

Customer case study

Siemens Energy MDR

White paper

siemens-energy.com

SIEMENS energy

Foreword



Leo Simonovich
Global Head,
Industrial Cyber and Digital Security
Siemens Energy

Competition continues to drive rapid change in the energy sector as companies digitize legacy assets and build new business models around digital technologies like distributed solar, electric vehicle charging stations, and remote management for hard-to-reach sites. At the same time malicious actors target energy infrastructure with ever-more frequent, more sophisticated cyberattacks, sometimes backed by nation-state resources. Together, these ongoing trends make strong cybersecurity a core capability for the reliable delivery of energy.

Siemens Energy brings deep experience with industrial operations. We understand the drive to increase efficiencies and support innovations – and the need to protect production uptime amid a harsh global threat environment. Siemens Energy's deep knowledge of operational technologies helps our customers navigate the complex choices they must make as they choose how to manage the cyber risks that come with digitized OT environments.

We are proud to partner in the journey to stronger cybersecurity.

We hope this paper, which tells the story of one customer's cybersecurity journey, will help leaders across the energy sector understand what implementing OT cybersecurity looks like, and how insights into OT data can protect and enhance operations and production. I want to personally thank our partners at Middle River Power for agreeing to share their experiences, feedback, and insights.



High Desert Power Plant, operated by Middle River Power

Content

04 Executive summary

05 The challenge

06 The challenge as seen in the real world

07 The solution

10 The results seen in the real world

Executive summary

Middle River Power is a Chicago-based private equity firm, with approximately 3,000 MW of power generation assets in operation or development. Middle River Power determined that cyber risks were a growing threat to the High Desert Power Plant, a 830 MW natural gas-fired combined cycle plant they operate in San Bernadino County, California.

To protect against escalating cyber threats that target digitized operational technologies (OT) in critical infrastructure, Middle River Power sought a partner experienced in OT environment and cybersecurity.

Middle River Power selected Siemens Energy's Managed Detection and Response, powered by EOS.ii™. Siemens Energy experts set up and now monitor the MDR system, which leverages machine learning, artificial intelligence (AI), and Siemens Energy's deep OT expertise to efficiently provide visibility into the High Desert Power Plant and its workflows. OT experts assisted by AI prioritize and investigate consequential anomalies, sending Middle River Power's operators clear and actionable reports.

For Middle River Power, the deployment resulted in no disruptions to production, and significantly reduced risks. Financial risks from potential attacks have been mitigated, as have the costs of stronger cybersecurity. Compliance risks are reduced as Siemens Energy automation assists with reporting. Workforce risks associated with recruiting, retaining, training and securing cybersecurity and OT experts has been shifted to Middle River Power's partners. Risks posed by evolving threats are mitigated by Siemens Energy's ongoing updates to its MDR monitoring, and the visibility provided by MDR reduces the scope of uncertainty that executives have with regard to the health of their operating assets.

Thanks to increased confidence in its strengthened cybersecurity, Middle River Power was able to proceed in pursuing further automation at the High Desert Power Plant.



High Desert Power Plant, operated by Middle River Power

The challenge

Across the energy sector, companies have invested in digitizing operational technology systems (OT). Digitized OT environments are powerful, profitable, and here to stay. They enable business and process efficiencies that range from better fuel efficiency to remote management, and can open doors to further automation. Some business models – like distributed generation or electric vehicle charging – are only possible when the operational technologies are digitally managed and continuously network-connected.

Cyber risk becomes more important as a company's profit center increasingly relies on digitization in key production workflows. Yet many companies struggle to address cyber risks to OT.

Frequently IT and OT teams do not understand that process data is extremely valuable for cybersecurity. OT teams often assume that cybersecurity teams already have enough information to detect attacks and secure the plant when this is not the case. OT teams may believe IT cybersecurity teams are responsible for monitoring cybersecurity, while IT cybersecurity teams believe OT teams are responsible for monitoring OT. Shared responsibility can mean responsibility gets lost. Meanwhile, neither team can fully trace cause and effect across the digital and physical worlds – with the result that the company's biggest profit center overlaps with its biggest cybersecurity blind spot.

