AIIC 2025
CONVEGNO NAZIONALE
ASSOCIAZIONE ITALIANA
INGEGNERI CLINICI

NAPOLI 14-17 GIUGNO 2025
MOSTRA D'OLTREMARE

AIIC
associazione
italiana
ingegneri clinici

Esperienze di gestione di problemi di cybersecurity in contesto DM

Paolo Piaser

RELATORI
TECNOLOGIE, SOSTENIBILITÀ, AMBIENTE
Il contributo dell'innovazione alla sanità del futuro

La cybersecurity cos'è?

NIST IR 7298 Revision 2, *Glossary of Key Information Security Terms*

cybersecurity |ˌsībərsiˈkyo͝oritē| :

The ability to protect or defend the use of **cyberspace** from **cyber attacks**.

Or

The **process** of protecting information by **preventing**, **detecting**, and **responding** to **attacks**.

Cyberspace:
A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Cyber Attack:
An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information

Fonte: Bechelli L.; Cyber Risk Management
Webinar CLUSIT 24/01/2020

La cybersecurity cos'è?

- Riservatezza (Confidenzialità)

  la protezione delle informazioni mediante l'accesso consentito soltanto agli autorizzati, la protezione delle trasmissioni, il controllo degli accessi, ...

- Integrità

  la salvaguardia della correttezza dei dati, la difesa dalle manomissioni e da modifiche non autorizzate, il monitoraggio automatico degli accessi, ...

- Disponibilità

  la garanzia per gli utenti di poter disporre dei dati, delle informazioni e dei servizi, evitando la loro perdita o riduzione

Autenticità

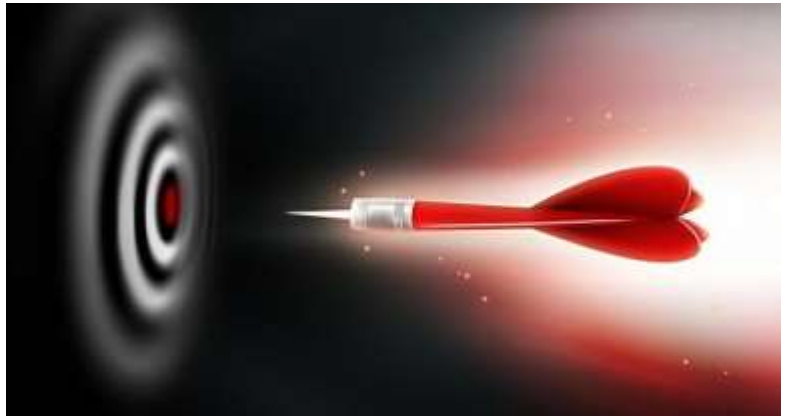
In Sanità?

In sanità abbiamo una necessità ulteriore:

LA SALUTE DEL PAZIENTE

Approccio Ingegnere Clinico

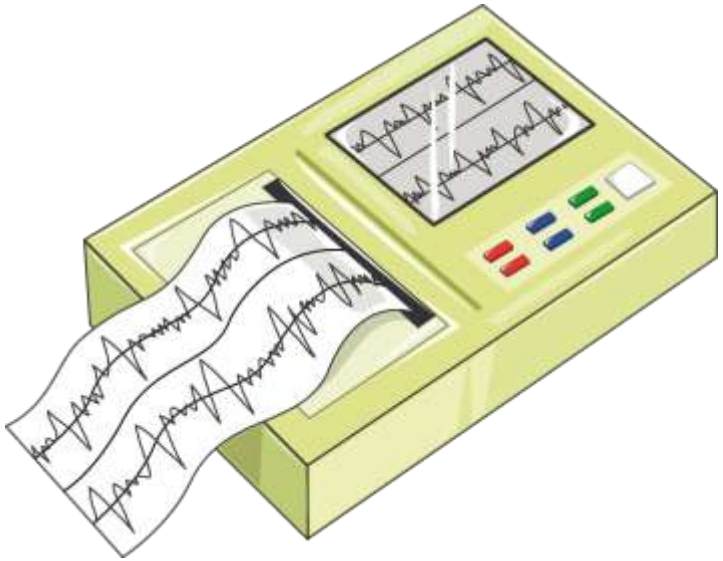
- Da un approccio focalizzato



- Ad un approccio integrato

Approccio Ingegnere Clinico

- Ormai la maggioranza dei DM per essere sfruttata al meglio necessita di integrazioni (diagnostica di laboratorio, ECG, ECT, centrali di monitoraggio, ...)
- Utilizzo degli standard
- Connettività di rete
- .



