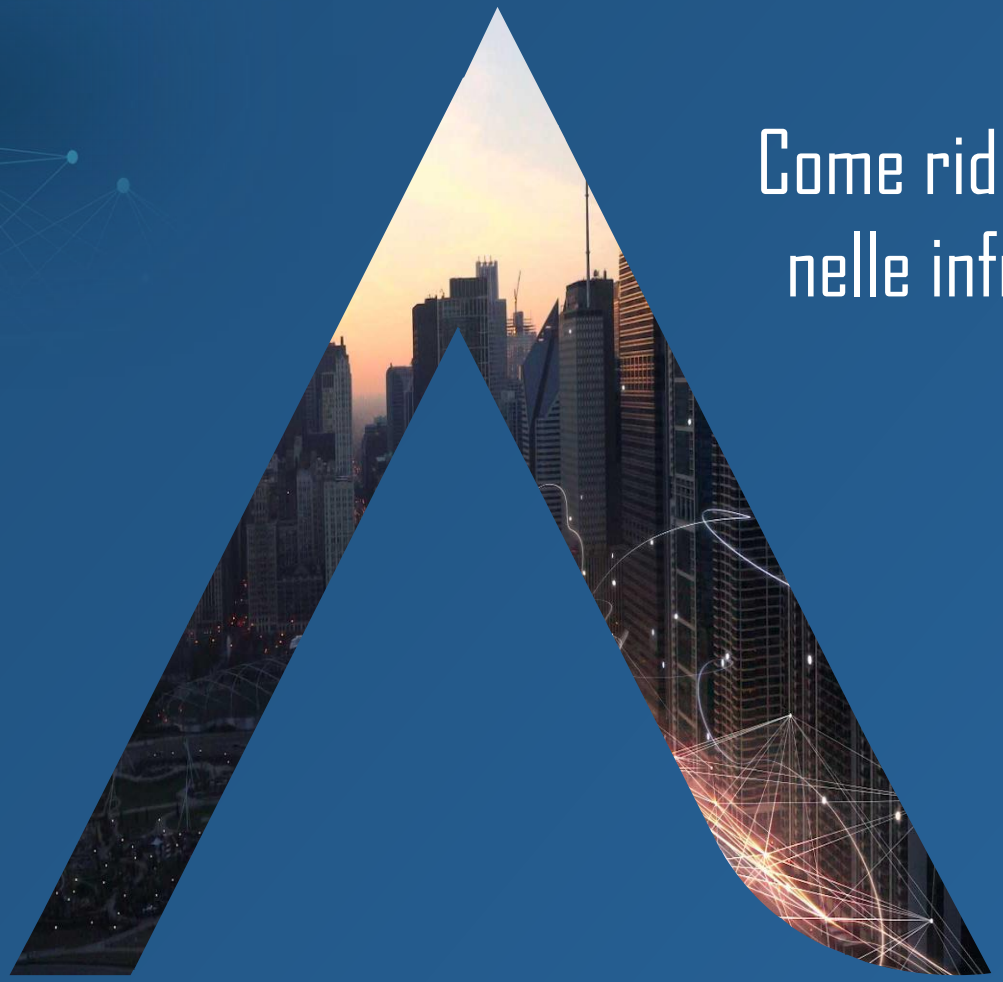
Almaviva

JOSHUA
CYBERISKVISION



Come ridurre la superficie di attacco nelle infrastrutture sanitarie e nelle piattaforme di telemedicina

Connected Care e Telemedicina

L'evoluzione delle tecnologie digitali abilita nuovi modelli di gestione e presa in carico dei pazienti (*connected care*).

Nell'ambito sanitario la pandemia (Covid) ha accelerato lo sviluppo di alcuni servizi digitali ed in particolare la telemedicina.

Il **PNRR e le recenti iniziative nazionali** (Piattaforma Nazionale di Telemedicina e i futuri sistemi di Telemedicina Regionali) stanno imprimendo una forte accelerazione alla diffusione di sistemi di Telemedicina sul territorio nazionale.

Nuovi modelli di *Connected Care* si stanno consolidando con l'avvio del nuovo assetto della sanità territoriale, **DM 77/2022 - Nuovi modelli e standard per lo sviluppo dell'assistenza territoriale nel SSN**.

