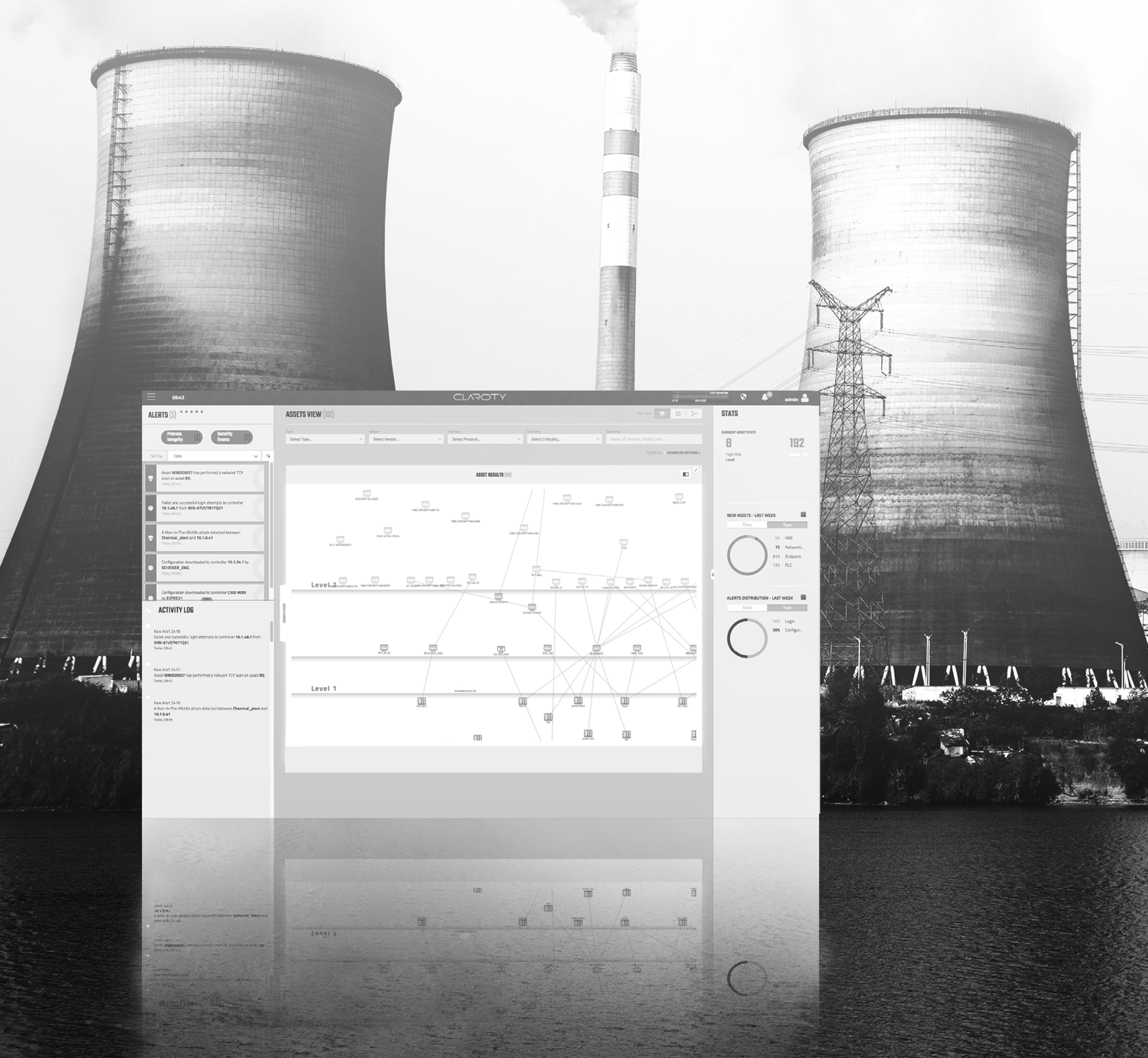
CLAROTY
Clarity for OT Networks

Data Sheet

# Claroty Platform:

## Continuous Threat Detection



Asset **WINDOWS7** has performed a network TCP scan on asset **RO**.
Today, 09:42 |

Failed and successful login attempts to controller **10.1.48.1** from **WIN-67VSTM77Q31**
Today, 09:42 |

A Man-in-The-Middle attack detected between **Chemical_plant** and **10.1.0.41**
Today, 09:39 |

Configuration downloaded to controller **10.1.34.1** by **SCHEIDER_ENG**
Today, 09:38 |