DICOM
Digital Imaging and Communications in Medicine

Approccio Ingegnere Clinico

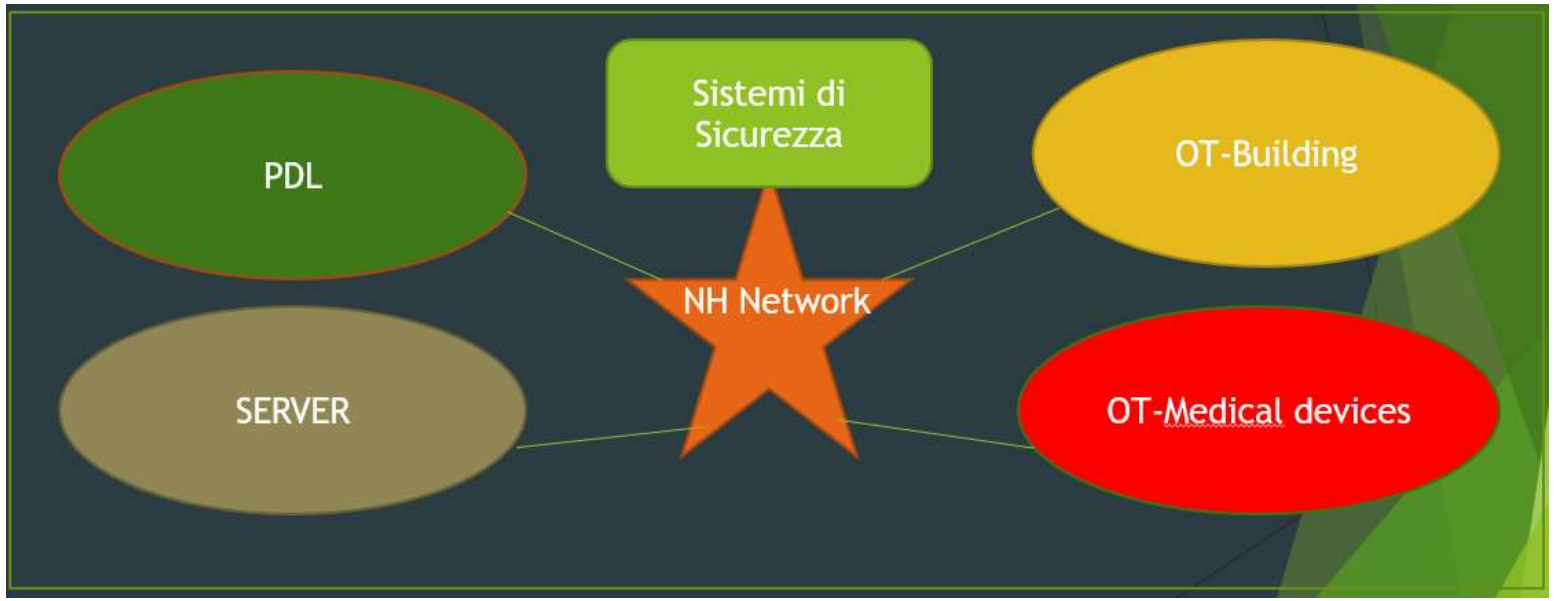
- Occorre un cambio di paradigma per una gestione integrata
- Il focus resta la safety del paziente ma non è più data dalla sola sicurezza elettrica e dal percorso manutentivo a cui sono sottoposti DM e sistemi di DM

Tanto tempo fa in una gal…..

- ISO IEC 80001
- Le key properties
  - SAFETY
  - EFFECTIVENESS
  - SECURITY
- E la gestione del

SAFETY e SECURITY

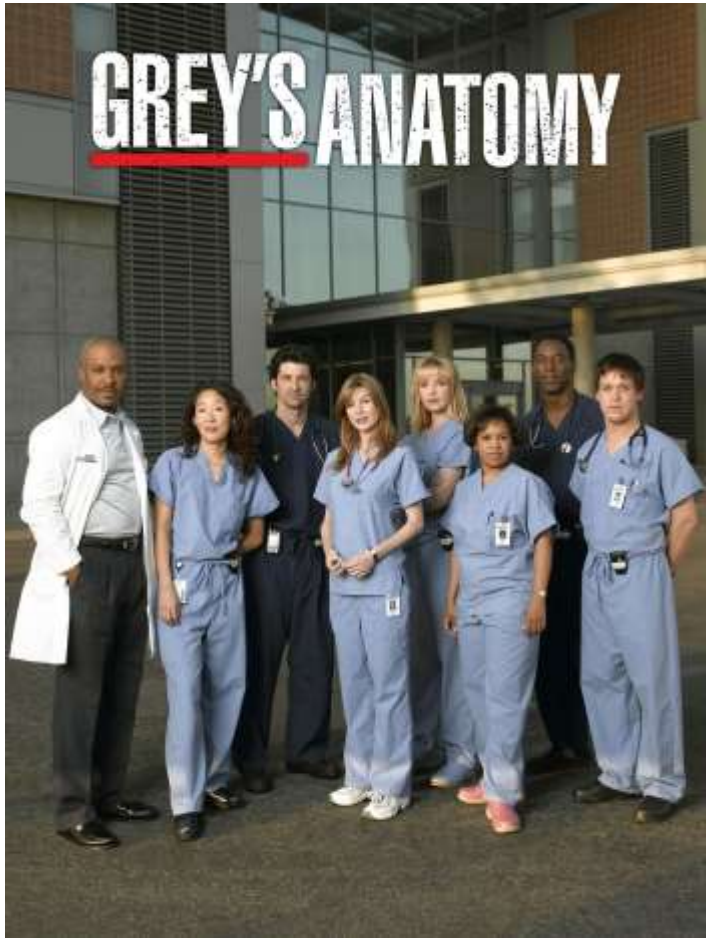
- In un mondo sempre più connesso e integrato dobbiamo ragionare che oltre ai nostri sistemi e ne sono altri nell'ecosistema sanitario



- Potrebbero essere i nostri sistemi la minaccia
- Potrebbero essere i nostri sistemi il target

Quando la Security si traduce in Safety

- Grey's Anatomy
  - Temperatura locali
  - CCE
  - Sistemi diagnostici
  - Frigoemoteche
  - …



