OTORIO

Electric Utilities

Empowering Grid Resilience and Efficiency with OTORIO Advanced OT Cyber Security platform

Customer case study

Protecting the Operational Environment

The customer is an electric utility company that ranks among the top 100 of the Fortune 500 list. It is involved in electricity generation, petrochemical product manufacturing, oil and gas exploration and production, and gasoline retailing businesses.

The company contacted OTORIO for an efficient and effective solution to:

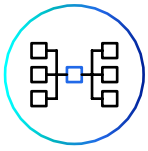
- Provide accurate and comprehensive asset inventory visibility of its SCADA in the operational technology (OT) environments.
- Identify vulnerabilities and critical risks
- Continuously monitor the company's expanding OT environment, including energy transmission lines and substations
- Simplify its OT cyber security management

Customer Challenges

- Had unclear and partial asset visibility, with limited details and poor context.
- Risk assessment was done with manual tools (e.g., spreadsheet software) and with limited knowledge to address OT cyber security.
- Lacked information about its security environment to properly manage risk.
- Growing complexity of the OT network - multi-vendor environment with hundreds of OT assets spread geographically across numerous facilities.
- The network's attack surface is expanding as it is undergoing a migration from Serial-based RTUs to IP-based connectivity due to limitations on serial connection refresh rates.

OTORIO's Solution

OTORIO's RAM² OT risk management solution was deployed at the Electric Utility company OpsCenter for monitoring of up to 400 sites; many of these are small substations. RAM² proactive security posture assessment provided the Electric Utility company with:



Enriched Asset Inventory

RAM² discovers and identifies assets in the company operational environment using various integrations, including passive network monitoring, safe active querying using industrial native protocols, and by connecting with security and industrial systems in the network (e.g., Firewalls and IPS, backup systems, SCADA, asset management applications and even Excel files). RAM² delivered high-fidelity asset detail with a deeper, richer understanding of its role, impact, vulnerabilities, and organizational structure.

Risk Assessment:

Using RAM², the company can proactively assess and reduce OT security risks in the network, rather than be reactive and try to minimize damage only after a breach has already occurred, or even understand whether an attack actually happened.

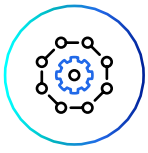
RAM² assesses the cybersecurity risk from several perspectives:

- Segmentation analysis
- Endpoint security analysis, including asset-level compliance and hardening of security configurations (e.g., for HMIs)
- Vulnerability management
- Providing clear, feasible mitigation steps for each risk that are suitable for the operational environment

RAM² prioritized vulnerabilities according to their risk impact on the OT environment and provided the company with best practices to harden its security configurations and network interfaces, along with context-based mitigation steps for each risk. These mitigations were presented in a simple, actionable way suitable for the operational environment.

Ongoing Risk Monitoring

RAM² continuously monitors the OT-IT-IIoT operational environment for security posture violations and rogue activities. It alerts about changes such as new assets that are discovered (whether actively communicating or even dormant ones), assets that stopped communicating, or configuration changes (e.g., firmware). It correlates events from multiple network sources to detect risk scenarios and provide contextual insights with mitigation steps to reduce the risk.



Integration to SCADA

OTORIO's RAM² integrated and analyzed the company's Supervisory Control and Data Acquisition (SCADA) system that monitors and controls the operational electricity remote terminal units (RTU's). This analysis resulted in valuable information about its security posture. RAM² identified security control gaps within the operational database of the system, it then delivered contextual OT insights with vulnerability alerts and corresponding mitigation steps (e.g., created an attack detection layer at the infrastructure level to protect the network).

RAM² was able to provide valuable OT risk protection for SCADA environments by:

- Connecting and querying the OT security environment and industrial systems together (e.g., servers infrastructure, Firewall communication along with SCADA system)
- Identifying OT security gaps
- Delivering prioritized and contextual security vulnerability notifications

OTORIO

Electric Utilities

RAM² integrates with SCADA systems at several levels, including:

- **Asset inventory** - Extracting Industrial project files and enriching asset information.
- **Monitoring** - Alerting on events that are generated by the SCADA and correlating those events with data from other systems to detect potential risks.
- **Security and compliance gap identification** - At the Operation Systems (OS) and SCADA application level, including security hardening of the SCADA against malware.

Boosting SOC efficiency

RAM² exports alerts and insights to the company industrial SOC. It enables the managed detection and response service team (MDR's) scalability by providing context, prioritizing risk in the OT network, and reducing noise. RAM² enables SOC analysts to focus on factors that pose risks to safety, efficiency, and operational continuity, while also facilitating improved collaboration between the SOC analysts and the company operational teams.

Benefits for Electric Utility

- Comprehensive OT assets visibility with a unified view of risk for OT, IT, and IoT-aligned network security systems and industrial systems in the OT environment.
- Proactively reduce the likelihood of cyber security incidents.
- OTORIO's RAM² insights improved the company's MTTD and MTTR, reduced noise, and highlight which risks and vulnerabilities to prioritize.
- It improved its ROI for pre-existing security controls and solutions by integrating them with OTORIO's RAM² platform to leverage the company's technology investments.
- Empower operational team to take action with clear risk mitigation playbooks to harden site-specific OT network risks and vulnerabilities.
- Reduce the complexity of OT cyber security operations management.
- Increased efficiency enabling scalability of the SOC and Industrial MDR service.

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 090723