Configuration downloaded to controller **C300 #099** by **EXPDEV1**

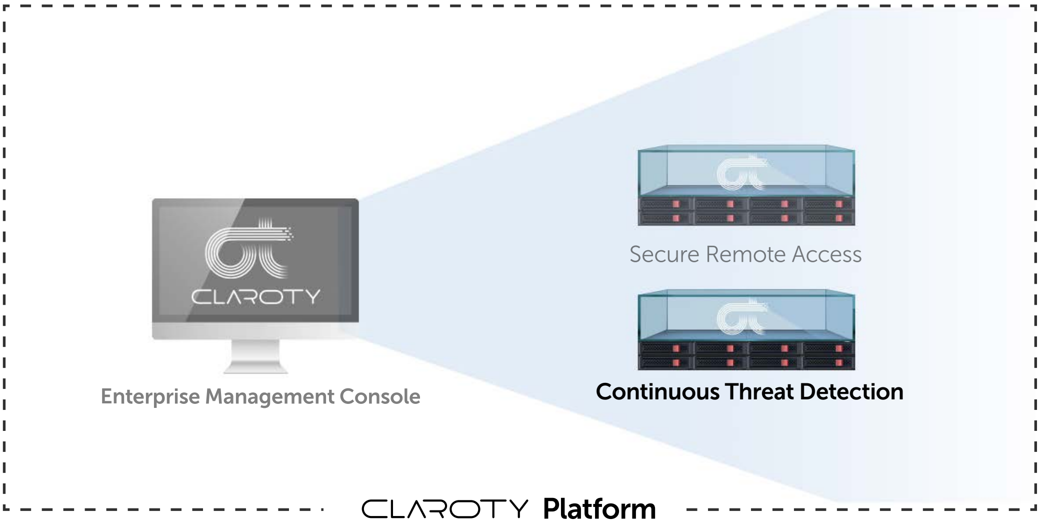
New Alert 2418
Failed and successful login attempts to controller **10.1.48.1** from **WIN-67VSTM77Q31**
Today ,09:42

New Alert 2417
Asset **WINDOWS7** has performed a network TCP scan on asset **RO**.
Today ,09:42

New Alert 2416
A Man-In-The-Middle attack detected between **Chemical_plant** and **10.1.0.41**
Today ,09:39

# Continuous Threat Detection

Continuous Threat Detection is the **anomaly detection** product within the Claroty Platform for ICS networks, providing rapid and concrete situational awareness through real-time alerting.



Claroty **Continuous Threat Detection** constantly monitors industrial control system network traffic and generates alerts for anomalous network behavior that indicates a malicious presence and for changes that have the potential to disrupt the industrial processes.

Continuous Threat Detection software is installed on a server or run as a VM. The system connects to the SPAN port on managed switches or to dedicated hardware taps. Employing deep packet inspection (DPI) on a real-time copy of network traffic, the system uses a safe, fully passive approach that never impacts industrial control systems or the safety and reliability of the process.

When connected to an industrial network, Continuous Threat Detection automatically discovers assets, learns network topology, models the networks unique communication patterns and creates a fine-grain behavioral baseline that characterizes legitimate traffic.  The system provides important insights about network hygiene, configuration issues and vulnerable assets.

Following the learning period, the system shifts to operational mode where alerts are triggered for any violation of the baseline. Continuous Threat Detection generates actionable alerts that are clear, consolidated and context rich. This provides security and control teams rapid situational awareness of potential and actual process disruptions, and enables teams to quickly and efficiently respond to events and maintain the safety and reliability of industrial processes.

# Benefits

## Asset Discovery

The system discovers assets across the entire industrial network – IP assigned, nested assets and assets that communicate over serial connections.  This real-time visibility can be utilized for asset inventory and management tasks, and for addressing various regulatory and internal audit requirements.

