Integration Brief

CLAROTY CONTINUOUS THREAT DETECTION & SWIMLANE SOAR

The integration between Claroty Continuous Threat Detection (CTD) and Swimlane SOAR unifies, streamlines, and automates IT/OT asset discovery and enrichment, vulnerability management, and alert triage workflows. The result is optimal IT/OT security operations from a single-pane-of-glass that eliminates the need for OT-specific monitoring expertise and dedicated tools.

Asset Discovery & Enrichment

Effective network security starts with an accurate asset database. This has historically been challenging in OT networks due to their use of legacy systems, proprietary communication protocols, and diverse sets of operational equipment.

Supporting the broadest list of OT protocols in the industry and multiple asset discovery methodologies, Claroty's integration with Swimlane allows the SOAR platform to retrieve detailed OT asset information through available plugin commands, including:

- Unique asset ID
- Asset type
- List of asset CVEs
- Asset criticality
- Firmware version
- Risk level
- And more

Integration Specs

Requirements

Claroty CTD v4.2+ | Swimlane SOAR

Highlights

- Identify and compile all OT asset data into the SOAR system
- Automate vulnerability management with context-rich playbooks for event resolution
- Threat detection engines identify and parse events to alert Swimlane for further ticketing and analysis

About Claroty CTD

Claroty CTD provides full visibility and security controls for OT environments. Powered by Claroty's proprietary DPI technology, CTD extracts precise details about each asset on the OT network, profiles all communications and protocols, generates a behavioral baseline that characterizes legitimate traffic, and alerts you in real-time to anomalies, exact-match vulnerabilities, and known and zero-day threats

About Swimlane SOAR

Swimlane is a leader in security orchestration, automation and response (SOAR). By automating time-intensive, manual processes and delivering powerful, consolidated analytics, real time dashboards and reporting from across your security infrastructure, Swimlane maximizes the incident response capabilities of over-burdened and understaffed security operations.

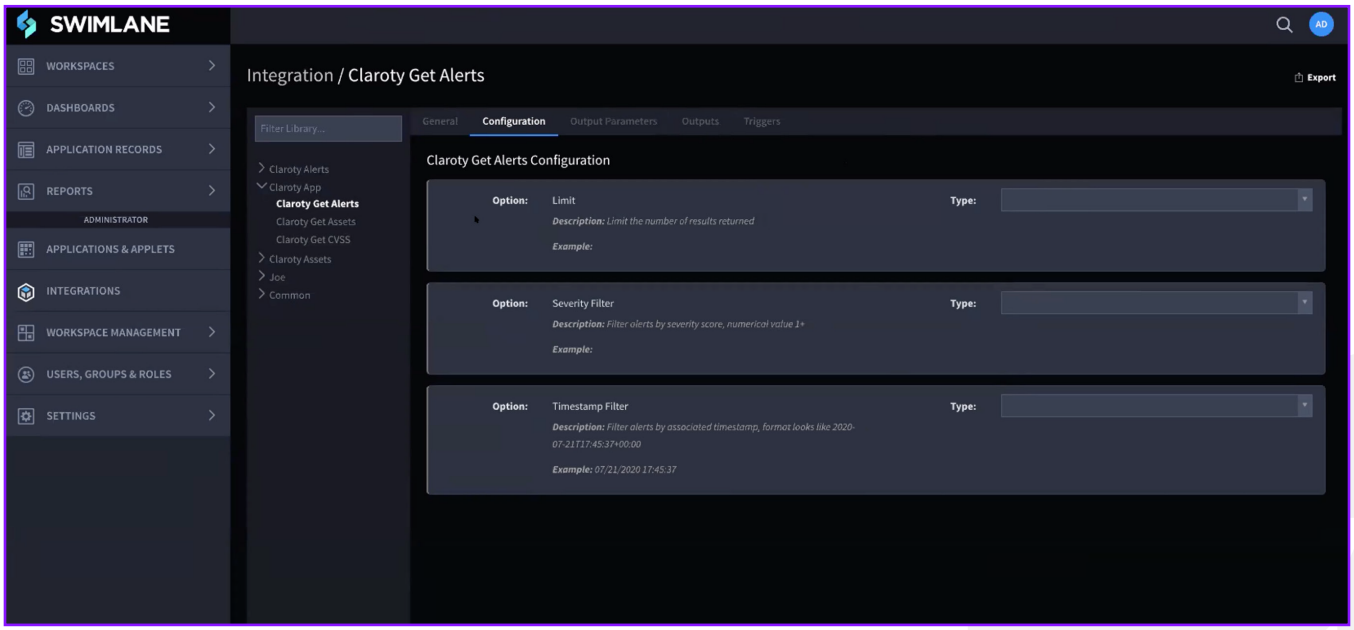
Vulnerability Management

With the latest OT-specific threat intelligence, including unique insights and threat signatures from the Claroty Research Team, Indicators of Compromise (IoCs), and common vulnerabilities and exposures (CVE) data from the National Vulnerability Database (NVD), Claroty CTD is able to support Swimlane in creating context-rich tickets with actionable information. Within Claroty CTD, insights are available for all network assets including:

- **Full-Match CVEs**: Real-time discovery and assessment of exact-match CVEs in network assets
- **Attack Vectors:** Automatically provides the most likely scenario of network compromise
- **Risk Dashboard**: Customizable dashboard that provides an overview of risk analytics

Threat Detection & Swimlane Workflows

Reduced Alert Fatigue: CTD utilizes its advanced Threat Detection Engines, Risk Definition Algorithm, and Root Cause Analysis features to evaluate the context and risk of each event and consolidate interrelated events into a single alert. This produces both fewer false positives and fewer alerts in general, resulting in reduced alert fatigue.



Claroty App configuration within Swimlane

OT Events & Alerts: CTD utilizes five threat detection engines to identify events in OT environments, resulting in full OT security monitoring coverage without the need for OT expertise. These threat detection engines include:

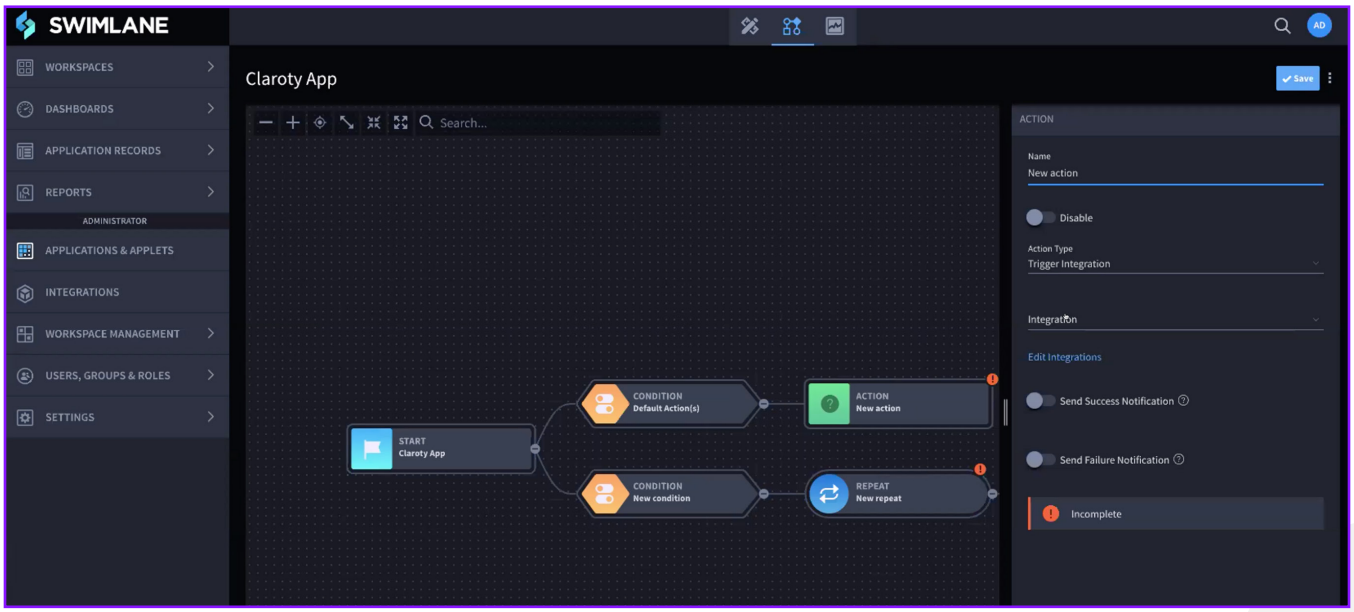
- Anomaly Detection
- Security Behaviors
- Known Threats
- Operational Behaviors
- Custom Rules

The Claroty plugin within Swimlane provides a host of commands available to retrieve relevant information about alerts on the network, and can be customized with options like alert type, asset vendor, and time of day. Each OT event identified by CTD is automatically ingested by Claroty's Risk Definition Algorithm to assess whether it poses a real risk to the environment or a false positive, in which case an alert is created or the event is automatically archived.

Swimlane Workflows

When CTD detects an event, the integration enables Swimlane to ingest it and automatically implement a corresponding workflow. These workflows can consist of many different actions to triage events and are highly customizable based on defined procedures.

Alert workflows begin when an event is triggered within the system, either manually or by an automated adapter such as the Claroty Get Alert command. The workflow contains a list of resolution tasks specific to the triggering event, as well as conditional gateways that take output from the workflow and determine the appropriate next steps. Additional plugins can be used within the task list to provide a more holistic view of a given incident, such as indicator databases, notification, and project management tools. Once an alert has been remediated, Swimlane can also kick off automated workflows to update affected systems and alert teams to the issue to ensure no detail is left behind.



Swimlane alert workflow

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