CUSTOMER CASE STUDY

In Partnership with Senkron.Energy

Securing critical infrastructure against escalating cyberthreats is imperative. A targeted OT security strategy ensures operational continuity, safeguards assets, and fosters organizational resilience.

Securing the Future: Advancing OT Security in Critical Infrastructure for Enhanced Resilience and Efficiency

March 2024

Written by: Yesim Arac Ozturk, Research Manager, IT Security

Forging Resilience: Navigating the Complexities of OT Security in the Age of Digital Transformation

In today's rapidly evolving digital landscape, where industrial control systems (ICS) form the backbone of critical infrastructure sectors, operational technology (OT) security emerges as a pivotal concern. As industries increasingly embrace digitalization, the convergence of IT and OT presents both opportunities and challenges. This integration facilitates unparalleled efficiencies and data-driven decision-making but also exposes ICS to sophisticated cyberthreats. These systems, vital for the management of power generation, water treatment, and other essential services, become targets for attackers aiming to disrupt, exploit, or damage public services and safety.

The unique characteristics of OT environments — such as their reliance on legacy systems, proprietary protocols, and the prioritization of availability over confidentiality — demand a specialized approach to security. Unlike IT environments, where data breach and privacy concerns often take precedence, the primary concern in OT security is maintaining the uninterrupted operation of physical processes. This focus on availability and integrity poses distinct challenges, including how to update and patch systems that cannot afford downtime without compromising their functionality.

SOLUTION SNAPSHOT

ORGANIZATION:

EnerjiSA Uretim is an electricity production, trading, and powerplant management company

ORGANIZATIONAL CHALLENGE:

- Difficulty in managing assets and inventory
- Challenges stemming from the convergence of IT and OT
- Prioritizing availability over confidentiality
- Complicating the implementation of a uniform security solution

SOLUTION:

The integration of Senkron.Energy's OT SOC (security operations center) services

BENEFIT:

- Stronger cybersecurity posture
- Improved asset visibility and management
- Increased OT cybersecurity awareness
- Detection of unauthorized changes to the OT infrastructure

Given these challenges, the importance of implementing robust OT security measures becomes evident. It is not only about protecting data but also ensuring the continuous operation of services that society relies upon. The failure to secure OT systems can have far-reaching consequences, from the disruption of essential services to potential environmental disasters and threats to public safety. As such, the focus on OT security is a crucial aspect of national security, economic stability, and public health and safety.

Enhancing Operational Security Through Strategic Implementation

The implementation of Senkron.Energy's OT SOC services at EnerjiSA Uretim marked a significant step toward securing its critical OT infrastructure. This process, essential in safeguarding the integrity and availability of EnerjiSA Uretim's vast energy production operations, unfolded through a structured approach:

- **Identifying Key Challenges:** The onset of the project highlighted the immediate need to address asset and inventory management, visibility issues, and the integration of legacy systems that posed significant security vulnerabilities.

- **Solution Design and Customization:** In partnership with Senkron.Energy, EnerjiSA Uretim embarked on a tailored solution design process. This involved defining the "crown jewels" of its OT environment, identifying critical network points, and establishing comprehensive monitoring strategies to protect these assets.

- **Overcoming Implementation Hurdles:** The deployment phase encountered its fair share of obstacles, notably the integration of security measures within live OT environments and the initial resistance from vendors against installing third-party monitoring software on their platforms. These included non-invasive techniques for gathering security logs and ensuring installations complied with the Purdue model and global OT/ICS security best practices. These challenges were adeptly navigated through Senkron.Energy's expertise in OT security and its innovative approach to non-invasive monitoring solutions.

- **Initial Assessments and Continuous Monitoring:** Senkron.Energy conducted thorough initial assessments at each site to map out existing protocols, vendors, vulnerabilities, and assets. This foundational understanding enabled the establishment of a robust monitoring framework that could adapt to the unique aspects of each operational site.

- **Adapting to Vendor-Specific Requirements:** Given the diversity of equipment and software across EnerjiSA Uretim's operations, a significant part of the implementation involved customizing solutions to meet vendor-specific requirements. This ensured that security enhancements were compatible with existing systems without compromising their operational integrity.

- **Operationalizing the Solution:** The final phase of the implementation saw the operationalization of Senkron.Energy's OT SOC services, marked by the integration of security operations into EnerjiSA Uretim's daily workflows. This integration facilitated real-time monitoring, incident response, and a proactive approach to OT security management.

