Claroty Significantly Strengthens its Industry-Leading OT Security Platform

Enhanced Continuous Threat Detection and Secure Remote Access provide enterprises with comprehensive visibility, threat detection, vulnerability management, and triage & mitigation controls for industrial environments

Claroty, the global leader in industrial cybersecurity, today announced it has strengthened the Claroty Platform to deliver the industry's broadest range of operational technology (OT) security controls in a single solution, thereby empowering enterprises to more easily and effectively reduce risks posed by increasing connectivity between OT and information technology (IT) networks. "Enterprises have been transformed through digitisation initiatives, causing once-isolated OT networks to be interconnected with the rest of the enterprise. However, those OT networks remain invisible to security teams since they communicate on proprietary protocols and have very different characteristics than IT networks," said Galina Antova, Co-founder of Claroty. "The Claroty Platform extends core security controls to OT environments, thereby closing the 25-plus year gap between the security posture of IT and OT networks, and delivering comprehensive governance and risk reduction across the parts of enterprise networks that were previously invisible and unsecured." Enriched by newly enhanced Continuous Threat Detection (CTD) 4.1 and Secure Remote Access (SRA) 3.0 components, the platform addresses four areas integral to risk reduction: visibility, threat detection, vulnerability management, and triage & mitigation. All of Claroty's OT security controls deploy rapidly and integrate seamlessly with existing IT security infrastructure, eliminating the burden of complex deployments, steep learning curves, and unfamiliar tools—all of which have long been barriers for achieving stronger industrial cybersecurity. These controls also improve IT and OT practitioners' ability to protect the availability, reliability, and safety of their industrial environments. The Claroty Platform includes: Visibility: Before the risk to an industrial environment can be reduced, it must be assessed. This requires full visibility into the environment's OT network, which has historically been difficult to attain due to the prevalence of unfamiliar OT assets, architectures, and protocols. The Claroty Platform tackles this challenge by leveraging unmatched protocol coverage, scanning, segmentation, and secure remote access capabilities to grant complete visibility across all three OT dimensions critical to risk reduction: assets, network sessions, and processes. Claroty is the only vendor to provide this calibre of visibility. With CTD 4.1, users can see and customise their view of critical information with greater ease. SRA 3.0 not only enables secure OT remote access, but it also provides real-time monitoring and recordings of all remote sessions for painless auditing and risk assessments. Threat Detection: Swiftly detecting threats is essential to reducing risk. But aside from visibility, OT threat detection also requires distinguishing true threats from false positives. This can be challenging for reasons ranging from the incompatibility of traditional detection tools with OT networks to a deficit of OT threat intelligence, among others. The Claroty Platform makes effective detection attainable by automatically weeding out false positives and alerting users in real-time to anomalies and known and zero-day threats. Now with CTD 4.1, users can also access and act on the latest OT threat intelligence faster than ever before with automatic updates via the Claroty Cloud, as well as utilise a customisable dashboard to quickly identify the threats that matter most. Vulnerability Management: Effective vulnerability management is necessary for reducing risk in industrial environments. The prevalence of legacy systems means vulnerabilities are common, but so are false positives and negatives due to visibility and bandwidth limitations. The Claroty Platform resolves these issues by automatically identifying and comparing each OT asset to an extensive database of vulnerabilities tracked by Claroty's research team, as well as to the latest Common Vulnerabilities and Exposures (CVE) data from the National Vulnerability Database (NVD). And with CTD 4.1, users can now pinpoint the riskiest vulnerabilities and attack vectors in their environments, receive mitigation recommendations and filter out any noise faster and more easily than ever before. Triage & Mitigation: Time can significantly impact risk. The longer it takes for an alert to be evaluated, a threat neutralised, or exposure mitigated, the greater the risk to OT availability, reliability, and safety—as well as the entire enterprise—is likely to be. New features within CTD 4.1 and SRA 3.0 combine purpose-built automation with deep OT context to further streamline and accelerate triage & mitigation processes. The Claroty Platform's unique root cause analysis feature, which groups all alerts related to the same event or series of events, produces a higher signal-to-noise ratio and lower alert fatigue. As a result, users can more effectively and efficiently handle alerts and ultimately reduce risk without being overwhelmed by false positives or lengthy investigations. "Being alerted to vulnerabilities in real-time is a must-have for our Manufacturing operations," said Kevin Tierney, Vice President of Global Cybersecurity for General Motors. "We need solutions that allow our organisation to quickly identify which assets have potential vulnerabilities and prioritise the actions we need to take in order to reduce and eliminate potential risks." "Securing critical infrastructure and industrial networks has become more important than ever, with all the new, unexpected obstacles and challenges that CISOs must overcome," said Grant Geyer, Chief Product Officer of Claroty. "The Claroty Platform, strengthened even further by these latest updates, is a complete OT security solution perfectly positioned to mitigate the emerging risks to OT environments." CTD 4.1 will be available this month and SRA 3.0 will be available in May. To learn more about the Claroty Platform and its new features, please request a demo. About Claroty Claroty bridges the industrial cybersecurity gap between information technology (IT) and operational technology (OT) environments. Organisations with highly automated production sites and factories that face significant security and financial risk especially need to bridge this gap. Armed with Claroty's converged IT/OT solutions, these enterprises and critical infrastructure operators can leverage their existing IT security processes and technologies to improve the availability, safety, and reliability of their OT assets and networks seamlessly and

without requiring downtime or dedicated teams. The result is more uptime and greater efficiency across business and production operations. Backed and adopted by leading industrial automation vendors, Claroty is deployed on all seven continents globally. The company is headquartered in New York City and has received $100 million in funding since being launched by the famed Team8 foundry in 2015. For more information, visit www.claroty.com.

Contacts

Elaine Banoub
02 92123888
mailto: ebanoub@primary-pr.com