SOLUTION OVERVIEW

Enabling Rapid and Portable OT and CPS Security for DoD and Civilian Agility

Background

Hunt kit. Assessment kit. DCO kit. Flyaway kit. SOC in a Box. Expeditionary kit. Mobile Air Cyber Kit. Regardless of the name, Claroty understands that those responsible for securing OT and the broader cyber physical system footprint have a mission that requires agility, expediency, and of course tools with requisite OT- and broader CPS-specific protocol, configuration and communications expertise.

These kits can meet a number of operational needs for tactical, field-based operations. They enable OT vulnerability assessments that provide insights on current security and process integrity threats to OT and broader CPS networks. They support national security, mission assurance, and resilience while also enabling agility – supporting scarce expertise where and when needed.

What Claroty Offers: 5 x 5 x 2

Reduce your attack surface – swiftly, with agility, wherever and whenever needed. Asset discovery to exposure management to swift threat detection. The Claroty Platform was purpose-built for the cyber physical industry. Claroty has been named a Leader in the first ever Gartner® Magic Quadrant™ for CPS Protection Platforms (CPS PP), positioned highest for Ability to Execute and furthest for Completeness of Vision.[1]

The Claroty Platform offers **5 collection options** for swiftly discovering every cyber physical asset in your environment. It uses **5 detection engines** to swiftly detect 5 categories of threats to cyber physical assets, zones and networks. And it generates **2 categories of alerts** relevant to these environments to assist your teams with deep details on the priority threats to address.

5 Collection Options

With 5 collection options to choose from, most of which are SPAN-less, including the industry's first "zero infrastructure" collection capability, Claroty Edge, we can help you find and profile every asset down to individual line cards on OT assets.

- **Edge –** the industry's first "zero infrastructure" collection capability lightweight .exe that collects and builds a complete asset inventory in minutes.
- **Active/Safe queries –** using queries to actively detect devices.
- **Project File analysis –** extracting device data from the device project files between engineering workstations and PLCs.
- **Passive –** non-intrusive, using SPAN and Claroty DPI to passively listen to network activity.
- **Ecosystem enrichment** - capitalizing on information within your existing CMDB, disaster recovery, EDR, and other cybersecurity and operational technologies.

The SPAN-less options enable these teams to get the job done without change or disruption to production networks.

5 Detection Engines

The Platform uses the following 5 engines to discern threats to the network and its assets.

- **Behavior anomaly detection:** for changes in communications between network assets or zones.
- **Operational behavioral pattern detection:** to monitor the context and detail of ongoing operations down to reveal any changes made to an asset's configuration.
- **Signature-based detection:** to trigger on YARA and SNORT rules from Claroty's Team82 threat research, known IOCs and signatures, and user-created rules.
- **Security behavior pattern detection:** to detect attacks like man-in-the-middle and network scans.
- **Rule-based threat detection:** to detect activity based on custom criteria that operators create to target specific events.

2 Alert Categories

The Platform generates alerts based on anomalies, rules, threat signatures and operational behaviors discovered with the aforementioned algorithms. It identifies all threats to these specialized networks in 2 categories:

- **Security threats** - known threat attacks, zero day attacks, and attacks involving sophisticated OT payloads early in the killchain, as well as
- **Process integrity issues** - critical changes to a production-level process, such as critical changes in temperature and other important values, configuration downloads, new hardware assets being added to the network, and other policy violations.

With built-in automations that identify, profile and categorize assets, establish behavioral baselines for legitimate OT communications, and even establish virtual zones to add additional protection, The Claroty Platform helps bridge the gap between IT and OT. The Platform even comes fully loaded with recommendations for compensating controls where needed. Threat detection security alerts provide step by step guidance and timeline insights for each alert. And process integrity alerts provide built-in resources to understand vulnerabilities, misconfigurations, and help ensure swift mitigation.

