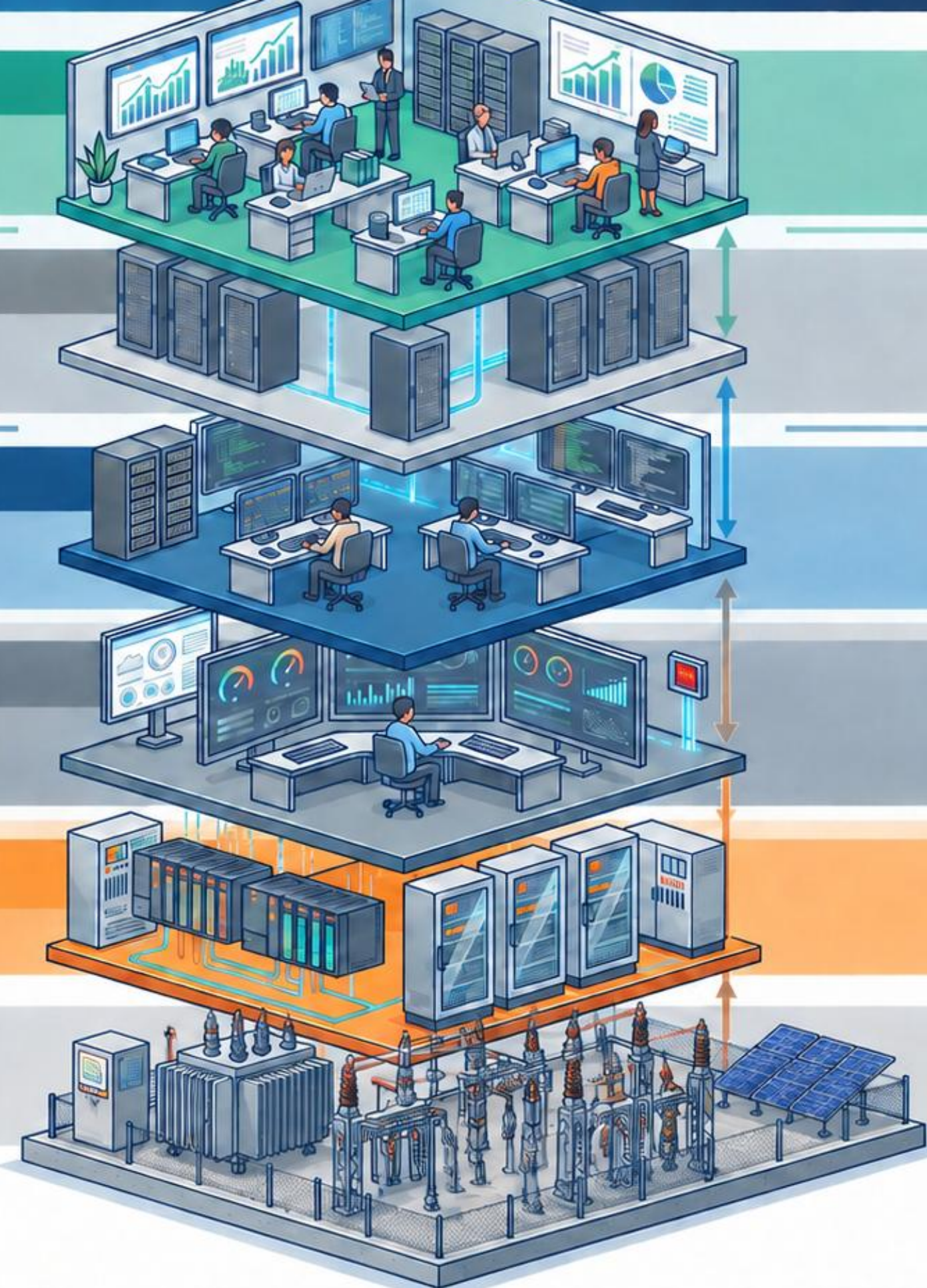
Interfacce HMI (Human-Machine Interface),
Server Allarme.

LIVELLO 1 (OT - CONTROLLO DI BASE)

PLC (Programmable Logic Controllers), RTU, IED.

