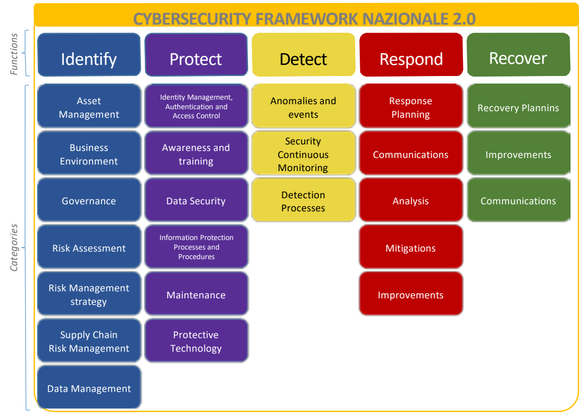
Asset Discovery e Vulnerability Management dei dispositivi medicali presso la Fondazione IRCCS Policlinico San Matteo

Dott. Ing. Andrea Gelmetti

Direttore SC Sistemi Informativi – Fondazione IRCCS Policlinico San Matteo Pavia

Contesto



Functions	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management strategy	ID.RM
	Supply Chain Risk Management	ID.SC
	Data Management	DP-ID.DM
Protect	Identity Management, Authentication and Access Control	PR.AC
	Awareness and training	PR.AT
	Data Security	PR.DS
	Information Protection Processes and Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.PL
	Communications	RS.CO
	Analysis	RS.AN
	Mitigations	RS.MI
	Improvement	RS.IM
Recover	Recovey planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

laboratorio SANITÀ 2030™
14-15 GIUGNO 2023 LOMBARDIA
FIERA DI BERGAMO

A fronte dello scenario italiano (dove l'HealthCare è uno dei settori più colpiti da attacchi informatici) risulta prioritario dotarsi di una piattaforma di Cybersecurity e Asset Management per apparati medicali che sia:

- agentless
- passiva
- real-time
- semplice da utilizzare

#sanita2030

www.sanita2030.it

See Everything: Control and Secure Every Unmanaged Device

Asset Inventory	Vulnerability	Risk
• Identificare tutti i device medicali connessi alla rete senza agent e senza scanning • Classificarli in base alla tipologia / utilizzo • Ricevere dati da altre sorgenti già presenti nell'infrastruttura (Rete/Sicurezza/Inventory)	• Identificare le vulnerabilità che esistono su ogni device • Fornire una prioritizzazione delle vulnerabilità in base all'impatto sulla sicurezza dei dati • Gestire e aggiornare le vulnerabilità	• Identificare il fattore di rischio di ogni device • Evidenziare eventuali comportamenti anomali dei dispositivi • Gestire il Life Cycle del dispositivo

laboratorio SANITÀ 2030 14-15 GIUGNO 2023 LOMBARDIA FIERA DI BERGAMO

Configurazione

La sonda, inserita in rete, oltre a ricevere il traffico si interfaccia e raccoglie ulteriori dati di contesto da elementi di gestione, di rete e di sicurezza già presenti nell'infrastruttura, il che consente di avere una visione completa ed esaustiva di tutti i dispositivi e delle loro caratteristiche, dando ancora più valore all'ecosistema di sicurezza implementato. In particolare sono stati integrati:

- Sistemi di autenticazione (Active Directory)
- vCenter VMware per la gestione degli Asset virtuali
- Firewall Fortinet per la raccolta del traffico anche fra diverse zone di sicurezza
- DHCP
- Switch
- WLC WiFi Cisco

laboratorio SANITÀ 2030™
14-15 GIUGNO 2023 LOMBARDIA
FIERA DI BERGAMO

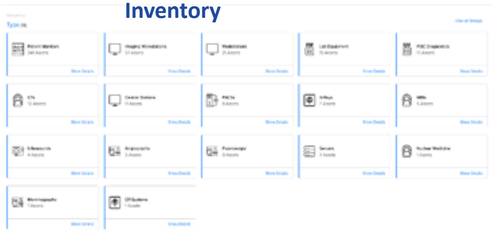
Obiettivi

Unica console centralizzata che sia in grado di realizzare tutte le necessarie funzionalità di Cybersecurity, Asset Management, Vulnerability Management e di implementare automaticamente regole di sicurezza, il tutto in modalità continua e real time attraverso un approccio completamente “passivo” (senza quindi impattare/modificare l’infrastruttura in produzione).

