Claroty Delivers Groundbreaking Protection for Industrial Networks

The Claroty Platform Provides Extreme Visibility across ICS Layers/Protocols; High-Fidelity Models and Advanced Algorithms Detect both Cybersecurity Threats and Process Integrity Issues

NEW YORK – September 13, 2016 – Claroty, an innovator in Operational Technology (OT) cyber threat protection, today announced a groundbreaking new platform that ensures the highest levels of security and reliability for the networks that are running the world's critical industrial systems. The Claroty Platform provides extreme visibility into industrial control system (ICS) networks. With the broadest support for control system manufacturers and deepest inspection of protocols available in the market, the platform employs high-fidelity models and advanced algorithms to monitor ICS communications and provide security and process integrity alerts. This unmatched visibility enables organizations to discover hidden problems in OT networks, protect critical systems against cyberthreats and fix issues that impact process integrity and performance.

In a separate release, the company also announced its initial funding and executive team. *(See: Claroty Exits Stealth with $32 Million in Funding to Protect Industrial Networks)*

"Marker LLC and Innovation Endeavors looks to invest in companies that can drive transformative change, not incremental improvement," said Yuval Shachar, partner at Marker LLC and Innovation Endeavors. "As we make all manner of critical infrastructure more connected and 'smarter,' we have opened a Pandora's box with regards to cybersecurity. The Claroty team has developed advanced technology to protect these critical networks and is establishing a foundation for what will be one of the next major pillars in the cybersecurity marketplace."

Meir Ukeles, partner at ICV and chairman of Claroty's board, added, "Industrial operations are becoming networked operations across every segment of industry, infrastructure and manufacturing. The benefits of this connectivity are too great to ignore, but the challenge is to enjoy the benefits without compromising the resiliency of operations and the security of core assets. Claroty enables its customers to get the most from their networked operations in a secure and dynamically manageable manner."

From the Ukraine power grid attacks to a German steel mill, examples of critical infrastructure compromises are growing every day – in some cases being discovered or revealed years after the fact. While "cyberwar" and kinetic nation-state attacks grab headlines, there are many other threats to OT infrastructures that tend to be overlooked and can be just as damaging – from competitive sabotage, to IP theft or espionage, and even human errors that can severely impact systems and the critical production processes they support. Further, recent reports show a precipitous rise in ICS vulnerability reporting. This increasing risk is driving the need for deeper insight and specialized products for OT security.

“Industrial control systems are very different from traditional business IT. These unique environments require security tools that have a deep understanding of ICS devices and protocols and are designed not to break the critical processes they are being used to secure,” noted Eric Cosman, a pioneer in the ICS cyber industry and co-chair of the ISA99 Committee. “I have been very impressed with the visibility the Claroty Platform provides into activities that could represent a potential threat, and other control system changes that can impact key processes.”

The Claroty Platform was born from deep expertise in both industrial control systems and cybersecurity. It was designed from the ground up with an unprecedented ability to safely monitor ICS, SCADA and other critical OT networks, uncover previously hidden issues and alert cybersecurity teams and system operators to malicious attacks and process integrity issues.

Claroty Advantages:

- Deepest Visibility – Unlike tools that only cover control system assets in Level 3 and 4 of the Purdue Enterprise Reference Architecture, the Claroty Platform provides unparalleled visibility into assets and communications across each level of the OT environment.
- Broadest Coverage – Claroty inspects the largest number of industrial control protocols, with support for both open and proprietary protocols from vendors including Siemens, Rockwell Automation/Allen Bradley, Yokogawa, Emerson, GE, Schneider Electric, Mitsubishi, Honeywell, ABB and more.
- Real-Time Monitoring – Claroty constantly monitors all communication within an industrial control network, in contrast to other tools that use periodic queries that can easily miss significant network events or important changes to critical assets.
- Superior Anomaly Detection – With this extreme visibility, Claroty is able to create high-fidelity models and employ advanced behavioral algorithms to detect potential attacks and noteworthy changes that can adversely impact operations – including a variety of security attacks and environmental changes that could harm system integrity or damage industrial processes.
- “Do No Harm” Passive Monitoring Approach – Unlike other tools that use “active” queries or simply have blind spots at the lower OT layers, Claroty employs “passive” deep packet inspection (DPI) that is safe for all devices within OT environments.
- Enterprise Scalability – Optimized for complex, real-world OT networks that often have constrained bandwidth or even unreliable network links. The system also features an enterprise console that consolidates information from multiple geographically distributed sites.

The power and insight of the Claroty Platform is supported by the world-class Claroty Research Team and more than 45 experts hailing from world-renowned ICS, SCADA and cybersecurity vendors. The Claroty Platform is generally available and the team has sold and implemented the system for multiple, complex enterprise-class customers. In April, the Claroty Platform was recognized by Gartner as a “Cool Vendor” in its publication *Cool Vendors in Smart City Application Solutions, 2016*.

“We are using Claroty to add security monitoring to our control systems around the world – an important part of our business where security was not previously thought of or architected in,” noted a CISO from a global Fortune 100 organization. “We selected Claroty to give us greater visibility into the shop floor environment – both the assets that are there and the activities taking place. Equipped with this additional visibility we are able to increase productivity and make process improvements in addition to enhance security.”

About Claroty

Launched as the second startup from Israel’s famed Team8 foundry, Claroty combines an elite management team 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 systems, the Claroty Platform provides the deepest and broadest coverage of ICS systems, protocols and networks available on the market today. For more information, visit www.claroty.com.

###