Vantaggi

Migliore allocazione delle risorse

La possibilità di gestire i pazienti a distanza consente di ottimizzare la distribuzione delle risorse (medici) superando i vincoli territoriali.

Razionalizzazione nell'accesso alle strutture ospedaliere

La connessione continua con i pazienti a domicilio contribuisce a ridurre gli accessi alle strutture di emergenza

Riduzione dei costi

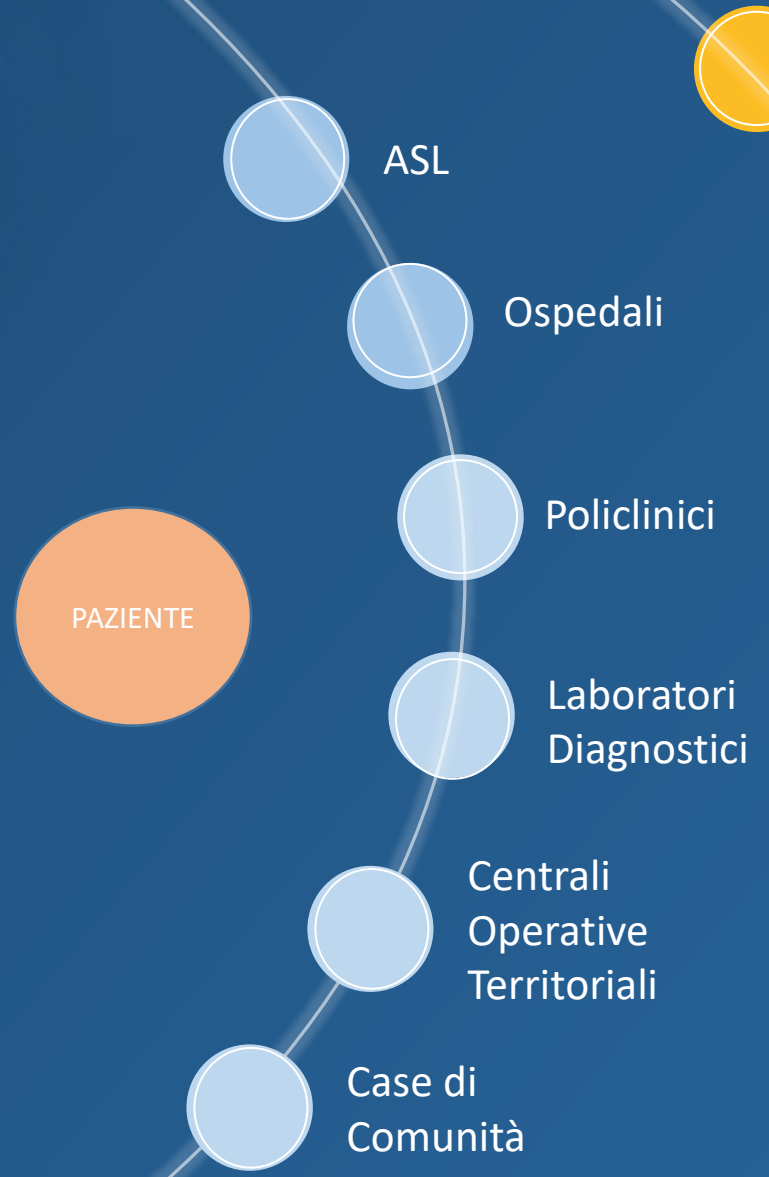
La gestione dei pazienti nelle strutture intermedie (CdC, OdC) rende maggiormente coerente la compliance tra richiesta di assistenza e setting assistenziale

Aderenza ai piani di cura

Il monitoraggio continuo migliora il coinvolgimento del paziente nel processo di cura e l'aderenza al percorso terapeutico

TELEMEDICINA

La **Telemedicina è un metodo innovativo** per fornire servizi di assistenza sanitaria tramite tecnologie avanzate, offrendo la possibilità di trasmettere in modo sicuro informazioni e dati medici in varie forme, come testi, suoni e immagini.
Questo approccio è utile **per la prevenzione, la diagnosi, il trattamento e il monitoraggio dei pazienti**.