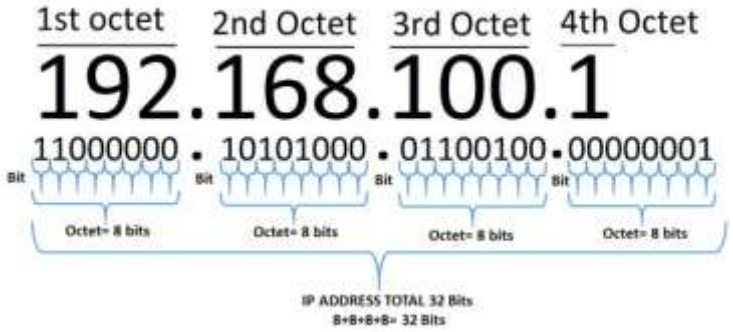
Quando la Security si traduce in Safety

Quando la Security si traduce in Safety

- Quindi quando siamo nel campo dei DM anche la security si traduce in safety in alcuni casi
- Dati corrotti o non disponibili
  - Errata diagnosi
    - Errato trattamento
      - Potenziale rischio di salute per il paziente
        - Potenziale morte del paziente

Quando inizio a fare sicurezza in ambito Sanitario?

- Dalla richiesta dell'IP?
- Dal collaudo del dispositivo/sistema?
- Quando mi chiamano i servizi IT e mi chiedono cosa ho collegato?



Quando inizio a fare sicurezza in ambito Sanitario?

Adozione di una politica condivisa di cybersecurity aziendale basata su:

- Identificazione di ruoli e figure chiave in ottemperanza alla normativa vigente (NIS 2, DL 90/2025, …)
- Organizzazione multidisciplinare specifica (ICT, Ingegneria clinica IC, Uffici tecnici OT)
- Formazione differenziata degli utenti (Security Awareness) ICT e IC, con pianificazione anche per OT
- Creazione di procedure specifiche per fase di acquisto di nuove soluzioni, gestione incidenti, …

Quando inizio a fare sicurezza in ambito Sanitario?

E ancora:

- Adozione delle best practice per la configurazione e implementazione di nuove soluzioni
- Acquisto di servizi specifici per attività di VA e PT
- Utilizzo di framework riconosciuti per l' analisi dello stato di fatto e la individuazione dell'obiettivo da raggiungere con misurazione degli step
- Il tutto revisionato con cadenza annuale

I ruoli e le figure

Quali sono i ruoli?

- CIO? CISO? Referente per la Cybersecurity? Punto di Contatto? Responsabile per le violazioni?
- Un ingegnere clinico può ricoprire certi ruoli?
- Un ingegnere clinico può supportare i decision makers?
- Cosa può o deve fare un ingegnere clinico per contribuire al percorso verso un livello più alto di resilienza cibernetica?

Organizzazione Multidisciplinare

Le strutture aziendali possono lavorare a compartimenti stagni?

- L'IC deve sapere di IT e di UT
- L'IT deve sapere di IC e di UT
- L'UT deve sapere di IT e IC
- Insomma ci vuole un linguaggio comune per affrontare problemi comuni che richiedono approcci diversi

Formazione differenziata per ruolo

- Ruoli diversi, rischi diversi e competenze da acquisire diverse
- Un unico obiettivo:
  - Aumentare la resilienza cibernetica della propria infrastruttura

Procedure specifiche

- Nuove procedure che tengano conto anche di aspetti di cybersecurity
- **Procedure d'acquisto**
- Procedure di collaudo
- Procedure di manutenzione pre
- Procedure di manutenzione cor
- Procedura di dismissione

Una nuova procedura di gara

Come progetto/costruisco una gara che sia conforme anche alla normativa sulla cybersicurezza? Conta di più la cybersecurity o la normativa sui dispositivi medici?

Risposta di un ingegnere clinico:

- Le due cose devono possibilmente coesistere… in ogni caso, prima la salute del paziente!
- Nella progettazione si sceglie il livello di rischio che si è disposti a tollerare
- Si deve distinguere tra le semplici postazioni di lavoro e i MD e, quindi, utilizzare sistemi di sicurezza diversi, sia tecnologici che procedurali
- Si devono attuare tutte le misure, sia tecniche che organizzative, che si è in grado di mettere in campo, pur sapendo che i fondi non sono illimitati

Cyber-acquisti

Perché cominciare dalla progettazione di una gara per la fornitura di un dispositivo/sistema?

Nel programmare e avviare la procedura per l'acquisto di un bene/servizio si ha ancora la possibilità di decidere quale livello di rischio accettare e quale sia la disponibilità economica per renderlo tollerabile

Nella predisposizione della documentazione di gara si può vincolare l'operatore economico a fornire il necessario supporto amministrativo oltre che tecnico

Si spinge il mercato a proporre soluzioni più mature e aderenti alle esigenze della realtà sanitaria

Posso ancora imporre al fornitore l'adozione di soluzioni che mi consentano di monitorare la supply chian così come previsto dalla NIS 2

Cyber-acquisti

Costruzione di un nuovo documento per l'integrazione di dispositivi medici in rete:

- Cosa voglio comprare?
- Come voglio garantire la sua funzionalità?
- Come lo voglio proteggere?
- Dovrà parlare con altri sistemi aziendali? Se si come lo integro?
- È un dispositivo/ sistema di supporto vitale?
- Che livello di complessità comporta l'adozione e la gestione della configurazione che voglio adottare?
- Come voglio gestire la manutenzione della parte software?