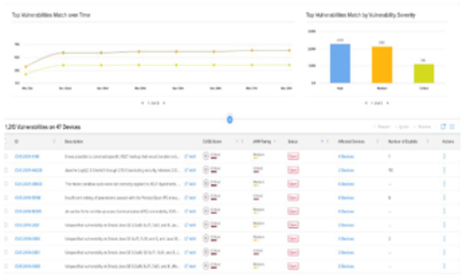
- Scoprire tutti i medical device connessi alla rete con le relative informazioni di contesto e di comportamento.
- Identificarne il rischio attraverso una valutazione in tempo reale che tenga conto del profilo del dispositivo (tipo, applicazioni, sistema operativo, locazione, connessioni, etc.), delle vulnerabilità e del comportamento approfondito dell’apparato.
- Gestirne le vulnerabilità

Risultati

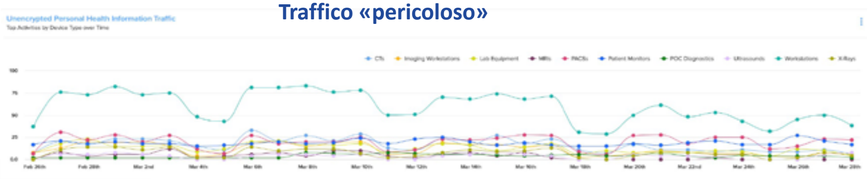
Inventory



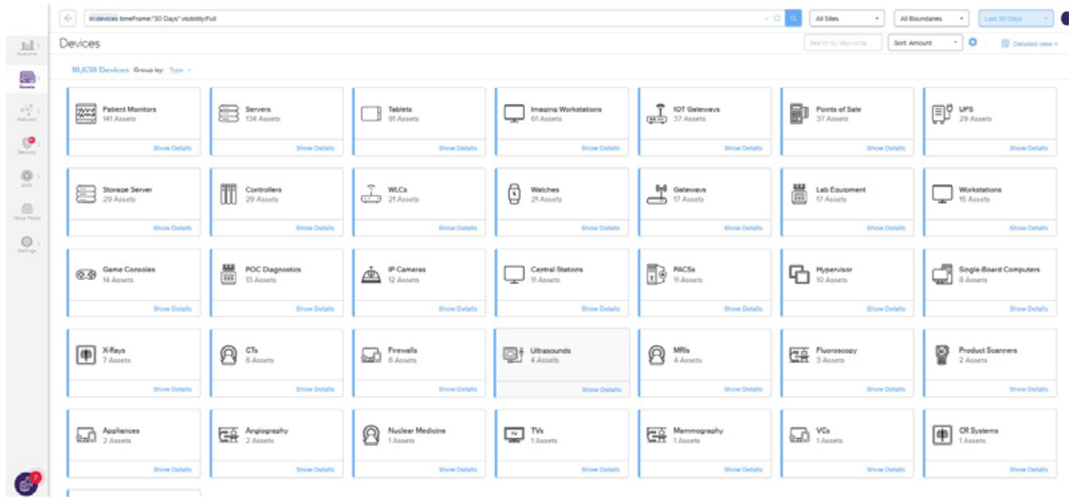
Vulnerabilità



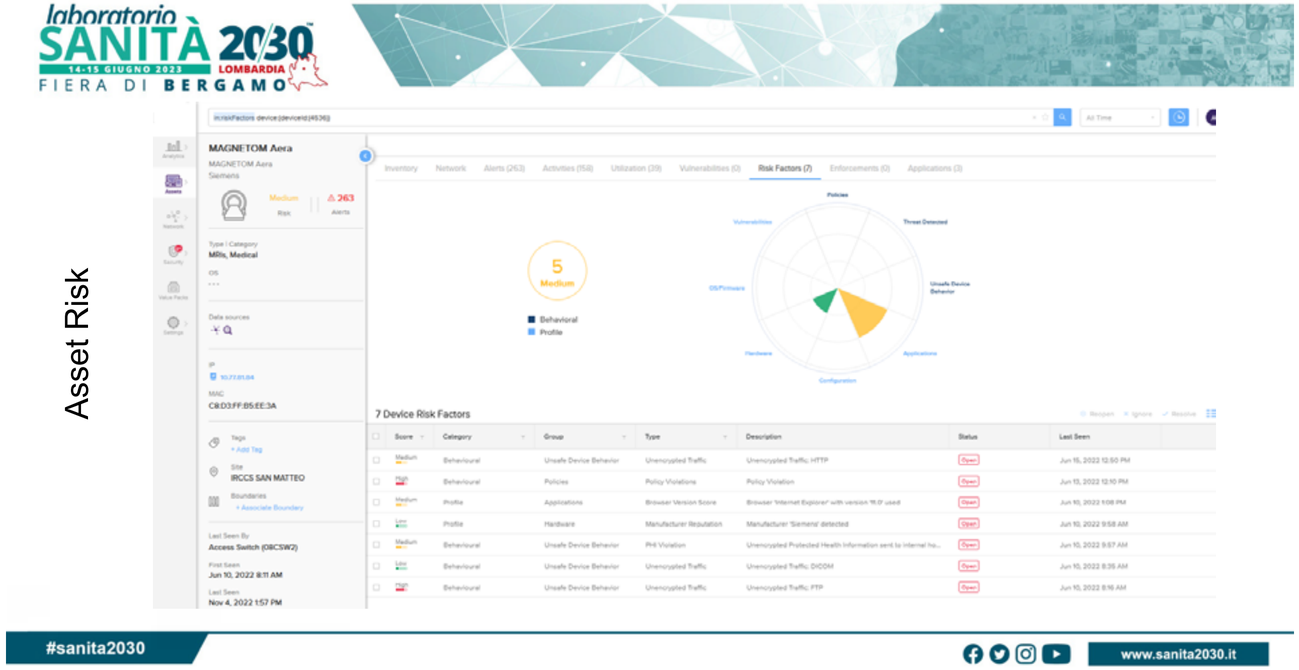
Traffico «pericoloso»