LIVELLO 0 (OT - PROCESSO FISICO)

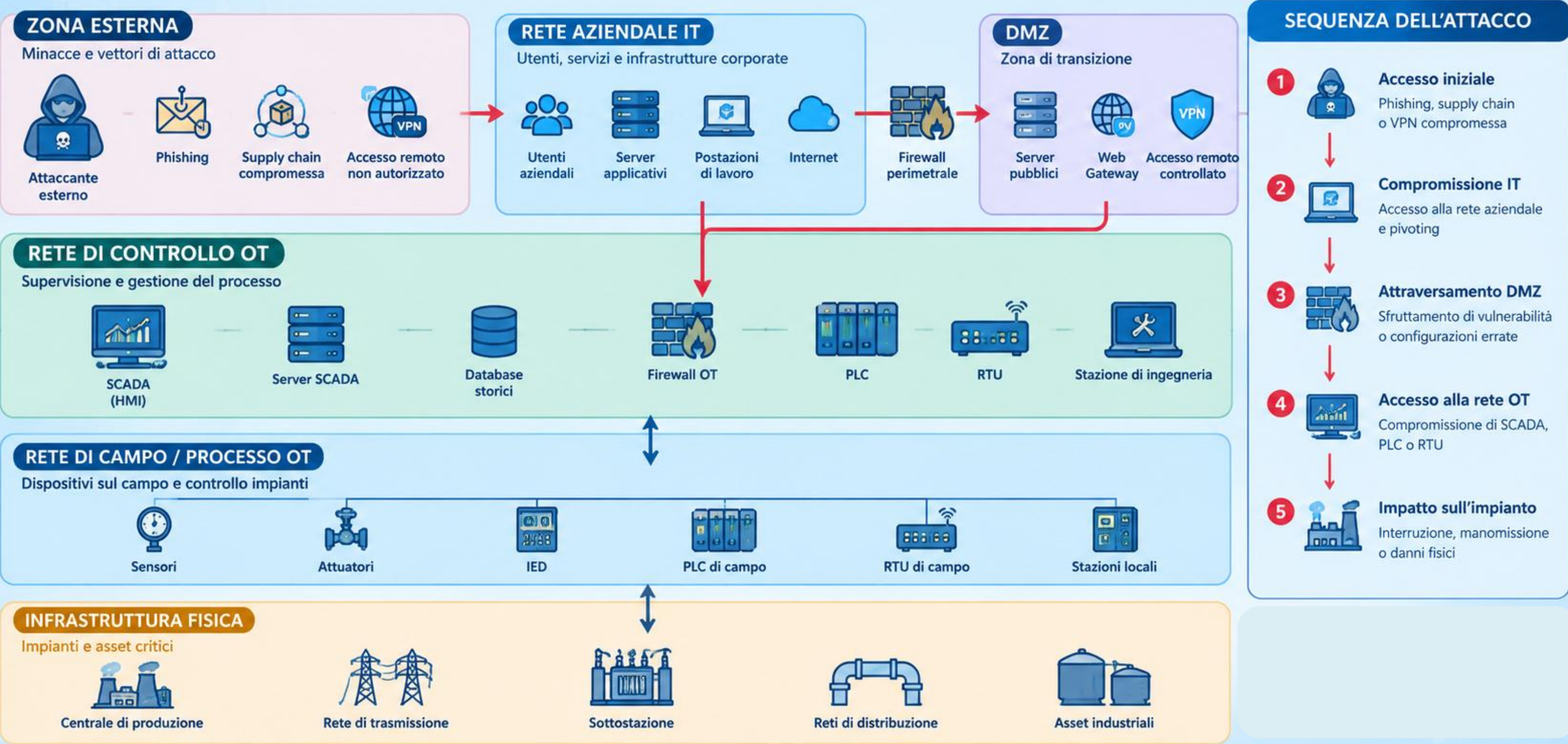
Sensori intelligenti, Attuatori, Trasformatori, Interruttori AT



CYBER ATTACK IN AMBITO OT

DALLA ZONA ESTERNA ALL'INFRASTRUTTURA FISICA

Una sola rete compromessa può mettere a rischio l'intera infrastruttura energetica.



PIPEDREAM / INCONTROLLER: Capacità ICS Modulare

Caso di studio: dall'accesso in rete alla potenziale manipolazione del controllo industriale.



MODULARITÀ

Framework OT-specifico

Componenti orientati a discovery e interazione con PLC, OPC UA e protocolli/servizi industriali.