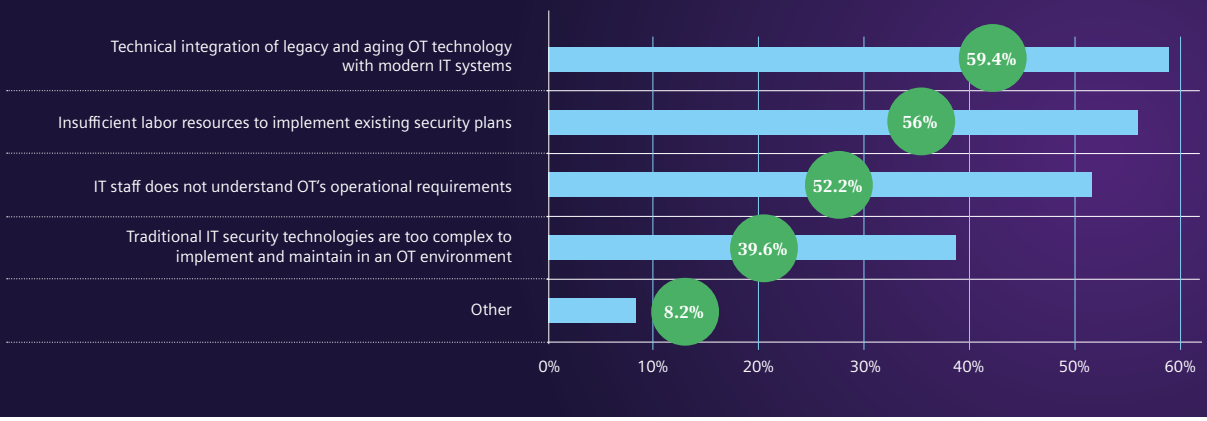
Industry surveys show that the technical hurdles that come with integrated IT and OT are a major barrier to securing OT against cyber threats. Tracing cause and effect across virtual and real world requires OT knowledge, but the pool of personnel experienced with both cybersecurity and OT systems is limited. IT security teams frequently do not understand OT operational requirements, and rarely have sufficient in-house resources to deploy strong OT security while performing their other responsibilities.

The technical barriers to OT monitoring and detection are steep. Monitoring systems need to bring together IT and OT data flows, analyze them with cybersecurity and OT expertise, and ensure that solutions don't yield self-inflicted disruptions to production. Once designed and implemented, in-house monitoring presents further operational challenges. Any time devices are added to the network, or reconfigured within the network, security would need to update. Determining what conditions should trigger an alert requires understanding the underlying OT systems and their safe operating parameters – and monitoring the relationships between digital and physical inputs and outputs. Applying traditional IT security methods would not be adequate to secure OT systems, and worse, would risk drowning out real breach detections with endless waves of false-positive security alerts.

Regulators, operators, OEMs, and insurers are all converging on monitoring as a necessary component of OT cybersecurity. Whether these capabilities are labeled monitoring and detection, Internal Network Security Monitoring (INSM) or something else, the common theme is to decrease risk by ensuring operators have the visibility they need to assess asset health, or better yet, detect attacks before damage occurs. To secure digitized OT environments, operators need monitoring and detection.

Industry survey demonstrates obstacles to securing OT

What are the biggest challenges your organization faces in securing OT technologies and processes?



The challenge as seen in the real world

To understand what these challenges look like in the real world, consider the example of Middle River Power. Middle River Power is a Chicago-based private equity firm, with many assets in the energy sector. Their largest power plant is the High Desert Power Station, an 830 MW natural gas-fired combined cycle plant in San Bernadino County, California. It is one of the ten highest-capacity natural gas plants in California, and critical to supplying power to 4 million people in the greater Los Angeles area.

While deploying digital management tools in the High Desert Plant, Middle River Power team identified that cyber threats posed growing risks. This awareness came from experience. "We have had to deal with tracking down and repairing breaches in the plants that we've acquired," explained Vice President of Operations Claude Couvillion, "It really brought cybersecurity to the fore."

