

SOLUTION OVERVIEW

Claroty Continuous Threat Detection

Comprehensive On-Premise CPS Cybersecurity for The Modern Federal OT Network

Federal organizations have complex and diverse cyber-physical systems (CPS) environments. Keeping them secure means knowing that all assets are accounted for and their security status known. But due to their unique architectures, proprietary protocols and environmental and operational constraints, CPS networks need security built for them where traditional IT solutions fall short.

Claroty Continuous Threat Detection (CTD) provides comprehensive reach to identify your assets across the Federal government's variety of OT, IoT, BMS, IoMT, and physical security functions. Employing multiple discovery methods, it provides the industry's most comprehensive, in-depth asset profiles. CTD provides the vendor, model, firmware, OS version, and protocol, along with the security profile, including unpatchable end-of-life assets and vulnerabilities, for precision-driven asset discovery and automated enhancement.

Claroty Continuous Threat Detection (CTD) was created to help operational and/or cyber practitioners overcome the challenges of cyber-physical connectivity. Achieving resilience is far from impossible – and it requires a robust set of requirements that cannot be satisfied by traditional IT-centric solutions. Powered by an unmatched library of CPS communication protocols and in-depth industry knowledge, CTD provides superior visibility to OT environments. This enables the further implementation of core cybersecurity controls that span the entire cyber-physical security journey. These controls cover:

- Exposure Management
- Threat Detection
- Remote Incident Response

At A Glance

- Multiple discovery methods and deployment mechanisms
- Full cyber-physical system (CPS) cybersecurity journey support from asset discovery to network integration and optimization
- Detailed network mapping for automated zoning and virtual network segmentation
- Contextualized root-cause analysis and risk-based scoring for all alerts
- Secure remote access and remote session incident response and investigation when integrated with Claroty xDome Secure Access
- Integrations with existing IT infrastructure such as SIEM, Firewalls, SOAR, CMDB tools to extend core cybersecurity capabilities to OT environments

Asset Discovery

Effective OT cybersecurity starts with knowing what needs to be secured. CTD leverages the broadest and deepest OT protocol coverage in the industry and employs multiple discovery methods to ensure the most complete network profile.



Passive Monitoring

Continuous monitoring of network traffic to identify asset profiles



Safe Queries

Targeted discovery of assets in their native protocol



Clarity Edge

Speedy, host-based asset profiling through localized queries



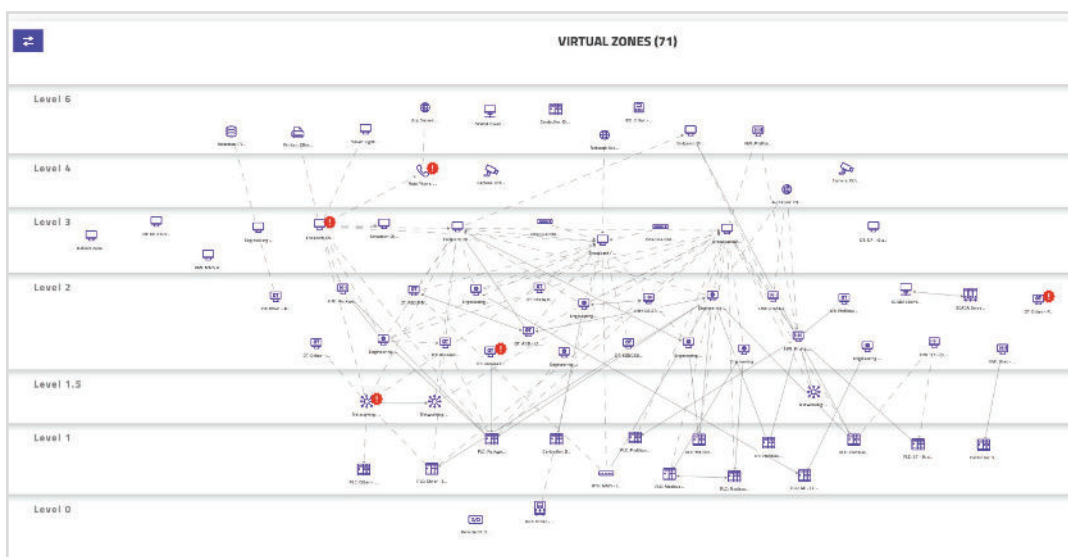
Project File Analysis

Regular ingestion of offline configuration files for asset enrichment

Clarity CPS discovery methods

This multi-spectral approach helps to uncover parts of the network that are not suitable for a single discovery method and results in unmatched visibility into CPS environments. This depth of discovery is seen across three aspects of visibility:

- 1. Breadth of Discovery:** Employ distinct, highly flexible methods that can be combined or used separately to create comprehensive asset profiles
- 2. Zone-Based Mapping:** Leverage in-depth asset profiles and communication monitoring to automate virtual segmentation of the OT network into Virtual Zones.
- 3. Identify Asset Changes:** Additions to the network, configuration changes, and anomalies are some of the many variables monitors by xDome to support MoC programs

