Managed Detection and Response (MDR)

Powered by Eos.ii™

siemens-energy.com

Cyber threats are evolving daily. Evolve with them.

The severity and frequency of cybersecurity attacks in the energy sector are increasing as cyber criminals, terrorist organizations, and nation state actors become more sophisticated.

These threats are moving beyond information technology (IT) and are now directly targeting critical operational technology (OT) infrastructure. Couple this trend with increased investment in digital solutions, and threat actors are presented with an expanding surface area for executing attacks, leaving many organizations even more vulnerable.

Energy companies increasingly recognize that their likelihood of being attacked is nearly 100%, and that they must strengthen their agility and resiliency so they can respond when - not if - they are attacked.

Attacks targeting OT are particularly important to thwart because they have the potential to threaten uptime and availability, the health and safety of staff and customers, and brand reputation. The need for effective, OT-specific continuous monitoring capabilities has never been greater.

The three biggest impediments to effective continuous monitoring for OT environments...

1. Decentralized data sources with no integration platform
OT data often sits in disconnected repositories. This dispersion restricts visibility into the OT environment and the ability to synthesize information to feed threat analysis and alerting.

2. Inability to create insights from data at scale
Methodologies such as machine learning and data-rich rule-based alerting are needed to review large quantities of data at scale. Without these approaches, real-time detection and monitoring capabilities are restricted to what analysts can manually review.

3. Limitations of existing toolsets
Current tools for detection and monitoring are rarely designed with the OT environment in mind. Instead, they are primarily IT tools applied to OT. This limits their usefulness for collecting and analyzing OT environment data effectively.

Fully managed cyber solutions with industry-leading expertise

Siemens Energy's Managed Detection and Response (MDR) solution is a fully managed continuous monitoring service that delivers unparalleled threat detection for the OT environment. MDR addresses customers' continuous monitoring needs by leveraging our unique combination of **Methodology**, **Technology**, and **Human Intelligence** (Figure 1). Each of these components empowers our organization to support advanced real-time cyber threat detection and alerting from our Security Operations Center (SOC). Our OT cybersecurity experts provide further analysis and insight into detected events to support fast, actionable, and proportionate responses.

Figure 1: MDR Solution Composition

Unlike tradition IT security managed services, MDR integrates process and security data into its detection methodology, **Process Security Analytcs (PSA)**. This enables Siemens Energy to capture a more robust and complete data set, better correlate meaningful data points, and understand impacts to production. PSA's efficacy is an outcome of our comprehensive OT data sources, expert-developed rules engine, machine learning capabilities, and proprietary artificial intelligence (AI) platform, **Eos.ii™**. The result is scalable and automated detection supported by analyst-driven monitoring, analysis, and reporting. MDR is also a vendor-agnostic solution that is not limited to Siemens Energy systems. We provide hands on expertise to cover any industrial control system.

With MDR, customers can expect enhanced visibility into their OT environment and actionable insights delivered by our security experts. Customers don't need to worry about maintaining technology stacks, staffing a security team, or interpreting alerts. Siemens Energy takes these roles and provides a complete continuous monitoring offering uniquely adapted for the OT environment.

Secure your OT cyber environment without the headache

By relying on Siemens Energy, a trusted partner for OT cybersecurity solutions, you will unlock the most value from MDR because we tailor each deployment to your organization's unique requirements. Siemens Energy configures all relevant technologies, ensures that all connections are correct, and validates and data flows. The result is a solution designed for complex environments across vendors, asset functions, and operational requirements.

Siemens Energy is committed to working with your organization – guiding you on your journey to enhanced visibility, capable detection, increased security, and improved reliability.

Contact our Global Cybersecurity Portfolio leaders to learn how Siemens Energy MDR powered by Eos.ii™ can help your organization secure its OT environment

For further information:

Leo Simonovich
Vice President and Global Head
Industrial Cyber and Digital Security
Leo.Simonovich@Siemens-Energy.com

Stephen Hiser
Global Portfolio Manager
Industrial Cyber and Digital Security
Stephen.Hiser@Siemens-Energy.com

Daniel Kolomeets-Darovsky
Global Portfolio Lead
Industrial Cyber and Digital Security
Dan.Kolomeets-Darovsky@Siemens-Energy.com

Published by

Siemens Energy Inc.
Controls and Digitalization
4400 N Alafaya Trail
Orlando, FL, 32826, United States of America

Unrestricted