

Cybersecurity dei dispositivi elettromedicali

Un progetto integrato nell'Azienda Ospedaliera di Alessandria

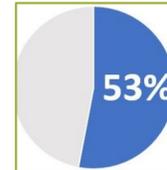
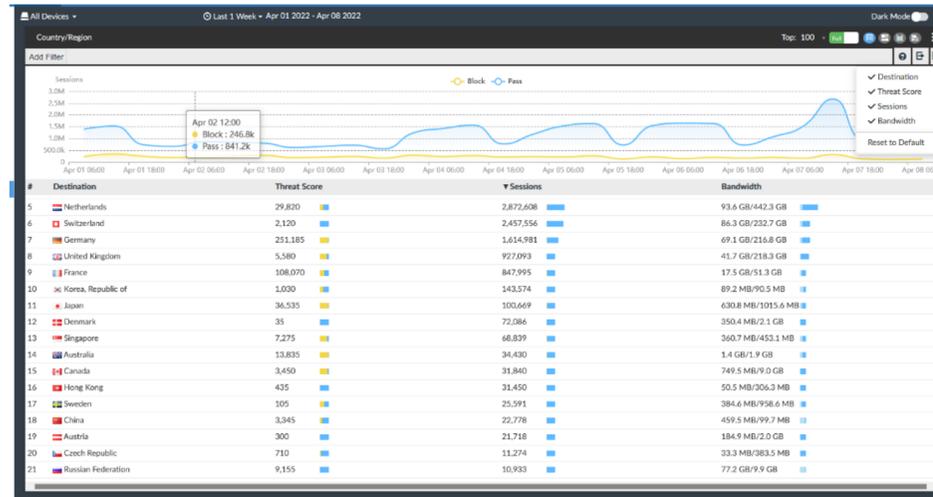
Ing. Dario Ricci
Direttore SC ICT e Innovazione Tecnologica
AO «S.S. Antonio e Biagio e C. Arrigo», Alessandria (AL)

#ForumRisk18



www.forumriskmanagement.it

Tutto è collegato, tutto è in pericolo



Dispositivi connessi con vulnerabilità note

- Pompe per insulina
- Defibrillatori cardiaci
- Telemetria cardiaca mobile
- Pacemaker
- Pompe antidolorifiche intratecali



6,2

n. di vulnerabilità per Dispositivo Medico



<https://www.agendadigitale.eu/sicurezza/pa-nel-mirino-degli-hacker-il-caso-emblematico-dellospedale-di-alessandria/>

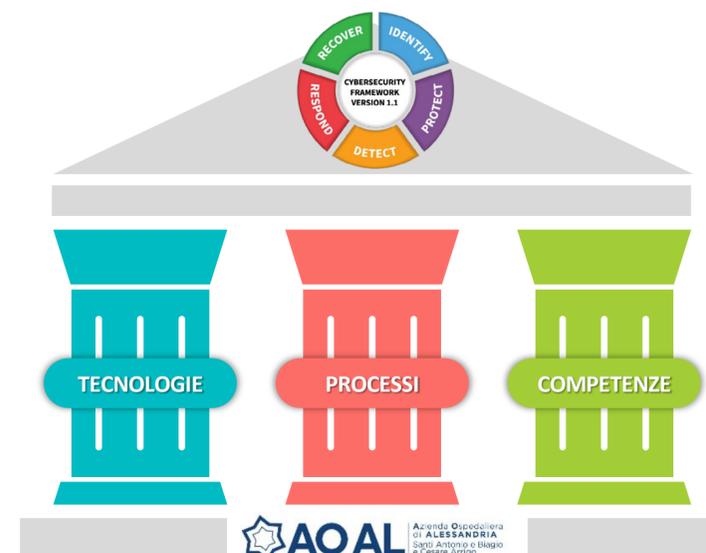
Fonte: Private Industry Notification FBI, Settembre 2022

#ForumRisk18



www.forumriskmanagement.it

Un fronte unico contro le vulnerabilità informatiche degli elettromedicali



MDSP (Medical Device Security Platform)
Business Continuity / Disaster Recovery
Segmentazione della rete

Revisione organizzazione aziendale
Revisione procedure di manutenzione
Revisione contratti (installazione)
Revisione procedure controllo (VA, TIA)