Attori coinvolti

- **Medici**
- **Operatori Sanitari**
- **Tecnologi**
  Fornitori di piattaforme di telemedicina
- **Servizi Cloud**
  Fornitori che offrono infrastrutture e piattaforme per le applicazioni di telemedicina basati su cloud
- **Assicurazioni sanitarie**
  Compagnie assicurative che forniscono copertura per i servizi di telemedicina
- **Regolatori**
  Agenzie governative che regolano la pratica della telemedicina e la gestione dei dati medici.
- **Cyber Security**
  Fornitori di soluzioni di sicurezza dell'informazione a tutela dei dati relativi a Pazienti e Medici.

Tipologie di prestazioni

- Televisita: situazione dove il medico interagisce con il paziente a distanza, richiede la presenza attiva del paziente.
- Teleassistenza: favorire lo svolgimento di attività di tipo assistenziale attraverso un’interazione a distanza tra professionista e paziente o con il caregiver. Può essere rivolta ad anziani, persone fragili e diversamente abili.
- Telerefertazione: rilascio da parte del medico di una relazione trasmessa con sistemi digitali o di telecomunicazione.
- Telecooperazione: utilizzo delle tecnologie dell'informazione e della comunicazione per facilitare la cooperazione tra professionisti sanitari a distanza.
- Telemonitoraggio: utilizzo di dispositivi medici per inviare dati medici rilevanti a un professionista sanitario che si trova in un'altra posizione.

Tecnologie utilizzate

Sistemi hardware e software, apparati biomedicali

Acquisizione ed elaborazione di segnali, immagini e dati del paziente.

Applicazioni web

Trasmissione bidirezionale delle informazioni sanitarie.

Dispositivi medici portatili (IoMT)

Monitoraggio dei segnali vitali in fase di riabilitazione, recupero e cronicità.

Almaviva

Cyber Security

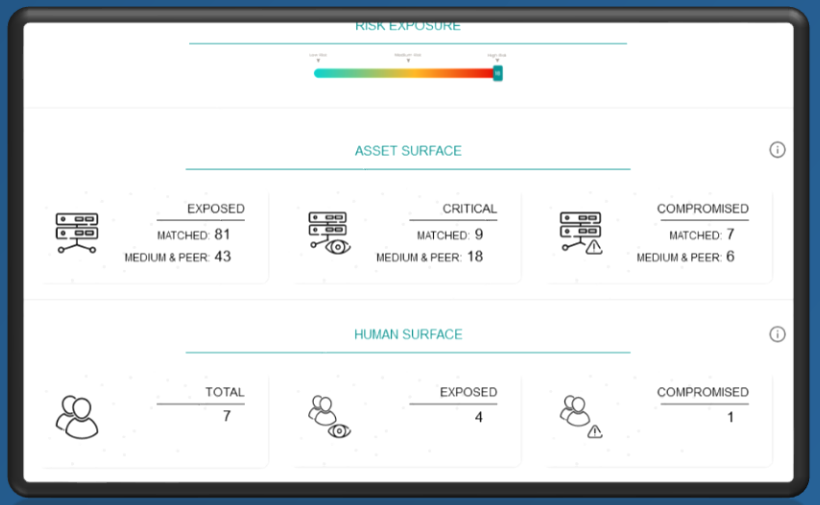
Superficie d’attacco AS-IS

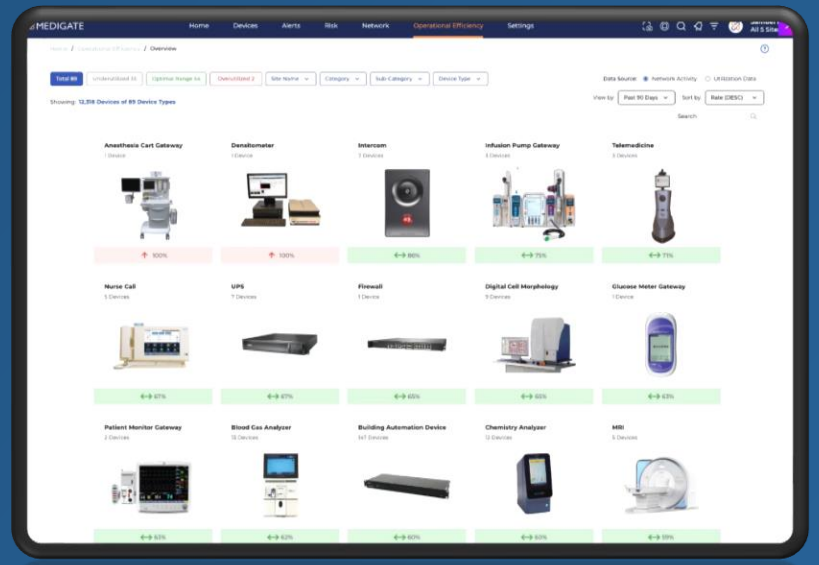
La telemedicina ha rivoluzionato il modo in cui i professionisti sanitari offrono cure ai pazienti, rendendo più facile e conveniente l'accesso alle cure mediche.

