



**Forum Risk Management**

obiettivo sanità salute

**26-29 NOVEMBRE 2024**  
**AREZZO FIERE E CONGRESSI**

**19**

# Protezione avanzata degli Elettromedicali

**Riccardo Coradeschi**

Systems Engineer – Fortinet Italia

## Criticità dispositivi IoMT



### A LUNGA DURATA

- Il 50% dei dispositivi medici può funzionare per più di 10 anni
- Sistemi operativi obsoleti (Windows 98, 2000)
- Non aggiornabili



### RESISTENTI AL CAMBIAMENTO

- Difficili da sostituire
- Attrezzature costose



### DIFFICILI DA INDIVIDUARE

- Reti proprietarie
- Protocolli proprietari
- Non è possibile effettuare scansioni attive sui dispositivi

**2008**                      **2012**                      **2015**                      **2017**                      **2019**                      **2021**

**Vulnerabilità in pacemaker e defibrillatori**

Ricercatori dimostrano la possibilità di hackerare pacemaker e defibrillatori impiantabili

**Hacking mortale di pacemaker**

Barnaby Jack dimostra la capacità di assassinare una vittima hackerando il suo pacemaker durante la conferenza di sicurezza BreakPoint.

**Attacchi "MEDJACK"**

Hacker compromettono dispositivi medici per creare backdoor nelle reti ospedaliere

**Attacco ransomware WannaCry**

Il ransomware colpisce duramente il settore sanitario, compromettendo dispositivi medici e sistemi ospedalieri

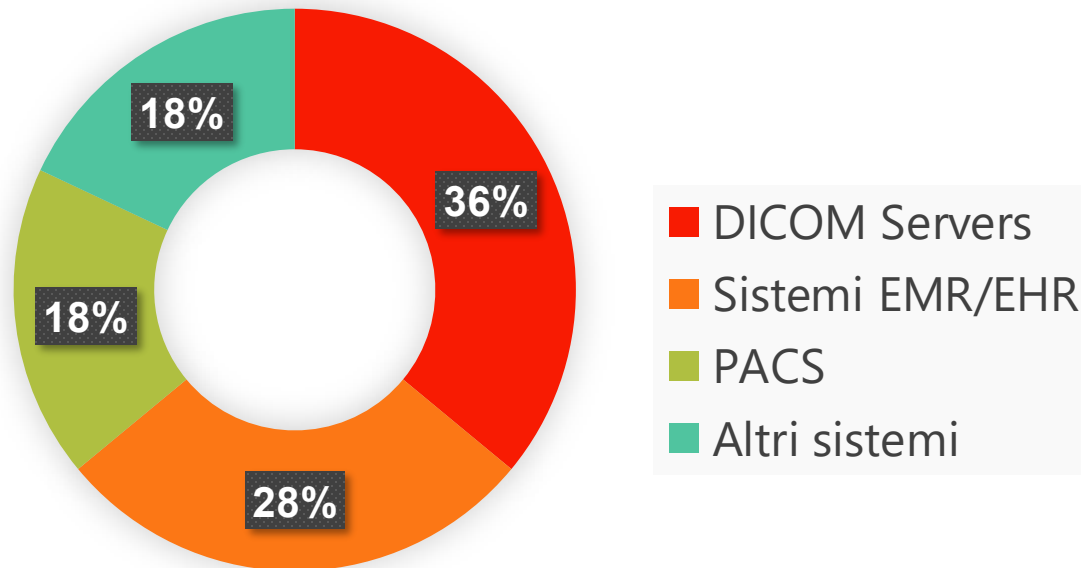
**Vulnerabilità nei dispositivi Medtronic**

La FDA ha emesso un avviso riguardante vulnerabilità nei dispositivi cardiaci impiantabili

**Attacco ai Sistemi di Elekta**

Gli hacker interrompono il funzionamento delle macchine per la radioterapia oncologica a livello globale per circa sei settimane.

