Integration Brief

THE CROWDSTRIKE-CLAROTY JOINT SOLUTION

Full-spectrum IT/OT Visibility & Threat Detection Coverage for ICS Networks

The Challenge

Digital transformation has shifted the security posture of industrial enterprises and critical infrastructure organizations by creating connectivity between previously isolated operational technology (OT) environments and their usually highly connected information technology (IT) counterparts.

These conditions have given rise to converged IT/OT industrial control system (ICS) networks with expanded attack surfaces that provide threats with clear pathways across the once-impenetrable IT/OT boundary.

Protecting these inherently insecure ICS networks is increasingly becoming the responsibility of IT and security operations center (SOC) teams. However, since the OT environments within such networks are incompatible with traditional IT security tools, they are largely invisible to these teams. The result is an incomplete inventory of IT/OT assets and inability to effectively detect, assess, and mitigate the threats and corresponding risks they face.

Highlights

The CrowdStrike-Claroty Joint Solution provides:

- Enhanced detection of ICS threats across the IT/OT boundary, as well as in the plant's HMI and EW systems, by integrating CrowdStrike's threat detection platform for identifying targeted and compromised endpoints with Claroty's comprehensive OT security platform
- Greater visibility and a single source of truth for IT/OT assets across all connected sites by enabling Claroty to identify and enrich HMIs, in addition to OT assets controlled by the HMIs, in ICS networks —all without having to connect to those networks
- Increased ROI of CrowdStrike Falcon and The Claroty Platform by bringing together OT-specific network information from Claroty with the broad endpoint telemetry from CrowdStrike and giving joint customers the ability to further capitalize on their existing investments in these solutions

From The Claroty Platform

- OT Asset Discovery & Management
- Continuous ICS Monitoring
- Broad OT Indicators of Attack

From CrowdStrike Falcon

- IT Endpoint Protection
- Vast Global Install Base
- Broad IT Indicators of Attack

The Solution

Endpoint protection leader CrowdStrike and industrial cybersecurity leader Claroty have partnered to deliver a complete ICS security solution that bridges the gap between the IT/OT boundary and ICS networks and enhances the already-extensive capabilities of each company's respective offerings.

By combining Claroty's unmatched OT expertise, threat signature database, and asset discovery and monitoring technology with CrowdStrike's industry-leading endpoint telemetry and vast install base, the joint solution delivers full-spectrum IT/OT visibility and threat detection coverage for ICS networks.

	Use Case	Benefits
Threat Detection	The joint solution fuses CrowdStrike's ability to identify targeted and compromised endpoints with Claroty's extensive OT monitoring capabilities directly within The Claroty Platform. The result is a combined database of proprietary and open-source YARA and Snort rules from both CrowdStrike and Claroty, making it the industry's largest and most-actionable IT/OT threat signature database for ICS networks. All signatures can be immediately pushed from The Claroty Platform's Enterprise Management Console (EMC) to all connected sites in just one click.	• Surface even more potentially malicious events—including those indicative of the targeting of ICS-specific processes—in ICS networks • Better detection of ICS threats that initially enter the IT environment before penetrating the OT environment • Reduction in false positives—and thus in alert fatigue and mean times to detect (MTTD) and respond (MTTR)—with more-actionable threat signatures • Unified, highly scalable ICS threat detection capabilities that extend seamlessly across all connected sites
Asset Discovery & Enrichment	Combining both ICS endpoint and network sources, the joint solution enables Claroty to automatically identify and enrich certain IT-oriented ICS assets, such as human machine interfaces (HMIs), historian databases, and engineering workstations (EWs), in which a CrowdStrike agent is installed in OT environments. Claroty does this by fetching each asset's configuration file from CrowdStrike and then parsing that file, so it does not require connecting to the ICS network.	• The ability to gain greater visibility into isolated OT environments, as well as a single source of truth for IT/OT asset information—all without having to connect to the ICS network • The caliber of OT visibility required to lay the foundation for optimal ICS threat detection, vulnerability management, and strengthened security posture • The ability to safely install CrowdStrike agents in OT environments within ICS networks, thereby harnessing The Claroty Platform to extend the capabilities of CrowdStrike Falcon from IT to OT

The Technology

The CrowdStrike-Claroty Joint Solution encompasses two core functionalities:

1) Enhanced Detection of ICS Threat across the IT/OT Boundary

This solution enables the automated population of YARA and Snort rules from CrowdStrike's threat signature database, which is largely IT-oriented, alongside those from Claroty's database, which is largely OT-oriented, directly within The Claroty Platform.

While most joint customers already utilize signatures from both CrowdStrike and Claroty, configuration differences between IT and OT threat signatures have historically required some signatures to be manually reconfigured before being executed for detection in ICS networks.

The CrowdStrike-Claroty Joint Solution addresses this issue. It enables joint customers to not only execute all IT and OT threat signatures from both databases without requiring manual reconfiguration-but also to push those signatures from The Claroty Platform's EMC to all connected sites in just one click.