Tuttavia, come qualsiasi sistema basato su tecnologia, la telemedicina presenta una superficie d'attacco per i cybercriminali, che possono sfruttare le vulnerabilità del sistema per accedere a dati sensibili dei pazienti o interrompere le cure mediche.

OSINT

JOSHUA CYBERISKVISION





CLAROTY

CLOSINT

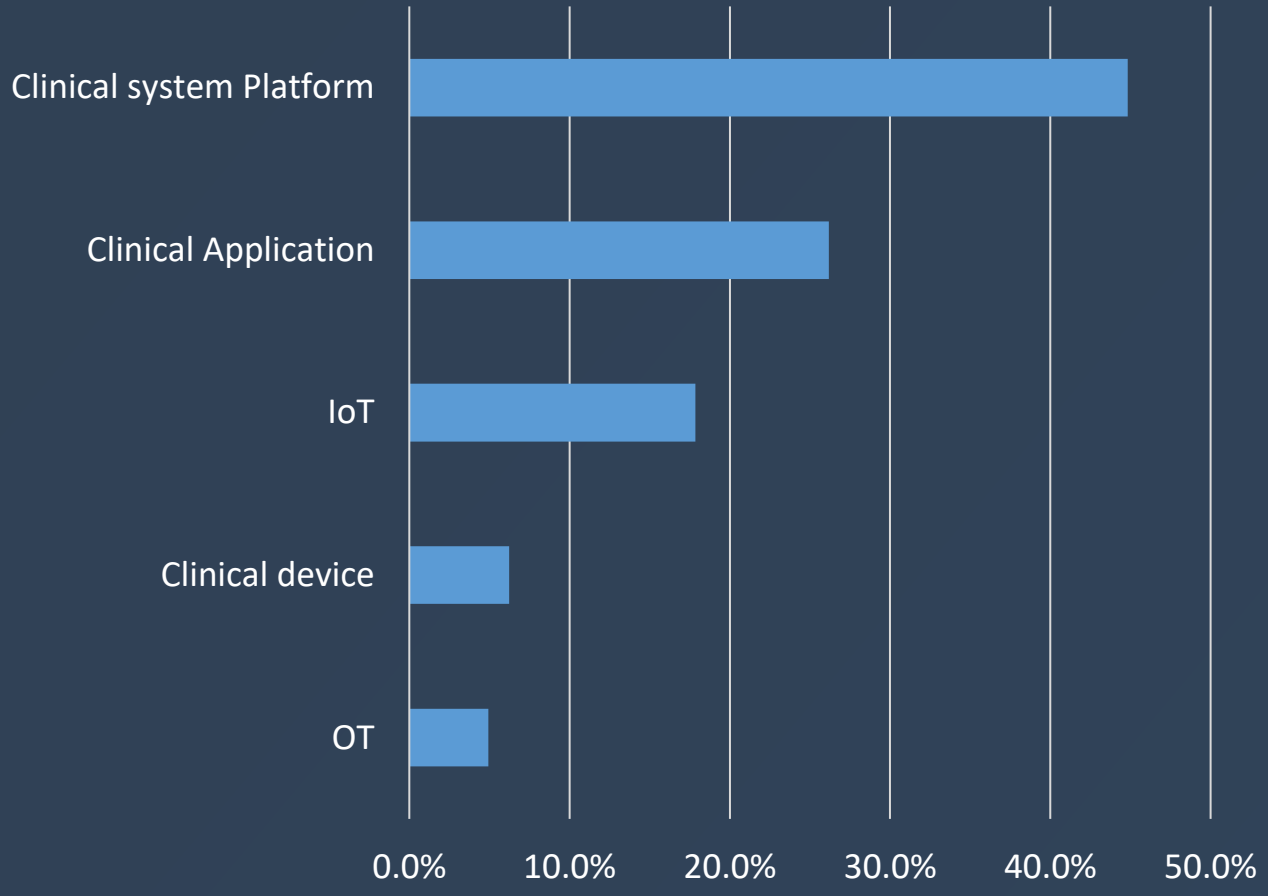
Superficie d’attacco

Dati basati su campione rappresentativo di strutture sanitarie nazionali

Vulnerabilità potenziali	34.880
Vulnerabilità rimediabili	27.000
Vulnerabilità confermate	4.081
Vulnerabilità critiche	476
Dispositivi compromessi	12

