

Industrial Cybersecurity

Managed Detection and Response Service

powered by Eos.ii™

Intelligent Illumination to Secure the Energy Transition from Cyberattacks

Visit Our Website

SIEMENS energy



ACRONYMS

Eos.ii™	Siemens Energy's proprietary illumination intelligence technology platform
MDR	Siemens Energy's Managed Detection and Response
OT-SoC	Operating Technologies Security Operations Center
PSA	Process Security Analytics
SIEM	Security Incident Event Management System

Content

04 Executive Summary

06 The Energy Industry Can't Protect What It Can't See

07 The Mega-Trend Keeping Defenders in the Dark

08 Understanding the Threats to Operating Environments

12 Intelligent Illumination with Siemens MDR

15 Out of the Darkness: Unifying an IT-OT Threat Stream

17 Into the Light: Looking Ahead with Digital Twins

18 Visualizing Insights: The Power of Human Intelligence

21 Insights into Action: Precision Defense™

22 Giving Defenders the Advantage

Executive Summary

In the past decade, critical infrastructure has become a prime target for cyberattacks. That threat brings a growing impediment to the ongoing technology revolution that's empowering energy companies, utilities and consumers to adopt new power generation, transmission, distribution and end-use technologies. These technologies reduce costs, improve efficiency and lower emissions, but along with these major benefits, increased digitalization in the energy sector creates inherent cybersecurity vulnerabilities. Energy infrastructure is becoming simultaneously easier to attack and harder to defend.

Achieving a future where energy technologies are digitally optimized will increasingly depend on strong cybersecurity. Companies need to detect and respond to cyberattacks before they can cause damage – though many aren't currently up to that task – due to technological and resource constraints. The energy industry's physical assets and digital control systems were never engineered to enable the insights needed for cybersecurity and industry business models have yet to catch up to the growing threat. Across the industry – and especially for medium and small-sized companies – the limitations of existing tools and organizational capabilities make it all but impossible to collect and analyze raw data from digitally connected energy assets, preventing early recognition of abnormalities that could represent a cyberattack.

Staying ahead of attackers requires a new approach to industrial cybersecurity.

Siemens Energy's artificial intelligence (AI)-based offering, Managed Detection and Response (MDR), powered by Eos.ii™, provides energy companies with the visibility and context to shine a light into their operating environment. MDR's monitoring methodology and technology platform leverages AI and machine learning to gather and model energy asset intelligence. Within our state-of-the-art Security Operations Center, Siemens Energy cybersecurity experts armed with actionable insights work with customers to uncover attacks before they execute.

Siemens Energy's MDR service enables companies of any size to access a built-for-purpose platform and world-class expertise. At Siemens Energy, we believe widespread access to high-quality AI-powered monitoring and detection will improve cybersecurity across the networks that make up the energy industry's value chain. That's why MDR is designed for all OT organizations – from the world's largest utilities, oil and gas, and renewable companies, to individual asset owners.

This is a consequential time for the energy sector. Technological change promises a low emissions, high-efficiency future complete with carbon neutral energy companies and smart cities run by intelligent, industrial systems.

The energy future is here. Now we must secure it.



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

Copyright 2020 Siemens Energy

Siemens Energy

Managed Detection and Response Service

powered by Eos.ii™

An AI-based service, powered by Siemens Energy's revolutionary monitoring platform, which provides energy companies with the visibility and context to shine a light into industrial operating environment to stop attacks before they occur.

Copyright 2020 Siemens Energy

The Energy Industry Can't Protect What It Can't See

An accounts manager at a rural utility company receives an email from a subcontractor containing a link to sign documents virtually. Months later, government agents arrive to inform the utility's CEO that its cybersecurity systems have been breached by malicious actors based overseas.

No one in the company – not the CEO or CIO, nor the operators responsible for monitoring the utility's network – had any idea even the slightest breach had occurred. Yet, for months, someone outside the company had the capability to cause catastrophic financial and physical damage whenever they pleased by cutting power to businesses, homes, and emergency and national security installations.

