CASE STUDY

OIL & GAS

Global Oil & Gas Company Secures Offshore Drilling Operations with Claroty

Direct connectivity between a global oil and gas company's corporate IT network and the OT networks aboard each of its contractor-managed offshore drilling ships enabled it to achieve impressive production efficiency. Recognizing that this connectivity also posed considerable risks to the availability, reliability, and safety of its offshore drilling operations, the company turned to Claroty for assistance assessing and mitigating these risks.

Challenges

The company noted several operational and structural challenges that hindered its ability to effectively and proactively secure its offshore drilling operations.

1. **Fragmented and vulnerable network architecture:** Each of the company's mobile offshore drilling units (MODUs) included four independent OT networks that were not air-gapped and thus were vulnerable to spillover attacks from the IT network.
2. **Heavy reliance on third-party contractors:** The company out-sourced management of its MODUs to exploration and production (E&P) contractors. Each MODU is managed by a different contractor who utilizes remote access connections to service it.

"Claroty is a comprehensive solution. Its single dashboard across all sites showing the real-time status of all of our OT assets was a key factor in our decision to use this platform. Claroty really gave our team an extreme level of visibility into our OT networks that other companies were unable to provide. The fact that they achieved this without impacting our existing systems made the decision even easier for us."

However, remote access is a common attack vector. If the remote party's device becomes infected with malware or their access credentials are stolen, for example, this can make the systems they access susceptible to compromise.

Additionally, since all remote connections were via third-parties, the company could not monitor them and had no insight into whether actions taken remotely were authorized and error-free.

3. **Limited OT visibility:** A consequence of having a different contractor manage each MODU is that each MODU's OT network comprises different assets that utilize different protocols. Given that OT protocols are typically proprietary and incompatible with traditional asset management tools, the company was unable to inventory its OT assets and thus unable to assess, much less mitigate, the risks to which they were exposed. The company's two aforementioned challenges further exacerbated these visibility limitations.

The Solution

The Claroty Platform was deployed on top of existing offshore OT network infrastructure and then connected to the company's onshore security operations center (SOC) via an existing satellite communication network. Platform components utilized include:

- **Continuous Threat Detection (CTD)** for full-spectrum OT asset visibility, continuous security monitoring, and real-time risk insights with zero impact to operational processes and underlying devices.
- **Secure Remote Access (SRA)** to safeguard OT networks from threats introduced via unmanaged and unmonitored access by remote users, including employees and third-party vendors.
- **Enterprise Management Console (EMC)** to simplify management overall, consolidating data from across The Claroty Platform and providing a unified view of assets, activities, and alerts across multiple sites. The platform also integrates via the EMC with existing tools within the IT technology stack.

Outcomes

Utilizing The Claroty Platform, the company was able to:

Discover and profile all OT assets, communications, and processes within two weeks of deployment for multiple MODUs around the globe.

Integrate the platform with its existing IT security infrastructure to create a highly effective and unified IT/OT SOC, greatly improving alignment and collaboration across IT and OT security, as well as with E&P contractors.

Leverage SRA's customizable user-access controls, least-privileges policies, and auditing features to monitor, manage, and minimize risks introduced by remote access.

Provide its E&P contractors with a user-friendly, OT purpose-built interface through which they easily connect remotely—and securely—to service OT assets.

Proactively protect against security incidents and thus reduce exposure to risks to the availability, reliability, and safety of its offshore drilling operations.

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.