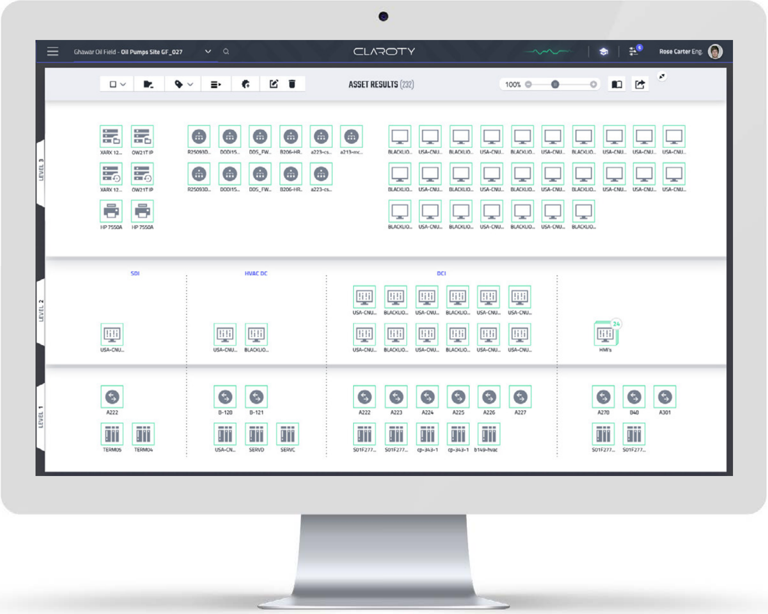


**Figure 1:  Asset Discovery**

**Examples of various data displays:**

- Network graphic representation (asset map).
- **Various graph filters:** Protocols, Asset Types, Criticalities, Risk Levels, Firmware Version, Address, MAC, and Name.
- **Table page, containing all the assets with the following identifiers:** Name, Address, MAC Address, OS, Protocol, Vendor, Type, Criticality Risk Level, Network.
- **Single asset page, containing additional unique identifiers:** Zone, First Seen, Vendor, Serial, Model, Firmware Version, asset network graph, and physical slots data (in a PLC that supports such architecture).
- **Report generation by applying 'Export' on a chosen filtered search.**
  While there are generic identifiers that apply to all assets (IPv4, MAC, Protocols), there are others that are unique to specific products\product groups.

While there are generic identifiers that apply to all assets (IPv4, MAC, Protocols), there are others that are unique to specific products\product groups.

**Examples of the latter include:**

- **PLC Rockwell 1756-L71/B-LOGIX5571:** Vendor, Serial, Number, Firmware Version, Rack Slots physical data.
- **Stratic_8000 Switch:** Host Names, Vendor, Model, Firmware Version.
- **Schneider Electric M430:** Vendor, Model, Firmware Version, Project.
- **Any Windows Endpoint:** OS Version, Host Name.

## Proactive Network Resilience

The system provides deep visibility into the network's assets, networking infrastructure, discovering:

- Networking hygiene issues and misconfigurations
- Weak passwords
- Insecure connections (outbound, or between seemingly segmented zones)
- Software vulnerabilities
- Active sites and remote connections

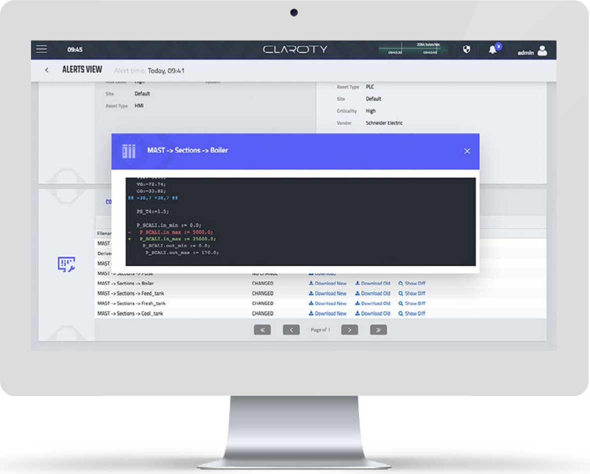
## Security and Operational Alerts

Continuous Threat Detection generates an alert upon occurrence of anomalous and critical events. An event might be a single deviation from an assets' baseline, such as a Windows endpoint issuing a Write command to a controller it has never communicate with before, or more complex, comprising multitudes of such deviations. In this case, the system would apply its analysis engine and conclude the event stream to a single, human readable alert.

Alerts fall into the following groups:

### Critical Change

Any asset communication that imposes direct potential or actual impact on an OT process. The risk of such event is determined by its context. For example, a configuration download to controller is benign when performed by a control engineer as part of operational routine, but poses a significant operational risk when executed by as attacker.



