CASE STUDY

SECURING CRITICAL OIL AND GAS INFRASTRUCTURE

Enhancing Cybersecurity and Remote Access with Claroty CTD and SRA

In the fast-evolving landscape of cybersecurity for critical infrastructure, an Eastern European energy and petrochemical company has made significant strides in enhancing its cybersecurity posture for its cyber-physical systems (CPS) across various operational technology (OT) environments. The lead process control engineer responsible for much of the success sheds light on the company's experiences, challenges, and achievements.

Challenges

The oil and gas company faced several intricate challenges:

- **Risks of IT/OT Convergence:** Keen to embrace innovation and further modernize its operations, the company had been gradually integrating its Information Technology (IT) environment with OT — yet this also exposed the company to new cybersecurity risks stemming from this convergence.
- **Rising OT Cyber Threats:** The increasing number of cyber threats targeting OT environments in the oil & gas sector raised alarm bells within the organization.
- **Regional Incident Catalyst:** A major cyber incident in a similar company in 2017 served as a wake-up call, motivating the company to initiate systemic cybersecurity improvements.

"It has been a true partnership working together with Claroty, both on business and engineering levels. The transparency is so high that it greatly helps feeling like a true, trusted relationship. Feedback from us on product use, limitations, and suggestions, are all absorbed and communicated back on. And we've seen results materialize in new versions of products. That's very impressive and very encouraging as a customer."

Lead Process Engineer

- **Inefficiencies from Automation Gap:** Despite an IT/OT convergence initiative and the desire for automated data collection from field operations, manual processes for OT asset inventory, vulnerability correlation, and others still prevailed in the field, posing operational bottlenecks.

Over the past several years, the company's lead process control engineer had taken on the responsibility of spearheading a transformational maturation program. The primary objective of this digital transformation program was to establish a sustainable foundation for OT resilience and security within the organization. To achieve this, the company developed and implemented a comprehensive work process, formed a dedicated team, and deployed a suite of supporting tools.

The engineer's unique position within the field maintenance organization allows for deep interaction with various engineering disciplines and operational representatives. This engagement was instrumental in gaining maximum traction for the program and fostering collaboration across the organization.

Searching for a Solution

The first step in the maturation program was to identify top priorities. This was done by mapping out the relevant cyber controls needed for impact risk reduction effect versus implementation effort and the lapsed time required and then prioritizing those that offered the biggest risk & impact reduction effect when implemented.

This resulted in the need to:

- Establish governance and assurance around a single work process to be managed.
- Generate an automated and centralized OT asset inventory to better keep track of the OT devices within the company's environment and the current cybersecurity posture of those devices.
- Establish an organization-wide standardized secure architecture to enable delivery of common services to all OT areas, and help reduce the overall Total Cost of Ownership.

The company's journey began with evaluating various cybersecurity tools, including Claroty and other leading vendors. Ultimately, Claroty's Continuous Threat Detection (CTD) emerged as the preferred choice. The engineer highlights that CTD's deep understanding of communication protocols and its insights into field automation components set it apart. This deep understanding allowed CTD to provide more comprehensive insights and align with the company's priorities. Moreover, the availability of the solutions through an existing Claroty reseller within the region's regulatory framework played a crucial role in the decision.

Operationalizing Cybersecurity

The company began implementing Claroty's CTD solution in phases. It started with the most impactful production unit, aligning with their prioritization strategy. Their multi-year program focused on 13 key areas, and establishing a governance and assurance framework was the first priority. Automating asset inventory was the next critical step, replacing manual processes and spreadsheets with CTD.

This capability has expanded from a partial deployment to a full field-wide deployment, covering about 1,500 TCP/IP connected endpoints and infrastructure components across multiple production units and a wide geographic area. The ability to assess the vulnerability of field automation components to emerging threats was greatly improved, allowing for faster responses and significantly increased resilience.

The journey didn't stop with CTD. Initially, remote access was considered a luxury, with a traditional approach involving sending personnel to the field. However, the company recognized the need to standardize access environments, train personnel, and enable remote access to improve efficiency and security. The introduction of Claroty SRA played a vital role in achieving these goals, allowing engineers to work from a centralized location, reducing exposure to sites with hazardous areas, and enhancing both operational and cost efficiency. The shift from isolated components to increased connectivity was driven by improved network infrastructure and a better understanding of the benefits of secure remote access.

The shift from isolated components to increased connectivity was driven by improved network infrastructure and a better understanding of the benefits of secure remote access.

The lead engineer noted, "We have field automation components everywhere — also in red, hazardous zones. If we can avoid sending people there, and they can do exactly that same work as if they're standing at a local console, that significantly reduces the risk of exposure from being in those hazardous locations. Additionally, this saves on travel and their ability to respond to an unplanned outage becomes much faster. There are many advantages that we really wanted to leverage because they are measurable."

The operational use of Claroty's SRA solution began at the end of 2022. The transition involved shifting network infrastructure connections to a new secure architecture with SRA. The operational use has gradually increased, with many users recognizing its value. The company expects continued growth in SRA usage, reaching a tipping point where users actively seek its adoption, driven by the efficiency and usability of the system. Ultimately, the goal is to achieve widespread adoption of SRA across its facilities, streamlining operations and reducing exposure to hazards.

Quantifying the Benefits

While specific monetary figures couldn't be provided, a recent yearly evaluation showed a noticeable spike in the usage of Claroty SRA among the company's personnel. The organization is currently analyzing this increased usage to quantify the savings and benefits realized. They are collecting data through tools like Splunk to gain detailed insights into user activities, both remotely and on-site, to help quantify the benefits in monetary terms. This data-driven approach will enable them to better understand the efficiency gains and cost savings achieved through the adoption of Claroty's solutions.

Looking Forward

The company's focus is not only on expanding secure access but also on aligning its governing framework with industry standards. They plan to measure compliance in conjunction with the data provided by tools like CTD and SRA, particularly in addressing obsolescence. In the near term, they plan to further extend their use of SRA to continue lowering hazardous exposure on site along with significantly reducing diagnostics, maintenance, and engineering times. They will also look to further integrate CTD's automated asset visibility with its other existing services, such as operational alerting, threat hunting, and obsolescence management in the field.

The strategic partnership with Claroty has significantly enhanced the organization's OT resilience and security. The holistic approach taken by the company, combined with Claroty's expertise and technology, has enabled them to effectively combat evolving cyber threats while optimizing operations and reducing risks in the challenging oil & gas environment.

About Claroty

Claroty empowers organizations to secure 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.