Superficie d’attacco - Italia

Sistemi Potenzialmente Vulnerabili



Clinical system platform: piattaforma software che permette l'integrazione di dati clinici provenienti da diverse fonti, facilitando la gestione, l'analisi e l'utilizzo di queste informazioni.

Clinical Application: applicazione software utilizzata dai professionisti sanitari per raccogliere, documentare e gestire informazioni sulle condizioni e i trattamenti dei pazienti.

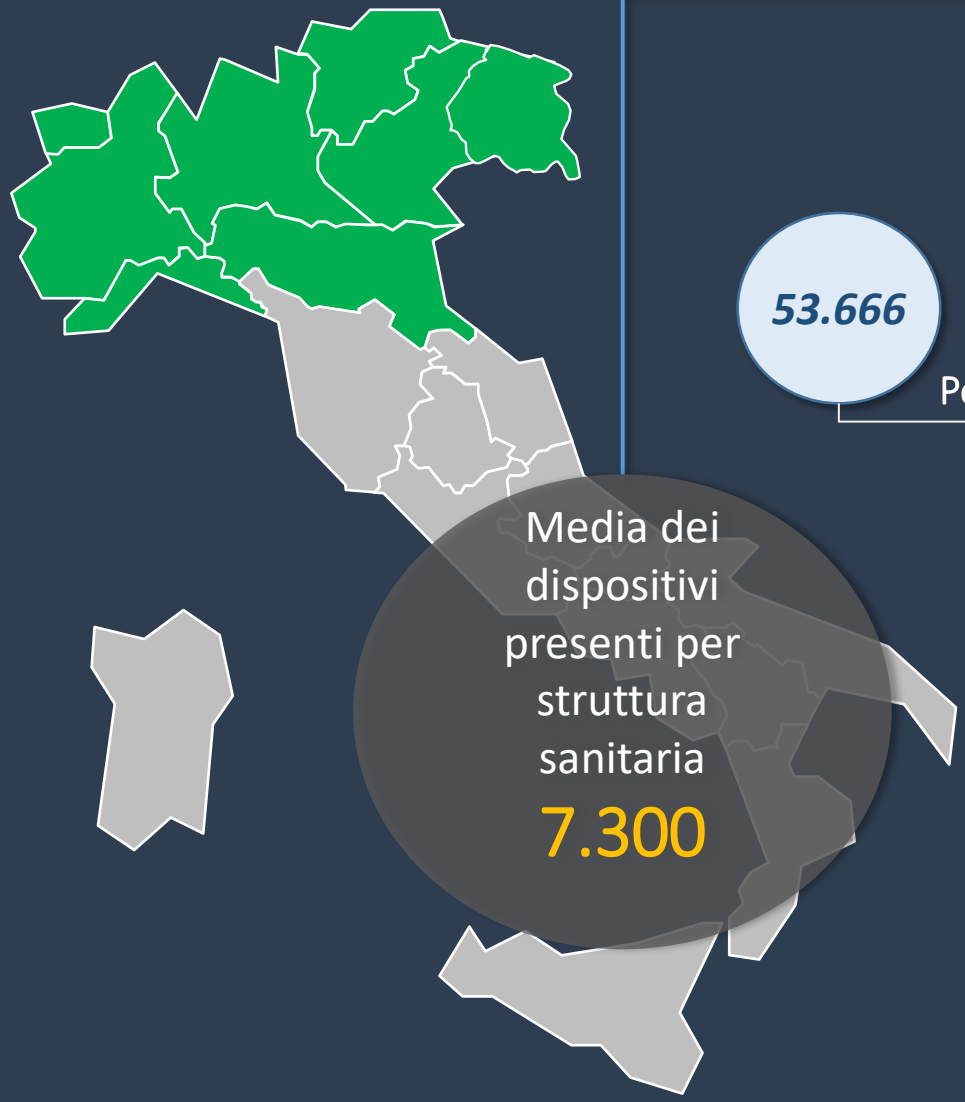
IoT: insieme di dispositivi interconnessi in rete che raccolgono e trasmettono dati per scopi specifici.