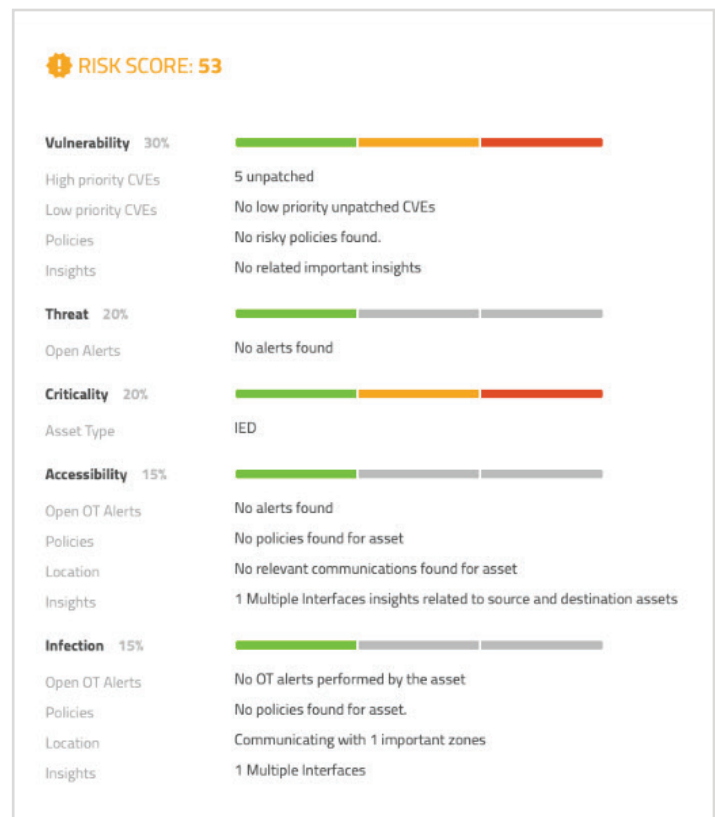


Clarity CTD segmentation view with virtual zones

Exposure Management

CTD automatically compares each asset in an OT environment to an extensive database of insecure protocols, CVEs, configurations, substandard security practices, and other vulnerabilities tracked by Claroty's award-winning Team82 researchers. As a result, users can identify, prioritize, and remediate risk exposures in OT networks more effectively.

- **Identify Exposures:** Profile assets to identify their exposure to risk, including vulnerabilities, misconfigurations, end-of-life insights, and more
- **Attack Vector Mapping:** Contextualize and validate exposures by analyzing known risks to calculate the most likely scenarios in which an attacker could compromise the network
- **Risk-Based Scoring:** Automatically evaluate and score vulnerabilities based on the unique risk they pose to your network, enabling more efficient and effective prioritization and remediation