The management team identified that they lacked visibility into High Desert's OT, and that this was a risk. Managers and security personnel had no way to quickly determine the scope of a breach. Should one occur they would be unable to verify whether the plant was safe to operate. "As Vice President of operations, cybersecurity is probably in the top 10% of things that I worry about on a day-to-day basis," said VP Couvillion. Recent high-profile breaches in the energy sector underscored the need for visibility, and renewed regulatory scrutiny for critical infrastructure.

Responsibility for securing the High Desert Power Plant rested with on-site OT teams. Frontline workers operating the plant bore the responsibility for defeating global cyber threats, and the burden of regulatory compliance paperwork for cybersecurity, piled on top of existing operational duties.

Middle River Power sought a more systematic approach to addressing cyber risk. However, developing the appropriate skills and knowledge in-house would be costly. "We (just like many private equity shops) are small and we don't have the personnel to stand up an OT department," said VP Couvillion.

Technical barriers to building automation for cybersecurity were significant. For example, the High Desert plant's gas turbines, heat recovery steam generators, and steam engine are made by three different manufacturers. To secure the plant, engineers would need to understand the function of each piece of equipment, its role in workflows, and how to integrate its particular machine language into overall defenses. Any equipment incorrectly configured or omitted from OT defenses would provide a possible pathway for attack.

Middle River Power did not have the correct personnel to undertake this technical challenge – not at the plant level, and not at the corporate level. They needed to find a solution.



The solution

Siemens Energy offers monitoring and detection as a service called Managed Detection and Response (MDR). Cybersecurity and OT experts analyze customer data, using Siemens Energy's EOS.ii™ platform to quickly prioritize what's consequential, and whether anomalies require action. Customers receive actionable reports, written by OT experts in terms clear to operators.

Once set up by Siemens Energy experts, the EOS.ii™ platform automatically creates a unified data stream from OT environments, even when those environments include equipment from many vendors. Using artificial intelligence and machine learning to understand the relationships between variables, and using a rules-based engine developed by Siemens Energy OT experts, the EOS.ii™ platform flags anomalies in the data for human investigation, and prioritizes the most consequential alerts.