## Esposizione degli apparati IoMT sul web<sup>1</sup>

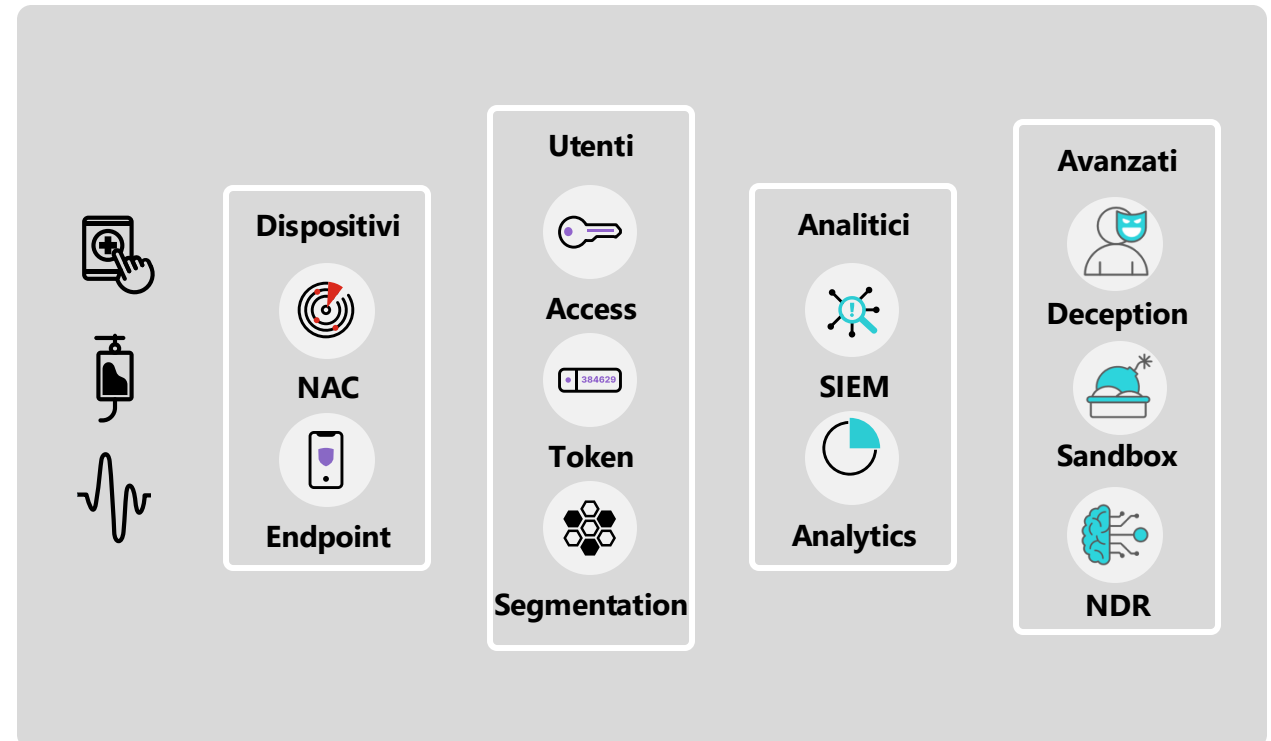


- **Totale dispositivi esposti:** 14.004 indirizzi IP unici che espongono dispositivi e sistemi sanitari su Internet.
- **DICOM Servers:** 5.100 host esposti.
- **Protocollo DICOM insicuro:** vulnerabilità note e può essere vettore di malware (PEDICOM).
- **EMR e EHR sono progettati per essere disponibili online:** molti non implementano l'autenticazione a più fattori o il tunneling VPN come funzionalità standard, mettendo a rischio dati sanitari sensibili.

[1] – Censys, The Global State of Internet of Healthcare Things (IoHT) Exposures on Public-Facing Networks, 10/10/2024