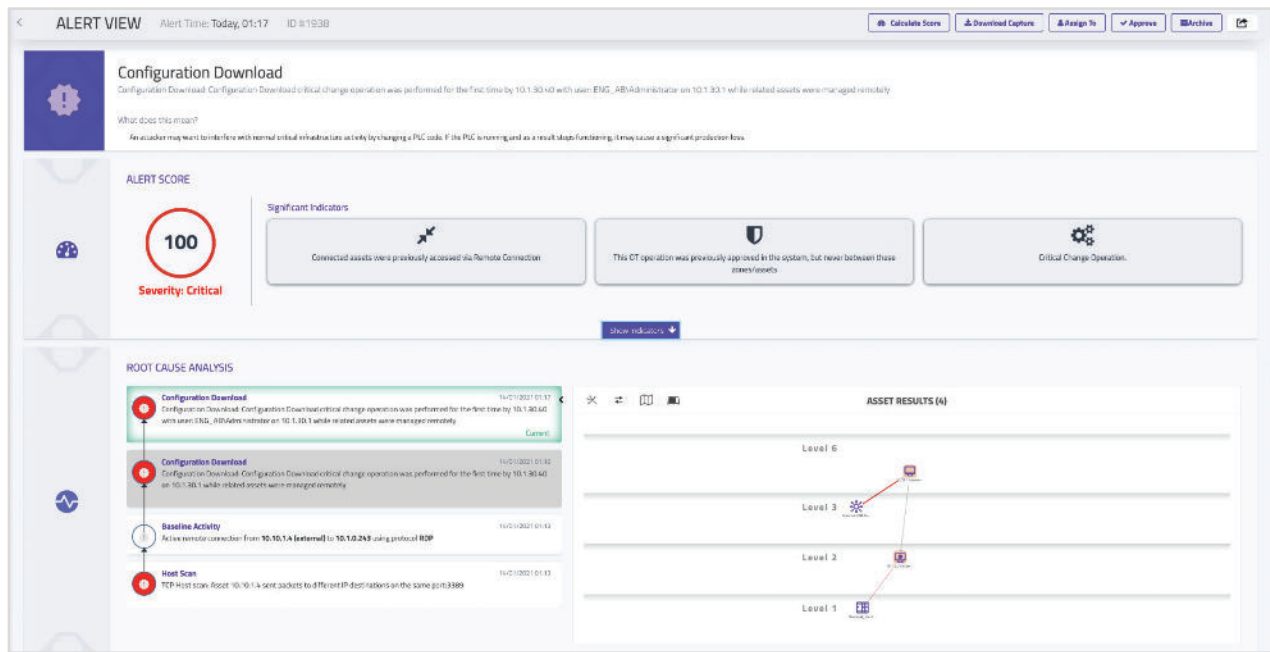


CTD Risk Score comprised of five unique factors

Threat Detection

Threats to OT networks are often innovative yet can be deceptively simple, exploiting our compulsion toward process adherence to introduce risk. CTD utilizes multiple detection engines to automatically profile all assets, communications, and processes in OT networks, generate a behavioral baseline that characterizes legitimate traffic in order to weed out false positives, and alert users in real-time to anomalies and known, unknown, and emerging threats. Highlights:

- **Detect Known and Unknown Threats:** Characterize legitimate traffic to detect anomalous communications, identify threat signatures, weed out false positives, and alert users in real-time to known, unknown, and emerging threats.
- **Operational Event Alerting:** Continuously monitor critical change operations in the industry environment to help ensure your process integrity and uptime, receiving alerts for actions like configuration downloads which provide insights into the exact code changes within a file.
- **MITRE ATT&CK Alert Mapping:** Incoming alerts are mapped to the MITRE ATT&CK for ICS Framework to help increase the context surrounding the event and assist in identifying known remediation measures.
- **Root Cause Analysis:** Reduce network noise, false positives, and overall alert fatigue by correlating related alerts and indicators into a single chain-of-events, providing a consolidated view of the activities surrounding an alert.



Clarity CTD alert view showing root-cause analysis and chain of events

Remote Incident Response

As part of a holistic approach to CPS cybersecurity, CTD and Clarity xDome Secure Access join forces to drive enhanced alert response capabilities across the two solutions—enabling users to detect, investigate, and respond to incidents from any location. As a result, organizations can adapt their overall security posture and workflows for a remote, distributed, or hybrid work environment with:

Receive alerts and related indicators for events during remote sessions directly within CTD

Investigate remote user activity with access to remote logs, live monitoring, and recorded sessions

Respond to remote incident alerts with the ability to immediately disconnect remote sessions

CPS Protection with Clarity

Clarity's breadth of cyber-physical-system (CPS) knowledge sits at the foundation of our comprehensive portfolio of cybersecurity solutions. This protection begins with Clarity's intimate understanding of CPS networks and all assets within them. Recognizing that no two CPS networks are the same, there cannot be a one-size-fits-all approach to discovering them.

Our solutions, paired with on-premises or cloud-based deployment modes, eliminate the need to purchase and maintain multiple point products and provide the flexibility to choose the deployment approach that best suits scalability needs, cost considerations, and compliance requirements. This dynamic approach to CPS cybersecurity is why Clarity is able to help Federal organizations reduce the cyber risk that results from increased connectivity with the quickest time-to-value (TTV) and a lower total cost of ownership (TCO)—regardless of the scale or maturity of the CPS cybersecurity program.

CTD Benefits

- Deployment flexibility, providing an on-premises OT security solution option to those organizations with unique needs, air-gapped environments or not ready for SaaS in OT environments;
- Ease of best practices adoption, including virtual segmentation
- Faster-time-to-action and protection from exposures and threats with swift identification, prioritization, and remediation of risk exposures
- Comprehensive and deep visibility across all OT assets - physical access to building management to process control
- Comprehensive IT integration with industry's leading firewall, SIEMs, HelpDesk and other vendors

The Clarity Difference

- Purpose-built and designed from actual customer sites, with battle-tested deployment in many high-risk, low-latency, high-availability OT networks
- Sensorless device discovery - within minutes, creating an asset inventory of all devices in the OT / ICS / SCADA environment, without necessitating hardware deployment and added complexity
- Extensive asset protection across ICS / SCADA, FRCS and BMS, and medical and laboratory devices
- Unmatched library of CPS communication protocols, for deep and comprehensive visibility to model, vendor, firmware, OS, protocol version, vulnerable end-of-life devices, and those using insecure protocols
- Validation from the big 3 control system vendors in their control systems labs, increasing speed to deployment, avoiding solutions validation wait time.
- Swift updates, and thus protection from threats and critical device vulnerabilities, from ongoing breadth and depth of Clarity Team82 research
- Risk scoring of vulnerabilities based upon 5 unique factors
- At a Technology Readiness Level (TRL)-9 for many DoD installations

About Clarity

Clarity 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, Clarity 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.