



CLAROTY E AXONIUS COLLABORANO PER ESTENDERE LA GESTIONE DELLA PROTEZIONE DELLA SUPERFICIE DI ATTACCO DEI SISTEMI CYBER-FISICI.

La soluzione combinata consente alle aziende di proteggere l'intera superficie di attacco su risorse cloud, IT e XIoT.

Milano, 3 aprile 2024 - [Claroty](#), azienda specializzata nella protezione dei sistemi cyber-fisici (CPS), e Axonius, leader nella gestione delle risorse di sicurezza e nella gestione SaaS, hanno recentemente siglato una partnership che unisce le rispettive tecnologie per estendere la gestione della superficie di attacco a tutte le risorse presenti sulle reti aziendali, inclusi IT, cloud ed Extended Internet of Things (XIoT), la vasta rete di CPS tra cui OT, IoT, BMS e IoMT.

Combinando la conoscenza di Claroty degli ambienti CPS alle oltre 1.000 integrazioni offerte da Axonius, che si estendono anche al cloud, i clienti possono finalmente ottenere una visione e un profilo unificati di tutte le risorse presenti nei diversi ambienti. Inoltre, l'unione delle due piattaforme permette di effettuare una profilazione delle vulnerabilità, di monitorare l'esposizione della superficie di attacco e di gestire tale esposizione grazie a misure protettive e controlli di accesso, che consentono di limitare e segmentare la comunicazione di rete consentita, favorendo una risposta intelligente e tempestiva in caso di incidenti.

*"Siamo entusiasti di collaborare con Claroty per offrire alle aziende un sistema di registrazione unificato per la gestione dei dati, finalizzato alla protezione dell'infrastruttura digitale", ha affermato **Mark Daggett, Vice President of Worldwide Channel Alliances di Axonius.** "Insieme siamo in grado di fornire un inventario completo ed esauriente delle risorse, utile a migliorare i controlli effettuati dalle aziende per raggiungere un obiettivo chiave della propria strategia di sicurezza: la riduzione dei rischi".*

L'integrazione delle piattaforme Claroty e Axonius offre alle aziende tutti gli strumenti di cui hanno bisogno per ridurre i rischi e raggiungere la resilienza informatica. Questo permetterà loro non solo di far fronte a condizioni informatiche avverse, ma anche di prosperare nonostante esse. Le aziende saranno così ben protette e preparate a qualsiasi tipo di emergenza, dai ransomware agli attacchi alla supply chain, fino alle minacce interne. In questo modo, potranno sposare la trasformazione digitale e gli innegabili vantaggi dell'XIoT in modo protetto e sicuro.



*“In un’era caratterizzata dal lavoro da remoto, tecnologia mobile 5G di nuova generazione e un vasto panorama di attacchi informatici, che spaziano dai dispositivi on-premise ai servizi cloud, capire esattamente cosa comprende la propria infrastruttura connessa e iperconvergente è più impegnativo e critico che mai”, afferma **Stephan Goldberg, Vice President of Business Development di Claroty.** “La combinazione dell’impareggiabile competenza di Claroty negli ambienti CPS, delle loro applicazioni aziendali e delle caratteristiche tecnologiche con la capacità di Axonius di fornire un contesto di livello Business a tutte le risorse, dal cloud all’on-premise, offre una visione olistica di tutte le risorse connesse, delle vulnerabilità e della superficie di attacco dinamica, comprese le diverse esposizioni, differente da qualsiasi altra proposta presente oggi sul mercato”.*

Maggiori informazioni su Claroty e Axonius sono disponibili al seguente [integration brief](#).

About Axonius

Axonius gives customers the confidence to control complexity by providing a system of record for all digital infrastructure. With a comprehensive understanding of all assets including devices, identities, software, SaaS applications, vulnerabilities, security controls, and the context between all assets, customers are able to mitigate threats, navigate risk, decrease incident response time, automate action, decrease costs and eliminate waste, and inform business-level strategy — all while eliminating manual, repetitive tasks. Recognized as creators of the Cyber Asset Attack Surface Management (CAASM) category and innovators in SaaS Management Platform (SMP) and SaaS Security Posture Management (SSPM), Axonius is deployed in minutes and integrates with hundreds of data sources to provide a comprehensive asset inventory, uncover gaps, and automatically enforce policies and automate action. Cited as one of the fastest-growing cybersecurity companies in history, with accolades from Deloitte, CNBC, Forbes, and Fortune, the Axonius Platform covers millions of assets for customers around the world.

Claroty

Claroty è specializzata in soluzioni di sicurezza volte a proteggere i sistemi cyber-fisici in ambienti industriali (OT), sanitari (IoMT) e aziendali (IIoT): il cosiddetto Extended Internet of Things (XIIoT). 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