DATA SHEET

Claroty Continuous Threat Detection

The Industrial Cybersecurity Challenge & Claroty CTD

The Industrial Security Challenge

Digitalization initiatives and the expansion of remote workforces have transformed enterprises, causing once-isolated operational technology (OT) environments to become interconnected with their information technology (IT) counterparts. The result is the rise of converged IT/OT networks that offer great opportunities to enhance innovation and efficiencies within industrial environments. Despite the clear benefits of cyber-physical connectivity it creates an expanded attack surface across a host of unique and unfamiliar device types, communicating with often proprietary protocols which render traditional IT security solutions unsuitable for protection.

In the pursuit of both cyber and operational resilience, Claroty Continuous Threat Detection (CTD) was created to help industrial environments overcome the challenges of cyber-physical connectivity. Achieving resilience is far from impossible – but it requires a robust set of requirements that cannot be satisfied by traditional solutions or generalized approaches.

CTD is backed by the unmatched library of industrial protocols, asset discovery methods, and proprietary DPI technology that is required to achieve unmatched visibility in industrial environments. This enables the further implementation of core cybersecurity controls that span the entire cyber-physical security journey. These controls cover:

- Asset Discovery
- Vulnerability & Risk Management
- Network Protection
- Threat Detection
- Asset & Change Management
- Remote Incident Management

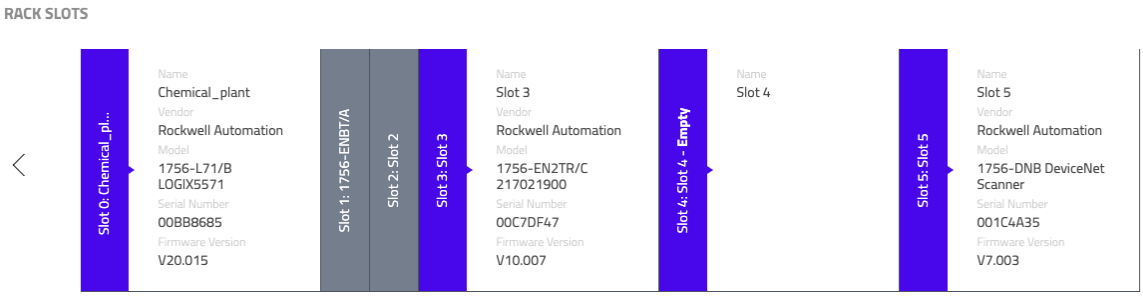
CTD Benefits At A Glance

- Delivers complete visibility into industrial environments with multiple discovery methods and deployment mechanisms
- Supports the full cyber-physical system (CPS) cybersecurity journey from asset discovery to network integration and optimization
- Provides a contextualized root-cause analysis and risk-based scoring for all alerts
- Integrates with Claroty Secure Remote Access (SRA) to enhance remote session incident response and investigation
- Integrates with existing IT infrastructure such as SIEM, Firewalls, SOAR, CMDB tools, and others to extend core cybersecurity capabilities to industrial environments

Asset Discovery

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

- **Asset Visibility**: This encompasses all CPS assets on an industrial network, including serial networks, as well as extensive attributes about each asset
- **Session Visibility**: This includes all industrial network sessions along with their bandwidth, actions taken, changes made, connectivity paths, and other relevant details
- **Process Visibility**: This includes tracking of all industrial operations, the code section and tag values of all processes with which CPS assets are involved, and any abnormal changes to these assets' process values that could indicate threats to process integrity

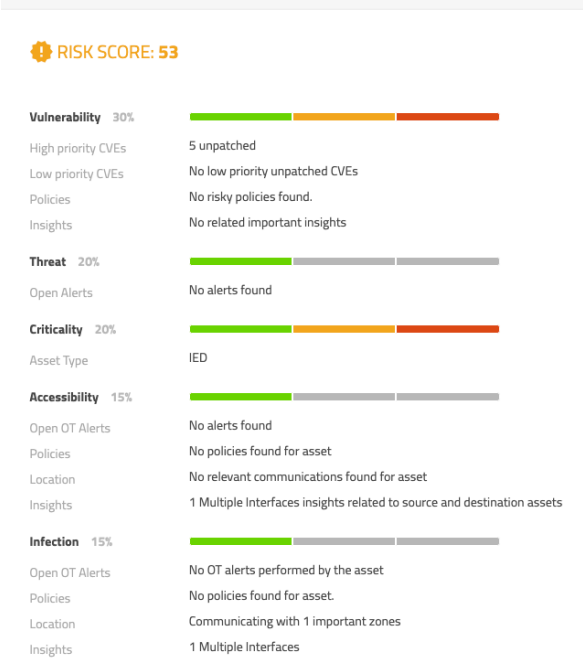


Asset rack slot visibility with Claroty CTD

Vulnerability & Risk 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 vulnerabilities in industrial networks more effectively.

