OT Security · Radiflow Partner · CASE STUDY · TELECOMUNICAZIONI

18.000+ siti RAN protetti

con visibilita OT real-time su una rete mobile nazionale.

Come un operatore mobile europeo ha trasformato il proprio IT SOC in un SOC IT/OT completo, scoperto oltre 4.200 device OT sconosciuti e raggiunto la conformita NIS2 come Essential Entity — senza modificare l'infrastruttura esistente, con Radiflow.

18.000+	14M	4.200+	<1%
Siti RAN monitorati	Abbonati serviti	Device OT scoperti in 30gg	Impatto sul backhaul RAN

IL CLIENTE

Operatore Mobile Europeo — Rete 4G/5G Nazionale

Operatore mobile con 18.000+ siti RAN attivi, sistemi OT critici alle stazioni radio base e infrastruttura centrale distribuita su 6 switching center regionali e 2 data center nazionali.

SETTORE Telecomunicazioni — Mobile Network Operator	**CLASSIFICAZIONE NIS2** Essential Entity — Infrastruttura digitale
SITI ATTIVI 18.000+ siti RAN (4G/5G)	**INFRASTRUTTURA** 6 switching center regionali, 2 data center
SISTEMI OT CRITICI BTS/BBU, UPS/rettificatori, HVAC, BMS	**ABBONATI** 14 milioni

LE SFIDE

Infrastruttura OT invisibile, normativa in scadenza, scala impossibile

Quattro ostacoli critici che impedivano all'operatore di garantire visibilita OT e conformita normativa su una rete di 18.000 siti.

01 **NIS2: obblighi da Essential Entity con scadenze operative**
In seguito alla classificazione come Essential Entity nel settore infrastrutture digitali, l'operatore era soggetto a monitoraggio OT obbligatorio, notifica degli incidenti entro 24h e gestione documentata del rischio, con scadenze normative applicabili dal 2025.

02 **Sistemi OT completamente fuori dal perimetro SOC**
I controller delle stazioni radio, i sistemi di alimentazione e i BMS degli edifici exchange operavano in segmenti di rete isolati, invisibili al SOC IT esistente. Nessun asset inventory, nessun alerting, nessuna correlazione con gli eventi di sicurezza IT.

03 **Convergenza IT/OT: percorsi di movimento laterale non monitorati**
Le reti di management IP dei siti RAN erano interconnesse con il core aziendale, creando potenziali percorsi di attacco laterale verso i sistemi di controllo operativo. L'accesso remoto di vendor terzi amplificava ulteriormente la superficie di attacco.

04 **18.000 siti: scala impossibile per il monitoring tradizionale**
Portare sensori OT completi su 18.000 siti era economicamente e logisticamente impraticabile. Serviva un approccio leggero, ad alta compressione e con aggregazione centralizzata — senza impatto misurabile sul backhaul radio gia congestionato.

LA SOLUZIONE

iSID + iSAP + iCEN + CIARA — dal core ai siti RAN

Architettura Radiflow distribuita su core, switching center regionali e 18.000 siti RAN, con raccolta dati a bassa impronta e risk management continuo.

Radiflow iSID	Sensori passivi deployati al livello core network e nei 6 switching center regionali. Monitoraggio di nodi EPC/IMS, interfacce BSS/OSS e punti di interconnessione IT/OT sul backbone, con deep packet inspection su protocolli industriali e IP.
Radiflow iSAP	Smart Collector ultra-leggero deployato sui siti RAN campione (urbano, suburbano, rurale). Raccolta passiva tramite SPAN port su BTS/BBU, sistemi di alimentazione e cooling. Compressione dati integrata: impatto sul backhaul inferiore all'1%.
Radiflow iCEN	Management centralizzato di tutti i sensori e collector dal NOC. Aggregazione di alert, inventory OT cross-layer, topologia unificata e integrazione con il SIEM IT esistente per convergenza SOC IT/OT senza incremento di headcount.
CIARA	Risk scoring continuo per layer di rete (core, regionale, RAN), attack path modeling dal sito radio al core, OT-BAS senza impatto sull'infrastruttura live. Report NIS2-aligned con evidenze automatiche per notifiche entro 24h.

Fasi di Implementazione

01 **Core network e switching center**
Deployment iSID sui 6 centri regionali e sul core EPC/IMS. Prima visibilita OT sul backbone in meno di 30 giorni dal kick-off.

02 **Pilota RAN multi-topology**
Installazione iSAP su siti campione urbano, suburbano e rurale. Validazione della compressione, calibrazione degli alert e verifica dell'impatto sul backhaul.

03 **Attivazione iCEN e convergenza SOC**
Consolidamento di tutti i feed nel NOC, integrazione con il SIEM IT esistente, training del team SOC sugli alert OT e definizione degli escalation path.

04 **CIARA risk management e NIS2 compliance**
Attivazione dello scoring per layer, primo report NIS2 in 60 giorni, setup del workflow di notifica incidenti conforme ai requisiti Essential Entity.

I RISULTATI

OT visibile, SOC convergente, NIS2 soddisfatta

4.200+
Device OT scoperti in 30 giorni
Prima inventory OT completa del core e dei siti RAN

NIS2
Essential Entity compliance
Evidenza automatica e notifica incidenti a 24h

0
Headcount aggiuntivi al SOC
Convergenza IT/OT con servizi MDR MSSP

<1%
Impatto sul backhaul RAN
Compressione dati integrata in iSAP

18.000+
Siti RAN coperti
Copertura nazionale su tutte le topologie

60 gg
Primo report NIS2
Dal kick-off alla prima evidenza di conformita

> *"Non avevamo idea di quanti device OT fossero connessi alla nostra rete di management. In 30 giorni dal deployment abbiamo scoperto oltre 4.000 asset ignoti. CIARA ci ha dato per la prima volta un quadro di rischio OT che il nostro board capisce."*
>
> Head of Network Security
> Operatore Mobile Europeo

Perche Radiflow

- v Architettura scalabile dal core a migliaia di siti remoti
- v Raccolta dati ultra-leggera con impatto minimo sul backhaul
- v Convergenza SOC IT/OT senza nuovo headcount
- v Risk management continuo con CIARA, allineato a NIS2

TRINITY LABS

sede_legale
Piazza IV Novembre 4, Milano

web
https://trinity-labs.it

linkedin
linkedin.com/company/trinity-labs-cyber

Tested. Trusted. Delivered.