As a result, joint customers are able to more-effectively and efficiently detect threats across the IT/OT boundary for the ICS networks across all of their connected sites via The Claroty Platform. This functionality ensures ICS monitoring efforts are unified, scalable, and consistent, further reduces false positives, MTTD, and MTTR, and further increases the ROI of both solutions.

2) Greater ICS Network Visibility & a Single Source of Truth for IT/OT Asset Information

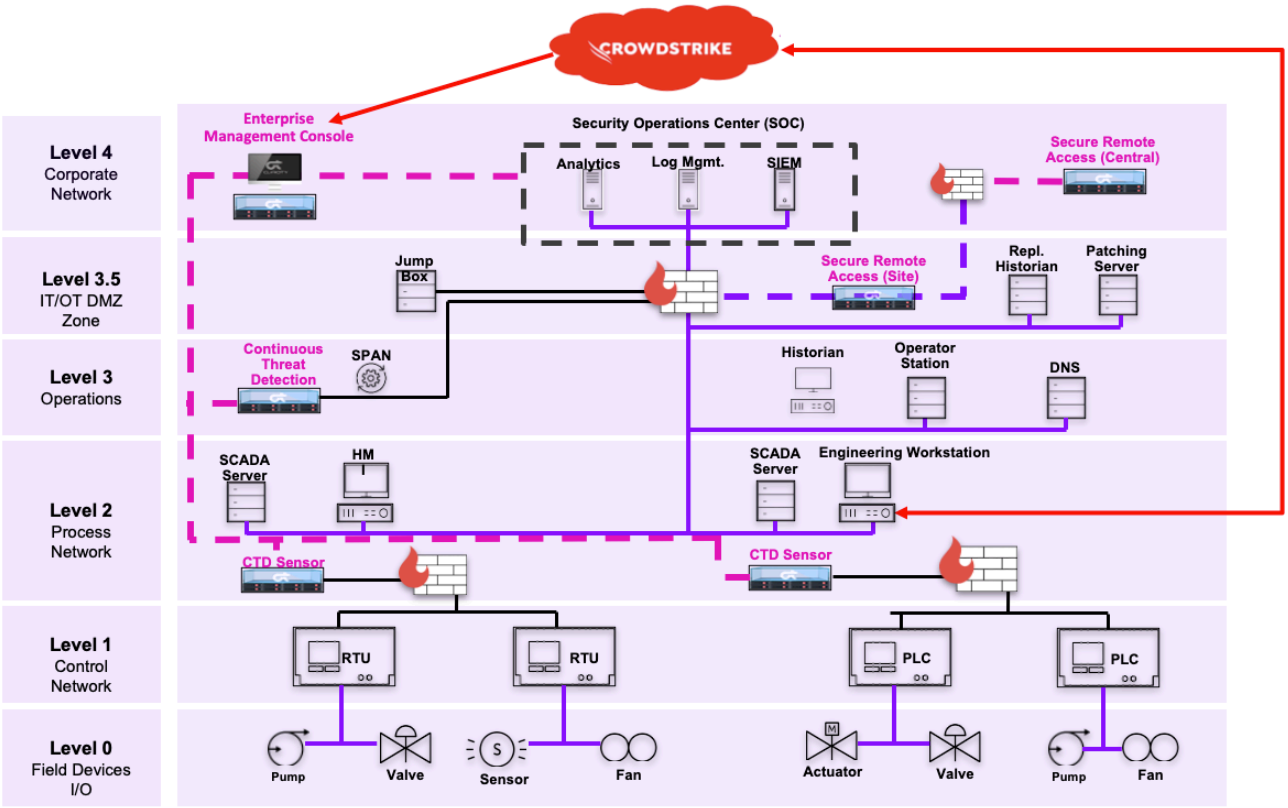
The OT environments within ICS networks typically include various types of IT-oriented assets such as HMIs, EWs, and historian databases. The CrowdStrike-Claroty Joint Solution makes it possible for The Claroty Platform to automatically identify and enrich any such assets in which a CrowdStrike agent is installed.

After The Claroty Platform utilizes its passive scanning technology to identify such an asset, it triggers a request to CrowdStrike Falcon to fetch the configuration file present on that asset.

Next, Claroty parses this file to obtain additional information about the asset, including its programs running, removable media, configuration files, and other details that can further enrich joint customers' asset database and create a single source of truth for IT/OT asset information within The Claroty Platform.

The result is even greater visibility into the ICS network, which consequently leads to fewer false positives, stronger security, and the ability to safely and seamlessly extend existing benefits and use cases of CrowdStrike Falcon from the IT to OT environments within ICS networks.

Joint customers whose OT environments do not currently include HMIs, EWs, or other IT assets in which CrowdStrike is installed are encouraged to install it accordingly to harness the benefits of this functionality.



Sample deployment architecture diagram of The CrowdStrike-Claroty Joint Solution

About CrowdStrike

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over two trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: We stop breaches. Learn more: https://www.crowdstrike.com/

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.

CONTACT US
contact@claroty.com