E ancora altro….

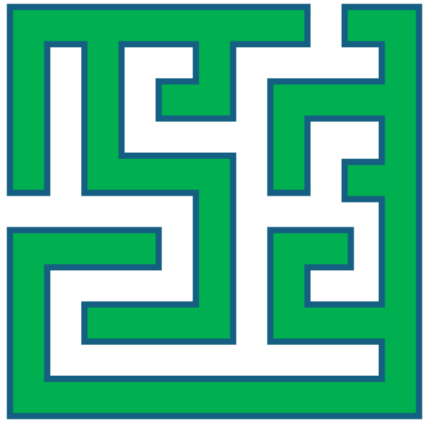
- Acquisire informazioni relative alla soluzione
- Imporre un registro per la gestione degli aggiornamenti che accompagna il libro macchina del DM/sistema
- Acquisire le informazioni relative ai tecnici che eseguiranno le attività da remoto
- Acquisire il dettaglio delle transazioni (porte, standard, servizi, ….) che consentono al DM/sistema di integrarsi con l'ambiente ospedaliero

Cyber-acquisti

Risulta ovvio che dipendentemente da quello che voglio acquistare dovrò adottare politiche differenziate

Sistemi MD poco complessi e a basso impatto

- OS di tipo corporate altamente personalizzabili
- Antivirus
- Hardening delle soluzioni
- Mercato maturo delle soluzioni di sicurezza
- Politiche di messa in sicurezza direttamente applicabili, anche grazie alla omogeneità



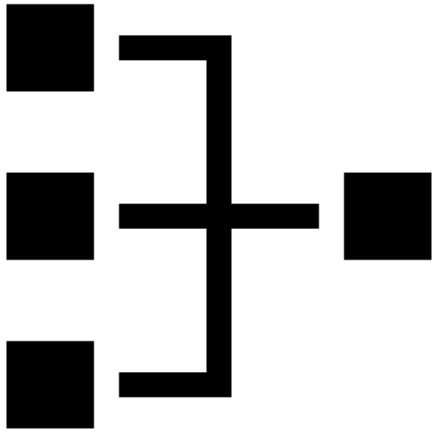
Sistemi MD complessi e di supporto vitale

- OS non modificabile
- Antivirus spesso non installabili
- Protezione dell'ambiente di lavoro
- Mercato in evoluzione con sistemi specifici
- Politiche differenziate per tipologia

Cyber-acquisti

Cerco di far convergere le soluzioni a casi d'uso che rientrano nel perimetro di gestione scelto e che sia sostenibile!

- Client Singolo
- Client Saas Ibrido
- Client Saas e eventuale Edge



Messa in sicurezza del sistema

Cyber-acquisti un esempio: centrale di monitoraggio

Devo aver ben chiaro cosa voglio comprare e come configurarlo

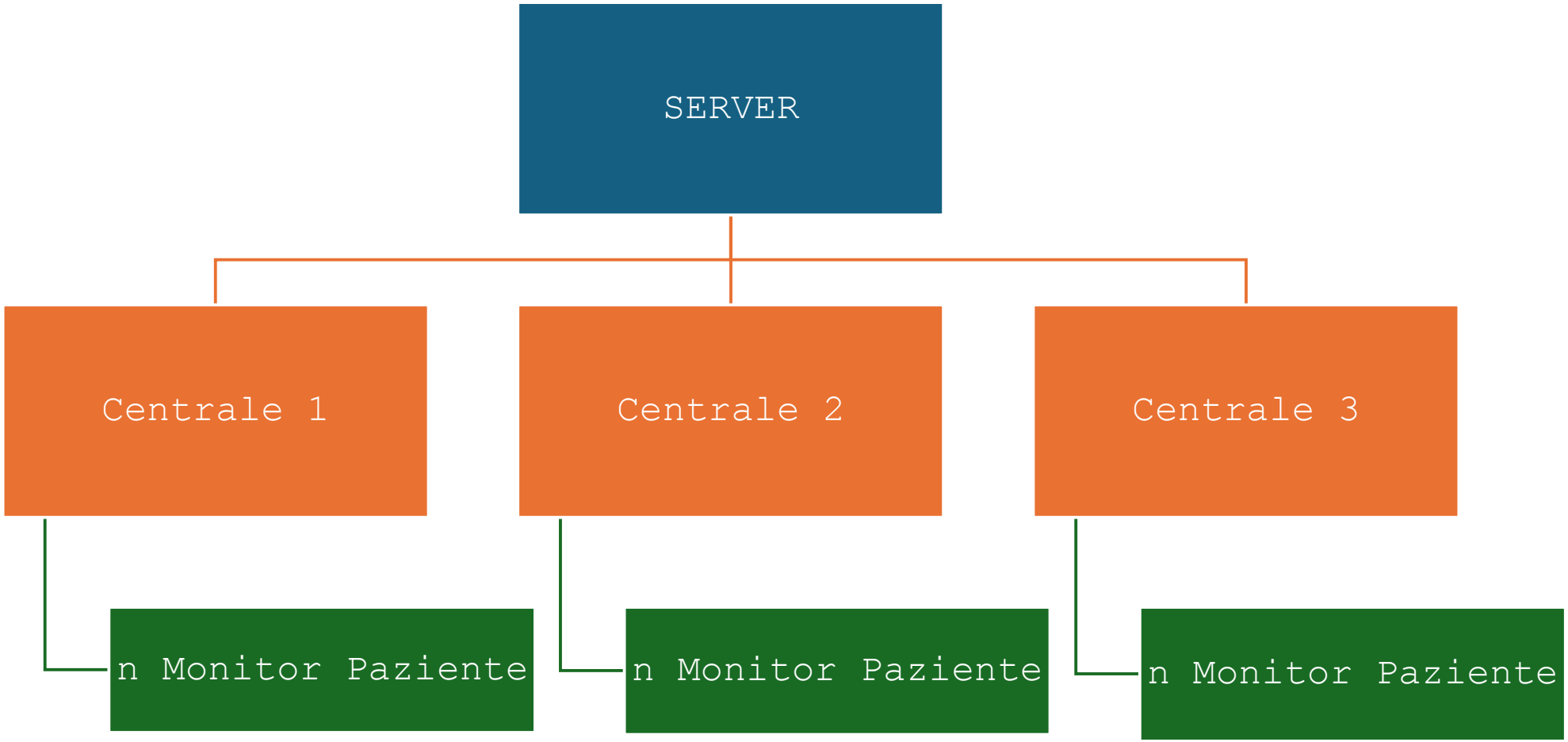
Ad esempio una centrale di monitoraggio nuova per la terapia intensiva

