CLAROTY

Industry Snapshot

MIDSTREAM AND DOWNSTREAM OIL & GAS

How Claroty Supports the Midstream and Downstream Sectors of the Oil & Gas Industry

Claroty customers include nearly 60% of the top 50 oil & gas refineries and pipeline operators globally. Our work with these midstream and downstream companies primarily focuses on strengthening their industrial cybersecurity to reduce their exposure to cyber risks, ensure the safety and integrity of their industrial processes, and preserve their operational and overall business continuity.

This document details the top industrial cybersecurity challenges in the midstream and downstream oil & gas sectors, how Claroty helps our customers overcome such challenges to achieve effective industrial cybersecurity, and sample architectures for deployments of The Claroty Platform among these customers.

Top Industrial Cybersecurity Challenges

The top industrial cybersecurity challenges among midstream and downstream oil & gas companies are arguably best exemplified by the **TRITON** cyber attack, which compromised the operational technology (OT) process safety systems and halted industrial operations at a Middle Eastern petrochemical plant in 2017.

Believed to have initially entered the company's corporate information technology (IT) network via phishing back in 2014, the TRITON attackers eventually found an unsecured pathway into the industrial network underpinning the industrial processes in the petrochemical plant. From there, they gained access to an engineering workstation connected to the plant's safety instrumented systems (SIS) and obtained details about those systems' hardware and firmware.

This information, along with a zero-day vulnerability in the firmware, ultimately enabled the attackers to develop and inject malware that allowed them to manipulate the SIS controllers remotely. But, amid the attackers' attempts to reprogram the SIS controllers—which could have disabled them and created an unsafe situation within the plant—the controllers entered a failed safe state, resulting in the automatic shutdown of the plant's industrial processes.

Considered the first-known incident to involve malware targeting OT safety systems designed to prevent an industrial disaster, the TRITON cyber attack underscores the following industrial cybersecurity challenges that remain prevalent among the midstream and downstream sectors of the oil & gas industry:

- **Digital transformation can expand the attack surface.**

Unsecured connectivity between the petrochemical company's IT and industrial networks is ultimately what enabled the TRITON attackers to access and compromise the SIS controllers. It's important to recognize that digital transformation initiatives—particularly those involving systems that boost the efficiency of refinery and pipeline operations and performance audits, among others—are often the culprit of such connectivity.

These types of initiatives usually require some degree of IT/OT connectivity, which is commonly implemented without fully accounting for the considerable risks inherent to convergence between already-widely connected corporate IT networks and their previously isolated—and typically, inherently insecure—industrialcounterparts.

The result, in many cases, is a greatly expanded attack surface that gives threats that originate in the IT network numerous direct or indirect pathways into the OT network and the critical systems and physical processes it underpins.

- **The composition of industrial networks can limit visibility.**

Widespread geographic distribution, the prevalence of legacy systems, and a diverse patchwork of assets from different vendors that use different proprietary protocols are all relatively standard characteristics of industrial networks at refineries, pipeline operators, and other types of midstream or downstream oil & gas facilities.

Unfortunately, these characteristics also tend to complicate efforts to establish and maintain a comprehensive inventory of OT, IoT, and IIoT assets and establish the behavioral baselines required to identify and address anomalous and potentially malicious events on the network.

In the TRITON cyber attack, the plant staff was unaware of the attackers' lengthy presence in the industrial network until their attempts to manipulate the SIS controllers were stymied by the automatic shutdown triggered by the failed safe state. As a result, it has been widely speculated that the staff lacked visibility into the lower levels of the industrial network, known as the process control network (PCN), because the attackers' activities were not immediately detected as deviations from the PCN's baseline behavior.

Establishing such a baseline is impossible without a full inventory of each asset within the PCN, the ability to identify and read the protocols they utilize, and an understanding of how they operate and communicate under normal circumstances.

- **Limited OT visibility also limits detection and vulnerability management capabilities.**

The limited visibility that likely prevented the petrochemical plant's staff from creating an OT baseline hindered their ability to detect not only the behavioral anomalies through which TRITON malware manifests—but also other types of threats and vulnerabilities. Specifically:

  - Known threats, such as those detectable via Snort signatures, YARA rules, or other types of indicators of compromise
  - Threats associated with high-risk security behaviors, such as port scanning, man-in-the-middle attacks, or TAG/address scans
  - Threats associated with high-risk operational behaviors, such as firmware downloads or read and write commands to programmable logic controllers (PLCs)
  - Threats associated with predefined high-risk activities, such as process value changes or abnormal communications between network zones
  - Full-match vulnerabilities. Identifying common vulnerabilities and exposures (CVEs) in any industrial network requires mapping each of that network's assets to the exact vendor, model, firmware version, and serial number, among other details, of each CVE's affected asset(s).