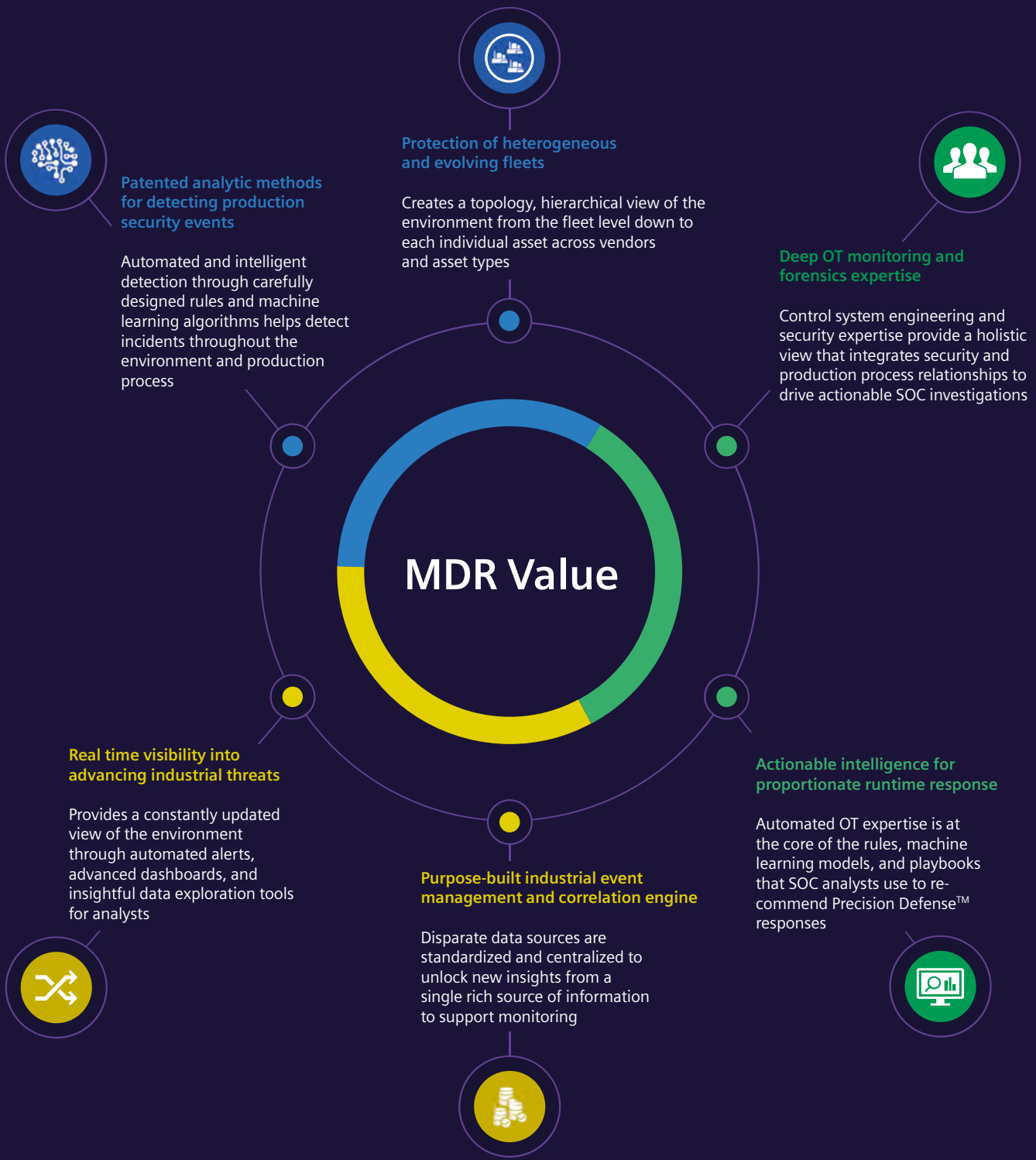
The combination of automation and expertise allows for breadth of monitoring and depth of investigations. Machine learning correlates events across IT and OT silos, differentiating between suspicious anomalies and normal variability in industrial processes. Several layers of automated analysis check for unsafe or unusual patterns, drawing on IT and OT data for context.

Siemens Energy experts sit at the heart of the MDR service. They leverage years of experience to deeply understand the specific worksites they monitor, their architecture, and their workflows. Understanding the systems under protection enables these experts to recognize when anomalies represent malicious intent, and how to close vulnerabilities and respond to attacks with minimal disruptions to production. Defenses improve over time as experts learn the worksite and fine-tune defenses to close known vulnerabilities and better filter false positives.

> ***"The biggest thing that Siemens Energy brought to bear is the human element, having the behind the scenes operators to sift through those alerts and evaluate them prior to sending them to the sites. The sites do not have the expertise in house to know if something is an attack or just a switch failing."***
>
> Claude Couvillion

