Contact:
Jenna Finn
Shift PR for Claroty
jfinn@shiftcomm.com
617.779.1875

Claroty Extends Visibility of Market-Leading Industrial Cybersecurity Platform to the Internet of Things

New IoT-OT visibility and security monitoring solution combines machine learning, behavioral analytics, and threat intelligence to contextualize and enrich alerts for large industrial enterprises.

NEW YORK, July 17, 2019 – Claroty, the global leader in industrial cybersecurity, today introduced several enhancements to Continuous Threat Detection (CTD), its award-winning operational technology (OT) security solution. The latest release of CTD now enables enterprises to discover and monitor their Internet of Things (IoT) devices, provides customers with greater network visibility, reduces deployment time, and eliminates the "noise" of non-critical alerts. The company also announced it has joined the Industrial Internet Consortium® (IIC™), the world's leading organization transforming business and society by accelerating the adoption of the Industrial Internet of Things (IIoT).

Claroty's announcements come as enterprises increase their use of IoT devices to drive digital transformation and increase the efficiency of their operations. Gartner Research has forecasted more than 65% of enterprises will adopt IoT products by 2020.

With the latest update to CTD (version 3.5), customers now enjoy all the benefits of Claroty's deep packet inspection technology across both IoT and OT devices. The solution automatically discovers IoT devices on the network and classifies each device based on both static and behavioral attributes. It then identifies known vulnerabilities and other risks associated with those assets, and continuously monitors the environment for threats and policy violations.

The new IoT functionality is part of a broader update to the Claroty CTD product. Other enhancements include:

Machine Learning Alert Algorithm – Optimizes signal-to-noise ratio by correlating all events on the network with online patterns and communication behaviors, prioritizing high-fidelity alerts worthy of investigation.

Root Cause Analytics — Contextual data and visualization tools illustrate the precise chain of events that triggered an alarm and help improve the speed, efficiency, and accuracy of incident response and threat hunting.

Claroty Threat Intelligence – Highly-curated and multi-source feeds enrich CTD's analytics with proprietary research of zero-day vulnerabilities and IoT and OT-specific indicators of compromises linked to threat actors' tactics, techniques, and procedures.

Virtual Zones+ — Automatically groups together network assets with similar behaviors and attributes. Once grouped, CTD identifies the relationship between the logical groups and automatically generates granular communication policies. The policies assign permission levels to each zone, along with a specific level of trust to help the end-user understand the risk posed by every logical connection between the zones.

Expanded Technical Ecosystem — As part of Claroty's expanding technology ecosystem, Continuous Threat Detection now integrates with the Aruba ClearPass network access control platform and Fortinet's Fortigate next-generation firewalls.

To further support the secure growth of IoT devices within the enterprise, Claroty also announced it has joined the Industrial Internet Consortium, a leading industry group whose mission is delivering a trustworthy IIoT in which the world's systems and devices are securely connected and controlled to deliver transformational outcomes. As a consortium member, Claroty will help in the organization's effort to drive a common security framework and a rigorous methodology to assess security in industrial internet systems.

Quotes:

Amir Zilberstein, CEO, Claroty

"Claroty's natural expansion into the IoT space enables us to empower customers with an unparalleled breadth and depth of visibility across their networked OT and IoT environments," said Amir Zilberstein, CEO of Claroty. "Leveraging our comprehensive IoT-OT platform, customers can now embrace digital transformation initiatives with a higher level of confidence than ever before."

Dr. Richard Soley, Executive Director, Industrial Internet Consortium

"With the number of connected IoT devices in a manufacturing facility, cybersecurity has become as important to industrial companies as worker safety and productivity," said Dr. Richard Soley, Executive Director, IIC. "We look forward the contributions Claroty will make in cybersecurity as a member of the IIC as we work together to establish a secure IIoT."

About Claroty

Headquartered in New York and launched as the second startup from the famed Team8 foundry, Claroty combines elite management and research teams with deep technical expertise from both IT and OT disciplines. The company is backed by an unrivaled syndicate of investors and partners, including some of the most important industrial control automation companies and asset owners on earth. With an unmatched understanding of ICS, SCADA and other essential OT/IIoT systems, Claroty built a fully integrated cybersecurity platform. Our award-winning suite of products provides extreme visibility into industrial networks – enabling unparalleled cyberthreat protection, detection and response. For more information, visit www.claroty.com.

###