PRECONDIZIONE

Accesso già ottenuto

Il rischio cresce quando l'attore raggiunge DMZ, bastion, engineering workstation o supervisione OT.



EFFETTO

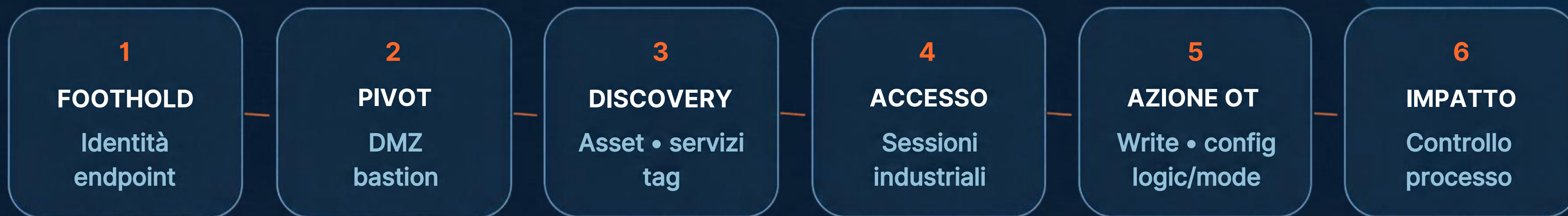
Dal cyber al processo

Possibili impatti su visibilità, controllo, configurazioni, logica e disponibilità: dipendono dalle difese e dal processo.

CYBERATTACCO

Catena di compromissione IT → OT

La ricostruzione Digital Forensics Incident Response deve dimostrare ogni passaggio con una fonte indipendente.



Domanda forense: quale identità ha agito, da quale postazione, su quale asset, con quale comando e quale effetto osservabile sul processo?

Protocollo legittimo non equivale a intenzione legittima: la prova nasce da contesto, baseline e correlazione.

OPC UA

Tag / NodeId

Client certificate
Session ID • audit

CODESYS / MODBUS

PLC Schneider

Project diff
Download / write history

FINS / HTTP

PLC OMRON

Mode/config event
Device log

PROCESSO

Historian / SOE

Trend • allarmi
state / quality flag

CASI RECENTI

Tre pattern documentati nel settore energia

Non solo blackout: edge compromise, persistenza e perdita di supervisione sono incidenti OT rilevanti.

REGNO UNITO • AGOSTO 2026

Centrale elettrica

Cyberattacco da hacker iraniani.
Blocco impianto per quattro giorni.
Generatore spento.



POLONIA • 2025

DER e CHP

Attacchi ad asset distribuiti;
comunicazioni con DSO degradate.
Telemetria multisito e distinzione tra
generazione e controllo.



DANIMARCA • 2023

22 operatori energia

Compromissione coordinata di
firewall Zyxel; alcuni operatori
adottarono island mode. Appliance
forensics e pivot DMZ.



NORMATIVE

NIS2, CER e compliance operativa

La conformità richiede capacità cyber, resilienza di servizio, governance e ricostruzione degli incidenti.

NIS2 • D.LGS. 138/2024

Gestione rischio cyber

Governance, misure tecniche/organizzative, incident handling, supply chain, notifica e vigilanza ACN.

CER • D.LGS. 134/2024

Resilienza del servizio

Rischi cyber, fisici, naturali, accidentali e ibridi; continuità e pianificazione per soggetti critici.

STANDARD

Evidenza e architettura

IEC 62443, NIST SP 800-82, NIST IR 8428, ISO 27001/22301: controlli, OT security, DFIR e business continuity.

DIGITAL FORENSICS INCIDENT RESPONSE

Raccolta delle evidenze: cinque layer, una sola timeline

Preservare prima le fonti volatili e quelle che consentono di collegare identità, percorso, comando e processo.

IDENTITÀ	IdP/AD • MFA • VPN • PAM	Chi ha ottenuto accesso?
DMZ	Bastion • firewall • ACL/NAT • NetFlow	Come è stato attraversato il confine?
ENGINEERING	RAM • EDR • tool log • project file	Da quale postazione è partita l'azione?
SUPERVISIONE	SCADA/HMI • OPC UA • historian • SOE	Quale comando/tag è stato modificato?
CONTROLLO	PLC/RTU/IED • config • firmware • state	Il controller ha accettato e cosa è avvenuto?

