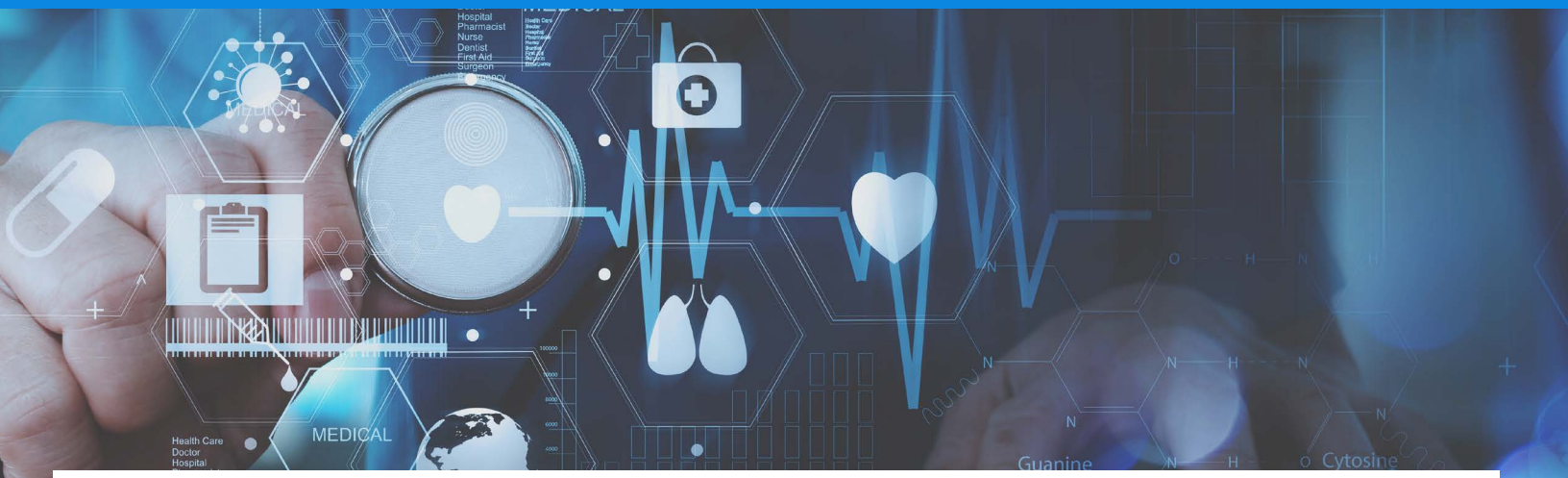

CASE STUDY

INNOVAZIONE DIGITALE E CYBERSICUREZZA ALL'OSPEDALE ISRAELITICO: INTRODOTTO MEDIGATE DI CLAROTY NEI SISTEMI DI PROTEZIONE DELLA INFRASTRUTTURA ICT.

La soluzione è il primo passo verso un progetto globale "health global security", per la messa in sicurezza dell'intero network ospedaliero.

Milano, 14 giugno 2023.

I dati relativi agli attacchi ai danni delle infrastrutture critiche sono sempre più allarmanti, soprattutto quando si parla del settore sanitario. Come confermato anche dal *Rapporto Clusit 2023*, gli ospedali sono uno dei nuovi obiettivi tra quelli maggiormente preferiti dai criminali informatici che, vista la complessità dei propri sistemi operativi e del servizio di prima utilità che erogano verso il cittadino, possono essere certamente annoverati anch'essi tra le infrastrutture critiche più vulnerabili da proteggere.

È proprio in questo contesto che è si inserisce l'innovazione tecnologica introdotta dall'Ospedale Israelitico - una delle strutture sanitarie più antiche di Roma con i suoi oltre 400 anni di storia - che integra la propria infrastruttura IT con soluzioni adeguate e maggiormente performanti a tutela della sicurezza.