- **Full-Match Vulnerabilities**: Accurately matches exact assets with known CVEs based on vendor, model, and firmware version, to ensure efficient prioritization and remediation of network vulnerabilities
- **Attack Vector Mapping**: Better contextualize your risk landscape by identifying and 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

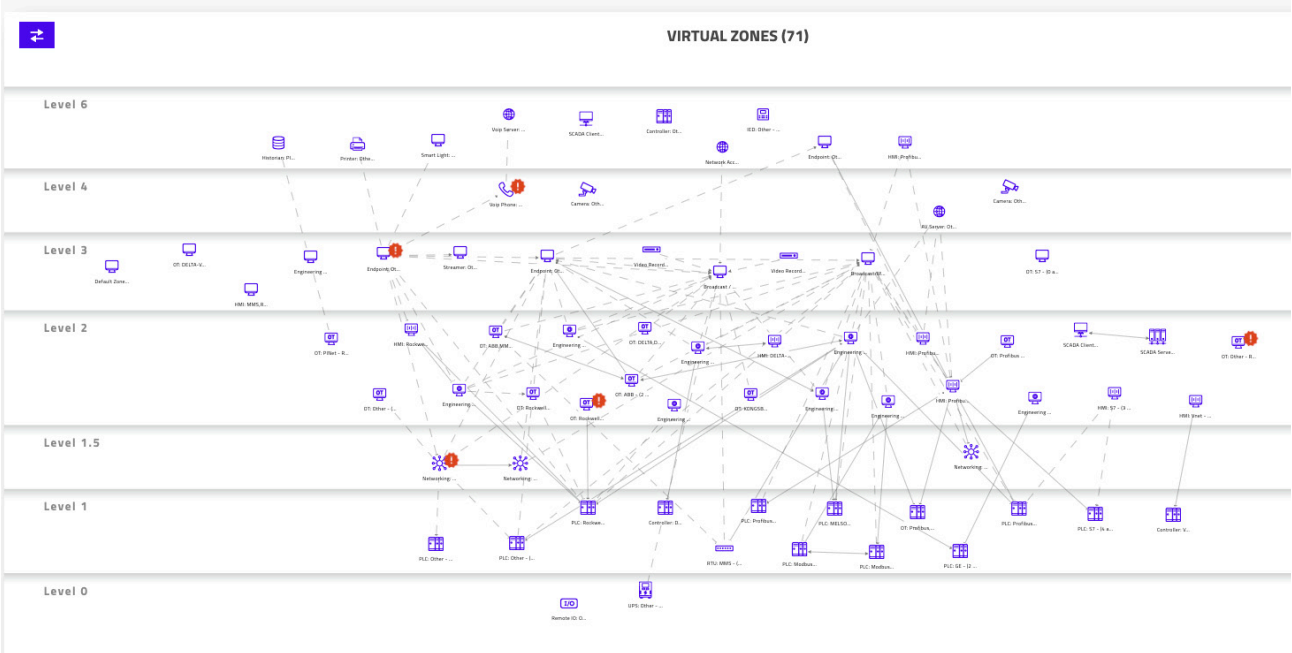


CTD's multi-factor risk scoring

Network Protection

Backed by Claroty's deep domain expertise, CTD leverages its in-depth visibility to automate virtual segmentation of your industrial network into Virtual Zones–logical groups of assets that communicate with one another under baselined circumstances. Virtual Zones can be tailored to fit the unique communication paths in your environment and provide a visualized look at "normal" network behavior. As a method of network segmentation, virtual zones help to:

Drive threat detection through anomalous communication alerting	**Provide a cost-effective alternative to costly physical segmentation programs**	**Extend existing network communication infrastructure into the industrial environment**

