Claroty Partners with CrowdStrike to Protect Industrial Control System Environments

Integration Provides Full-spectrum IT/OT Visibility and Threat Detection Coverage

Claroty, the global leader in operational technology (OT) security, today announced it is partnering with CrowdStrike, a leader in cloud-delivered endpoint and workload protection, on an integration between The Claroty Platform and the CrowdStrike Falcon platform. This integration delivers comprehensive visibility into industrial control system (ICS) networks and endpoints, with a one-stop-shop for information technology (IT) and OT asset information directly within The Claroty Platform. It also delivers enhanced detection of ICS threats across the IT/OT boundary without the need for added connectivity, signature reconfiguration, or manual updates. The result is more effective and efficient IT/OT security governance and strengthened security posture spanning all connected sites. Digital transformation has caused once-isolated OT networks to become interconnected with the rest of the enterprise through the IT network, and the COVID-19-induced shift to remote work has accelerated IT/OT convergence even more. These conditions have expanded the attack surface within ICS networks, giving threats such as ransomware clear pathways across the IT/OT boundary. At the same time, IT and security operations center (SOC) teams are increasingly responsible for protecting these new pathways, but they are hindered by the lack of integration between their OT tools and traditional IT security tools to provide effective measures for doing so. “In 2020, the top sector being hit with ransomware is manufacturing,” said Dawn Cappelli, VP Global Security and CISO of Rockwell Automation. “It is imperative that we secure the converged IT/OT environment, and the integration of Claroty and CrowdStrike brings two of the top security technologies together to do just that.” By combining Claroty’s OT expertise, threat signature database, and asset discovery and monitoring technology with CrowdStrike’s industry-leading IT endpoint telemetry, derived from 4 trillion endpoint-related signals per week from across the globe, the joint solution delivers full-spectrum IT/OT visibility and threat detection coverage for ICS networks. “Effectively protecting modern ICS networks requires IT and SOC teams to have a complete inventory of both IT and OT assets, as well as the ability to detect, assess, and mitigate threats and the corresponding risks they face,” said Matthew Polly, Vice President of Worldwide Alliances, Channels and Business Development at CrowdStrike. “This integration with Claroty allows our customers to leverage the CrowdStrike Falcon platform to improve the security posture of their OT environments, bridging the gap between IT and OT.” Key capabilities include: Threat Detection: By fusing CrowdStrike’s ability to identify targeted and compromised endpoints with Claroty’s extensive OT monitoring capabilities, the two companies have created an extensive and actionable IT/OT threat signature database for ICS networks. All signatures can be immediately pushed from The Claroty Platform’s Enterprise Management Console (EMC) to all connected sites in just one click. Asset Discovery and Enrichment: Claroty can automatically identify and enrich IT-oriented ICS assets, such as human machine interfaces (HMIs), historian databases, and engineering workstations (EWs), in which a CrowdStrike agent is installed. Claroty fetches the IT specific properties from the asset as well as the unique manufacturer configuration file from CrowdStrike and then parses that file, without needing to connect to the ICS network. “One of the most impactful benefits of The Claroty Platform is that it can leverage existing IT security infrastructure to protect OT assets and networks,” said Galina Antova, Co-founder and Chief Business Development Officer of Claroty. “This particular integration is uniquely beneficial to Claroty customers because it is the first in which data flows into The Claroty Platform rather than from it, making it a comprehensive repository of both IT and OT asset information. We are very proud to join forces with CrowdStrike to make our comprehensive OT security capabilities more accessible to IT and SOC teams, at a time when they are entrusted with protecting OT more than ever before.” To learn more about the CrowdStrike-Claroty joint solution, download the integration brief or visit the Claroty blog. On Thursday, December 3, Claroty and CrowdStrike will host a webinar, “Extending Security Controls to OT Networks with the CrowdStrike-Claroty Joint Solution.” Register here. 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