Supporting Hunt Team Requirements

When it comes to the needs of your in-field teams, The Claroty Platform has it covered, meeting typical "Hunt" team requirements:

- **Resource "light" –** meet size and weight constraints, installing in small kits and laptops with modularity and in line with international commercial airline requirements
- **Setup "light" –** installed in pelican case to laptop, agile for the mobility needs of the team
- **Standalone and airgapped operation –** independent of outside platforms or services to parse and/or view data, operate in austere environments without internet access, additional storage or processing resources from the existing field station's infrastructure
- **Deep discovery –** discover assets at all levels of the Purdue Model, including serial connections
- **OT network mapping –** see all ports, protocols and comms throughout the OT network
- **Vulnerability and exposure visibility –** find all vulnerabilities and other exposures in the OT network
- **Ease of use** - automations, in-tool descriptions and remediation guidance, plus swift resets for less configuration time
- **IR-enabled –** providing timeline-based, correlated event data with deep insights and packet captures, data ingestion and analysis capabilities for incident response when desired
- **SOC readiness –** through APIs and current partner integrations, Claroty insights are ready for swift export to SOC teams' SIEMs and SOARs and other tools if and when needed.
- **Flexible platform options –** Bare metal hardware or Hypervisor

In addition to the above, Claroty offers training for all users, enabling as deep and wide of capability knowledge as desired. Deploy confidently regardless of the level of OT expertise available in-field.

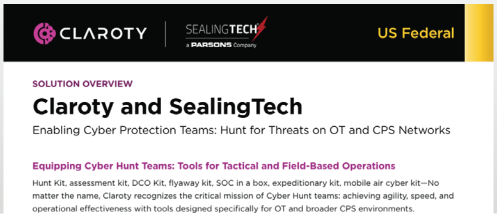
The Claroty Difference

Claroty's offering is truly unmatched in offering comprehensive protection for federal OT and CPS environments – and on the fly. Here are some of the key differentiators that make The Claroty Platform the clear choice for protecting Federal OT and CPS networks:

- **Unmatched Visibility:** With 5 collection methods, provides full asset visibility and vulnerability analysis, without hardware, configuration change or network changes.
- **Broadest Protocol Coverage:** Supports over 450+ protocols, covering thousands of OT devices: ICS / SCADA, IIoT, IoT, IT, IoMT, and Serial Devices for operational systems.

- **Deep OT expertise:** Deep understanding of CPS environments and OT targeted attacks enable the best identification of and context for threats to these networks
- **Partnerships:** Partnering with OT and CPS OEMs and integration into existing cybersecurity workflows enable you with comprehensive manufacturer-specific exposure insights and mitigations.
- **Distinguished OT threat intelligence:** Unique research insights from Claroty Team82 enable advanced nation state actor detection and support the US Government.
- **Proven OT Security at Scale:** With 10K+ sites deployed, and over 20M assets protected, Claroty cuts across every critical sector.
- **Ease of use and training** to support non-OT experts.

This differentiation and many other factors make Claroty the right partner in swift, agile, and accurate threat hunting across the US Federal OT and CPS footprint. Get in touch with our team today to support your deployment needs.


CLAROTY | SEALINGTECH a PARSONS Company US Federal

SOLUTION OVERVIEW

Claroty and SealingTech

Enabling Cyber Protection Teams: Hunt for Threats on OT and CPS Networks

Equipping Cyber Hunt Teams: Tools for Tactical and Field-Based Operations

Hunt Kit, assessment kit, DCO Kit, flyaway kit, SOC in a box, expeditionary kit, mobile air cyber kit—No matter the name, Claroty recognizes the critical mission of Cyber Hunt teams: achieving agility, speed, and operational effectiveness with tools designed specifically for OT and broader CPS environments.

READ MORE ABOUT OUR JOINT SOLUTION WITH SEALINGTECH.

READ MORE

Results

- Faster Time to Value: Faster deployment of OT security expertise where and when needed.
- Rapid adaptation to changing needs: Security needs and priorities can shift rapidly due to policy changes, emergencies, or evolving realities. Quickly pivot and adjust investments while adapting to change and achieving greater efficiency.
- Improved resource allocation: Optimize scarce talent only when and as needed, in a more cost-effective way.
- De-risked investment decisions: Enable small, incremental deployments where feasible, particularly in rapidly changing conditions, to gauge viability, identify potential risks and technical challenges, all while enabling critical, timely support.

[1] Gartner Objectivity Disclaimer: Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

About Claroty

Claroty empowers organizations to secure automation, control, and other cyber-physical systems across industrial, healthcare, commercial, and public sector environments: i.e. the Extended Internet of Things (XIoT). The company's unified platform integrates with customers' existing infrastructure to provide comprehensive controls for visibility, risk and vulnerability management, threat detection, and secure remote access. Backed by the leading investment firms and industrial automation vendors, Claroty is deployed at thousands of sites globally. The company is headquartered in New York City with U.S. federal headquarters in Leesburg, VA. To learn more, visit clarotygov.us.

CLAROTY