## Tecnologie per intervenire

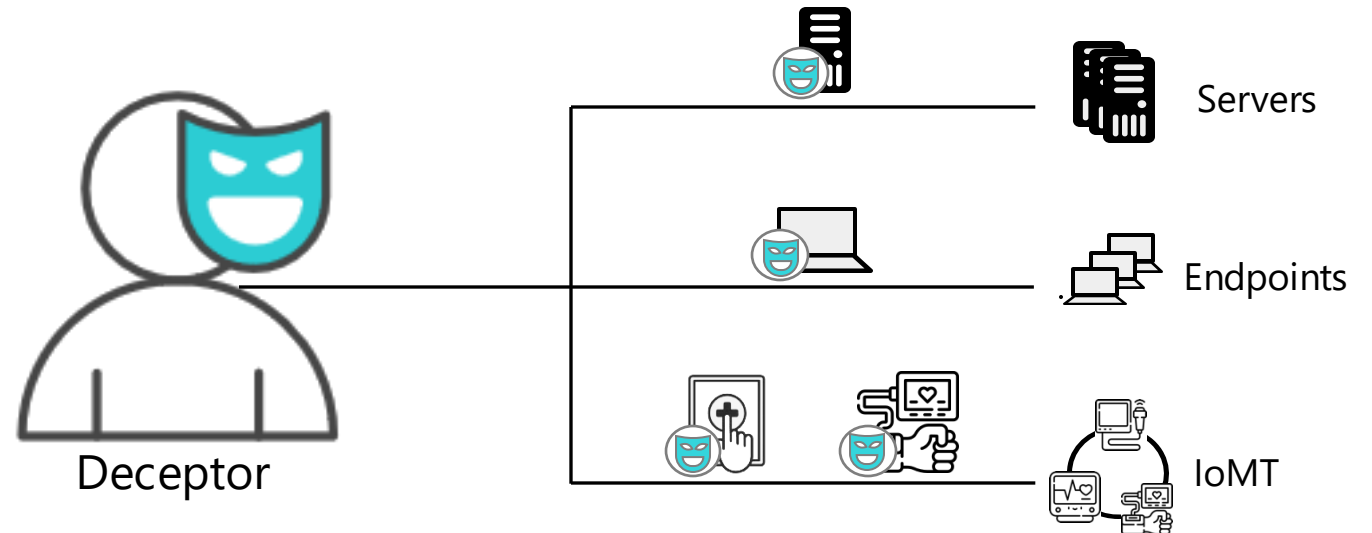
- **Segmentazione:** suddividere le reti in base alle esigenze aziendali.
- **Network Access Control** rileva e monitora i dispositivi IoMT connessi alla rete per garantirne sicurezza e conformità.
- **Protezione degli endpoint** protegge i dispositivi IoMT dagli attacchi.
- **Gestione delle identità e degli accessi** controllano l'accesso ai dispositivi sensibili.
- **Deception** creano ambienti falsi e simulazioni per rilevare, analizzare e contrastare gli attacchi informatici, migliorando la sicurezza complessiva.

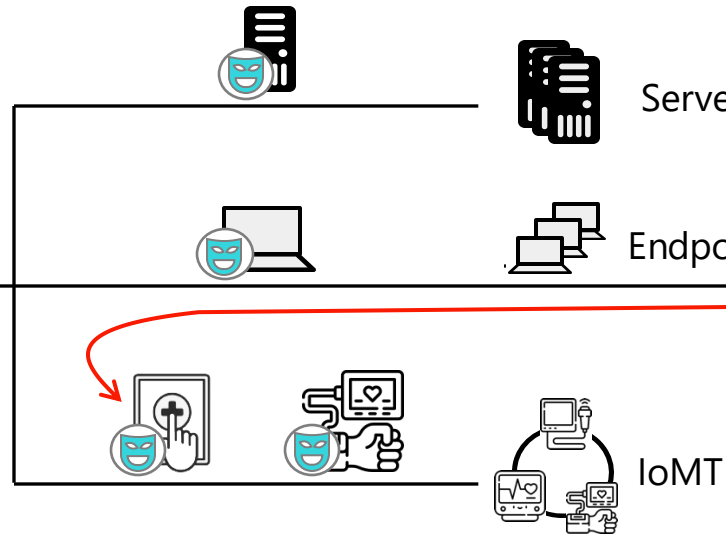
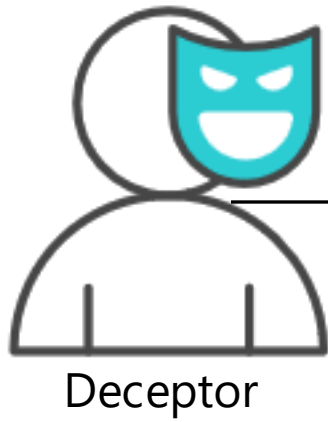
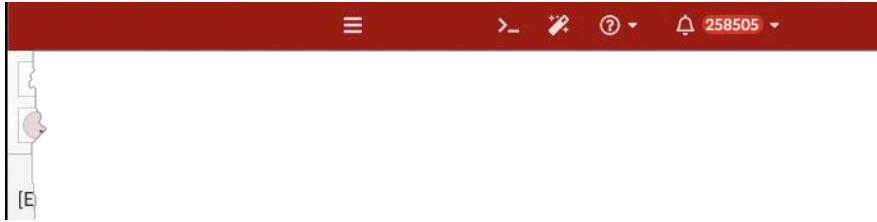


