Data Sheet

CLAROTY CONTINUOUS THREAT DETECTION (CTD)

Full Visibility and Fundamental Controls for OT Environments

The OT Security Challenge & Claroty CTD

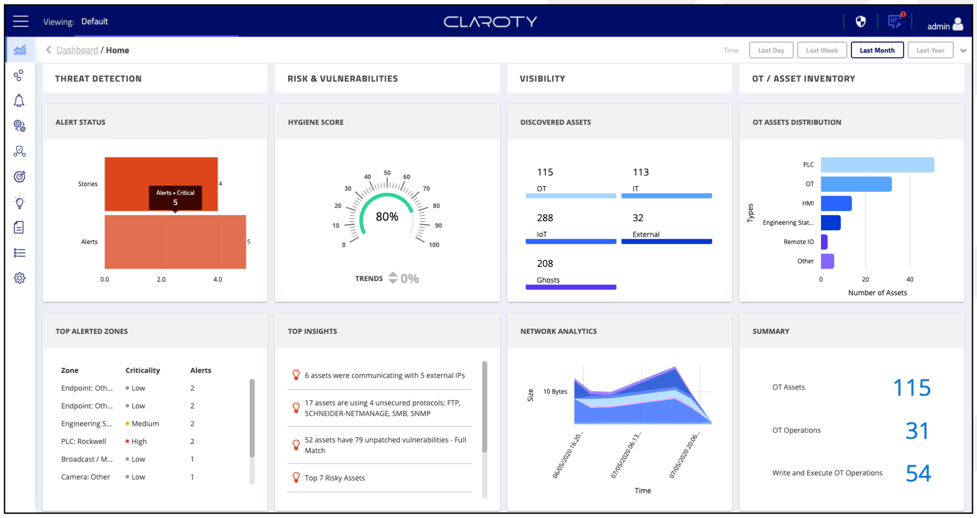
Digitalization initiatives have transformed enterprises, causing once-isolated operational technology (OT) networks to become interconnected with their information technology (IT) counterparts. The result is the rise of converged IT-OT corporate networks that IT security teams are increasingly responsible for protecting. The challenge is the OT portions of these networks typically comprise proprietary protocols and unfamiliar assets, making them incompatible with IT security tools and invisible to IT security teams.

Claroty Continuous Threat Detection (CTD) was designed to overcome this challenge. As the foundation of the Claroty Platform, CTD extends the same controls IT security teams utilize for minimizing risk in IT environments to OT environments. These controls cover:

- Asset Management
- Network Segmentation
- Threat & Anomaly Detection
- Vulnerability Management

Key Features & Capabilities

- Extends fundamental IT security controls to OT environments
- Provides complete visibility into previously invisible networks
- Continuously detects anomalies, known threats, and zero-day attacks
- Root-cause analysis and risk-based scoring for all alerts
- Real-time threat intelligence updates via the Claroty Cloud
- Prebuilt customizable reports and dashboards
- Seamless integration with IT security infrastructure



Zone	Criticality	Alerts
Endpoint: Oth...	● Low	2
Endpoint: Oth...	● Low	2
Engineering S...	● Medium	2
PLC: Rockwell	● High	2
Broadcast / M...	● Low	1
Camera: Other	● Low	1

- 6 assets were communicating with 5 external IPs
- 17 assets are using 4 unsecured protocols: FTP, SCHNEIDER-NETMANAGE, SMB, SNMP
- 52 assets have 79 unpatched vulnerabilities - Full Match
- Top 7 Risky Assets

OT Assets	115
OT Operations	31
Write and Execute OT Operations	54

Claroty CTD Dashboard

Asset Management

CTD leverages the broadest and deepest OT protocol coverage in the industry and unmatched Passive, Active, and AppDB scanning capabilities to provide comprehensive OT visibility and asset management controls. Claroty is the only vendor to offer this caliber of visibility across all three OT dimensions integral to effective risk calculation and reduction:

1. **Asset Visibility:** This encompasses all assets on an OT network, including serial networks, as well as extensive attributes about each asset, including model number, firewall version, and card slot, among others.
2. **Session Visibility:** This includes all OT network sessions along with their bandwidth, actions taken, changes made, and other details relevant to OT network sessions.
3. **Process Visibility:** This includes tracking of all OT operations, as well as the code section and tag values of all processes with which OT assets are involved.