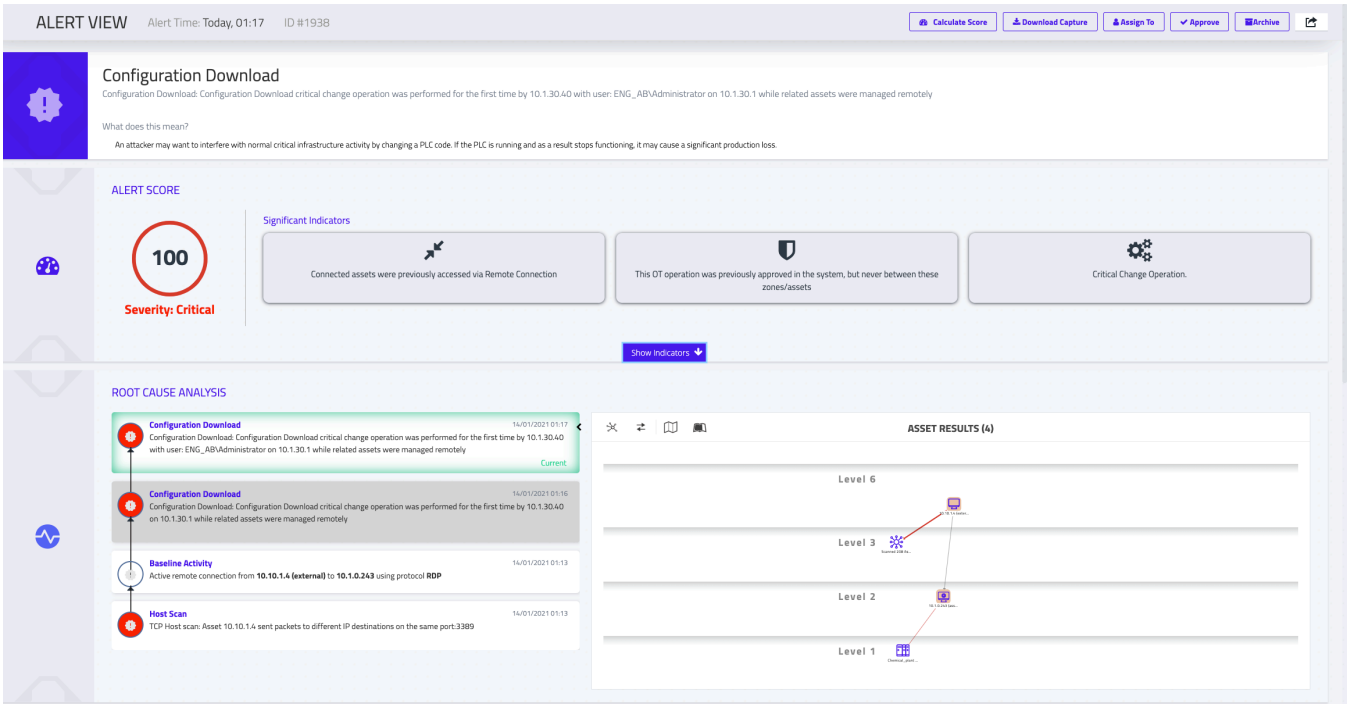


Network layer mapping of CTD Virtual Zones

Threat Detection

Threats to industrial networks are often innovative yet 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 industrial 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

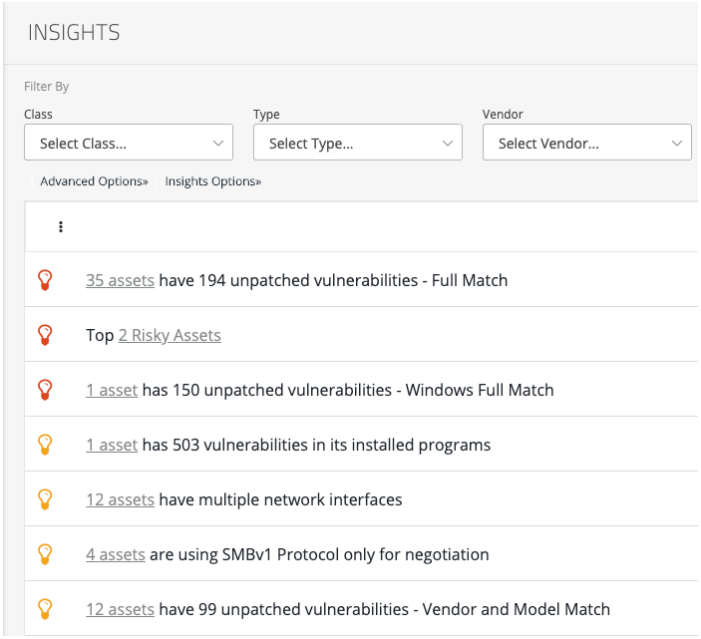


CTD Alert View with key indicators, chain of events, and root cause analysis

Asset & Change Management

Backed by robust and deep network visibility, Claroty CTD empowers organizations to streamline asset and change management. With custom attributes, indicators like end-of-life insights, identification of operational process values, and continuous monitoring for new, updated, or retired assets, CTD enables operators to streamline asset management workflows in order to save administration time and reduce maintenance windows for operations personnel. CTD equips users with the tools needed to:

- **Monitor for asset updates**: CTD continuously monitors for vulnerabilities, outdated software, EoL indicators, and other changes requiring updates to help preserve asset availability
- **Streamline SLA compliance**: CTD makes it easy to identify and report on the SLA compliance status of specific assets through availability and custom-defined attributes
- **Identify asset changes**: Additions to the network, configuration changes, and anomalies are some of the many variables monitors by CTD to support Management of Change programs



CTD Insights prioritized by risk to the network

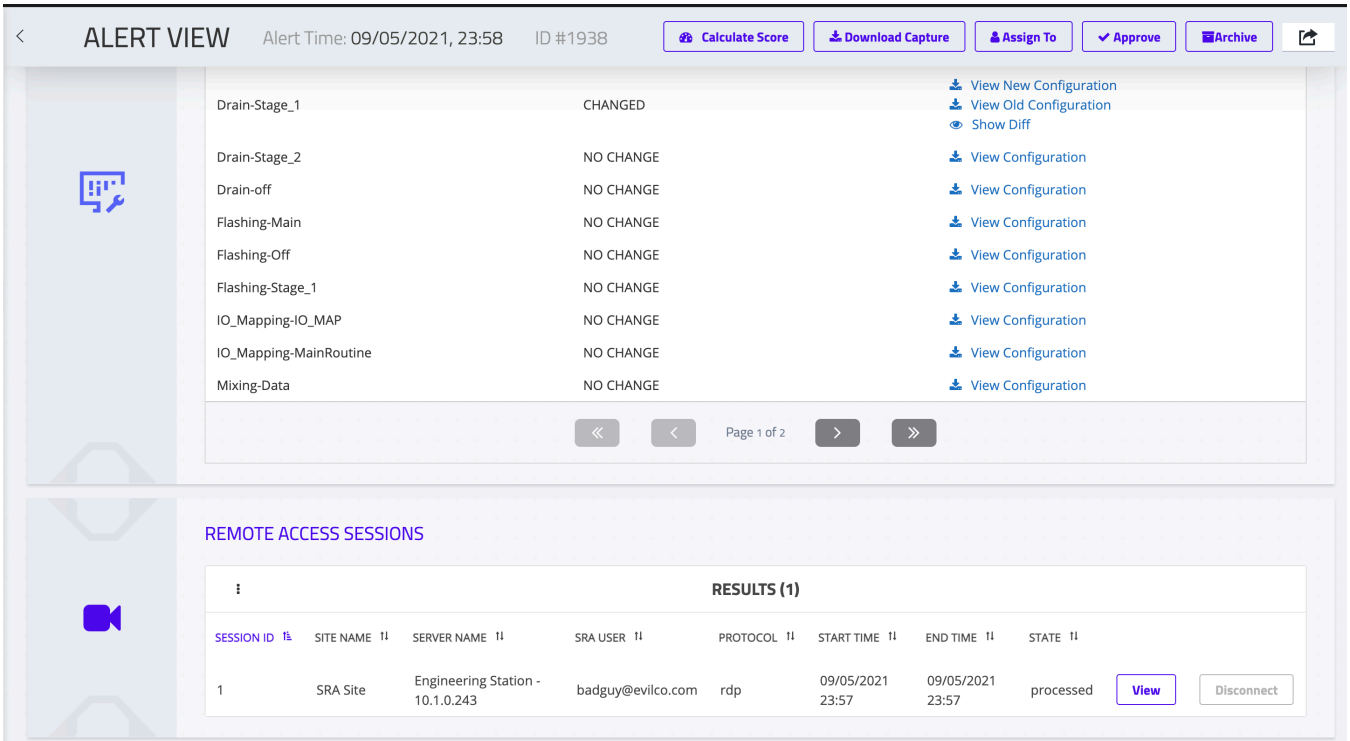
Remote Incident Management

As part of a holistic approach to CPS cybersecurity, CTD and Claroty Secure Remote Access (SRA) join forces to drive enhanced alert response capabilities across the two solutions. These solutions enable 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



CTD Alert View with configuration change details and a link to the associated remote session recording

About Claroty

Claroty empowers industrial, healthcare, and commercial organizations to secure all cyber-physical systems in their environments: the Extended Internet of Things (XIoT). The company's unified platform integrates with customers' existing infrastructure to provide a full range of controls for visibility, risk and vulnerability management, threat detection, and secure remote access.

Backed by the world's largest investment firms and industrial automation vendors, Claroty is deployed by hundreds of organizations at thousands of sites globally. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America.

For more information, visit claroty.com or email contact@claroty.com.