IBM QRadar

CLAROTY
Clarity for OT Networks

Integration Brief

QRadar and Claroty – Advanced Detection, Triage, Investigation and Response

Continuously monitor OT-Networks to protect against cyberattacks and operational issues

QRadar and Claroty – Advanced Detection, Triage, Investigation and Response

Solution Highlights

- **Unifies IT & OT Security** allows critical infrastructure organizations to assess, monitor and mitigate potential threats across their entire infrastructure
- **Reduces OT-Related Security Risks** proactively identify and fix configuration and other network hygiene issues that can leave your network vulnerable to attacks
- **Strengthens Operational Resilience** with real-time contextual alerting and immediate understanding of the implications on process integrity and cyber resiliency

Business Drivers

While many enterprises have made great strides in protecting their IT business networks, industrial control system (ICS) networks remain at risk. Commissioned decades ago, without cybersecurity in mind and sometimes running outdated software, many of these networks and underlying assets are being increasingly targeted with sophisticated cyberattacks or are connected to IT networks and at risk of a "spill-over" effect from broader attacks. In fact, a number of documented attacks such as Industroyer CrashOverride, WannaCry, NotPetya BlackEnergy and STUXNET have created significant operational damage, disrupting production and putting environmental and personal safety at risk.

Until now, gaining deep visibility into ICS networks, their underlying communications patterns and protocols, and detail on process-specific devices has been extremely challenging and has left industrial enterprises largely blind to potential security risks. Without this contextual insight, industrial operators have been challenged to proactively protect the control network from cyberattacks and avoid production disruptions.

Solution Overview

To address this lack of visibility into the security and resiliency of OT networks without burdening security teams with another monitoring tool, Claroty has partnered with IBM to provide a broad security solution which spans both IT and OT environments.

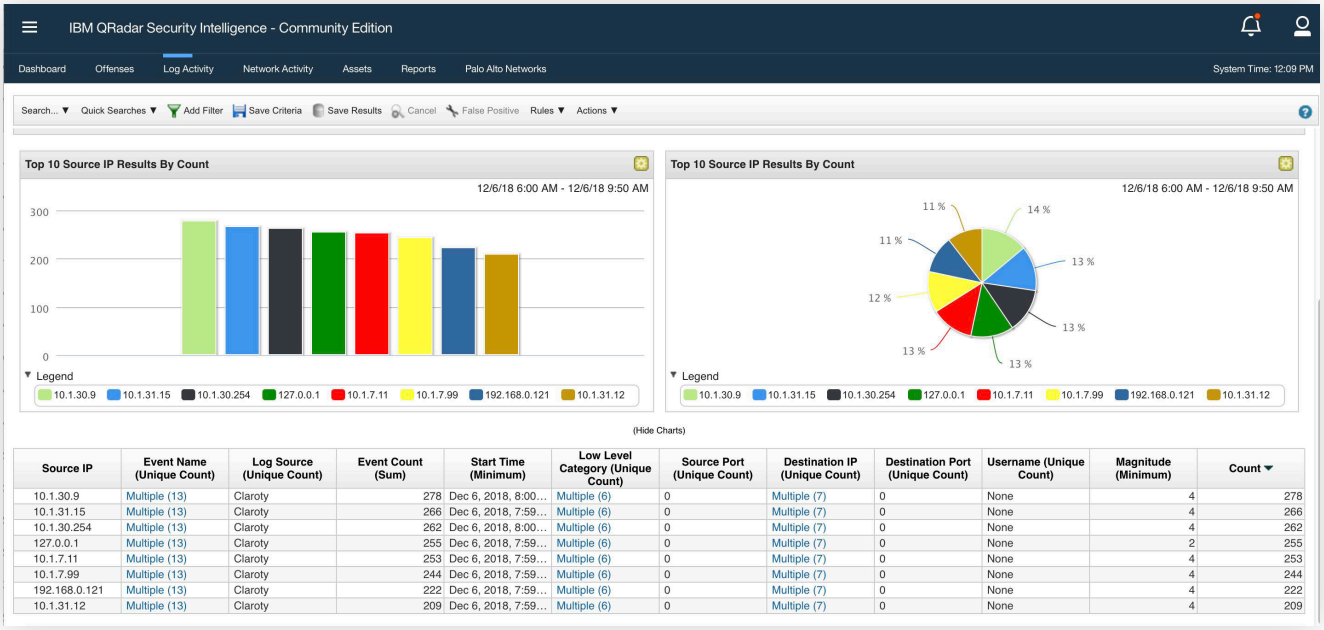
Claroty's industry-leading OT industrial cybersecurity platform provides deep OT visibility and threat detection, and tight integration with IBM's QRadar Security Information Event Management (SIEM) platform enables SOC teams to efficiently monitor and respond to both IT and OT security alerts from a single pane of glass.