Clinical Device: dispositivo medico utilizzato per diagnosticare, trattare o alleviare una malattia o un disturbo medico.

OT: tecnologie utilizzate per gestire e controllare i processi operativi di un'organizzazione, come ad esempio i sistemi di automazione industriale, i sensori e i sistemi di controllo di qualità.

Superficie d'attacco

Nord Italia

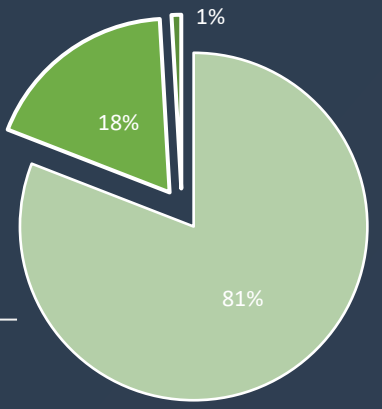


53.666

Potenziali vulnerabilità

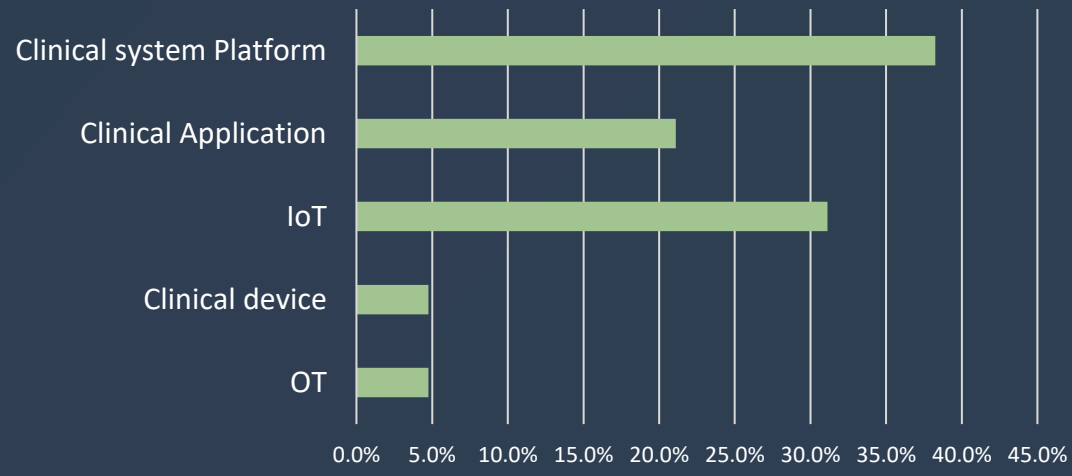
Media dei dispositivi presenti per struttura sanitaria

7.300



Classificazione Vulnerabilità	Nr
• Rimediabili	41.836
• Confermate	6.686
• Critiche	437

Sistemi potenzialmente vulnerabili



Fattori di criticità

La sezione seguente illustra un quadro delle principali vulnerabilità associabili alle piattaforme informatiche, alle applicazioni gestionali, ai dispositivi collegati ad esse e ai protocolli di comunicazione predominanti nell'elaborazione e la ricezione di dati e informazioni sui pazienti, oltre alla trasmissione di dati tra professionisti. Si intende ottimizzare e raffinare l'esposizione di queste criticità al fine di offrire un'analisi professionale e d'impatto.