"Da sempre la nostra struttura ha dimostrato una spiccata sensibilità verso questo tema ed è per questo che abbiamo maturato sul campo, giorno dopo giorno, la consapevolezza che è necessario avere un approccio alla sicurezza più ampio, che non si limiti alla protezione perimetrale dei dati, degli apparati IT e dei singoli processi gestiti. È indispensabile adottare soluzioni che garantiscano il monitoraggio e una copertura cyber a 360° di tutto ciò che concorre alla erogazione del Servizio di Diagnosi e Cura del Paziente. È necessario sviluppare

soluzioni che siano in grado di rilevare le vulnerabilità e suggerire tempestivamente azioni di 'messa in sicurezza' e protezione delle informazioni che determinano il profilo di salute dei nostri pazienti e soprattutto dei dati che gestiscono le loro terapie. Soluzioni che contribuiscano a salvaguardare in primis la continuità e l'accesso ai servizi non differibili, sempre più digitali, remoti e informatizzati, che offriamo ai cittadini", afferma il Dott. Riccardo Fragomeni - Responsabile dei Sistemi Informativi dell'Ospedale Israelitico.

Durante la fase di *analisi* del mercato, Claroty si è distinta per l'offerta di una soluzione unica, che garantiva full-monitoring, combinando prodotti e servizi in grado di cyber-proteggere sia l'infrastruttura che i processi. Inoltre, la proposta si è presentata assolutamente compatibile ed integrabile con le altre soluzioni e applicazioni operative presso la struttura (CUP, ADT, Registro Operatorio, OE, ecc). Nell'aprile di quest'anno, pertanto, l'Ospedale Israelitico ha implementato Medigate di Claroty, grazie al supporto di un System Integrator titolato e certificato, che è stato in grado di attivare la soluzione configurandole al meglio con le altre componenti di sistema.

Medigate di Claroty, piattaforma di cybersecurity per il settore sanitario, ha consentito all'Ospedale Israelitico di avere piena visibilità sui flussi informativi e di monitorare il corretto funzionamento delle postazioni di lavoro, degli elettromedicali e dei dispositivi wearable dei pazienti e di avere a disposizione un servizio di tipo SOC e SIEM, che si avvale di operatori specializzati nel funzionamento e nella reattività dei processi sanitari per identificarne eventuali anomalie e agire in tempi rapidi. Questa sinergia e interoperabilità con i sistemi ERP, di ausilio anche all'Ingegneria Clinica e le altre soluzioni poste a difesa cyber del network ospedaliero, si è rivelata fondamentale per l'implementazione di un sistema di monitoraggio e protezione proattivo, innovativo e all'avanguardia.

La soluzione di Claroty ha, inoltre, permesso al nosocomio ebraico di gestire in modo centralizzato, con cruscotti facili ed intuitivi, le attività e i volumi di produzione dei *devices medicali* collegati alla rete. Questo ha consentito di cambiare totalmente la modalità di interazione con le macchine e di semplificare la gestione dell'operatività dei sistemi e degli *end-point*. Attraverso una *dashboard* completamente user *friendly*, infatti, ogni operatore è in grado di monitorare, in real-time, tutti i sistemi e i processi di competenza, come il rilevamento di eventuali anomalie nelle strumentazioni, il monitoraggio del loro livello di produttività sulla base agli obiettivi preposti e il loro ciclo di vita per preventivare aggiornamenti straordinari. In questo modo è possibile intervenire tempestivamente per prevenire o arginare il problema.

A un mese dall'implementazione, l'Israelitico ha già riscontrato dei risultati più che positivi. Questi dati hanno permesso di pensare già a un'evoluzione futura della soluzione di sicurezza, in un'ottica di "Health Global Solution", ovvero di disporre grazie al progetto HGS di una ulteriore protezione delle cinque sedi del gruppo ospedaliero. La piattaforma Medigate di Claroty, infatti, inserita nel framework HGS, dà la possibilità di innestare nuovi algoritmi e appliance per il monitoraggio dei flussi informativi degli ambienti, delle sale di attesa, dei varchi di accesso, dei processori dei server, oltre a quelli provenienti dai medicali e dai dispositivi indossati dei pazienti allettati. Un nuovo concetto di sicurezza, appunto, 'GLOBALE'. Sarà possibile monitorare ad esempio, grazie a mappe di calore elaborate in *real-time*, il livello di criticità, di sovraffollamento o esagitazione, presente nelle sale d'attesa dell'ospedale. Oppure intercettare nei dialoghi tra l'operatore del call center e l'utente, parole chiave che manifestano chiaramente delle minacce. L'obiettivo finale è costruire una soluzione unica, un framework centralizzato di monitoraggio e di conseguente protezione di altissimo profilo, che adiuvata da algoritmi di *machine learning e intelligenza artificiale*, permetta non solo di analizzare i dati in modo preciso e puntuale, ma di attivare automatismi per l'attivazione di azioni di *remedations* automatiche e semiautomatiche di supporto all'intervento dei tecnici del settore.