This scenario is a nightmare for any energy company – but it's not fiction. It's an account of a real event made public by the Wall Street Journal in 2019. While U.S. law enforcement officials didn't confirm this attack's origin, the hackers were linked to nation-state actors who increasingly view critical infrastructure as a ripe target – even in developed countries like the United States. Unfortunately, this scenario is a harbinger for security across the energy industry.

Energy companies should learn a key lesson from this real-world incident: cybersecurity professionals can't defend against attacks they can't see. Companies need real-time understanding of malicious activities in their environment, their method of attack and how security professionals can intervene to proactively prevent any damage. But most companies today struggle with the complex challenge of detecting, monitoring and preventing cyberattacks on critical infrastructure because of both technological and economic barriers. The challenge is that the operational technologies (OT) and information technologies (IT) responsible for running energy systems today were never engineered to be secured in a digital environment.

Copyright 2020 Siemens Energy

The Mega-Trend Keeping Defenders in the Dark

Cyber risks have grown along with the digital and technological revolution sweeping through the energy sector. Digital technologies are rapidly accelerating innovation across the energy value chain in the same ways the smartphone transformed the telecommunications industry.

Just a few years after smartphones became ubiquitous, telecom's business model was forced to adapt as it no longer focused on landline, analogue connections between customers. Instead, these companies shifted to the business of managing data on smartphone platforms responsible for billons of connections and communications that have changed everyday life. Similarly, digitization is enabling an entirely new business model for the energy industry – one where power no longer flows from a centralized power plant to a transmission and distribution system, and eventually to consumers, businesses or end users.

Instead, today's energy ecosystem is a multi-directional, interconnected mesh network, which transfers information with internet-like speed and is responsible for controlling critical infrastructure. For most companies, OT assets are now connected with IT systems to improve efficiency and reliability while reducing costs and emissions. The resulting competitive advantages make it worthwhile for companies to build their business model around digitization of energy infrastructure, but only with cybersecurity at its core.

That means existing "brownfield" assets like gas turbines, pipeline compressors and electric substations, previously operated by isolated software programs or analogue controls, are being digitized and connected to broader networks. Meanwhile, digitally-native energy assets – whose control systems are engineered to function using IT commands – like renewable power generation, smart-grid technologies, and EV charging stations, are being deployed at a break-neck speed. Retrofitted and new assets will both play critical roles in future energy generation and distribution systems – and both introduce new and elevated risks that the energy industry must learn to manage.



Copyright 2020 Siemens Energy

Understanding the Threats to Operating Environments

Malicious actors are no longer just cyber criminals seeking financial gain. Attackers now include state and non-state actors seeking to use energy and critical infrastructure as a pawn in broader geo-political or adversarial conflict. A 2019 Ponemon Institute study surveying the energy sector's readiness to address this growing spectrum of cyberattacks found that 64% of respondents say sophisticated attacks, like ones designed by nation-states, are a top challenge. Moreover, 54% expect an attack on critical infrastructure in the next 12 months and 25% of respondents report being impacted by mega attacks with expertise developed by nation-state actors.

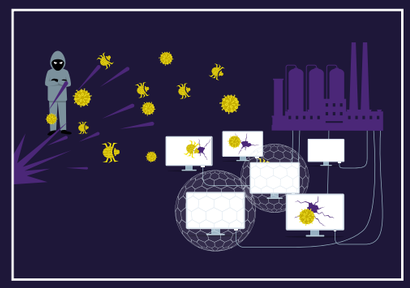
The Ponemon study also found that today's attackers are motivated by causing physical harm on industrial systems and show greater skill at finding weakened entry points by leveraging cheaply built malware. At present, simple exploits available to any malicious actor on the dark web for $16.99 can cause extraordinary damage to daily operations worth millions of dollars.