    Without full visibility into such details of each asset, it is largely impossible to determine with high confidence whether a given CVE is actually present within that network. This typically leads to an overabundance of false positives, inefficient and ineffective prioritization and remediation, and ultimately, an increased exposure to risk.

- **Reliance on OT remote access with insufficient controls increases risk exposure.**

The TRITON attackers' years-long ability to remotely access the targeted petrochemical plant's industrial network highlights the considerable risks inherent to OT remote access. These conditions suggest the plant lacked the ability to effectively control and monitor remote OT connectivity, thereby making it exceedingly difficult (if not impossible) for plant staff to identify unauthorized industrial network activity—including from the TRITON attackers—occurring via remote access.

Given that widespread geographic distribution, a vast physical footprint, and heavy reliance on various contractors and third-party OT vendors are common among oil & gas refineries and pipelines, OT remote access is typically a critical necessity for such companies. But without the ability to enforce granular policy- and role-based access controls, limit all remote sessions by activity, asset, time, and other variables, and properly secure user credentials, OT remote access remains extremely risky.

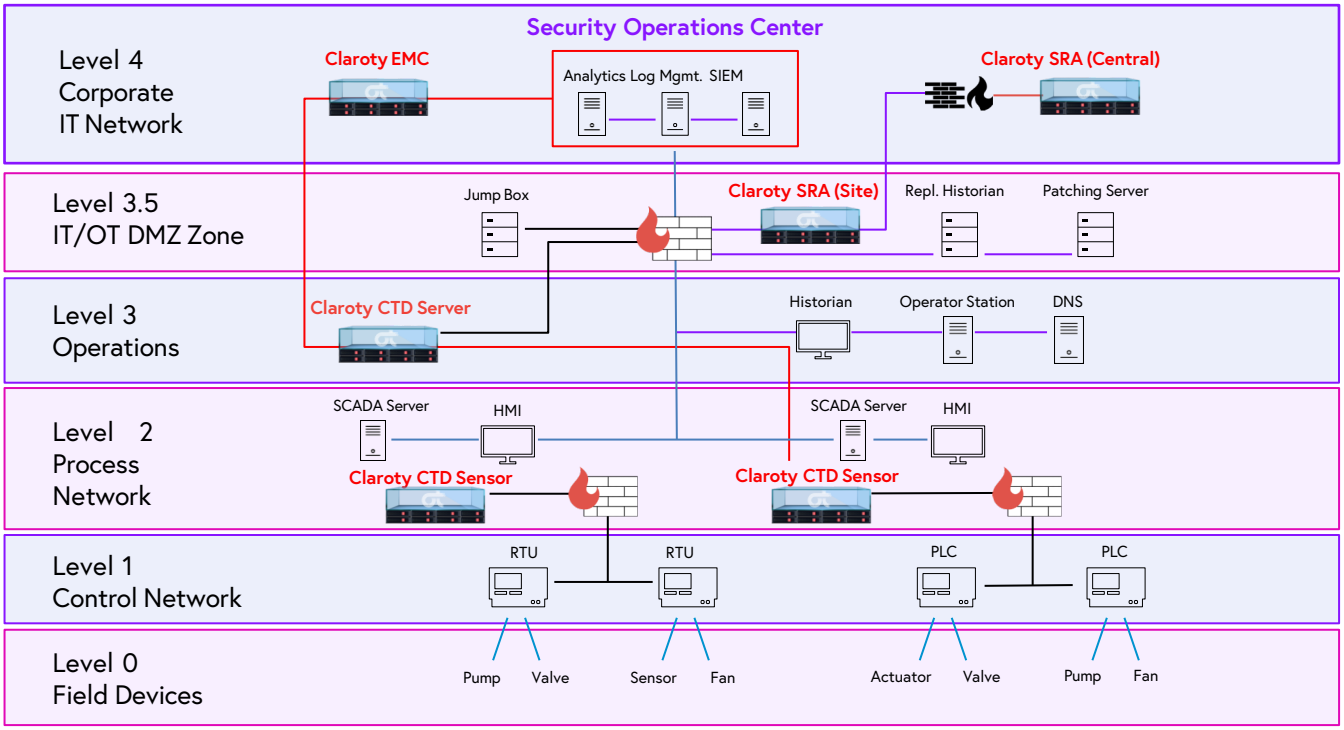
Indeed, more than 70% of the industrial control system (ICS) vulnerabilities disclosed during the first half of 2020 can be exploited remotely, underscoring the critical importance of properly securing all OT remote access connections.