Overcoming Obstacles to Secure Critical Infrastructure

The journey to bolstering OT security at EnerjiSA Uretim encountered a myriad of challenges, reflecting the complex and dynamic nature of securing critical energy infrastructure.

- **Complex Asset and Inventory Management:** The foremost challenge was enhancing the management, inventory, and visibility of assets across EnerjiSA Uretim's sprawling OT environment. Outdated systems, which were non-updatable due to contractual limitations and the inherent characteristics of the OT/ICS infrastructure, further complicated this issue.

- **Adapting to IT-OT Convergence:** The blending of IT and OT through digitalization and data analytics introduced new vulnerabilities. This convergence, coupled with supply chain risks, significantly increased the exposure of OT sites to cyberattacks targeting these specific environments.

- **Diverse OT Environment:** The OT landscape at EnerjiSA Uretim is marked by a variety of protocols, hardware, and software, where the priority shifts from confidentiality to availability. This diversity necessitated customized security solutions for each vendor, adding layers of complexity to the security strategy.

- **Vendor Resistance and Innovative Solutions:** A notable hurdle was the initial resistance from key vendors against the installation of SIEM agents on their platforms. This challenge was creatively addressed by Senkron.Energy through the adoption of previously abandoned methods, such as non-invasive data collection techniques and the implementation of data diode solutions for one-way communication. These methods ensured compliance with the Purdue model and global OT/ICS security best practices.

- **Solution-Oriented Approach:** Open communication and a solution-oriented mindset were pivotal in navigating obstacles.

Key Outcomes and Unanticipated Benefits of OT Security Enhancement at EnerjiSA Uretim

The implementation of Senkron.Energy's OT SOC services at EnerjiSA Uretim has led to significant improvements and measurable benefits in the organization's operational technology security posture. Key results from this initiative include:

- **Enhanced Asset Visibility and Management:** Immediate visibility into assets, inventory, and asset management marked a crucial improvement, facilitating more efficient and reliable inventory management processes. This enhanced visibility allowed for the detection and remediation of previously unnoticed vulnerabilities, such as unused yet connected ghost entities within the OT infrastructure.

- **Increased OT Cybersecurity Awareness:** The constant stream of SOC notifications has heightened awareness and readiness regarding OT cybersecurity within the organization. This increased vigilance has led to the identification and resolution of policy violations and the detection of malware on OT/ICS assets.

- **Operational Uptime:** The solution enabled EnerjiSA Uretim to increase the uptime of its plants, thereby maintaining continuous operation and reducing the risk of potential security incidents. The transition from a lack of visibility and evaluation by non-experts to robust monitoring and evaluation by OT/ICS experts has significantly improved the organization's ability to prevent and respond to security incidents.

- **Collaborated Outputs:** The SOC's use of security orchestration, automation, and response (SOAR) capabilities has led to the development of comprehensive security playbooks. This collaboration between security and OT/ICS teams has enhanced risk management and operational efficiency.
- **Unexpected Benefits:** One unanticipated benefit was the detection of unauthorized changes to the OT infrastructure by internal personnel. This capability has enforced stricter compliance with security policies and procedures.

The broader impact includes improved organizational processes, heightened cyber awareness, and the establishment of new, secure business processes, contributing to a safer, more resilient operational environment. These outcomes underline the critical success factors for such projects, including comprehensive visibility, deep OT/ICS expertise, and a tailored approach to threat intelligence and security solutions.

Methodology

The project and company information in this document was obtained from multiple sources, including information provided by Senkron.Energy and questions asked directly to EnerjiSA Uretim by IDC.

About the Analyst

Yesim Arac Ozturk, *Research Manager, IT Security*

Yesim Arac Ozturk is the research manager for IDC's Türkiye cybersecurity practice. In this role, she is focused on security and, in collaboration with regional IDC team members, engages in topics spanning a wide and evolving spectrum of security and trust topics. In the broad security landscape, Yesim focuses on impactful developments in solutions, markets, cyberthreats, and end-user requirements and offers thought leadership and actionable research for IT buyers and suppliers.

MESSAGE FROM THE SPONSOR

More About Senkron.Energy

Senkron.Energy creates inspiring energy technologies empowered by data and industry know-how for all who share our planet. Through its team of experienced energy technologists, the company drives awareness around the responsible consumption of resources. In its role as a trusted global partner, Senkron.Energy provides proven or co-generated new technologies for customers, preparing energy sector stakeholders for disruption with its trendsetting software, IoT, cybersecurity, data, and green energy technologists.

IDC Custom Solutions

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.