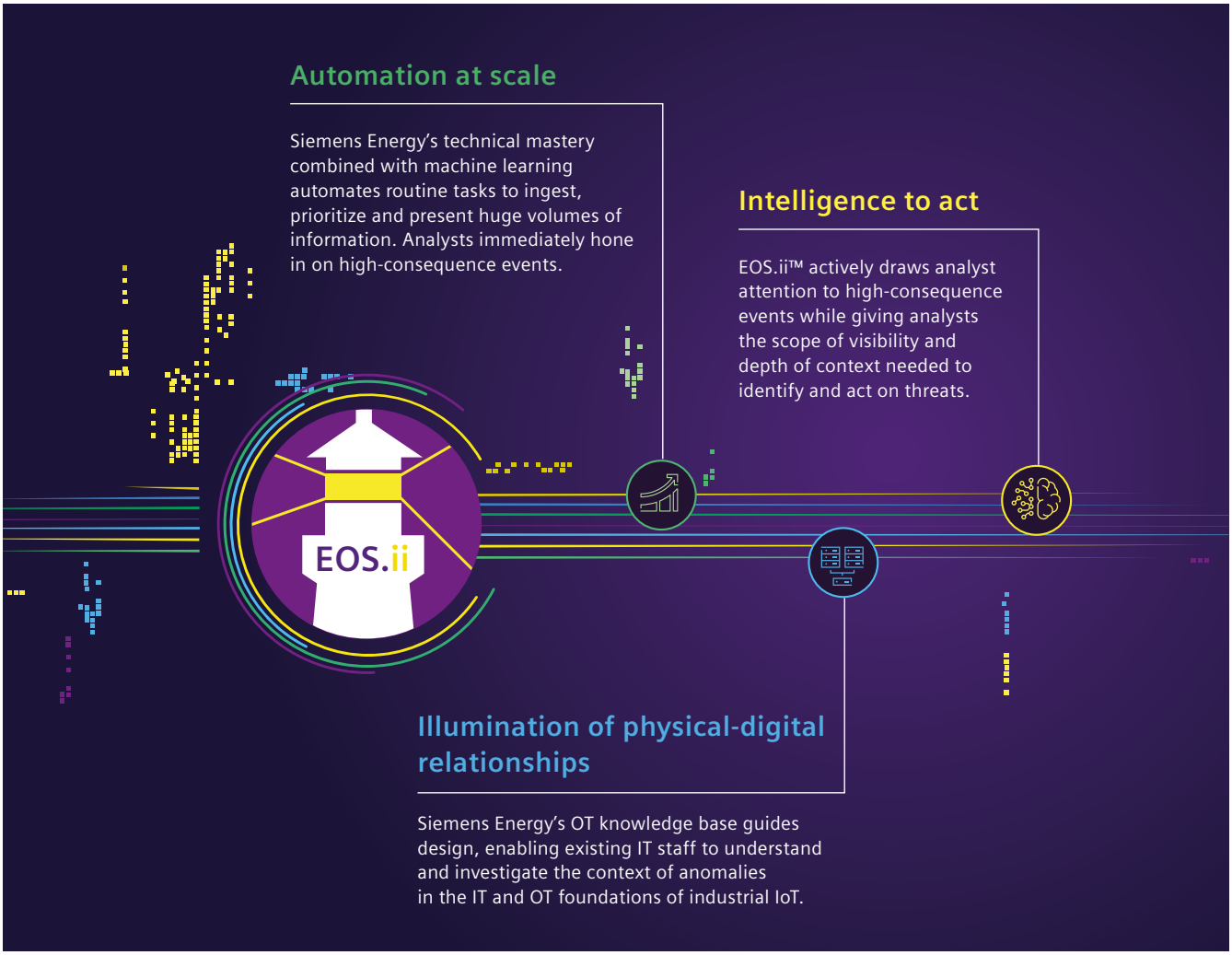
Managed detection & response's value to Middle River Power

Siemens Energy's proprietary methods, technology & human intelligence



Human analysts are cybersecurity's scarcest resource – so Siemens Energy makes them efficient and powerful. Automating routine tasks enables analysts to spend more time where they make the most difference: investigating anomalies and hunting threats. Threat hunting is made more efficient by ensuring broad, deep access to monitoring data and global threat intelligence – and by automatically mapping the digital architecture of network-connected assets to keep the platform current as devices are added or removed from workflows. Automation can update protections based on global threat intelligence feeds, and can prepare cybersecurity reports required by regulation. Analysts can quickly update the rules-based engine to respond to new threats and learn new patterns.

The EOS.ii™ platform makes it easy for analysts to trace cause and effect across IT and OT, identifying which specific machines are affected. For example, automation might detect that a rotating component starting and stopping more frequently than normal, note a configuration change initiated by an off-duty administrator, and flag these events for review. The human analyst would quickly assess the context, check whether known attacks against this equipment match this pattern, the activity of the account and – if needed – alert plant operators. Reports identify the extent and intent of a cyberattack, but may also identify early signs of mechanical failure signaled by OT data.