Misura postura di parco degli elettromedicali
OWASP Vulnerability Assessment

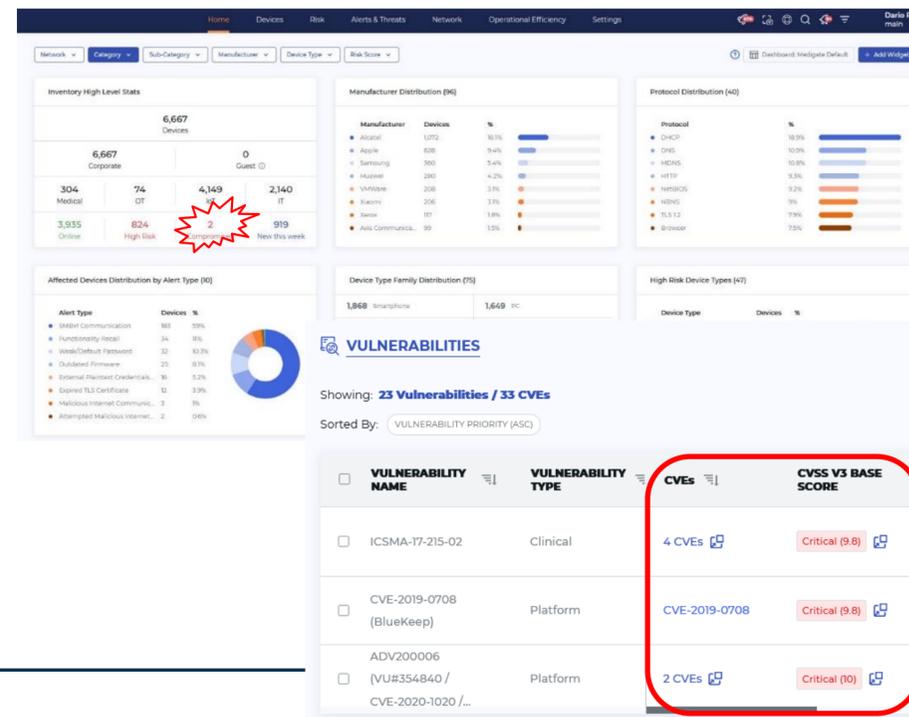


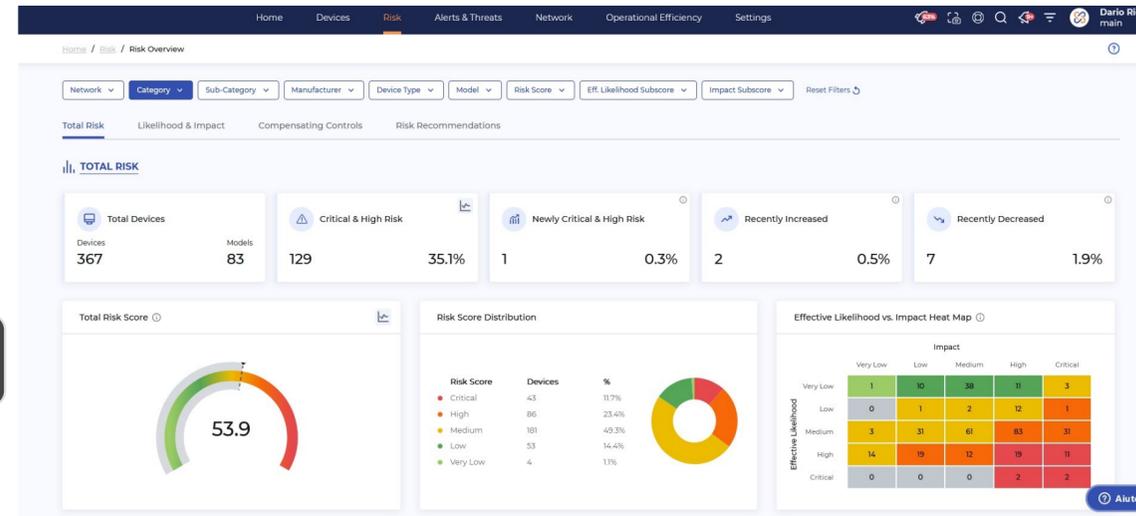
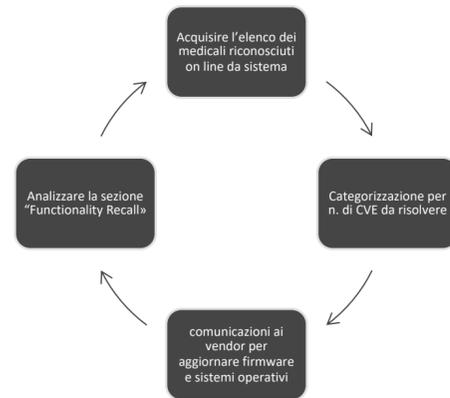
TECNOLOGIE
MDSP (Medical Device Security Platform)
Business Continuity / Disaster Recovery
Segmentazione della rete

**CVE (Common Vulnerabilities and Exposures)
Vulnerabilità ed esposizioni comuni**

- inventario delle risorse attive (discovery dei dispositivi collegati)
- calcolo Rischio della Vulnerabilità
- allarmi in caso di anomalie, qualificando i sistemi connessi alla rete attraverso l'analisi del loro traffico.

