

Armis protegge la struttura del Policlinico San Matteo di Pavia per garantire un'assistenza sanitaria efficiente e sicura

La sfida

Supportare l'allineamento ai requisiti europei di cybersecurity, inclusi NIS e NIS2, per i servizi critici.

Stabilire un asset inventory continuo e accurato, individuando dispositivi connessi non gestiti o sconosciuti.

Migliorare l'identificazione delle vulnerabilità e la prioritizzazione del rischio sugli apparati connessi.

Arricchire la governance operativa integrando le informazioni sugli asset nei processi esistenti (incluso il CMDB).

La soluzione

Implementazione di Armis Centrix™ come piattaforma di cyber exposure management sull'intero ambiente connesso.

Rafforzamento della visibilità end-to-end degli asset, dell'identificazione delle vulnerabilità e della governance basata sul rischio a supporto dell'allineamento a NIS/NIS2.

Adozione scalabile attraverso l'integrazione con l'ecosistema esistente e il miglioramento della governance della cybersecurity.

Creazione di un asset inventory accurato e completo.

Accelerazione delle attività di vulnerability management per il team IT.

I risultati

100% di visibilità su tutti gli asset connessi, gestiti e non gestiti.

Miglioramento della gestione delle vulnerabilità grazie a una prioritizzazione più chiara basata sul contesto e sull'esposizione degli asset.

Riduzione dei tempi di inattività e aumento del numero di esami effettuati, con potenziale riduzione dei tempi di attesa per gli esami strumentali, grazie all'analisi dell'utilizzo degli apparati elettromedicali.

Settore: **Healthcare**

Posizione: **Pavia, Italy**

Misurare: **Oltre 3.500 dipendenti.**
Il team IT include 25 dipendenti e 5 consulenti esterni



Armis Centrix™ for
Medical Device Security

La Fondazione IRCCS Policlinico San Matteo, riconosciuta per i servizi di ricovero e cura ad alta specializzazione nonché per le attività di ricerca e didattica, ha consolidato le proprie capacità di cyber exposure management implementando Armis Centrix™.

Il dipartimento IT del San Matteo comprende 25 dipendenti e 5 consulenti esterni, organizzati in team focalizzati sull'ambiente applicativo e sull'infrastruttura (reti, sistemi e cybersecurity). Operando in un contesto clinico con un elevato numero di asset connessi, l'organizzazione necessitava di visibilità continua e governance sull'intero ambiente tecnologico, dai sistemi on-premises alle risorse connesse al cloud, per supportare decisioni basate sul rischio e garantire la continuità operativa.

“Grazie al supporto di Armis, abbiamo introdotto una funzionalità specifica che analizza il tasso di utilizzo degli apparati elettromedicali. Questo ci ha permesso di ottimizzarne l’impiego, riducendo i tempi di inattività e aumentando il numero di esami effettuati, con un miglioramento significativo dei servizi offerti ai cittadini e un impatto positivo per l’ent”

Andrea Gelmetti,
CISO presso il
Policlinico San Matteo

La sfida

Uno dei principali fattori trainanti per il San Matteo è stato l’allineamento ai requisiti europei di cybersecurity, tra cui NIS e NIS2, che elevano gli standard in termini di sicurezza e governance dei servizi critici. In questo scenario, l’ospedale aveva la necessità di definire e mantenere un inventario costantemente aggiornato e accurato, includendo anche i dispositivi non pienamente gestiti attraverso strumenti tradizionali; migliorare la prioritizzazione del rischio, a partire dall’identificazione e valutazione delle vulnerabilità dei dispositivi connessi e rafforzare la governance operativa, integrando nei processi e nei sistemi esistenti i dati sugli asset rilevanti per la sicurezza.

La soluzione

Per rispondere a queste esigenze, il San Matteo ha implementato Armis Centrix™, una piattaforma di cyber exposure management alimentata da un Asset Intelligence Engine basato su intelligenza artificiale, distribuendola in integrazione con l’ecosistema tecnologico e i workflow operativi esistenti. Armis Centrix™ ha permesso di identificare numerosi dispositivi non gestiti, garantendo una corretta prioritizzazione delle vulnerabilità. La piattaforma fornisce dettagli su ogni dispositivo connesso, consentendo un controllo esteso e piena consapevolezza della loro posizione nella rete. Inoltre, il San Matteo ha potuto arricchire il Configuration Management Database (CMDB) esistente con informazioni dettagliate precedentemente non disponibili, migliorando il tracciamento e la gestione degli apparati elettromedicali.

Fin dall’inizio, Armis Centrix™ si è dimostrata la piattaforma ideale per l’asset inventory, l’identificazione e la valutazione delle vulnerabilità dei dispositivi connessi.

Armis Centrix™ offre una panoramica completa delle informazioni, numerose integrazioni con vendor e tecnologie già presenti nella struttura, oltre a un importante supporto al team del San Matteo. Grazie all’analisi del traffico basata su intelligenza artificiale, la piattaforma rileva anomalie nei comportamenti dei dispositivi e segnala tempestivamente eventuali rischi di intrusione. Inoltre, Armis fornisce queste informazioni in tempo reale, rendendo gli interventi automatizzati efficaci e immediati.

“Le funzionalità di monitoraggio e gestione introdotte hanno supportato il miglioramento della visibilità sugli asset” ha dichiarato Andrea Assunto, CISO del Policlinico San Matteo. “In particolare, la disponibilità di informazioni dettagliate sui dispositivi, come dati identificativi, stato del software e ciclo di vita, consente una gestione più strutturata e tempestiva degli aggiornamenti e delle eventuali criticità segnalate dai produttori. Questo contribuisce a supportare la continuità operativa e il mantenimento di adeguati livelli di servizio”.



100%

di visibilità su tutti gli asset connessi, gestiti e non gestiti

Significativa riduzione delle vulnerabilità

Gestione più efficiente delle apparecchiature elettromedicali

I risultati

Il monitoraggio continuo degli asset ha portato il team IT del San Matteo a compiere un ulteriore passo avanti verso il servizio al pubblico:

“L’analisi dei dati relativi all’utilizzo degli apparati elettromedicali ha reso possibile una valutazione più puntuale dei livelli di impiego delle risorse”, ha dichiarato Andrea Gelmetti, Direttore dei Sistemi Informativi presso il Policlinico San Matteo. “Questo ha consentito di individuare margini di ottimizzazione nell’organizzazione delle attività, con effetti sulla riduzione dei tempi di inattività delle apparecchiature e sul miglior utilizzo delle stesse. Tali elementi possono contribuire, in prospettiva, al miglioramento dell’efficienza dei servizi erogati”.

Nel complesso, l’implementazione ha rafforzato il livello di sicurezza del San Matteo migliorando la visibilità, l’accuratezza dell’inventario e il monitoraggio in tempo reale degli asset connessi, supportando al contempo una prioritizzazione del rischio più strutturata. Riducendo le aree di scarsa visibilità e migliorando la qualità dei dati sugli asset, il San Matteo ha iniziato a ridurre il debito tecnico, rafforzare la gestione del rischio e l’allineamento alla conformità normativa, e migliorare l’efficienza e la continuità operativa, costruendo una base scalabile nel tempo e abilitando una governance condivisa della cybersecurity all’interno dell’organizzazione.



 **ARMIS**® from ServiceNow

See how leading organizations secure their environments with Armis.

[See Armis Centrix™ in Action](#)

Armis from ServiceNow protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.



+1 888 452 4011
armis.com