CLAROTY

US Federal

SOLUTION OVERVIEW

Claroty Continuous Threat Detection

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

Federal agencies and the Service Branches 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, federal OT 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, FRCS / BMS, 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 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

- Choice of device discovery methods designed to meet unique operational needs—including hardware-free options
- 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
- Integrates with Claroty xDome Secure Access to enhance remote session incident response and investigation
- Integrations with existing IT infrastructure such as SIEM, Firewalls, SOAR, CMDB tools to extend core cybersecurity capabilities to OT environments

Asset Discovery

CTD delivers a comprehensive, centralized asset inventory for effective OT cybersecurity. With the choice of five asset discovery methods, CTD removes the need for costly and time-consuming hardware upgrades. Collection can be completed in minutes — and can expand across multiple sites and bases, CONUS and OCONUS. Get deep visibility with actionable insights.

Passive Monitorning

Continuous Monitoring of network traffic to identify asset profiles

Safe Queries

Targeted discovery of assets in their native protocol

Claroty Edge

Speedy, host-based asset profiling through localized queries

Project File Analysis

Regular ingestion of offline configuration files for asset enrichment

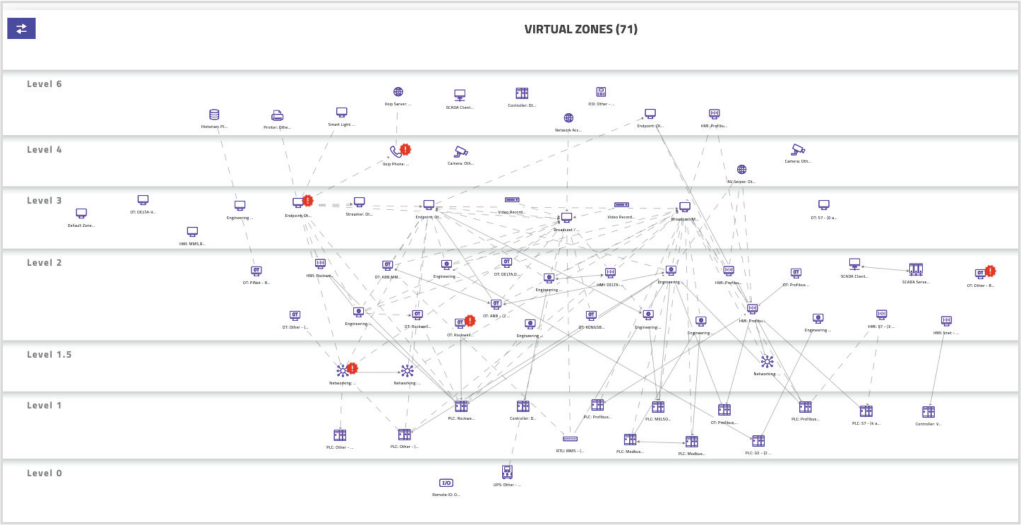
Integrations

Enriching visibility with your existing technology investments

Claroty asset 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 OT 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:** Monitor additions to the network, configuration changes, and anomalies.

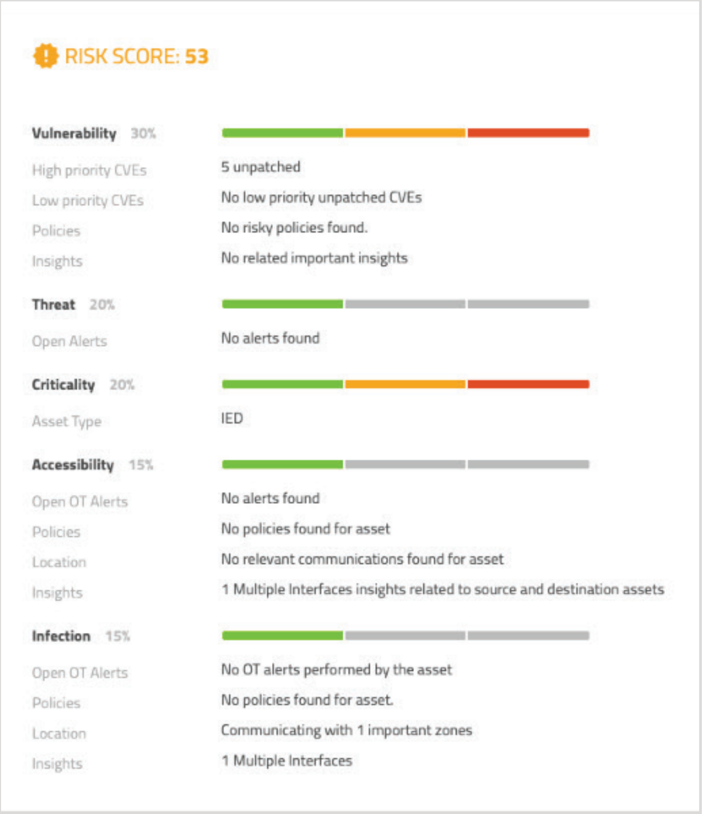


Claroty CTD segmentation view with virtual zones

Exposure Management

CTD automatically assesses each OT asset against an extensive database of insecure protocols, CVEs, misconfigurations, and other vulnerabilities tracked by Claroty's award-winning Team82 researchers, along with the latest KEV and EPSS reports from external sources. As a result, users can identify, prioritize, and remediate risk exposures more effectively.

- **Identify Exposures:** Profile assets to identify their exposure to risk, including KEVs, 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.



