CLAROTY ANNUNCIA LA RELEASE DI ADVANCED ANOMALY THREAT DETECTION DI MEDIGATE PER POTENZIARE GLI STANDARD DI SICUREZZA INFORMATICA DELLE AZIENDE DEL SETTORE SANITARIO.

Questa nuova funzionalità garantisce una maggiore conoscenza nel rilevamento delle minacce nel contesto clinico, per il monitoraggio continuo dei rischi della rete sanitaria.

Milano, 19 marzo 2024 – Claroty, azienda specializzata nella protezione dei sistemi cyber-fisici, annuncia la release del modulo Advanced Anomaly Threat Detection (ATD) per la piattaforma Medigate. La nuova funzionalità offre alle organizzazioni sanitarie una panoramica del contesto clinico per identificare, valutare e dare priorità alle minacce rivolte ai dispositivi medici connessi, all'IoT e ai sistemi di gestione degli edifici (BMS).

Le funzionalità del modulo ATD avanzato sono basate sulla conoscenza specializzata di Claroty degli ambienti sanitari e sulla visibilità approfondita e fondamentale dei dispositivi CPS, tra cui:

- Contesto e rilevamento delle minacce in ambito clinico, senza agent, per affrontare gli indicatori noti di compromissione in CPS;
- Rilevamento delle minacce a livelli più profondi della rete clinica oltre che nelle aree in cui vengono implementate soluzioni firewall;
- Monitoraggio continuo delle misure di rafforzamento della comunicazione tra i dispositivi e dei controlli di conformità.

Secondo quanto affermato dalla rete di cliniche tedesche Ortenau Klinikum, grazie al modulo ATD avanzato, "*ora abbiamo visibilità di cosa accade sulla nostra rete in ogni momento. Soprattutto quando si parla dei dispositivi medici, ciò che un tempo era solo un quadro poco definito è ora diventato chiaro, trasparente e di qualità*".

Con l'aumento della connettività all'interno degli ambienti sanitari, gli attacchi informatici stanno diventato sempre più frequenti anno dopo anno, colpendo principalmente i dispositivi medici e i BMS che servono a mantenere in funzione l'attività ospedaliera. Secondo il Global Healthcare Cybersecurity Study 2023 di Claroty, il 78% delle organizzazioni sanitarie ha subito almeno un incidente legato alla sicurezza informatica nell'ultimo anno e il 60% di questi ha avuto un impatto grave o moderato sull'erogazione dell'assistenza sanitaria ai pazienti.

Non solo la proliferazione degli attacchi ha spinto le organizzazioni sanitarie ad adottare strumenti di sicurezza informatica avanzati, ma anche il contesto normativo in continua evoluzione sta contribuendo a guidare il cambiamento. Il Department of Health and Human Services (HHS) degli Stati Uniti, ad esempio, ha recentemente pubblicato gli Healthcare and Public Health (HPH) Cybersecurity Performance Goals (CPGs) che includono misure specifiche per rilevare e rispondere a minacce, tattiche, tecniche e procedure rilevanti (TTP), per "*assicurare alle organizzazioni la consapevolezza e la capacità di individuare minacce rilevanti e TTP sugli endpoint*" e per "*garantire che le aziende siano in grado di difendere gli entry ed exit point della rete grazie alla protezione degli endpoint*".

Il modulo ATD avanzato di Claroty consente alle strutture sanitarie di rafforzare la propria sicurezza informatica e ottenere la conformità normativa necessaria con funzionalità quali:

- **Il Signature-based detection** migliora il rilevamento, l'analisi e la risposta delle minacce sulla base di firme e indicatori di compromesso (IoC) noti. Il contenuto della firma può essere visualizzato a scopo di indagine e abilitato o disabilitato, a seconda delle necessità, per ottimizzare il sistema.
- **Gli avvisi di comunicazione personalizzati** comprendono e analizzano i modelli di comunicazione dei dispositivi attraverso la rete per identificare comportamenti anomali e il traffico tra i dispositivi connessi, come ad esempio un BMS che comunica con una rete guest o un dispositivo IoMT che utilizza un protocollo non protetto.
- **Gli avvisi di modifica del dispositivo** individuano, per effettuare ulteriori indagini, i cambiamenti significativi relativi ai dispositivi all'interno degli ambienti sanitari. Un esempio si ha quando un dispositivo riappare dopo essere stato offline per un periodo prolungato e questo porta a un cambiamento significativo nella profilazione del rischio o a una modifica dello stato della rete.
- **La mappatura delle minacce MITRE ATT&CK for Enterprise** fornisce ulteriori informazioni sul contesto e sulla correzione mappando gli avvisi su varie tattiche e tecniche all'interno del framework MITRE ATT&CK. Ciò aiuta gli operatori a comprendere meglio gli obiettivi dei malintenzionati per rispondere in modo rapido e appropriato e semplificare i processi, allineandosi a un framework che potrebbero essere già in uso.

"*Le organizzazioni sanitarie stanno affrontando da anni una dura battaglia contro la minaccia, sempre più incombente, degli attacchi ransomware. Gli attacchi informatici contro i dispositivi clinici e le risorse OT delle aziende del settore, infatti, hanno conseguenze concrete sull'assistenza ai pazienti*", ha affermato **Grant Geyer, Chief Product Officer di Claroty**. "*Le funzionalità offerte dal nostro modulo ATD avanzato aiutano le organizzazioni sanitarie a compiere un passo fondamentale verso il raggiungimento della piena visibilità delle risorse, con una comprensione approfondita e una visione trasparente delle principali minacce. Quando sono coinvolti i flussi di lavoro clinici e la cura del paziente, non c'è spazio per punti ciechi*".

La release del modulo ATD avanzato di Claroty per la piattaforma Medigate arriva in concomitanza con una nuova ricerca condotta da Team82, il pluripremiato team di ricerca di Claroty, che ha rilevato come le aziende sanitarie debbano far fronte a profonde lacune nella sicurezza dei dispositivi medici. Questa nuova ricerca è contenuta nel "The State of CPS Security Report: Healthcare 2023".

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