CLAROTY

CASE STUDY

OIL & GAS

Southeast Asian Oil & Gas Giant Reduces the Attack Surface & Secures Operations with Claroty

The Challenge

This southeast Asian oil and gas industry firm's security, engineering, and executive personnel all recognized that preserving the availability, integrity, and safety of its hydrocarbon production operations required a robust operational technology (OT) cybersecurity program. However, the company's head of OT cyber operations also knew it would not be possible to achieve this alone due to the following conditions:

- Like most critical industrial organizations, this organization had historically struggled to maintain a comprehensive, up-to-date inventory of the diverse range of assets that underpin operations at each of its industrial plants and production sites.
- The existing security and inventory tools were not sufficiently compatible with the complex systems and proprietary protocols used by this diverse range of assets.
- The above visibility and technical challenges meant the company's security and engineering personnel were limited in their ability to not only identify and mitigate vulnerabilities affecting industrial assets, but also to monitor for and respond to threats to its hydrocarbon production operations.

"We are now able to secure the entire OT environment thanks to the in-depth information and controls provided by Claroty."

Head of OT Cyber Operations

"I can look at Claroty and see how the system communicates, understand where the disconnection is happening, and when the last communication started."

Head of OT Cyber Operations

The Need

The OT cyber operations head recommended the company deploy a cybersecurity solution capable of delivering the visibility, risk management, and monitoring capabilities required to protect the company's entire OT environment. The chosen solution would need to satisfy the following key criteria:

1. Provide comprehensive asset & risk visibility

The solution must automatically reveal and contextualize all assets, connectivity paths, and processes spanning all sites comprising their vast OT environment.

Additionally, the solution must also effectively assess, prioritize, and inform the mitigation of risk at the asset and site levels with the overarching goal of delivering insight into how "dirty" or "clean" each site's risk hygiene is — as well as what can be done to reduce risk.

2. Enable centralized management & actionable reporting

The solution must centralize, ensure the accuracy of, and serve as the single source of truth for all information generated and consumed by the systems and personnel involved in the day-to-day upkeep and strategic optimization of their vast OT environment.

Key insights must also be accessible and actionable via reporting that can be tailored to the needs of an extensive assortment of security, engineering, and executive users and use cases.

3. Be powered by OT purpose-built technology

The solution must be designed for — and backed by deep domain expertise in — the unique specifications of OT. This requires being compatible with the proprietary protocols used by the industrial assets within the OT environment, as well as understanding their complex architectures, systems, and processes and what distinguishes normal from abnormal behavior.

Furthermore, the solution must also be completely safe and non-disruptive to industrial operations. Adverse impacts on availability, process integrity, and/or safety are unacceptable in any capacity.

The Results

After consulting with industry experts and rigorously evaluating multiple options based on the above criteria, the firm selected Claroty's Continuous Threat Detection (CTD) solution to bring visibility and security to its more than 100 industrial sites.

Key results with Claroty CTD include:

1. Full — and fully-automated — visibility

Before deploying Claroty CTD, this company had handled asset inventory the old-fashioned way: with spreadsheets. Personnel not only had to manually account for each asset at each site, but they also had to manually visit each asset's vendor's website, look-up whether any new vulnerability disclosures or other advisories had been published, determine which advisories were relevant, and then decide which actions were warranted. The tedious, time-consuming nature of this process meant it was only undertaken every eight to ten years. In the intervening years, their asset inventory would become increasingly inaccurate and the risk of blindspots became increasingly prevalent as more assets were added and more vulnerabilities went unaddressed.

Claroty CTD changed this process drastically. Taking advantage of the solution's fully automated asset discovery and vulnerability correlation capabilities, the customer has since gained full, real-time visibility into all of its assets and all relevant vulnerabilities — without the need for time-consuming site visits, error-prone manual processes, or unwieldy spreadsheets.

"We can see full visibility of the systems that are interconnected with each other."

Head of OT Cyber Operations

"Our engineers don't have to manually make and maintain that asset inventory anymore, everything is retrievable online, and we have the latest version from the asset inventory perspective. That's very useful for day-to-day operations."

Head of OT Cyber Operations

2. Accessible, trustworthy insights that drive confident decisions

Beyond granting full visibility into the OT environment, Claroty CTD has also helped synergize the long-siloed (and often geographically disparate) security, engineering, and executive functions supporting the company's hydrocarbon production operations at its more than 100 sites. By serving as the single source of truth for all asset, system, process, and risk information, the solution ensures such information is accessible, consistent, and actionable to all personnel, workflows, and decisions that depend on it. Examples shared include:

- Receiving and responding to alerts specific to the complexities of industrial networks, such as when a given process goes beyond established parameters after an update or configuration change.
- Pinpointing unusual activities in real-time before potential damage occurs, such as an attempt to "access an asset via remote desktop protocol (RDP) at night when we don't usually work and maintenance windows aren't usually scheduled."
- Using granular risk scoring to understand and prioritize the order and extent to which vulnerabilities should be remediated or other wise compensated for. "CTD will tell us exactly what the highest risks are and what to do about them."

"Having this solution means that I can clearly see everything from the asset perspective, what changes have been done to particular networks or equipment over time, and — most importantly — where my biggest gaps are in terms of security."

Head of OT Cyber Operations

- OT device troubleshooting and investigation via contextual alerting, baseline details, and historical data. "The insights CTD provides often save me from having to get in touch with a device's vendor to look into issues. More often than not, all the details I need to understand what's going on and what to do are right there in the system. This translates to considerable operational cost savings due to a lowered reliance on third-party vendors for troubleshooting and drastically reduced mean time to respond (MTTR) overall."

3. Highly adaptable, efficient, and non-disruptive cybersecurity

Claroty CTD's adaptability, ease of deployment, and non-proprietary hardware requirements were among many reasons why it was selected as the solution initially, but these characteristics continue to bring value to the entire team today. Thanks to powerful yet non-disruptive sensors, Claroty CTD ensures the industrial asset inventory and monitoring scope can easily scale to support new or expanded production sites as the company — and its OT environment — grow and evolve over time.

The company's team has also since taken advantage of Claroty CTD's technical ecosystem by integrating the solution with its existing SIEM platform, Microsoft Azure Sentinel. This functionally enables alerts, events, and related insights from Claroty CTD to populate within Sentinel, equipping security operations center (SOC) personnel to monitor and manage all alerts from the company's entire enterprise and industrial environments on a single pane of glass. This flexibility and visibility "shortens the SOC's MTTR and ultimately helps harden operations against malware and other threats."

At the heart of these capabilities is the fact Claroty CTD is built for OT by experts in OT. Case in point is the solution's unmatched ability to identify and interpret the proprietary protocols used throughout the OT environment. This protocol coverage, "rich feature set, and information that really is attuned to the inner workings of the OT environment" are not only what differentiate Claroty CTD from other solutions, but are also integral to the firm's OT cybersecurity strategy and overall reduction of risk enterprise-wide.

About Claroty

Claroty empowers organizations to secure all cyber-physical systems across industrial (OT), healthcare (IoMT), and enterprise (IoT) environments: the Extended Internet of Things (XIoT). The company's unified platform integrates with customers' existing infrastructure to provide a full range of controls for visibility, risk and vulnerability management, threat detection, and secure remote access. Backed by the world's largest investment firms and industrial automation vendors, Claroty is deployed by hundreds of organizations at thousands of sites globally. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America.

For more information, visit claroty.com or email contact@claroty.com.