OTORIO

Energy

OTORIO Helps Large Energy Company Rapidly Ramp-Up OT Network Security Posture

Case Study

The Business

Headquartered in South America and serving millions of customers in nine Latin American countries, an energy producer and distributor contacted OTORIO in order to assist them in ramping up their OT network security posture.

Improved Remote Access Security

Enhanced IT and OT Network Segmentation

Enforced SCADA PC Policies

The Challenge

Given the volatile cybercrime and cyberterrorism climate along with the energy industry's known vulnerability to cyberattacks, the company's senior management wanted to assess and improve their OT security posture. Their existing OT security was limited to vendor-based systems that were remotely monitored, and disconnected from the company's IT security.

Moreover, the energy company's regulatory obligation to report daily on energy creation and distribution necessitated the de facto convergence of their IT and OT networks – with data flowing constantly from OT-connected devices and equipment, through the IT network and to the Internet. This made an immediate OT network vulnerability scan, risk assessment, and security awareness training plan mission-critical.

What They Are Saying

> "We chose OTORIO because they understand the unique OT security needs of the energy sector. OTORIO's Threat Intelligence and Risks Assessment helped my team to improve our security posture. Likewise, our operations team benefited from learning OT cybersecurity best practices from the best in the business."
>
> Global Energy Company CISO

OTORIO

Energy

The Solution

The energy giant chose OTORIO to conduct a full and comprehensive OT network security assessment of the company's five core locations in Peru, Bolivia, Nicaragua, and Guatemala. These sites include hydroelectric, gas, coal, and wind power generation facilities.

Working fully remotely under COVID-19 pandemic restrictions, OTORIO first conducted in-depth workshops with the IT and OT teams at each site, to better understand the network architecture and topography. Once the OTORIO team had a clear picture of the networks in question, they leveraged OTORIO's RAM^2 technology to take a deepdive into each network's security posture, looking for gaps, holes and misconfigurations that could facilitate a breach.

OTORIO helped the energy company to improve existing OT cybersecurity policies and procedures including:

- Improve security controls and enforce cybersecurity policies on SCADA PCs connected to the internet
- Limiting remote access per demand to the supply chain
- Separate the IT and OT networks. Especially when it comes to company infrastructure, identity and data management, IT and OT network segmentation can have a major positive impact on OT cybersecurity

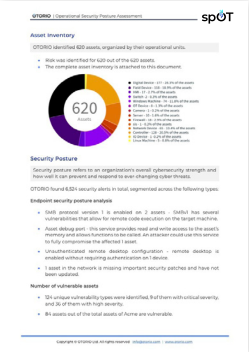
Finally, the OTORIO training team created and implemented **a security awareness training plan** for all relevant staff.

acme

Operational Security Posture Assessment

Technical Report

Empowered by OTORIO



OTORIO | Operational Security Posture Assessment

spOT

Asset Inventory

OTORIO identified 620 assets, organized by their operational units.

- Risk was identified for 620 out of the 620 assets.
- The complete asset inventory is attached to this document.

620
Assets
Digital Device - 177 - 28.3% of the assets
Field Device - 118 - 18.9% of the assets
HMI - 17 - 2.7% of the assets
Switch -2 - 0.3% of the assets
Windows Machine - 74 - 11.8% of the assets
OT Device - 8 - 1.3% of the assets
Camera - 1 - 0.2% of the assets
Server - 10 - 1.6% of the assets
Firewall - 18 - 2.9% of the assets
sis - 1 - 0.2% of the assets
Network Device - 65 - 10.4% of the assets
Controller - 128 - 20.5% of the assets
IO Device - 1 - 0.2% of the assets
Linux Machine - 5 - 0.8% of the assets

Security Posture

Security posture refers to an organization's overall cybersecurity strength and how well it can prevent and respond to ever-changing cyber threats.

OTORIO found 6,524 security alerts in total, segmented across the following types:

Endpoint security posture analysis

- SMB protocol version 1 is enabled on 2 assets - SMBv1 has several vulnerabilities that allow for remote code execution on the target machine.
- Asset debug port - this service provides read and write access to the asset's memory and allows functions to be called. An attacker could use this service to fully compromise the affected 1 asset.
- Unauthenticated remote desktop configuration - remote desktop is enabled without requiring authentication on 1 device.
- 1 asset in the network is missing important security patches and have not been updated.

Number of vulnerable assets

- 124 unique vulnerability types were identified, 9 of them with critical severity, and 36 of them with high severity.
- 84 assets out of the total assets of Acme are vulnerable.

Copyright © OTORIO Ltd. All rights reserved info@otorio.com | www.otorio.com

OTORIO's Comprehensive Security Assessment Reports

The Benefits

OTORIO delivered a comprehensive security assessment report, providing senior management with a full picture of the company's OT security posture. Since the OTORIO team took the time to truly understand the OT-connected business processes of each company location, all vulnerabilities discovered were contextualized according to their potential real-world business impact – facilitating more efficient remediation prioritization.

Following the OTORIO assessment, the company was able to quickly remediate and tighten site-specific OT network vulnerabilities. Moreover, the company created and implemented granular OT network security policies regarding various attack scenarios, as well as minimum threshold security requirements for all site hardware and software. In addition, the company was able to segment their OT network more effectively, creating secure zones that helped restrict access for unauthorized users to sensitive equipment – including the equipment vendors themselves.

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

About OTORIO

OTORIO has pioneered an industrial-native OT security platform that enables its customers to achieve an integrated, holistic security strategy for industrial control systems (ICS) and cyber-physical systems (CPS).

Together with its partners, OTORIO empowers operational security practitioners to proactively manage cyber risks and ensure resilient operations. The company's platform provides automated and consolidated visibility of the entire operational network, enabling companies to take control of their security posture, eliminate critical risks, and deliver immediate business value across the organization.

OTORIO's global team combines the extensive mission-critical experience of top nation-state cyber security experts with deep operational and industrial domain expertise.

CN 110520