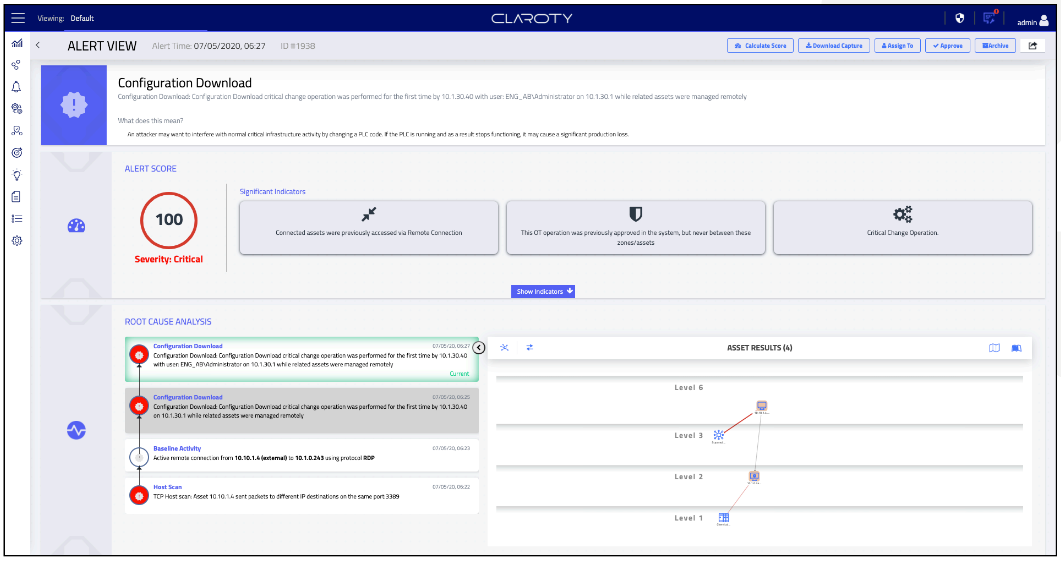
Threat & Anomaly Detection

CTD utilizes five detection engines to automatically profile all assets, communications, and processes in OT networks, generate a behavioral baseline that characterizes legitimate traffic and weeds out false positives, and alerts users in real-time to anomalies and both known and zero-day threats. Highlights:

OT Specific Threat Intelligence: CTD includes OT-specific threat intelligence that is updated in real-time via the Claroty Cloud to support swift detection of malware-related threats.

Contextual Alert Risk Scoring: This single metric is based on the unique context in which each alert is triggered, enabling users to easily filter out false positives and quickly understand and prioritize alerts for triage and mitigation.

Root Cause Analysis: This feature groups all events related to the same attack or incident into a single alert, providing a consolidated view of the chain of events, as well as a root-cause analysis. The result is a higher signal-to-noise ratio, fewer false positives, reduced alert fatigue, and thus more efficient and effective triage and mitigation.



ALERT VIEW Alert Time: 07/05/2020, 06:27 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 07/05/20, 06:27
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 07/05/20, 06:25
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 07/05/20, 06:23
Active remote connection from **10.10.1.4 (external)** to **10.1.0.243** using protocol **RDP**

Host Scan 07/05/20, 06:22
TCP Host scan: Asset 10.10.1.4 sent packets to different IP destinations on the same port:3389

ASSET RESULTS (4)

CTD Alert View with Root-Cause Analysis

Network Segmentation

The extensive OT visibility CTD provides enables it to automatically map and virtually segment OT networks into Virtual Zones, which are logical groups of assets that communicate with one other under normal circumstances. Key benefits:

Cross-zone violations yield real-time alerts that are automatically scored based on risk to help security teams prioritize

Customers without existing physical or logical segmentation can use Virtual Zones as a cost-effective alternative

Customers seeking to implement physical or logical segmentation accelerate such initiatives using Virtual Zones as the blueprint

Customers can integrate CTD with their existing firewalls and network access control (NAC) products to proactively enforce policy-based segmentation and mitigate active attacks

Vulnerability Management

CTD automatically compares each asset in an OT environment to an extensive database of insecure protocols, configurations, and other vulnerabilities tracked by Claroty, as well as to the latest common vulnerabilities and exposures (CVE) data from the National Vulnerability Database. As a result, users can identify, prioritize, and remediate vulnerabilities in OT environments more effectively. Highlights:

- **Exact-Match Vulnerabilities:** The complete OT visibility, including granular details about each asset, provided by CTD facilitates easy and accurate identification of exact-match vulnerabilities.
- **Attack Vector Mapping:** This feature identifies and analyzes all vulnerabilities and risks in an OT environment to automatically calculate the most likely scenarios in which an attacker could compromise the environment. It also provides mitigation recommendations for each scenario.
- **Risk-Based Prioritization:** All vulnerabilities are automatically evaluated and scored based on the unique risk they pose to each OT environment, enabling more efficient and effective prioritization.

About Claroty

Claroty bridges the industrial cybersecurity gap between information technology (IT) and operational technology (OT) environments. Organizations with highly automated production sites and factories that face significant security and financial risk especially need to bridge this gap. Armed with Claroty's converged IT/OT solutions, these enterprises and critical infrastructure operators can leverage their existing IT security processes and technologies to improve the availability, safety, and reliability of their OT assets and networks seamlessly and without requiring downtime or dedicated teams. The result is more uptime and greater efficiency across business and production operations.

Backed and adopted by leading industrial automation vendors, Claroty is deployed on all seven continents globally. The company is headquartered in New York City and has received $100 million in funding since being launched by the famed Team8 foundry in 2015.

CLAROTY

CONTACT US

contact@claroty.com

Copyright © 2020 Claroty Ltd. All rights reserved