The results seen in the real world

Middle River Power reported an easy deployment for MDR. Middle River Power gained visibility into their systems, confidence in compliance with regulations, and reduced overall risks. Their increased confidence in cybersecurity will enable Middle River Power to advance plans for further automation in their systems.

During the deployment phase of the MDR service, Middle River Power saw zero disruptions to production. Siemens Energy experts visited the High Desert Power Plant, mapped the physical location of equipment and mapped the digital architecture.

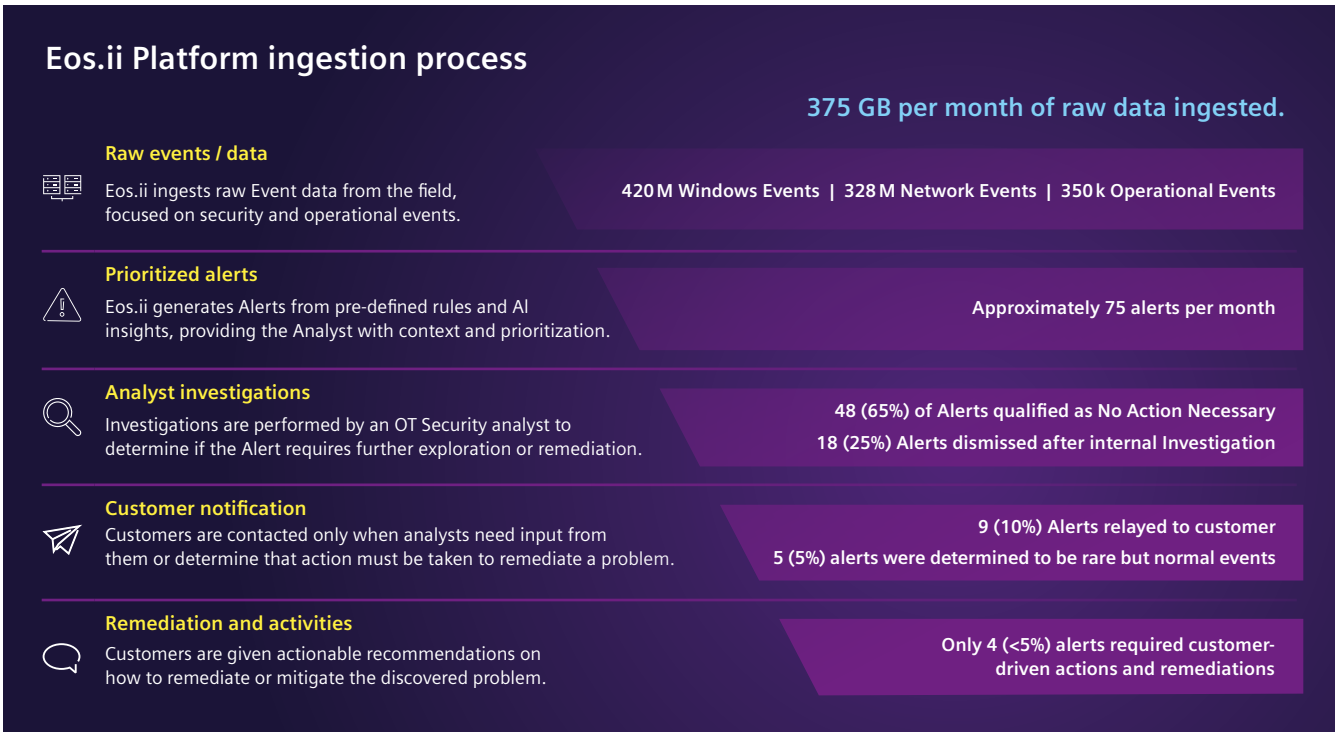
Middle River Power gained visibility into their asset base, with immediate positive results. During the deployment phase, Siemens Energy experts discovered and resolved a longstanding misconfiguration. “Right off the bat – honestly during installation – we found an issue,” VP Claude Couvillion said, “The OPC data link was misconfigured and had been misconfigured for years. It did not work redundantly as it was supposed to.” The issue was discovered by MDR alerts and was fixed, “something that had not been achieved in many previous attempts by both Emerson and T3000 technicians on site.”