Unified Visibility and Management
Claroty's unique network monitoring capabilities provide extreme visibility into the lowest levels of industrial networks, enabling security teams to identify OT threats more quickly. The insight Claroty delivers to SOC analysts into the assets and protocols deployed in their industrial environment, along with ICS-aware behavioral based-modeling to rapidly detect abnormal behavior. OT security alerts are delivered to QRadar, for a truly integrated IT/OT security monitoring, policy management and incident response solution.

Claroty Continuous Threat Detection (CTD) automatically discovers and monitors network assets, protocols, and communication patterns all the way down to the I/O level and build an operational baseline of "know good" behavior. Consequently, any anomalous activity is immediately creates an alert, enabling security teams to evaluate events as they emerge, determine consequent risk levels, and prioritize response as appropriate.

For example, when a high-risk activity is discovered, SOC teams can drill down to obtain a detailed view of the action/violation that resulted in the alert. Leveraging Claroty's extreme visibility, SOC and security personnel are provided with contextual real-time information to accurately and effectively investigate Indicators of Compromise (IoC) – materially reducing response times and enhance cyber resiliency.

QRadar and Claroty – Advanced Detection, Triage, Investigation and Response



Source IP	Event Name (Unique Count)	Log Source (Unique Count)	Event Count (Sum)	Start Time (Minimum)	Low Level Category (Unique Count)	Source Port (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Username (Unique Count)	Magnitude (Minimum)	Count
10.1.30.9	Multiple (13)	Claroty	278	Dec 6, 2018, 8:00...	Multiple (6)	0	Multiple (7)	0	None	4	278
10.1.31.15	Multiple (13)	Claroty	266	Dec 6, 2018, 7:59...	Multiple (6)	0	Multiple (7)	0	None	4	266
10.1.30.254	Multiple (13)	Claroty	262	Dec 6, 2018, 8:00...	Multiple (6)	0	Multiple (7)	0	None	4	262
127.0.0.1	Multiple (13)	Claroty	255	Dec 6, 2018, 7:59...	Multiple (6)	0	Multiple (7)	0	None	2	255
10.1.7.11	Multiple (13)	Claroty	253	Dec 6, 2018, 7:59...	Multiple (6)	0	Multiple (7)	0	None	4	253
10.1.7.99	Multiple (13)	Claroty	244	Dec 6, 2018, 7:59...	Multiple (6)	0	Multiple (7)	0	None	4	244
192.168.0.121	Multiple (13)	Claroty	222	Dec 6, 2018, 7:59...	Multiple (6)	0	Multiple (7)	0	None	4	222
10.1.31.12	Multiple (13)	Claroty	209	Dec 6, 2018, 7:59...	Multiple (6)	0	Multiple (7)	0	None	4	209

Figure1 – IBM QRadar Security Intelligence SOC dashboard displaying detailed ICS-specific threat information

Summary

The increased digitization and connectivity of OT networks has delivered monumental advancements in industrial productivity. However, this connectivity has also increased the risk of ICS-targeted malware attacks and spill-over damage from broad-based cyberattacks.

Enterprise security teams, already over-burdened by protection of expansive IT environments, are increasingly taking responsibility for securing OT networks into which they have had little visibility. To meet this challenge, cybersecurity solutions must provide an efficient means of detecting and responding to cyberthreats no matter where in the infrastructure they are. IBM and Claroty recognize these challenges and have moved aggressively to deliver a highly-effective, integrated cybersecurity solution. Leveraging Claroty's Continuous Threat Detection and IBM's QRadar platform, security teams can now continuously monitor for threats, evaluate events as they emerge, determine consequent risk levels, and prioritize response as appropriate.

QRadar and Claroty – Advanced Detection, Triage, Investigation and Response

The Claroty Platform

Claroty's fully integrated suite of cybersecurity products addresses the unique challenges of ICS systems so that engineers, operators, and cybersecurity professionals can protect even the most complex industrial networks.

The Claroty Platform enables enterprises to assess the security posture of their ICS network, protect critical systems, control access to network assets, continuously monitor and detect vulnerabilities and threats, and rapidly investigate and respond to cyber incidents.

IBM QRadar

Helps security teams accurately detect and prioritize threats across the enterprise and provides intelligent insights that enable teams to respond quickly to reduce the impact of security incidents. By consolidating log events and network flow data from thousands of devices, endpoints and applications distributed throughout your network, QRadar correlates all this different information and aggregates related events into single alerts to accelerates incident analysis and remediation.

Contact Us

CLAROTY

Claroty was conceived to secure the safety and reliability of industrial control networks that run the world from cyber-attacks. The Claroty Platform is an integrated set of cyber security products that provides extreme visibility, unmatched cyber threat detection, secure remote access, and risk assessments for industrial control networks (ICS/OT).

www.claroty.com | contact@claroty.com |