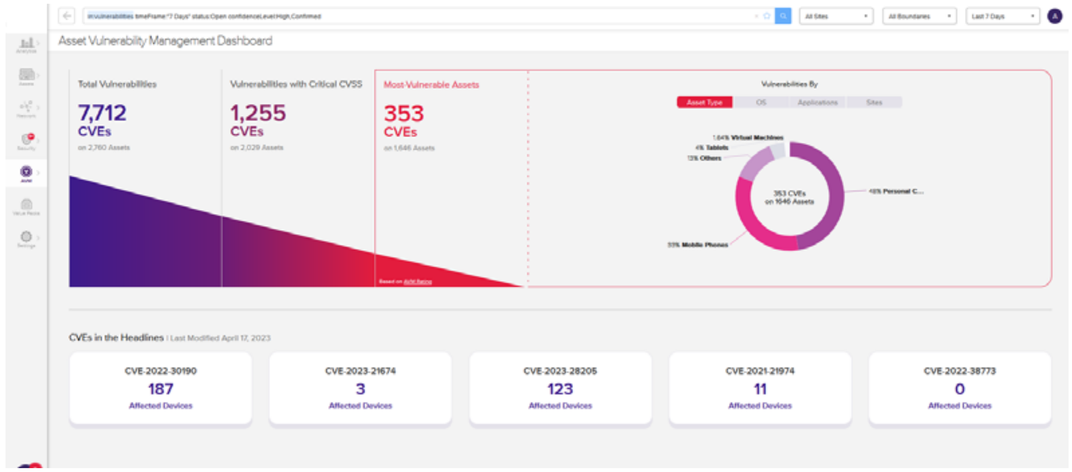
Asset Discovery



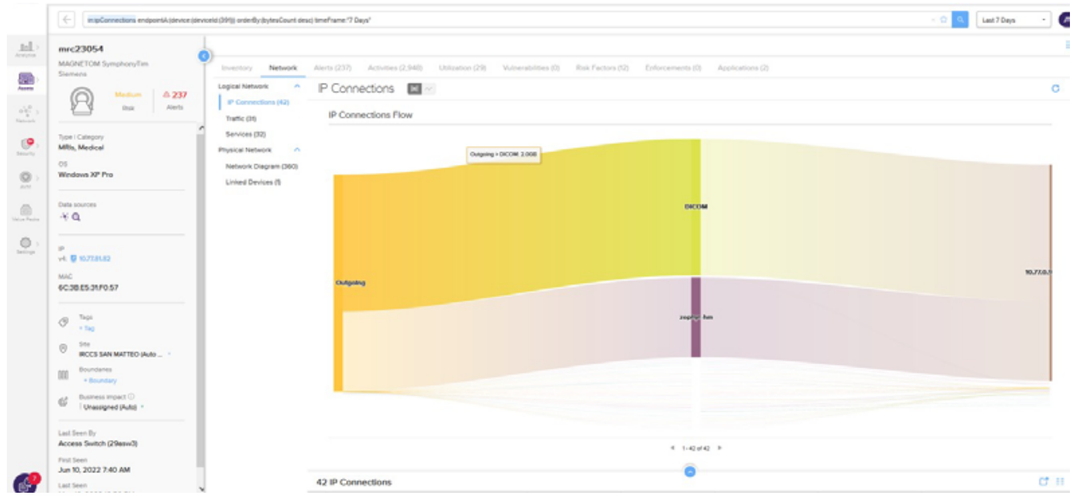
Asset Risk



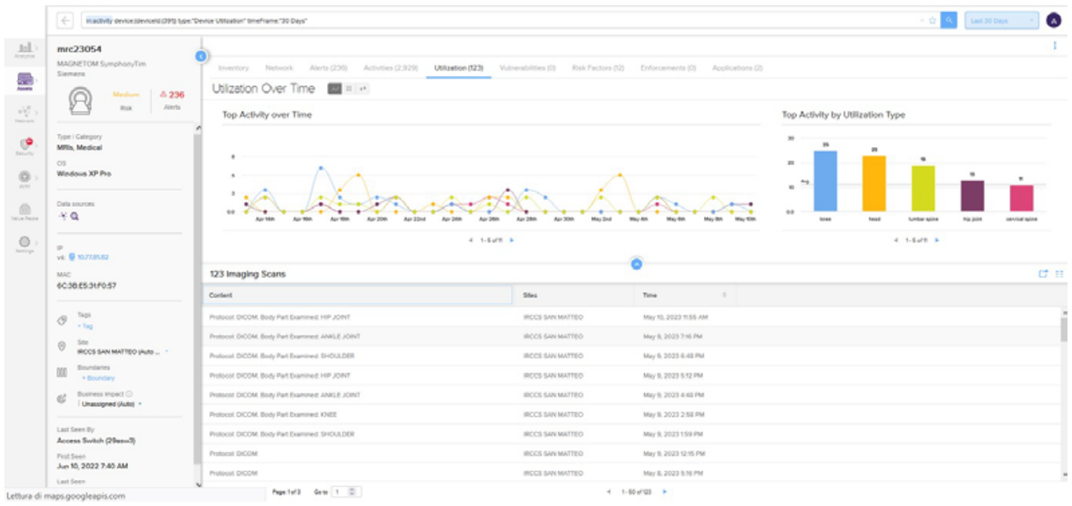
Vulnerability Management