How The Claroty Platform Addresses Top Industrial Cybersecurity Challenges

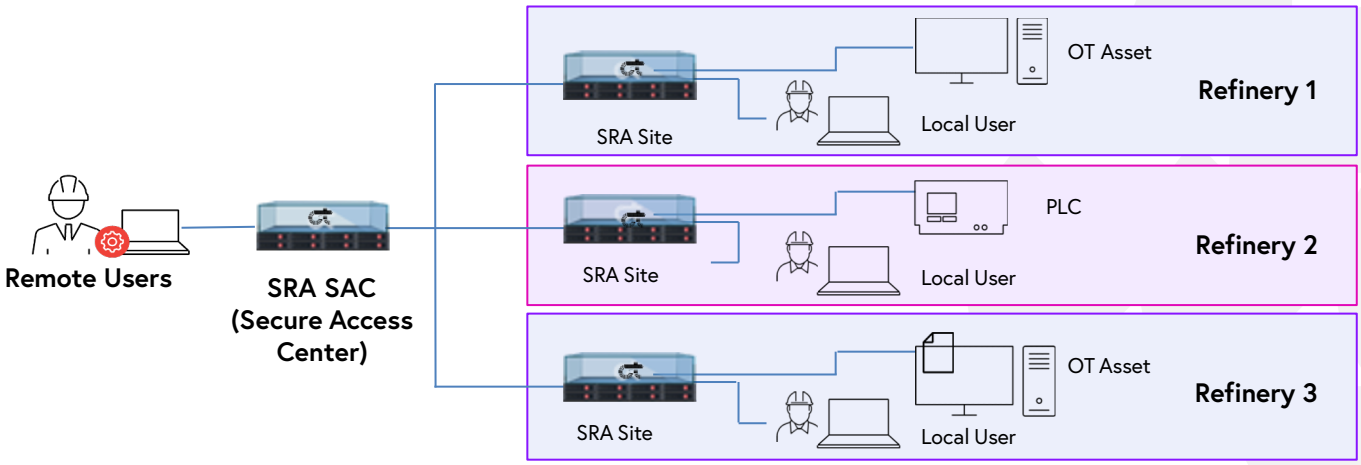
At Claroty, we empower our customers in the midstream and downstream sectors of the oil & gas industry to overcome the industrial cybersecurity challenges they face by implementing the following controls via The Claroty Platform:

Visibility	Threat Detection	Vulnerability Management	Triage & Mitigation	Secure Remote Access
• **Automated asset discovery & management** and full **asset, network, and process visibility** lay the foundation for stronger security, safety, and operational efficiency. • This caliber of visibility also drives Claroty's **Virtual Zones**, the industry's only suitable alternative to essential yet costly and labor-intensive physical segmentation.	• **Continuous security monitoring** via five distinct detection engines ensures real-time detection of both known and unknown threats. • **Proprietary threat signatures** uncovered and routinely updated by the Claroty Research Team further expedite and contextualize detection efforts.	• Full OT visibility enables rapid identification of **full-match vulnerabilities** with high confidence and minimal false positives. • **Ongoing risk assessment** at the asset, zone, site, and overall environment levels helps optimize prioritization efforts and inform compensating controls when patching cannot occur immediately.	• Claroty's **Root-Cause Analysis** alerting bundles and contextualizes interrelated events into one alert that shows the full chain of events across the cyber kill chain, enabling rapid triage and reduced alert fatigue. • **Attack Vector Mapping** and ongoing risk assessment of industrial networks further contextualize alerts for efficient triage & mitigation workflows.	• Claroty **Secure Remote Access (SRA)** is the industry's only native secure remote access solution for OT. • SRA's granular access and monitoring controls and architecture that preserves the Purdue Model **minimize the risks** posed by remote employees and third-parties. • SRA enhances alert response and investigation capabilities via **The Claroty Platform.**

The Claroty Platform: Sample Deployment Architecture



Claroty Secure Remote Access: Sample Multi-Site Deployment Architecture



About Claroty

Claroty is the industrial cybersecurity company. Trusted by the world's largest enterprises, Claroty helps customers reveal, protect, and manage their OT, IoT, and IIoT assets. The company's comprehensive platform connects seamlessly with customers' existing infrastructure and programs while providing a full range of industrial cybersecurity controls for visibility, threat detection, risk and vulnerability management, and secure remote access—all with a significantly reduced total cost of ownership.

Claroty is backed and adopted by leading industrial automation vendors, with an expansive partner ecosystem and award-winning research team. The company is headquartered in New York City and has a presence in Europe, Asia- Pacific, and Latin America, and deployments on all seven continents.

CONTACT US

contact@claroty.com