Cyber-acquisti

Che tipologia di sistema è? A quale delle mie casistiche si associa?

- Client Singolo
- Client Saas Ibrido
- Client Saas e eventuale Edge

Cyber-acquisti



Cyber-acquisiti

Come possiamo proteggere il sistema?

Lo intendiamo come singola bolla?

Lo intendiamo come tante piccole bolle che fanno parte di una bolla più grande?

Prima cosa definisco a livello di rete come voglio gestirla

Quindi considerata la tipologia di soluzione che stiamo acquistando potrebbe essere appropriato creare una subnet dedicata su cui inserire i vari dispositivi (segmentazione e segregazione del traffico)

Per ulteriore sicurezza la subnet verrà terminata sul firewall, in modo da poter gestire tutto quello che può entrare o uscire da quella rete

Attivare soluzioni di IDS e IPS

Cyber-acquisiti

Come possiamo proteggere il sistema?

Per queste tipologie di soluzioni non è spesso possibile gestire la sicurezza eseguendo attività di hardening sui dispositivi, ma posso farlo sull'ambiente, creare una bolla sicura

- Progettare soluzioni architetturali in HA, con comunicazioni cifrate tra sistemi in area core e edge
- scegliere le tipologie di apparati attivi di rete più pertinenti a livello di performance
- Scegliere la tipologia di accesso regolamentato alla rete del monitoraggio per gli endpoint attraverso l'implementazione di un NAC
- …

Cyber-acquisiti

Come possiamo proteggere il sistema?

A livello sistemistico la difficoltà si alza ancora di più, infatti occorre pensare a come far implementare/gestire al fornitore alcune attività specifiche:

- Resilienza alla indisponibilità di una centrale oppure del server
- Eventualmente chiedere se possibile sfruttare soluzioni di EDR/XDR compatibili
- Configurazione e profilazione utenti e integrazioni con il SIO
- Backup di centrali e server, fondamentale per implementare un sistema che consenta ridotti tempi di downtime, e se possibile utilizzando il paradigma 3-2-1 o meglio 3-2-1-0, differenziate sul livello di rischio
-

Cyber-acquisti

Devo trovare un bilanciamento:

- Quello che posso implementare io come azienda e che sia sostenibile (perimetro nel quel il fornitore si muove per mettere a terra la sua soluzione, parte integrante dell'allegato IT)

- Quello che devo richiedere al fornitore in fase di implementazione per raggiungere un livello di rischio tollerabile secondo la mia analisi (come il fornitore decide di implementare la soluzione nel perimetro per rispondere alle mie richieste)