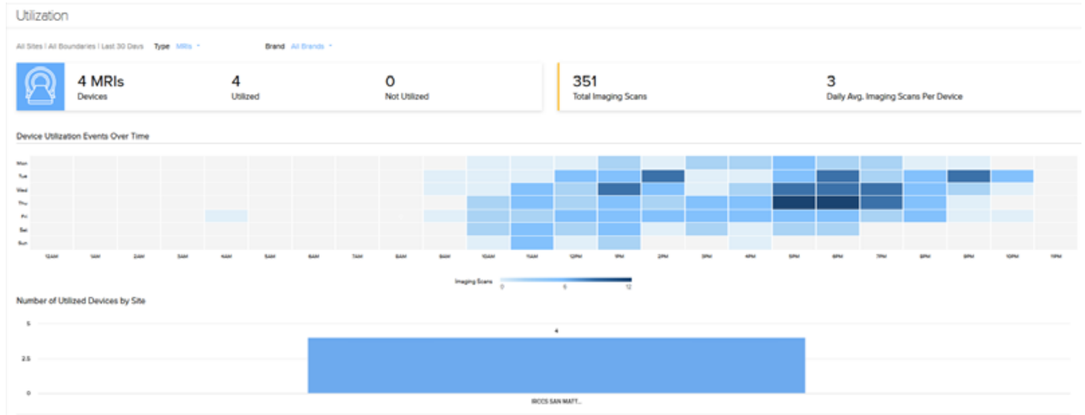
Analisi del Traffico



Utilizzo del Device



Utilizzo del Device



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