#ForumRisk18

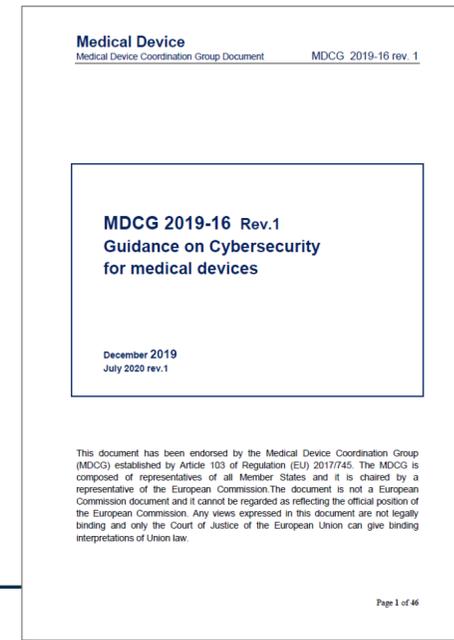




Un fronte unico contro le vulnerabilità informatiche degli elettromedicali

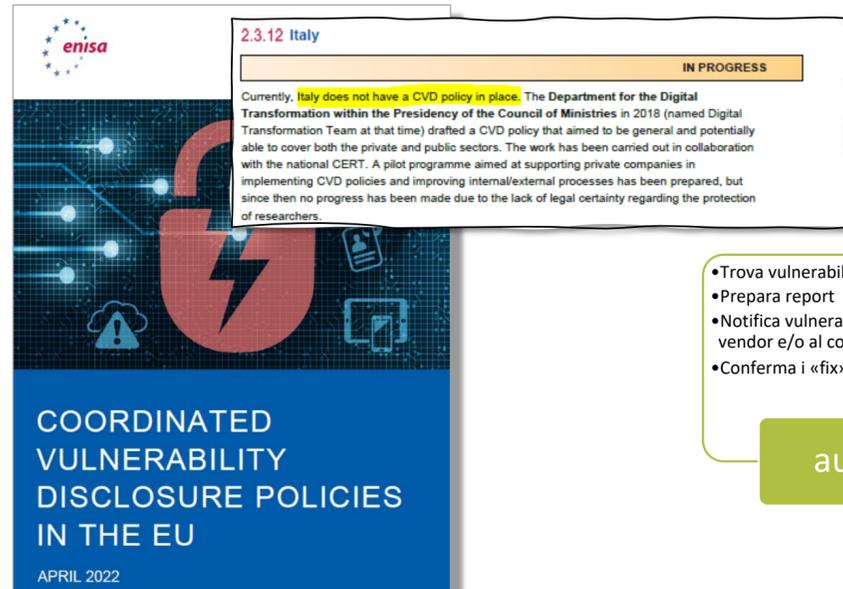


Misura postura di parco degli elettromedicali
 OWASP Vulnerability Assessment



#ForumRisk18

Coordinated Vulnerability Disclosure: anche i vendor hanno il loro ruolo



2.3.12 Italy
IN PROGRESS

Currently, Italy does not have a CVD policy in place. The Department for the Digital Transformation within the Presidency of the Council of Ministries in 2018 (named Digital Transformation Team at that time) drafted a CVD policy that aimed to be general and potentially able to cover both the private and public sectors. The work has been carried out in collaboration with the national CERT. A pilot programme aimed at supporting private companies in implementing CVD policies and improving internal/external processes has been prepared, but since then no progress has been made due to the lack of legal certainty regarding the protection of researchers.

COORDINATED VULNERABILITY DISCLOSURE POLICIES IN THE EU
APRIL 2022

#ForumRisk18

ISO/IEC 29147
The CERT® Guide to Coordinated Vulnerability Disclosure

www.forumriskmanagement.it

Ruoli processo CVD: un esempio

```

    graph TD
      Auditor[auditor] --> Coordinator[coordinatore]
      Vendor[vendor] --> Coordinator
      Coordinator --> Auditor
      Coordinator --> Vendor
  
```

- auditor**
 - Trova vulnerabilità
 - Prepara report
 - Notifica vulnerabilità al vendor e/o al coordinatore
 - Conferma i «fix»
- coordinatore**
 - Riceve i report
 - Agisce come facilitatore
 - Validazione e prove
 - Coordina le risposte tra i soggetti
- vendor**
 - Riceve i report
 - Validazioni e prove
 - Prepara i «fix e/o i «workaround»

Un fronte unico contro le vulnerabilità informatiche degli elettromedicali

Superare limiti tecnologici

- ! software scritti in modalità legacy
- ! Invio segnali con protocolli proprietari, e non tramite standard internazionali
- ! analisi e revisione delle vulnerabilità spesso focalizzato sui sistemi elettro-meccanici più che sulla cybersecurity

Superare limiti di governance: un processo coordinato di CVD



Delitti in materia di violazione del diritto d'autore (Art. 25-novies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 99/2009]

- Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa (art. 171, legge n.633/1941 comma 1 lett. a) bis)
- Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione (art. 171, legge n.633/1941 comma 3)
- Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171-bis legge n.633/1941 comma 1)
- Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171-bis legge n.633/1941 comma 2)
- Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa (art. 171-ter legge n.633/1941)
- Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171-septies legge n.633/1941)
- Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171-octies legge n.633/1941).

[Torna all'inizio](#)