MDR makes ongoing cybersecurity monitoring easier for Middle River Power. The difference between event data and alerts requiring customer attention is about eight orders of magnitude. In a recent month, 750 million events – windows, network, or operational events – yielded 9 alerts for customer attention. Automation ingested and processed 375GB of raw data, generating and prioritizing alerts for human review and investigation.

Siemens Energy analysts hunt threats, respond to alerts, and tune cybersecurity automation to align with day-to-day plant functions. Siemens Energy’s OT knowledge enables clear communication with the plant when situations must be addressed. Siemens Energy analysts understand what anomalies are consequential, and use terms familiar with operators when recommending interventions.

Middle River Power has gained confidence and efficiency in compliance. “The frontline guys were doing all the necessary reporting before, but this has made their jobs much easier,” said VP Couvillion. Siemens Energy analysts worked with Middle River Power to develop escalation chains. In the event that a cyber incident occurs, Siemens Energy and Middle River Power will be able to draw on these playbooks to seamlessly coordinate the response.

Several risks previously borne by Middle River Power are now reduced or mitigated.



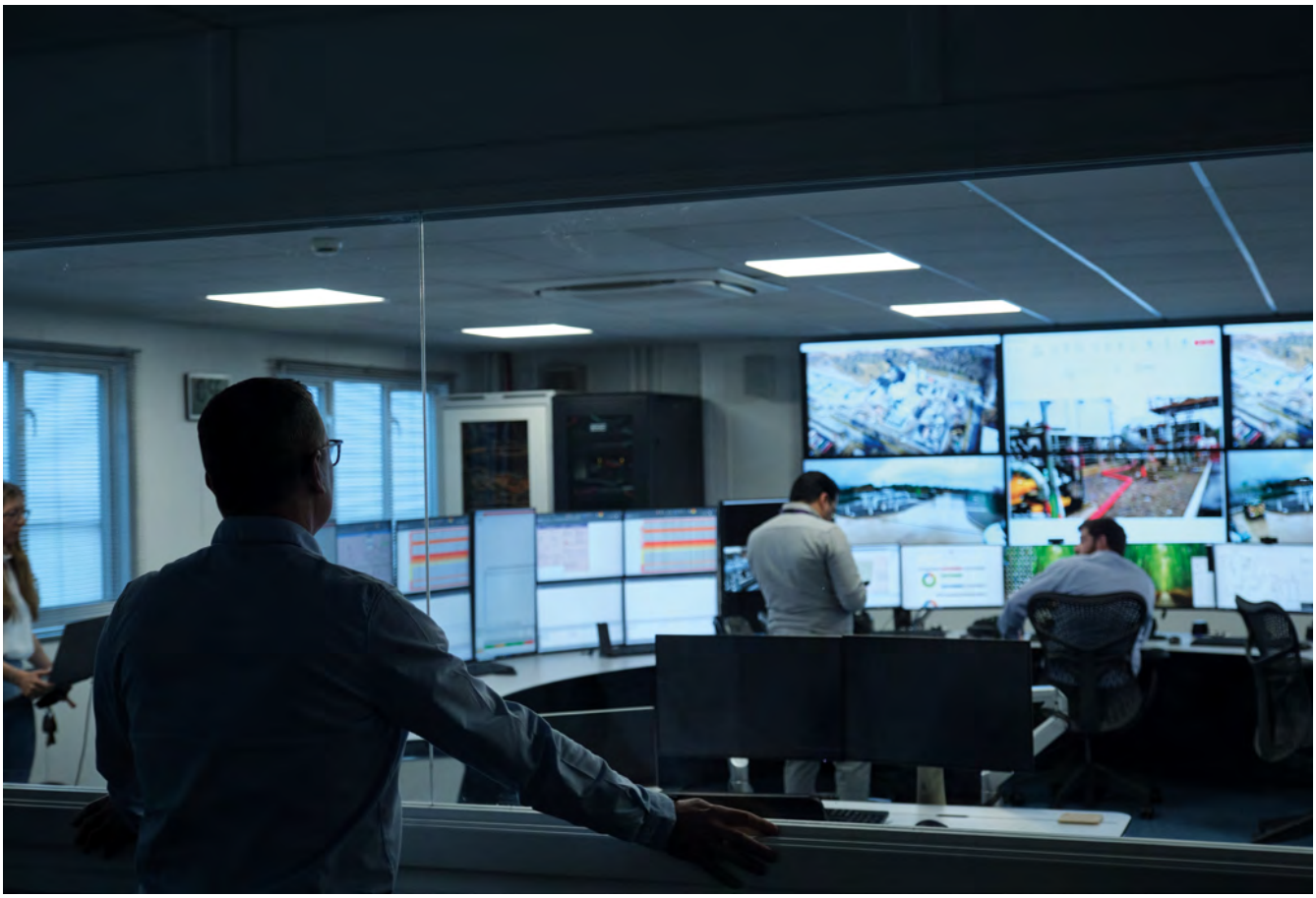
Financial risks are reduced in two ways. First, greater cybersecurity maturity reduces the likelihood and mitigates the expected consequences of a cyberattack targeting the High Desert Power Plant. Second, automation, AI and machine learning tools reduce the costs of achieving best-in-class cybersecurity.

