Komplette Visibilität für die OT

Solide Basis für den Schutz industrieller Anlagen und kritischer Infrastrukturen

Claroty: Die Highlights

- Umfassende Cybersicherheitslösung für Industrie, andere kritische Infrastrukturen und Gesundheitswesen
- Verschafft eine bisher nicht erreichte Visibilität im OT-Netzwerk (Claroty Edge)
- Erweitert die von der IT bekannte Kontrolle auf die OT
- Belastet OT-Anlagen, -Geräte und -Netzwerk nicht
- Ermöglicht sicheren Fernzugriff auf die OT-Verwaltung (Claroty SRA)
- Erkennt kontinuierlich Bedrohungen, die auf OT-, IoMT- und IoT-Anlagen zielen (Claroty CTD)
- Bereitstellung wahlweise als On-Premises oder in der Cloud

Claroty wurde 2015 in Israel gegründet und hat sich von Anfang an exklusiv auf Sicherheitslösungen für Operational Technology (OT) für industrielle Anlagen und kritische Infrastrukturen ausgerichtet. Das Unternehmen mit Hauptsitz in New York beschäftigt heute über 600 Mitarbeitende, bedient namhafte Kunden auf allen Kontinenten und zählt Branchengrössen aus der OT-Welt wie Siemens, Schneider Electric und Rockwell Automation zu seinen Investoren. Der direkte Kontakt zu diesen und anderen OT-Spezialisten verschafft Claroty umfassendes und tiefes Know-how bis auf die Ebene der einzelnen Geräte und OT- beziehungsweise herstellerspezifischen Protokolle. Auf dieser Basis kann Claroty Kunden und Partnern eine umfassende industrielle Cybersecurity-Lösung für Unternehmen und Organisationen mit kritischen Infrastrukturen anbieten. Das Produktportfolio von Claroty umfasst die drei Kerntechnologien Claroty Edge, Claroty Secure Remote Access (SRA) und Claroty Continuous Threat Detection (CTD). Die drei Komponenten bieten die volle Transparenz im OT-Netz bis ins Detail, streng abgesicherte Remote-Zugriffe auf die OT-Verwaltung sowie kontinuierliche Erkennung von Bedrohungen in allen Segmenten des OT-Netzwerks. Dazu kommt ein riesiges Ökosystem von Integrationen, etwa mit Cybersecurity-Lösungen aus dem IT-Bereich, industriellen Kontrollsystemen, Service-Management- und SIEM-Plattformen. Die Basis dafür bilden eine robuste API und flexible Deployment-Optionen, die sich für alle Arten von Infrastrukturen, Architekturen und Umgebungen eignen.

Beruhigende Cybersicherheit für kritische Infrastrukturen

Die Industrial-Cybersecurity-Lösungen von Claroty schlagen die Brücke zwischen IT- und OT-Security durch vollständige Transparenz für das OT-Netzwerk, sicheren Fernzugriff auf die Verwaltung der OT-Umgebung und kontinuierliche Überwachung und Erkennung von Bedrohungen, die auf die kritischen Infrastrukturen abzielen.

Die Claroty-Plattform setzt sich aus den drei Lösungen Claroty Edge, Claroty SRA und Claroty CTD zusammen und lässt sich auf Basis einer robusten API durch zahlreiche Integrationen mit anderen Cybersecurity- und Management-Lösungen ergänzen.

Claroty Edge: Transparenz für industrielle Netzwerke innert Minuten

Effektive industrielle Cybersicherheit erfordert ein vollständiges Inventar aller OT-, IoT- und IT-Ressourcen in der gesamten industriellen Umgebung. Standard-IT-Lösungen und Scanning-Methoden aus der IT-Welt sind in der Regel mit industriellen Netzwerken nicht kompatibel und unsicher.
Und herkömmliche Lösungen für die Inventarisierung von Industrieanlagen basieren oft auf kostspieliger und komplexer Hardware.
Claroty Edge ist anders: Die Lösung arbeitet als flexibler Edge-Datensammler auf Windows-Basis, hinterlässt in der OT-Umgebung keinen physischen Fussabdruck und erfordert keine Netzwerkänderungen. In wenigen Minuten liefert Edge eine nie dagewesene Visibilität in OT-Netzwerken mit umfassenden Angaben zu allen Anlagen und Geräten – inklusive anschaulicher grafischer Darstellung. Damit unterstützt Edge das Risiko- und Schwachstellenmanagement, Audits und Compliance.

Claroty SRA: Hochsicherer Remote-Zugriff auf OT-Umgebungen

Die Anforderungen an die Sicherheit von Fernzugriffen auf OT-Umgebungen sind mit Blick auf die enorme Tragweite von Sicherheitsvorfällen in kritischen Infrastrukturen besonders hoch und unterscheiden sich von denen für den Zugriff auf IT-Netzwerke. Bisher waren die meisten professionellen Remote-Access-Lösungen für OT-Remote-Zugriffe zu komplex und zentralisiert. Claroty Secure Remote Access (SRA) wurde speziell für Remote-Zugriffe auf OT-Umgebungen entwickelt und für OT-Anwendungsfälle und OT-Workflows optimiert. SRA unterstützt weltweit verteilte Standorte mit lokaler und zentraler Verwaltung über eine benutzerfreundliche, auf OT massgeschneiderte Konsole und ermöglicht eine umfassende Kontrolle privilegierter Zugriffe.

Claroty CTD: Visibilität und permanente Bedrohungsüberwachung

Die bisher oft von der IT isolierten OT-Netzwerke sind immer stärker mit den IT-Netzwerken vermischt, was das Cyberrisiko massiv erhöht. Claroty Continuous Threat Detection (CTD) liefert auf Basis umfassender Einsicht in die OT-spezifischen Protokolle und Geräte die erforderlichen Daten für die Claroty-Plattform, damit Sicherheitsteams die Risiken sowohl in IT- als auch in OT-Umgebungen minimieren können. Dabei nutzt CTD eine passive Erkennung über nicht intrusive Sensoren und bietet Funktionen wie Asset- und Schwachstellenmanagement, Risikobewertung sowie Erkennung von Bedrohungen und Anomalien. Darüber hinaus gibt die Lösung einen umfassenden Einblick in die Kommunikationsverbindungen: CTD zeigt auf, welche OT-Geräte und -Systeme mit welchen Gegenstellen im IT- und OT-Netzwerk sowie im Internet kommunizieren. Damit unterstützt CTD die Planung einer effektiven Netzwerksegmentierung.