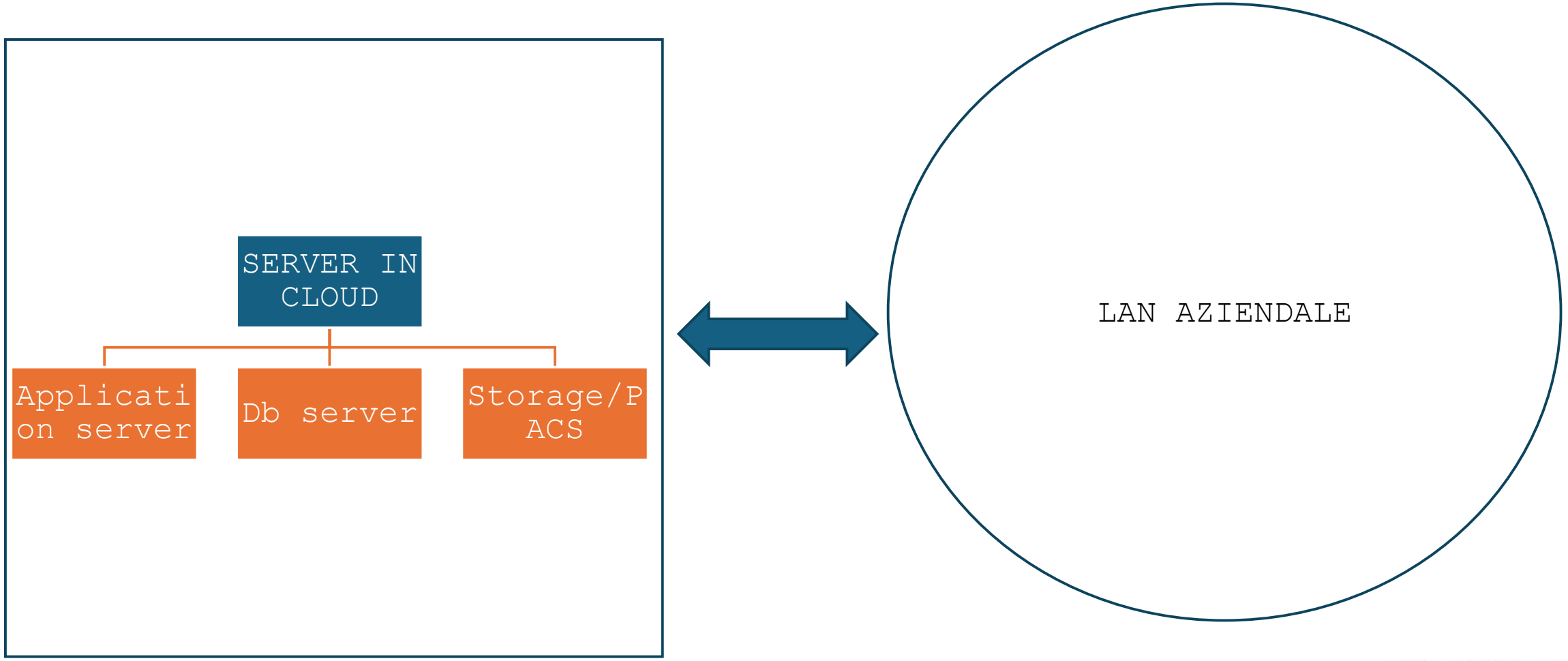
Cyber-acquisti Software per la Gastroenterologia

Cyber-acquisti

Che tipologia di sistema è? A quale delle mie casistiche si associa?

- Client Singolo
- Client Saas Ibrido
- Client Saas e eventuale Edge

Cyber-acquisti



Cyber-acquisti

La situazione qui è diversa:

- Abbiamo sia dispositivi medici che PDL che la parte server in cloud
- Dobbiamo pensare a come rendere sicure le comunicazioni, tra l'altro alcune escono dal perimetro aziendale
- La fruizione è fortemente orientata al servizio, quindi entrano in gioco considerazioni su RPO e RTO

Cyber-acquisti

Indicativamente vale quanto visto e progettato prima per il sistema di monitoraggio distribuito con alcuni accorgimenti ulteriori

- I PC medicali verranno trattati il quanto più possibile alla stregua dei normali PC aziendali e quindi:
  - Aggiornamento OS
  - Antivirus
  - Aggiornamenti di sicurezza
  - Messa a dominio
  - Client senza persistenza di dati sulla postazione al termine della sessione di lavoro (web based)
  - …

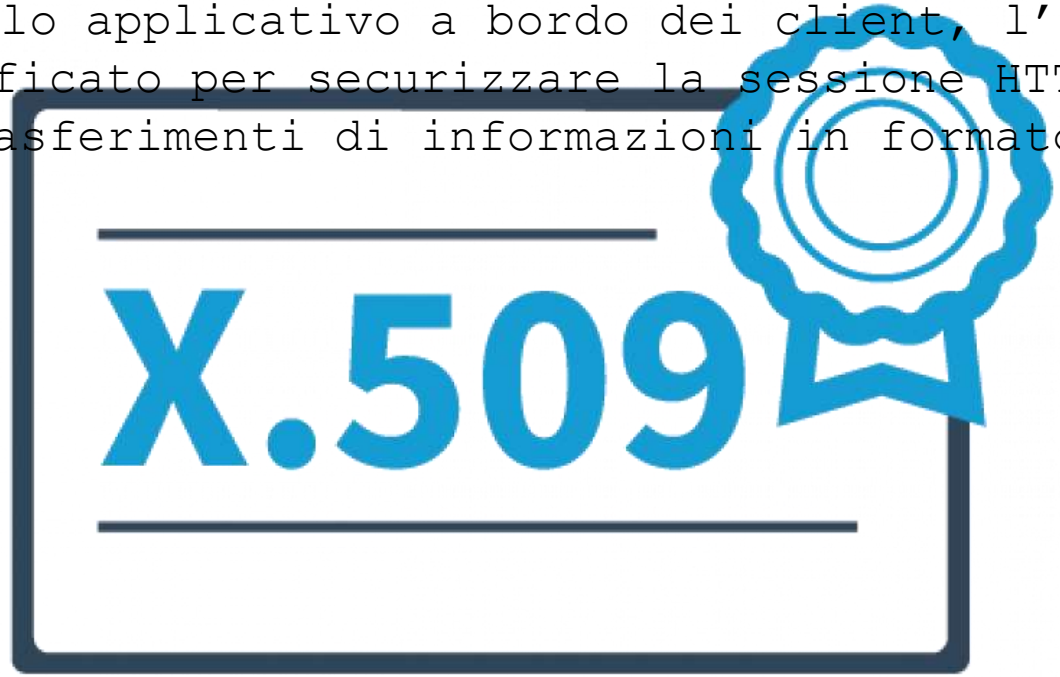
Cyber-acquisti

Indicativamente vale quanto visto e progettato prima per il sistema di monitoraggio distribuito con alcuni accorgimenti ulteriori