Workforce risks like recruitment, training, retention, and insider threat have shifted to Siemens Energy. Middle River Power gets to rely on the deep pool of OT knowledge and cybersecurity expertise available at Siemens Energy, instead of depending on a small internal team where the departure of any single person could degrade performance.

Attacker innovation risks are mitigated. Recognizing that threats continue to evolve and previously secure systems and practices can be vulnerable to novel threats, MDR analysts continuously tune EOS.ii™'s machine learning engine based on global threat intelligence and real data from customer sites. This continuous vigilance reduces the risk that technical debt will accumulate and unknown vulnerabilities will become or remain exposed.

Reduced uncertainty shrinks operational risks. Auditing the cyber health of Middle River Power's assets at the High Desert Power Plant no longer requires an interruption to production. When a suspected cyber incident occurs, analysts can quickly assess the scope of the incident, identifying which equipment may have been affected and limiting the scale of intervention needed to recover and return to normal operations.

These reduced risks enable Middle River Power to pursue a vision of further automation. "I want to free the technicians up to do their job, to actually be out changing oil, calibrating switches, changing switches, said VP Couvillion, "I want to let the computer do what the computer's good at, which is the repetitive task of operating the plant when everything's going well...I think in the future you could have a road operator monitoring 20, 30, or 40 simple cycle turbines and the computer will through programming be able to tell you when an issue needs to be escalated to thee human." Although this vision remains on the horizon, Middle River Power implemented new automation in parallel with the deployment of MDR. Increased confidence in the plant's cybersecurity played a role in the decision to move ahead. "Automation becomes very scary because as you give the computer the ability to take more direct action and more corrective action, it's very important that you maintain control of that computer and its various algorithms." said VP Couvillion, "Cybersecurity is absolutely the first step to effective automation.



Published by

Siemens Energy Global GmbH & Co. KG
Gas Services
Siemenspromenade 9
91058 Erlangen, Germany

Siemens Energy, Inc.
4400 Alafaya Trail
Orlando FL 32826, USA

For more information, please visit our website:
siemens-energy.com/omnivise

© Siemens Energy, 2025

Subject to changes and errors. The information given in this document only contains general descriptions and/ or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.
All product designations trademarks or products of Siemens Energy Global GmbH & Co. KG or other companies whose use by third parties for their own purposes could violate the rights of the owners.

Siemens Energy is a trademark licensed by Siemens AG.