01 Vulnerabilità Piattaforme

02 Vulnerabilità Applicazioni

03 Vulnerabilità IoMT

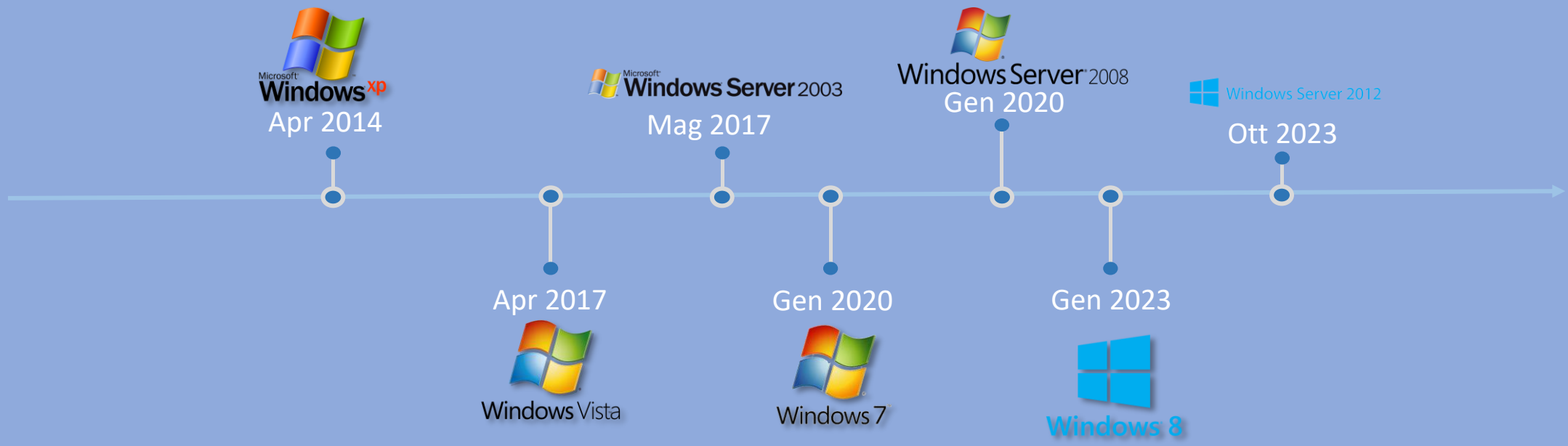
04 Vulnerabilità Device

05 Vulnerabilità Protocolli

Vulnerabilità delle piattaforme

Le versioni deprecate dei sistemi operativi presentano molte vulnerabilità poiché, per esse, i vendor non rilasciano più patch di sicurezza. Questo significa che i bug e le falle non vengono corretti, rendendo questi sistemi operativi vulnerabili agli attacchi informatici.

CVE-2021-24074	**Remote Code Execution**	**9.8**
CVE-2022-21849	**Remote Code Execution**	**9.8**
CVE-2021-26424	**Remote Code Execution**	**9.8**



Almaviva

Vulnerabilità delle applicazioni

CVE-2021-44228	Remote Command Execution	10

Log4j è una libreria Java sviluppata dalla Apache Software Foundation, ampiamente utilizzato nell'assistenza sanitaria e in molti settori. Recentemente, Log4j è stata al centro dell'attenzione a causa di una vulnerabilità che consente l'esecuzione di codice in modalità remota su server vulnerabili.

CVE-2019-7117	Arbitrary Code Execution	9,8

I prodotti Adobe, se non aggiornati, potrebbero consentire ad un possibile attaccante l'esecuzione di codice malevolo all'interno del sistema colpito. La vulnerabilità, causata da una gestione impropria della memoria durante la lettura di documenti PDF dannosi, potrebbe consentire il controllo completo del dispositivo vittima.

CVE-2020-15680	OS Command Injection	9,8

L'utilizzo di un browser come Firefox non aggiornato può consentire a possibili attaccanti di eseguire codice maligno sulla macchina dell'utente. In particolare, la rivelazione del problema è avvenuta su alcune versioni di Firefox che utilizzano la libreria grafica WebRender, in quanto la gestione di determinate condizioni può portare alla generazione di un bug che consente l'esecuzione di codice remoto.

Almaviva

Analisi superficie d'attacco - Vulnerabilità dispositivi

Vulnerabilità dei Dispositivi

Blood Gas System			
Nome Device	CVE	Vulnerability Type	CVSS
SSA-755010	CVE-2018-4845	Remote Command Execution	9.8

Portable Diagnostic Systems			
Nome Device	CVE	Vulnerability Type	CVSS
ICSMA-18-310-01	CVE-2018-17906	Improper Access Control	9.6

Nuclear Medicine			
Nome Device	CVE	Vulnerability Type	CVSS
SHSA-455016	CVE-2022-29875	Remote code execution	9.8