"La grande esposizione delle strutture sanitarie ai rischi cyber, e a quelli legati alla sicurezza in generale, ci ha spinto verso questa soluzione e ci ha mosso ad avviare d'intesa con altre strutture, un progetto evolutivo alimentato da un concetto di sicurezza che definiamo a 'geometria variabile'. Avevamo bisogno di una soluzione che ci permettesse di migliorare la nostra capacità di reazione in caso di attacco. Un framework grazie al quale essere sempre pronti a raccogliere le mutevoli informazioni sul campo che manifestano possibili vulnerabilità. Non sempre, infatti, si ha la possibilità di conoscere il problema in tempo e di reagire in maniera immediata alle nuove e sofisticate minacce introdotte dai criminali, anche per una mancanza di competenze mirate. Sappiamo infatti che una corretta protezione cyber si fonda su tre capacità di management, bisogna essere: predittivi, preventivi e proattivi. Claroty ci ha permesso non solo di includere questi tre elementi in un'unica soluzione, ma di ampliare ulteriormente la visione della sicurezza, lavorando sul concetto di ciclicità. È fondamentale analizzare ciò che è successo, decodificare gli eventi, effettuare l'analisi della situazione e della vulnerabilità riscontrate e misurare sempre l'efficacia dell'azione intrapresa. HGS si pone questo obiettivo. Solo in questo modo è possibile migliorare la difesa, diminuire i tempi di reazione e aumentare la capacità di resilienza della propria infrastruttura IT al fine di garantire la continuità dei servizi IT in risposta agli eventi avversi", ha spiegato Riccardo Fragomeni.

"La fiducia accordataci dall'Ospedale Israelitico è stata per noi un'ulteriore conferma della qualità e dei vantaggi che le nostre soluzioni possono offrire alle infrastrutture critiche, in particolare nell'Healthcare. L'evoluzione dell'Extended Internet of Things (XIoT) ha ampliato notevolmente l'efficienza e i vantaggi in termini di prestazioni delle aziende del settore sanitario, ma ha inevitabilmente portato alla luce nuovi rischi informatici che devono necessariamente essere arginati. Le aziende sanitarie sono pertanto chiamate a mettere in campo azioni mirate per proteggere i propri sistemi e salvaguardare la salute dei propri pazienti da eventuali minacce esterne. Questo è ciò che stiamo facendo con L'Ospedale Israelitico di Roma, con un occhio già proteso verso gli sviluppi futuri che aiuteranno la struttura a espandere e migliorare ulteriormente la messa in sicurezza di tutti i propri sistemi e apparati", ha dichiarato Alessandro Battella, Channel Manager Italia, Malta, Grecia e Cipro di Claroty.

Claroty

Claroty è specializzata in soluzioni di sicurezza volte a proteggere i sistemi cyber-fisici in ambienti industriali (OT), sanitari (IoMT) e aziendali (IoT): il cosiddetto Extended Internet of Things (XIoT). La piattaforma unificata dell'azienda si integra con l'infrastruttura esistente dei clienti per fornire una gamma completa di controlli per la visibilità, la gestione dei rischi e delle vulnerabilità, il rilevamento delle minacce e un accesso sicuro da remoto. Supportate dalle più grandi società di investimento e provider di automazione industriale del mondo, le soluzioni Claroty vengono distribuite da centinaia di organizzazioni in migliaia di siti in tutto il mondo. La società ha sede a New York e filiali in Europa, Asia-Pacifico e America Latina. Per maggiori informazioni: www.claroty.com

Ufficio Stampa

Meridian Communications Srl
Via Cuneo, 3 – 20149 Milano Tel. +39 02 48519553

Silvia Ceriotti	335 7799816	silvia.ceriotti@meridiancommunications.it
Viviana Bandieramonte	329 4776937	viviana.bandieramonte@meridiancommunications.it
Ilaria Malgrati	339 2143042	ilaria.malgrati@meridiancommunications.it