- I server sono in cloud, quindi anche qui va definito chiaramente a chi competono le seguenti attività:
  - Aggiornamento OS
  - Antivirus
  - Aggiornamenti di sicurezza
  - Gestione autenticazione utenti
  - Backup
  - RPO e RTO del servizio

Cyber-acquisti

- Connessioni:
  - Da servizio cloud a lan aziendale, con linea dedicata o VPN attiva site to site verso per accedere ai nostri servizi in cloud
  - A livello applicativo a bordo dei client, l'utilizzo di un certificato per securizzare la sessione HTTP al fine di avere trasferimenti di informazioni in formato cifrato



Cyber-acquisti

- Piccola riflessione sulle connessioni:
- Siamo sicuri che la connettività che ho o che mi porterà il fornitore sarà sufficiente a gestire le attività con i server in cloud?
- Come ci tuteliamo?
  - In gara definisco chiaramente le SLA, e dipendentemente dalla criticità della soluzione posso chiedere che venga proposto un sistema di edge computing di supporto, il quale dovrebbe garantire i requisiti richiesti, completamente gestito dal fornitore, **ricordiamoci che è un SaaS**

Cyber-acquisti

Cosa succede oggi?
Soprattutto nei service, spesso i fornitori offrono software per la gestione in Saas.
Possiamo usare quei software?
Nel caso di una azienda sanitaria pubblica la risposta è NO, il software offerto in Saas deve risultare disponibile all'interno del Marketplace di ACN

Di solito i fornitori inviano bellissime dichiarazioni della certificazione su cui appoggia la loro infrastruttura cloud, peccato che l'azienda sanitaria non sta comprando infrastruttura (IaaS) ma un servizio (SaaS)

Cyber-acquisti

Quindi il nostro allegato IT si arricchisce e si forma in modo tale da portare su piani gestibili le soluzioni tecnologiche che vogliamo acquistare.

Solo al momento della gara abbiamo ancora il potere contrattuale per portare su binari gestibili e nel perimetro da noi definito implementazione.

Cybersecurity- esempio di allegato IT

Allegato specifiche IT Medicali e Analitici AsFO

Introduzione

Il presente documento ha come scopo regolamentare, tramite informazione e categorizzazione in casi d'uso, l'ingresso dei nuovi sistemi forniti in qualsivoglia modalità (acquisto, noleggio, service, donazione, ...).

La parte informativa del documento rappresenta le specifiche che i sistemi/beni forniti dovranno rispettare relativamente all'area IT. Nel documento verrà fornita una panoramica che riporterà concetti fondamentali sulla tipologia di rete presente in AsFO e le metodologie legate all'integrazione dei sistemi offerti con quelli esistenti.

La categorizzazione dei casi d'uso viene definita in coerenza con la legislazione vigente, normativa generale e specifica di settore, linee guida e best practice, sempre e comunque a tutela di AsFO, nell'interesse dell'Azienda e dei fruitori dei servizi erogati. Casi d'uso non riconducibili alla categorizzazione presentata dovranno essere analizzati e validati prima dell'affidamento del contratto.

Cybersecurity- esempio di allegato IT

L'infrastruttura cloud dovrà essere tra quelle qualificate\adeguate di livello pertinente alla tipologia di dati e servizi che vengono trattati su tale infrastruttura secondo quanto indicato nel nuovo Regolamento Cloud di ACN, in vigore dal 1/7/2024, "REGOLAMENTO PER LE INFRASTRUTTURE DIGITALI E PER I SERVIZI CLOUD PER LA PUBBLICA AMMINISTRAZIONE".

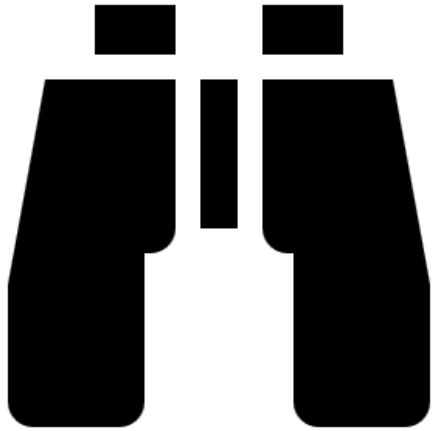
Sarà ammessa, e fortemente consigliata, la predisposizione di apparati edge (preferibilimente virtuali, eventualmente su infrastruttura messa a disposizione da AsFO), ovvero server applicativi che possano garantire la piena continuità di servizio in caso di irraggiungibilità del cloud, in un'ottica di applicazione delle best practice di Business Continuity come suggerito dalla norma ISO/IEC 22313:2020. Il server edge dovrà avere ridottissima profondità temporale. Gli apparati di edge

Cybersecurity- esempio di allegato IT

AsFO potrà avvalersi di supporto specialistico per l'esecuzione di VA/PT (vulnerability assesment/penetration test) dei sistemi collegati alla propria rete. Pertanto il fornitore potrebbe essere chiamato da AsFO per fornire supporto ed eseguire verifiche funzionali legate all'esecuzione dei VA/PT in giornate programmate e concordate. Il costo per il ripristino del funzionamento è da intendersi completamente a carico del fornitore.