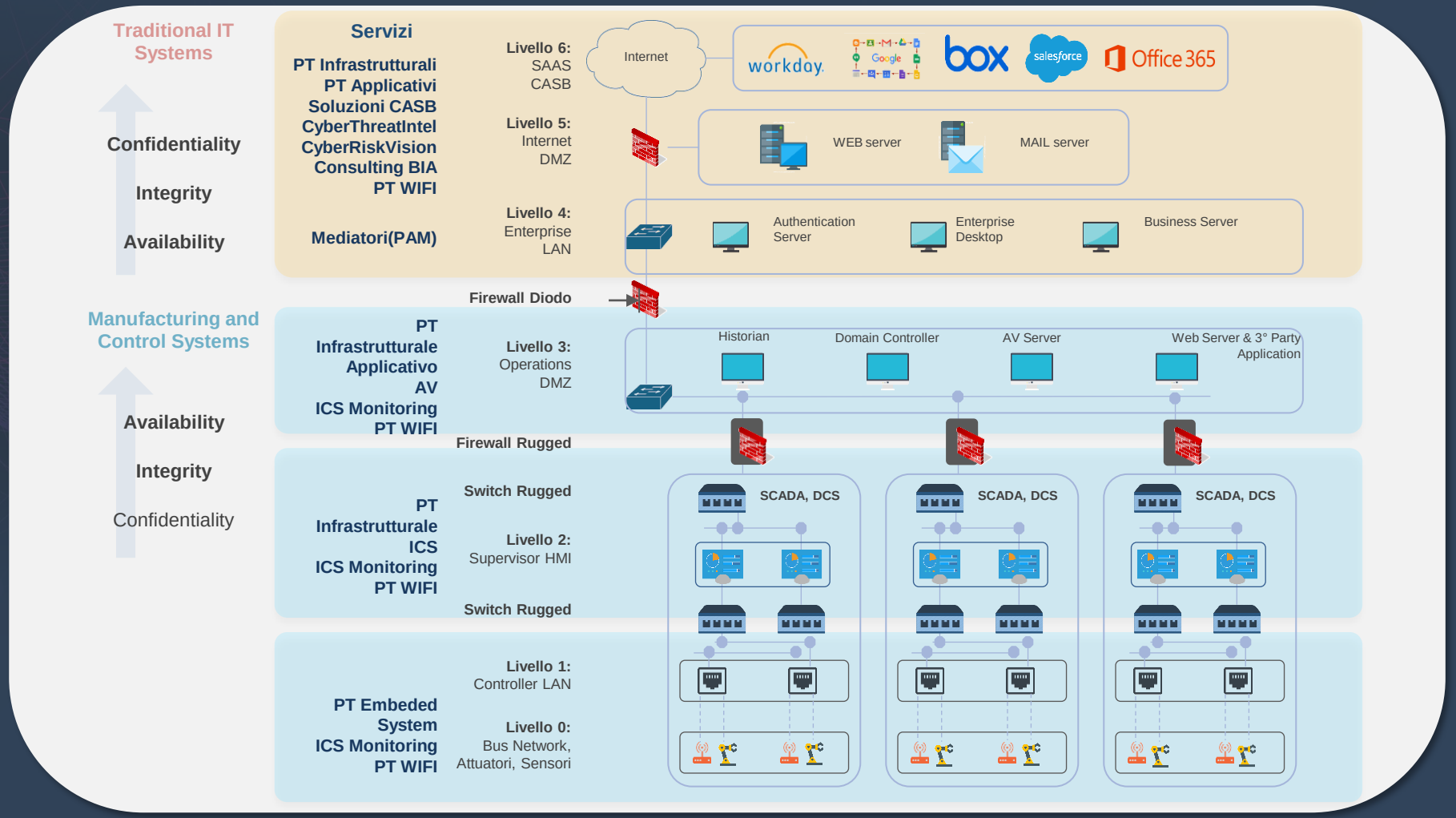
Computed Tomography			
Nome Device	CVE	Vulnerability Type	CVSS
ICSMA-18-123-01	CVE-2018-8857	Unauthorized access	8.8

Imaging Workstation			
Nome Device	CVE	Vulnerability Type	CVSS
ICSMA-18-312-01	CVE-2018-17906	Improper Access Control	8.8

Cosa possiamo fare?

- ✓ Il nostro modello di gestione e contenimento sposa e migliora quanto reso disponibile dall'ISO62443, standard di riferimento in ambito OT security :

- ICS Monitoring
- Privileged Access Management (PAM)
- Fixed Function Security
- Passive Security Assessment
- OT - Software Security Assessment
- OT - Hardware Security Assessment
- Red Teaming




Almaviva
Cyber Security