Site Default
Asset Type HMI

Asset Type PLC
Site Default
Criticality High
Vendor Schneider Electric

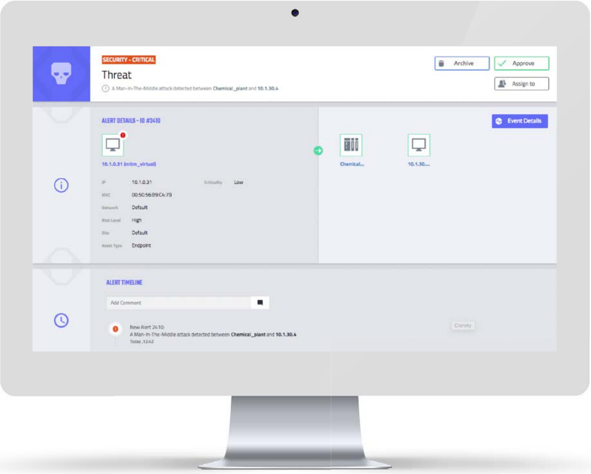
```
    VG:=72.74;
    CG:=33.02;
@@ -38,7 +38,7 @@

    PS_T4:=1.5;

    P_SCALI.in_min := 0.0;
-    P_SCALI.in_max := 5000.0;
+    P_SCALI.in_max := 25000.0;
     P_SCALI.out_min := 0.0;
      P_SCALI.out_max := 170.0;
```

| | | | | |
|---|---|---|---|---|
| MAST -> Sections -> Boiler | CHANGED | Download New | Download Old | Show Diff |
| MAST -> Sections -> Feed_tank | CHANGED | Download New | Download Old | Show Diff |
| MAST -> Sections -> Fresh_tank | CHANGED | Download New | Download Old | Show Diff |
| MAST -> Sections -> Cool_tank | CHANGED | Download New | Download Old | Show Diff |

Figure 2: Critical Change



A Man-In-The-Middle attack detected between Chemical_plant and 10.1.30.4

ALERT DETAILS - ID #2410

10.1.0.31 (mitm_virtual)

IP 10.1.0.31
Criticality Low
MAC 00:50:56:B9:C4:7B
Network Default
Risk Level High
Site Default
Asset Type Endpoint

ALERT TIMELINE

New Alert 2410:
A Man-In-The-Middle attack detected between Chemical_plant and 10.1.30.4
Today ,12:42

Figure 3: Malicious Activity

### Malicious Activity

Asset communication that clearly indicates malicious presence or activity in the network. This might be an early reconnaissance activity such as port scanning, or a more mature attempt to establish a Man in the Middle communication.

**Alert examples:**

- **Configuration Download:** engineering station downloads code to controller.
- **Configuration Upload:** engineering station retrieves controller's code.
- **Mode Change:** controller mode transition (Program, Run, Monitor)
- **Firmware Upgrade:** change in controller firmware.
- **Info Change:** change in an asset's unique identifiers (IP, Name etc.)
- **Online Edit:** change in the code while controller is running.
- **New Asset:** new asset initiates communications in the network.
- **Failed Login:** any connection attempt that
- **Man-in-the-Middle:** compromised device initiates assigns to itself two asset's IP addresses to intercept their exchanged traffic.
- **Network Scan:** asset scans open ports of multiple other assets.
- **Port Scan:** asset scans ports of single asset.

Either baseline deviations, critical change or malicious activity alerts provide the security and control team all the data and context to gain immediate understanding what happened, and which assets were involved. In the case of direct process disruption, such as configuration download or online edit, the alerts even show the exact change to the controller's code, enabling the control team to rapidly reverse the change and restore previous settings.

## Threat Hunting

Proactively search for threats in the network. This would be done in the initial transition from training to operational mode, as well as on ongoing basis to discover malicious operations at their utmost early stage.
Such actions may include:

- Filter assets' baselines on protocols that could be used for external communication (DNS, HTTP\S etc.)
- Closely examine suspicious assets' process changing traffic, such as Write commands and Online Edits
- In case of a discovered breach in certain site – document all the involved traffic patterns and search for them in other sites
- Examine all network traffic that involves file transfer