DIGITAL FORENSICS INCIDENT RESPONSE

Rispondere senza compromettere il processo

In OT la risposta deve salvaguardare simultaneamente safety, disponibilità, integrità delle evidenze e recovery.

TRIAGE

Safety assessment

Stato impianto, interlock, SIS, ridondanza, operatori locali e rischio dell'azione di response.

CONTAINMENT

Mirato e approvato

Revoca account/sessioni, ACL/conduit temporanei, monitoraggio: evitare reboot e isolamenti indiscriminati.

RECOVERY

Baseline validata

Golden configuration, test engineering/safety, change control, rollback e monitoraggio post-rientro.

FORENSIC READINESS

L'incidente si gestisce bene solo se asset, log, tempo, baseline e responsabilità sono già predisposti.

ASSET

Inventario + owner
funzione e criticità

LOGGING

Audit, retention
collector protetto

TEMPO

NTP/PTP/GPS
drift e UTC

BASELINE

Golden config
versioning + hash

GOVERNANCE

Playbook,
exercise e custody

Forensic readiness = capacità di raccogliere rapidamente evidenze affidabili, con costi e impatto operativo controllati.

DIGITAL FORENSICS INCIDENT RESPONSE

DFIR OT è un'attività congiunta, non una funzione SOC isolata

Safety, engineering e operations partecipano alla valutazione della prova e delle azioni di risposta.

DFIR

Piano evidenze
chain of custody
timeline/reporting

SOC / CISO

Detection
escalation
threat
intelligence

ENGINEERING

Logica PLC
semantic tag
recovery
validation

OPERATIONS

Stato
processo
priorità
servizio
fallback

SAFETY / HSE

Interlock / SIS
rischio fisico
autorizzazioni

Decision log obbligatorio: ogni acquisizione o contenimento deve indicare decision maker, rischio di processo, alternativa valutata e autorizzazione.

FORENSICS BY DESIGN

Digital Forensics by Design: dall'evidenza disponibile all'evidenza progettata

L'architettura nasce investigabile: non si limita ad aggiungere log dopo l'incidente.

REATTIVA

Dopo l'evento

Si cercano tracce disponibili, con rischio di log incompleti, retention insufficiente e clock incoerenti.

READINESS

Prima dell'evento

Si abilitano audit, retention, time sync e playbook su sistemi esistenti.

BY DESIGN

Dalla progettazione

Requisiti forensi influenzano architettura, procurement, sviluppo, contratti, test ed esercizio.

FORENSICS BY DESIGN – SUPPLY CHAIN

Contractual Forensics By Design

Se log, configurazioni, chiavi e strumenti di export sono in mano al fornitore, la readiness deve essere contrattuale oltre che tecnica.