AsFO eseguirà, come parte del collaudo tecnico dell'apparecchiatura/sistema, una valutazione primaria volta ad una valutazione sulla sicurezza dei dispositivi i sistemi che verranno collegati alla rete aziendale di AsFO. A seguito di questo, verrà stilato un documento sottoscritto da ambo le parti dove si riportano le evidenze individuate durante l'attività di valutazione.

Cybersecurity- continua



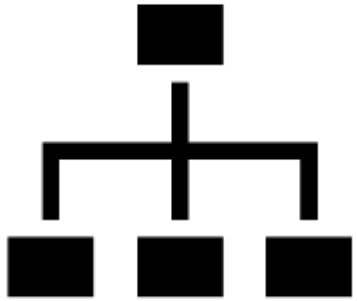
Una volta fatto l'acquisto e implementato come da policy definite in capitolato e con il fornitore blindato dai vincoli nella documentazione che ha firmato per partecipare alla gara sono in sicurezza?

No

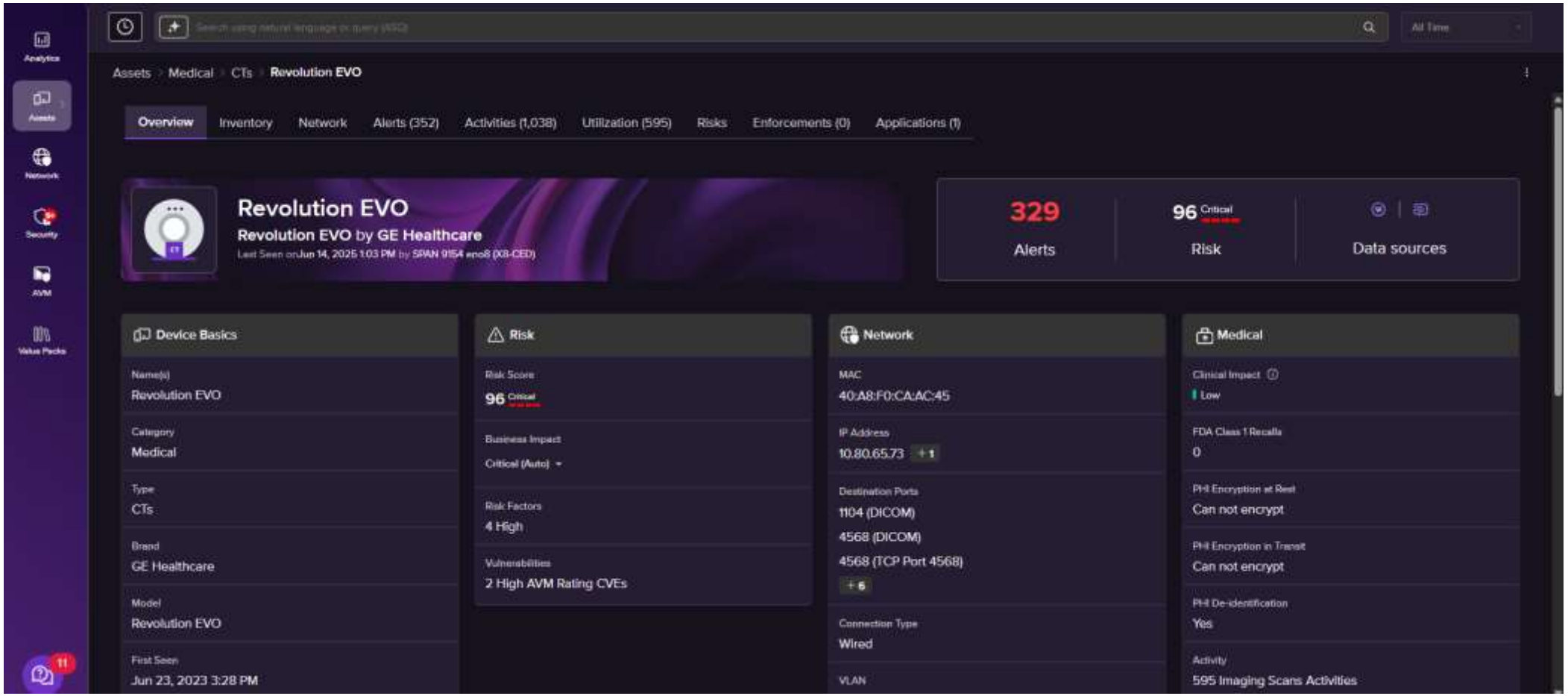
Devo monitorare e testare! Valutare continuamente il rischio e se del caso rivedere le priorità nella programmazione degli acquisti se il livello di rischio non è più accettabile

Cybersecurity

- Dobbiamo implementare delle soluzioni che consentano di rendere gestibile il nostro sistema
  - Sistemi di monitoraggio passivi
  - Sistemi di monitoraggio attivi
  - Strumenti per la gestione degli eventi di sicurezza
  - Strumenti di business intelligence
  - PT
  - Documentare!



Cybersecurity- monitoraggio passivo



Cybersecurity- business intelligence

Cybersecurity- sistema di gestione degli eventi

E molto Altro

AIIC 2025 CONVEGNO NAZIONALE ASSOCIAZIONE ITALIANA INGEGNERI CLINICI

NAPOLI 14-17 GIUGNO 2025 MOSTRA D'OLTREMARE

AIIC associazione italiana ingegneri clinici

Grazie per l'attenzione !

TECNOLOGIE, SOSTENIBILITÀ, AMBIENTE
Il contributo dell'innovazione alla sanità del futuro