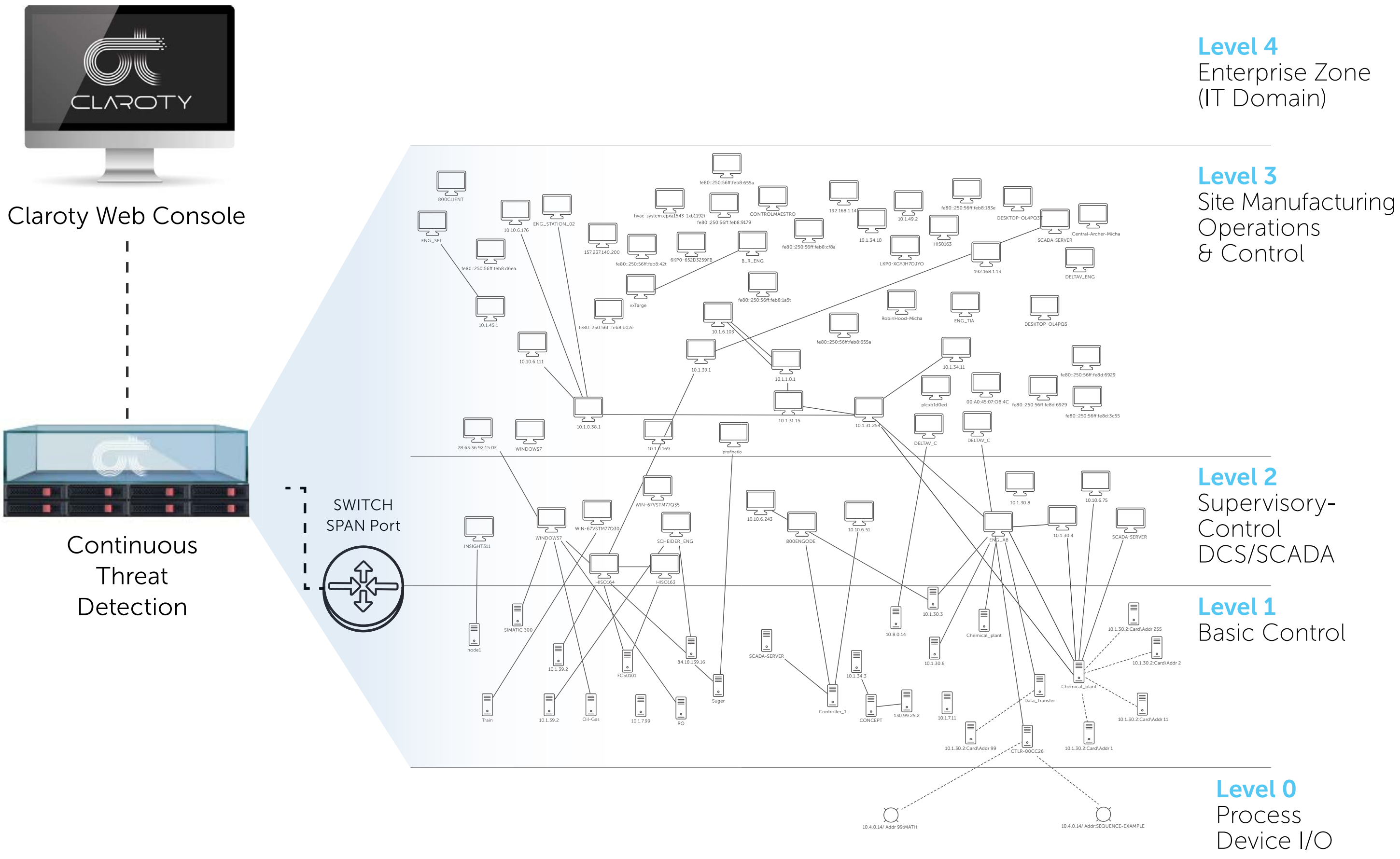
## Central Management and Integration

Continuous Threat Detection is integrated component of the Claroty platform. This includes integration with Secure Remote Access–enabling SOC and plant operations teams to see remote access session information within the timeline.

In a multisite installation (either physically remote sites or isolated production islands) each individual Continuous Threat Detection system sends its processed data to Claroty Enterprise Manager. Integration with Claroty Enterprise Manager supports data over various infrastructures, including data diode or low bandwidth connection (such as satellite communication).

Claroty Enterprise Manager aggregates data from multiple sites and provides a unified view of all sites' assets and alerts. Claroty Enterprise Manager is ideal for SOC deployments providing the security team with immediate insights into the OT network's security posture. The Enterprise Manager can send alert data to various SIEM and log management applications  enabling the security team to correlate OT and IT alerts and gain real time situational awareness to active and potential threats.

# Reference Architecture



Claroty Web Console

Continuous Threat Detection

SWITCH SPAN Port

**Level 4**
Enterprise Zone
(IT Domain)

**Level 3**
Site Manufacturing Operations & Control

**Level 2**
Supervisory-Control DCS/SCADA

**Level 1**
Basic Control

**Level 0**
Process Device I/O