Contact:
Carro Halpin
CHEN PR for Claroty
781-672-3132
chalpin@chenpr.com

Claroty Advances the State-of-the-Art in Industrial Control Systems Security

New Security Posture Assessment product combined with extensive new vulnerability and network hygiene monitoring and attack vector analysis capabilities update the industry's most comprehensive ICS cybersecurity platform

ARC INDUSTRY FORUM ORLANDO 2018 and NEW YORK, February 14, 2018 – Claroty, an innovator in operational technology (OT) network protection, today announced a new Security Posture Assessment product and significant enhancements to its award-winning Continuous Threat Detection product. Already the industry's most complete ICS cybersecurity platform, this release incorporates real-time vulnerability monitoring and network hygiene insights with attack vector analysis, enabling industrial asset owners to fully protect expensive, revenue-generating industrial systems from rapidly growing threats. The announcement was made in conjunction with ARC Industry Forum Orlando 2018 taking place this week.

From US-CERT to the UK's National Cyber Security Centre warnings and from ransomware to recent attacks on industrial safety systems, the exposure and probing of industrial control systems (ICS) is getting more urgent and concerning each day. C-suites and board members are taking notice and CISOs are becoming accountable, but protecting the networks that underpin critical industrial systems requires a comprehensive approach.

"Security teams simply don't have the time or resources to knit together point products to protect their most important industrial assets from cyberattacks," noted Dr. Benny Porat, CTO and co-founder of Claroty. "We set out to build a comprehensive integrated suite of products designed specifically for protecting industrial networks. We were the first to combine extremely deep, end-to-end visibility into industrial networks with safe, passive threat monitoring. With today's release, security and consulting teams can rapidly assess the security posture of industrial networks, and we have enabled customers to continuously monitor for new vulnerabilities and analyze pathways to their most important assets."

These products are all part of the **Claroty Platform** and built on Claroty's advanced **CoreX** engine. This fully integrated platform is unparalleled in its depth, coverage and scalability. It provides:

- **Real-time Threat Detection** including advanced anomaly and signature-based detection for complete coverage of known and unknown threats, and analysis tools for ICS threat hunting.

- **Continuous Vulnerability Monitoring** enabling customers to uncover and remedy network configuration "hygiene" issues and identify assets with known vulnerabilities (CVEs).
- **Secure Remote Access** with policy- and workflow-based access control and session monitoring.
- **Enterprise Scalability** including a consolidated "single pane of glass" management console for multiplant environments and integration with existing security systems (e.g., SIEM, log management, security analytics, etc.).
- **Cost-effective Deployments** in remote, bandwidth- or compute-constrained environments, leveraging an advanced sensor-based architecture suitable for use cases such as electric transmission or oil/gas pipelines.

The new **Security Posture Assessment** product is ideal for both consulting and security teams who want to conduct a quick but comprehensive assessment of a plant or operational environment. This new software product ingests a network capture (PCAP) file and generates a comprehensive report detailing the industrial network, its assets, and deep insights including network configuration and other weaknesses.

The new release of Claroty Continuous Threat Detection (Version 2.1) includes a large number enhancements including:

- **Continuous Monitoring for Vulnerabilities and Network Hygiene Issues** – Leveraging the same CoreX engine capabilities as Security Posture Assessment, customers receive real-time updates about industrial assets with known vulnerabilities. The system provides fine-grained CVE matching – for example, down to the firmware version on controllers – so that customers don't waste time on vulnerabilities that don't apply to their specific environment. This new capability also includes ongoing detection of network configuration issues and other "network hygiene" weaknesses that can leave industrial networks exposed.

- **OT Attack Vector Analysis** – A completely new ability to generate specific scenarios simulating possible attack vectors that have the potential of compromising critical OT assets. This empowers security teams with the visibility to proactively mitigate risk and prioritize activities along the paths of greatest potential impact to their processes.

- **Enhanced Threat and Vulnerability Intelligence** – Claroty Research continues to expand its curated intelligence, adding to its knowledge base of indicators of compromise (IOCs) and ICS-specific vulnerabilities. This comprehensive threat and vulnerability feed enables improved detection, more precise threat identification, rapid situational awareness and up-to-date information about the latest weaknesses in industrial devices.

The release of this latest version of the Claroty Platform is generally available to all existing clients as of the time of this announcement.

About Claroty
Launched as the second startup from Israel's famed Team8 foundry, Claroty combines elite management and research teams and deep technical expertise from both IT and OT disciplines, with backing from premier investors such as Bessemer Venture Partners and Innovation Endeavors. With an unmatched understanding of ICS, SCADA and other essential OT/IIoT systems, the Claroty team is

building an unparalleled suite of integrated products addressing the full spectrum of cybersecurity protection, detection and response requirements. For more information, visit www.claroty.com.

###

All product and company names herein may be trademarks of their respective owners.