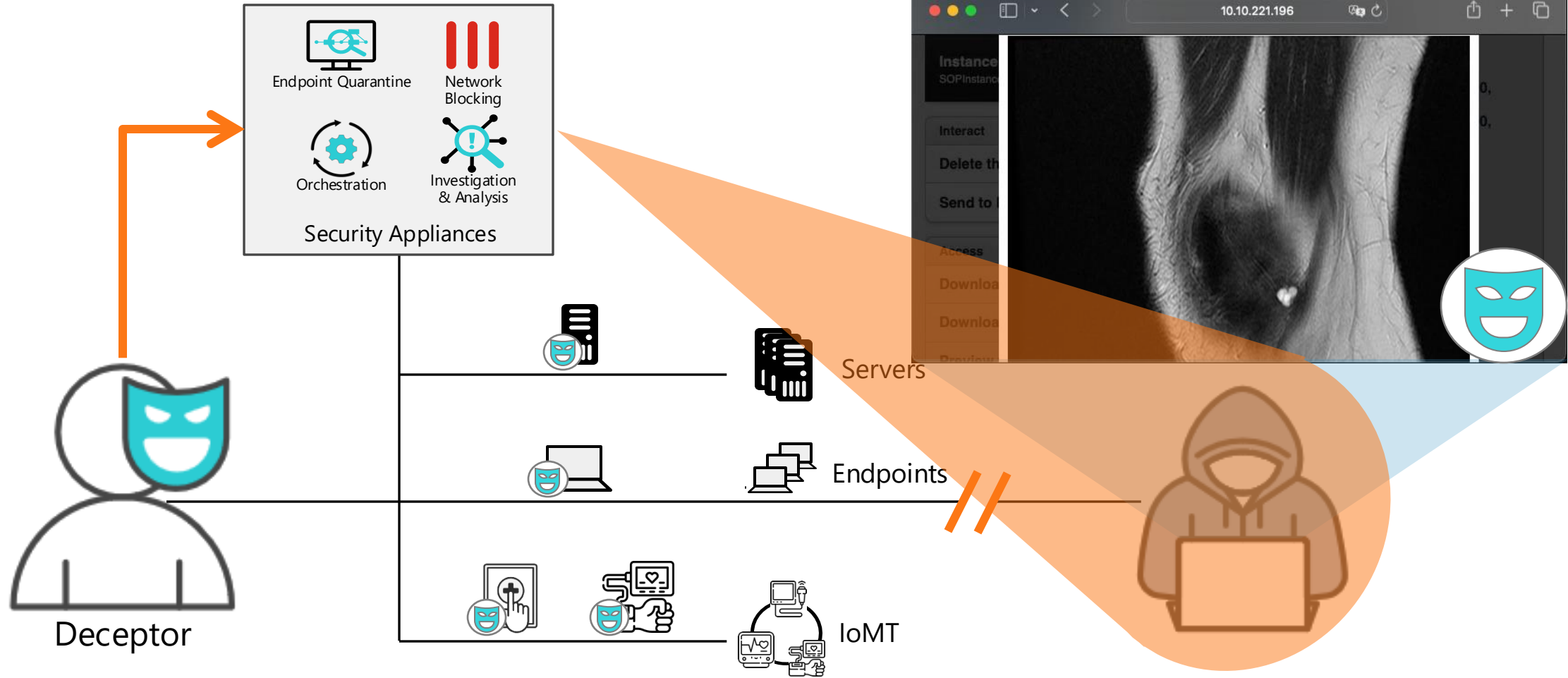


## Le tecnologie di Deception

- **Simulazione IoMT:** PACS Server, DICOM Server, Infusomat e altri
- **Monitoraggio Avanzato:** Tracciamento delle interazioni con i decoy per identificare le tattiche degli attaccanti.
- **Riduzione dei Falsi Positivi:** Filtraggio del traffico legittimo da quello malevolo.





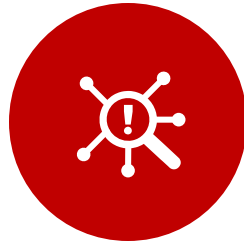




## Le domande che fanno la differenza



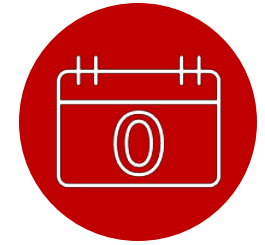
Sei in grado di **sapere se gli attaccanti sono già all'interno della tua rete?** Quanto velocemente riesci a rilevarli?



Come intendi **ridurre il tasso di falsi positivi?** Stai cercando di diminuire il tempo dedicato alla revisione degli avvisi?



Come **proteggi i dispositivi** che non possono fornire la propria telemetria o **che non possono essere protetti** tramite agenti di monitoraggio o patch di sicurezza?



Come puoi **proteggerti da minacce 0 day?**