Oil and Gas

How OTORIO's OT Cyber Security Risk Assessment Enhanced an Energy Company's Operational Security Posture

Case Study

Operational Security Posture Assessment for an Energy Company

The company is an international oil and natural gas refining company that sells a wide variety of products to businesses and consumers. It also has a large network of retail gas stations and distribution terminals around the world to deliver energy products and services to its customers.

In early 2022 with the rise of the war between Russia and Ukraine and the Colonial Pipeline ransomware attack in 2021, many international energy companies grew concerned about potential cyber security implications for their OT environments. The company trusted OTORIO and its OT-native security experts to evaluate what ramifications the crisis had on its OT environments and operations. It sought a realistic level of acceptable risk, exposure, and vulnerabilities for the company's operational network and business environments.

> "In a very short time frame, OTORIO was able to demonstrate credibility and a high degree of expertise which, when combined together, gave us a sense of trust and confidence"
>
> International Oil & Gas Company, CISO

Customer Challenges

The company had been relying upon an intrusion detection system (IDS), but struggled with several challenges. Its security posture led to only a partial understanding of the impact that OT security has on its operations, and it lacked the ability to proactively assess and mitigate risks. Despite the energy company's investment in cyber security generally, and OT security with some resilience, OTORIO's security posture assessment still found significant issues. The company:

- Lacked information about its security environment to properly manage risk.
- Had limited resources, skills and knowledge to address OT cyber security.
- Had unclear and partial asset visibility, with limited details and poor context.
- Was unable to leverage existing technologies and data sources to properly understand and secure its operational environment.
- Had collaboration challenges between its IT and OT teams, impacting their ability to assess, respond, and remediate risk.

OTORIO's Solution

OTORIO's team assessed the company's security posture from a cyber attacker's point of view. This involved both an external assessment, leveraging OTORIO's vast experience with industrial and operational penetration testing by red and purple teams. In parallel, the teams reviewed internal security operations, controls, and identified attack vectors. OTORIO also focused on analyzing IT to OT risks and attack paths.

OTORIO's technology-based services and products provided an integrated evaluation of the organization's true exposures, controls, posture, and vulnerabilities, while also revealing the operational impact this had upon the company. Findings included:

- The use of unsecured protocols.
- A lack of isolation between OT and IT, such as managing firewall policies for both IT and OT via a single firewall policy management platform located in IT - a critical security gap.
- Firewall management of IT and OT leading to unwarranted access of other applications and sensitive information in the OT environment.
- Misconfigurations in the Active Directory. These misconfigurations allowed users to gain domain admin privileges and exposed the OT environment to external third-party providers. This made the operational environment vulnerable to cyber security attacks.
- Gaps in coverage of existing security solutions such as IDS, Firewalls, and secure gateways which increased false positives and misrepresented the level of protection in the environment.

Using OTORIO's cyber security tools for proactive security posture assessment, the team provided the Energy company with a contextual OT security risk assessment, including:

- High-fidelity asset detail with a deeper, richer understanding of its role, impact, vulnerabilities, and organizational structure.
- An assessment of existing security controls while providing the client with best practices to harden its security configurations and network interfaces.
- Prioritizing vulnerabilities according to their risk impact on the OT environment.
- Contextualized mitigation steps for each risk, presented in a simple, actionable way suitable for the operational environment.

What is OT Security Context?

This refers to the totality of circumstances that affect an event (e.g., incident, alert, exposure discovery). Information is gathered and assessed together with any potential business and operational impact on operational processes (i.e., production, safety, financial, environmental, and regulatory matters). To provide necessary context for risk-based OT security situational awareness, these elements are analyzed together using a rich set of security and industrial data sources.

Results

At the conclusion of OTORIO's OT cyber security risk assessment, the international Energy company received a detailed and focused report. This included a complete summary of the investigation, steps for mitigating risk, and prioritized short and longterm recommendations.

All the vulnerabilities discovered were contextualized according to their potential realworld business impact, efficiently prioritizing remediations. The company was able to segment its OT network more effectively. This included creating secure zones that restricted access to sensitive equipment by unauthorized users, including equipment vendors themselves.

This valuable information triggered productive discussions and spurred collaboration between the IT and OT teams, who began to review and decide the company's cyber security strategy together.

OTORIO has a proven track record of professional services and extensive knowledge of OT cyber security. This is why this respected international company chose it to deploy a complete comprehensive solution for continuous risk-based management of its operational environment. An additional workshop regarding best practices to secure OT environments was scheduled with the customer's teams.

OTORIO's Benefits

- Ability to conduct a safe operational security posture assessment without disturbing ongoing operations.
- Improved ROI on pre-existing security controls and solutions by leveraging existing technology investments.
- A comprehensive security assessment report, providing senior management with a full picture of the company's OT cyber security posture.
- Quick risk mitigation and hardening of site-specific OT network risks and vulnerabilities.
- The company went from only relying upon detection to adopting a continuous, proactive risk-based assessment, mitigation, and management strategy to secure its OT environment.

With OTORIO, the company today faces existing and emerging cyber threats with a new confidence and advanced toolbox – ensuring energy production uptime and safeguarding business continuity.

About OTORIO

OTORIO is a leader in OT security solutions, dedicated to safeguarding enterprise IoT and OT environments for enhanced safety, productivity, compliance and resilience. Its flagship platform, OTORIO Titan, provides an all-encompassing suite of applications that brokers IIoT, OT, and CPS security controls into IT workflows, ensuring proactive protection and efficient risk management.