RISK SCORE: 53

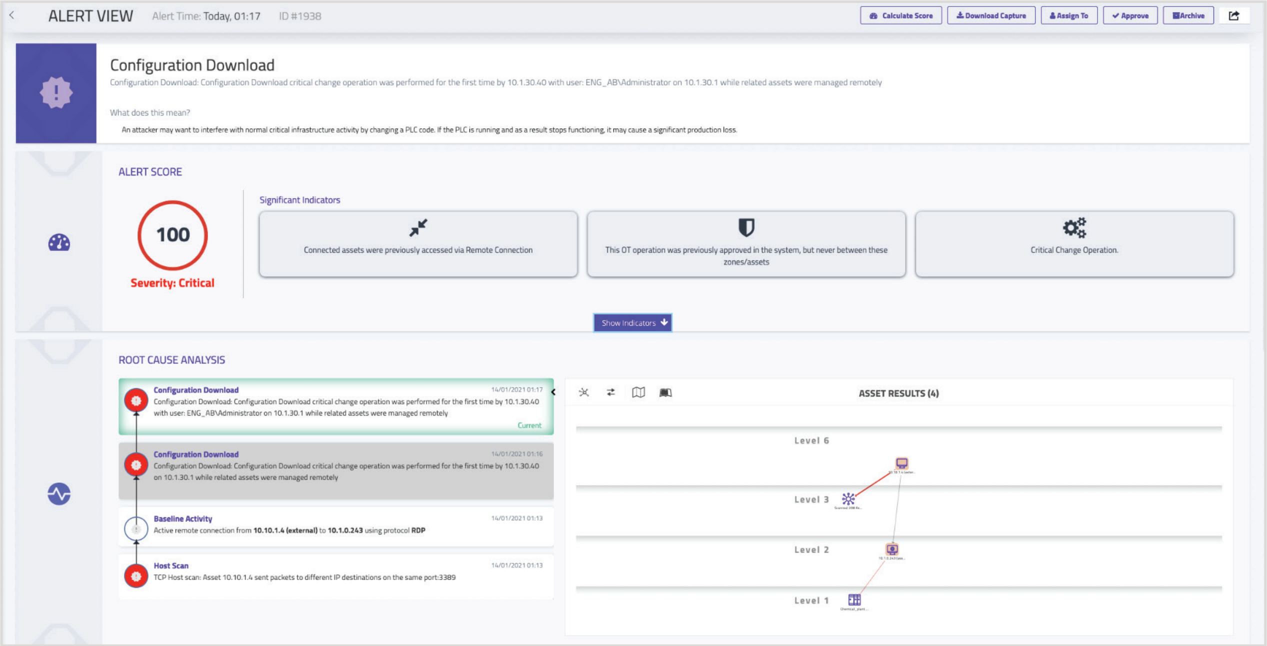
Vulnerability 30%	🟩🟧🟥
High priority CVEs	5 unpatched
Low priority CVEs	No low priority unpatched CVEs
Policies	No risky policies found.
Insights	No related important insights
Threat 20%	🟩▨▨
Open Alerts	No alerts found
Criticality 20%	🟩🟧🟥
Asset Type	IED
Accessibility 15%	🟩▨▨
Open OT Alerts	No alerts found
Policies	No policies found for asset
Location	No relevant communications found for asset
Insights	1 Multiple Interfaces insights related to source and destination assets
Infection 15%	🟩▨▨
Open OT Alerts	No OT alerts performed by the asset
Policies	No policies found for asset.
Location	Communicating with 1 important zones
Insights	1 Multiple Interfaces

CTD Risk Score comrpised of five unique factors

Threat Detection

Recognizing the U.S. federal government as a lucrative target for state-sponsored threat actors, CTD uses multiple detection engines to automatically profile all OT assets, communications, and processes; establish a behavioral baseline to filter out false positives; and alert users in real time to anomalies and known, unknown, or 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.



Alert Time: Today, 01:17 ID #1938

Configuration Download

Configuration Download: Configuration Download critical change operation was performed for the first time by 10.1.30.40 with user: ENG_AB\Administrator on 10.1.30.1 while related assets were managed remotely

What does this mean?

An attacker may want to interfere with normal critical infrastructure activity by changing a PLC code. If the PLC is running and as a result stops functioning, it may cause a significant production loss.

ALERT SCORE

100

Severity: Critical

Significant Indicators

- Connected assets were previously accessed via Remote Connection
- This OT operation was previously approved in the system, but never between these zones/assets
- Critical Change Operation.

ROOT CAUSE ANALYSIS

Configuration Download 14/01/2021 01:17
Configuration Download: Configuration Download critical change operation was performed for the first time by 10.1.30.40 with user: ENG_AB\Administrator on 10.1.30.1 while related assets were managed remotely
Current

Configuration Download 14/01/2021 01:16
Configuration Download: Configuration Download critical change operation was performed for the first time by 10.1.30.40 on 10.1.30.1 while related assets were managed remotely

Baseline Activity 14/01/2021 01:13
Active remote connection from **10.10.1.4 (external)** to **10.1.0.243** using protocol **RDP**

Host Scan 14/01/2021 01:13
TCP Host scan: Asset 10.10.1.4 sent packets to different IP destinations on the same port:3389

ASSET RESULTS (4)

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

Remote Incident Response

As part of a holistic approach to OT cybersecurity, CTD and on-premises Claroty 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, federal agencies and the Service Branches 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

OT and Broader CPS Protection with Claroty

Claroty's breadth of cyber-physical-system (CPS) knowledge — across ICS/SCADA, IoT, and physical security — sits at the foundation of our comprehensive portfolio of cybersecurity solutions. This protection begins with Claroty'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 Claroty is able to help U.S. Federal Agencies and the Service Branches 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.

The Claroty Difference

- Purpose-built and designed with real OT networks in mind, with battle-tested deployment across 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 Claroty Team82 research
- Risk scoring based on five unique factors, enriched with KEV and EPSS exploitability data
- At a Technology Readiness Level (TRL)-9 for many DoD installations

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