LOG ACCESS

Accesso ai log
SLA e retention

INCIDENT CLAUSE

Notifica e
reservation hold

CONFIG / BACKUP

Proprietà, export
versioning

VENDOR SUPPORT

Supporto DFIR
strumenti e firmware

AUDIT RIGHT

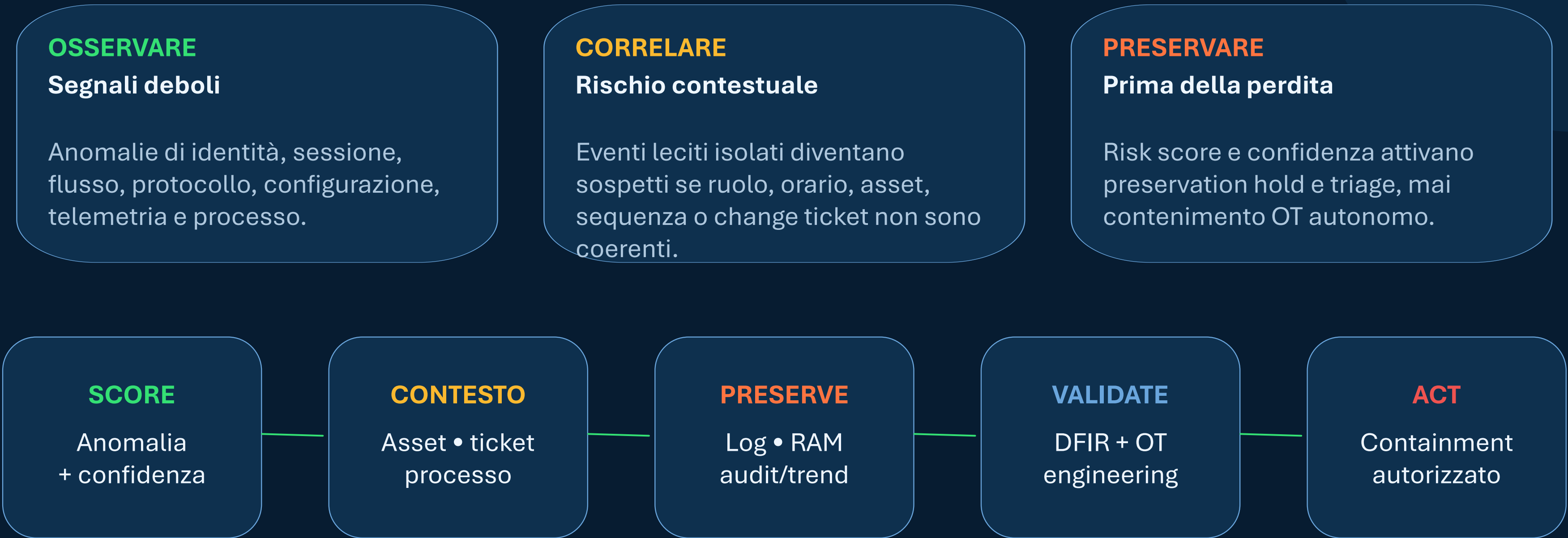
Audit, accessi
remote support

Un sistema non è investigabile se il proprietario dell'impianto non può ottenere tempestivamente project file, audit cloud, configurazioni, credenziali e assistenza vendor.

FORENSICS PREDITTIVA + AI

Dall'AI signal alla decisione sicura

AI/ML rilevano deviazioni, sequenze e relazioni anomale; gli esperti validano contesto, safety e impatto.





Capacità DFIR IT/OT continua, governata e pronta a intervenire senza compromettere safety e continuità

Non un SOC esternalizzato: un modello operativo che integra readiness, threat hunting, evidence management, incident command e recovery validation.



FORENSICS AS-A-SERVICE per infrastrutture energetiche critiche

Perché FaaS è rilevante in energia

L'operatore non può sempre mantenere H24 tutte le competenze DFIR, OT e probatorie necessarie per un incidente cyber-fisico.

COMPETENZE

Team composito

DFIR endpoint/cloud, network forensics, SCADA/HMI, PLC/RTU/IED, protocolli OT, legal e incident command.

DISTRIBUZIONE

Asset multisito

Centrali, sottostazioni, DER, parchi FV/eolici, storage, gateway LTE/APN, cloud e fornitori.

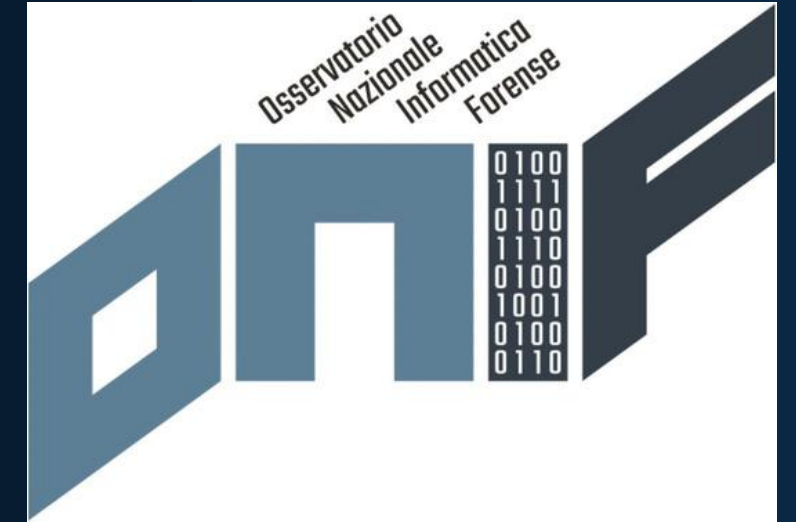


TEMPO

Finestra critica

Sessioni, log rotanti, PCAP, memoria, audit SCADA e trend di processo possono essere persi in ore o giorni.

Grazie per l'attenzione



fgiuliani@fabriziogiuliani.com



www.fabriziogiuliani.com



www.linkedin.com/in/fabriziogiuliani