Copyright 2020 Siemens Energy

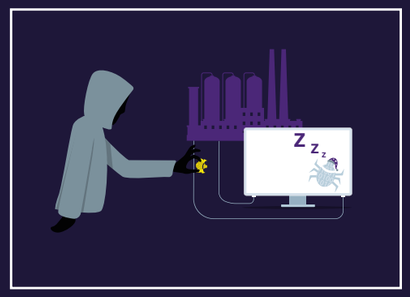
Evolving OT Threats

Spotlight on Attacks Targeting the Energy Sector



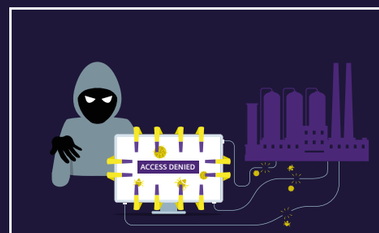
Scattershot attacks

Scattershot attacks target an identified weakness in widely used software, but aren't necessarily aimed at a specific organization. The Wannacry hack is a highly publicized example of this type. These attacks are sent around world looking for systems that they can infect, and attack those systems wherever they are found. Slightly more sophisticated versions of these attacks – like Stuxnet – can be designed to infect many computers but only execute when they find specific equipment configurations.



Sleeper strikes

Sleeper strikes attack a specified target to set up later disruption. This type of spearfishing attack maps the assets within the network, and embeds sleeper code or devices that can be activated later. These threats are often associated with nation-states, and may have disruption as a major goal, rather than financial gain. When targeted companies are hardened their defenses against, malicious actors may seek weaker points in the overall supply chain.



Ransomware attacks

Ransomware attacks use disruptive techniques for direct financial gain. These threats allow hackers to take control of critical systems and hold them hostage, often by encrypting data so that authorized users can't access relevant systems. They are often associated with criminal groups who demand payment in order to unlock the hostage systems, and may or may not return control after payment is provided.

Copyright 2020 Siemens Energy



Visibility is the cybersecurity team's ability to see what's happening across each individual digitally connected node in the ecosystem. Without visibility, a team is blind. Context is the team's ability to not only pin point the source of the breach but to also understand its implications, both for the assets that are impaired but as importantly for the system as a whole. Without context, an analyst can't determine whether the next command will break equipment or make it function normally.

 Copyright 2020 Siemens Energy

The Challenge of Defending an Ever-Expanding Threat Landscape

Each digitally connected node presents a possible cyber vulnerability – a point where malicious actors may potentially enter or manipulate energy infrastructure. In this ever-expanding threat landscape, cybersecurity professionals are forced to defend OT and IT systems that were never designed to integrate with a unified security architecture.

Defenders are unable to translate huge flows of raw OT and IT data and analyze it to monitor for credible threats in time to take decisive action. In practical terms, this means that defenders can't see what's happening within their own operations, and can easily miss attackers who are actively exploring the network in the search for vulnerabilities. When it comes to OT cybersecurity, most companies are operating in the dark – and they know it.

Why do we still lack a built for purpose industrial monitoring system?

So, if energy companies know they are increasingly vulnerable to cyberattacks – why do we still lack a built for purpose industrial monitoring system?

The answer is that most energy companies see their vulnerability to cyberattacks as a security problem, not a visibility and context problem. Many industrial cybersecurity approaches address the problem by air gapping assets in their operating environment to put them behind physical and digital security walls, and then chase after possible breaches. By the time an attack is detected, it's too late.

With visibility and context, cybersecurity teams can do more than just detect anomalies. They can determine whether an attack is in progress, assess probable operational impacts, and create proportionate and fast responses that resolve the attack with minimal disruption. Strong visibility and context enable a fight with eyes wide open and a home field advantage – so operators can intervene before attackers can achieve their goals.

Copyright 2020 Siemens Energy

Intelligent Illumination with Siemens MDR

The core challenge of protecting critical infrastructure from cyberattacks is the complexity of monitoring, gathering, analyzing and then acting on intelligence across the entire energy ecosystem. The digital revolution is expected to add 2.5 billion industrial devices in the next two years. Most OT environments include tough technical challenges like heterogenous legacy systems, differences between IT and OT computer languages, and a huge volume of data generated on a minute by minute basis.

Any approach providing visibility into the OT needs to solve these problems and present the unified results to human operators in an intelligible form within seconds. The failure to execute these steps will result in shutdowns or running an ever-escalating risk of preventable safety events.

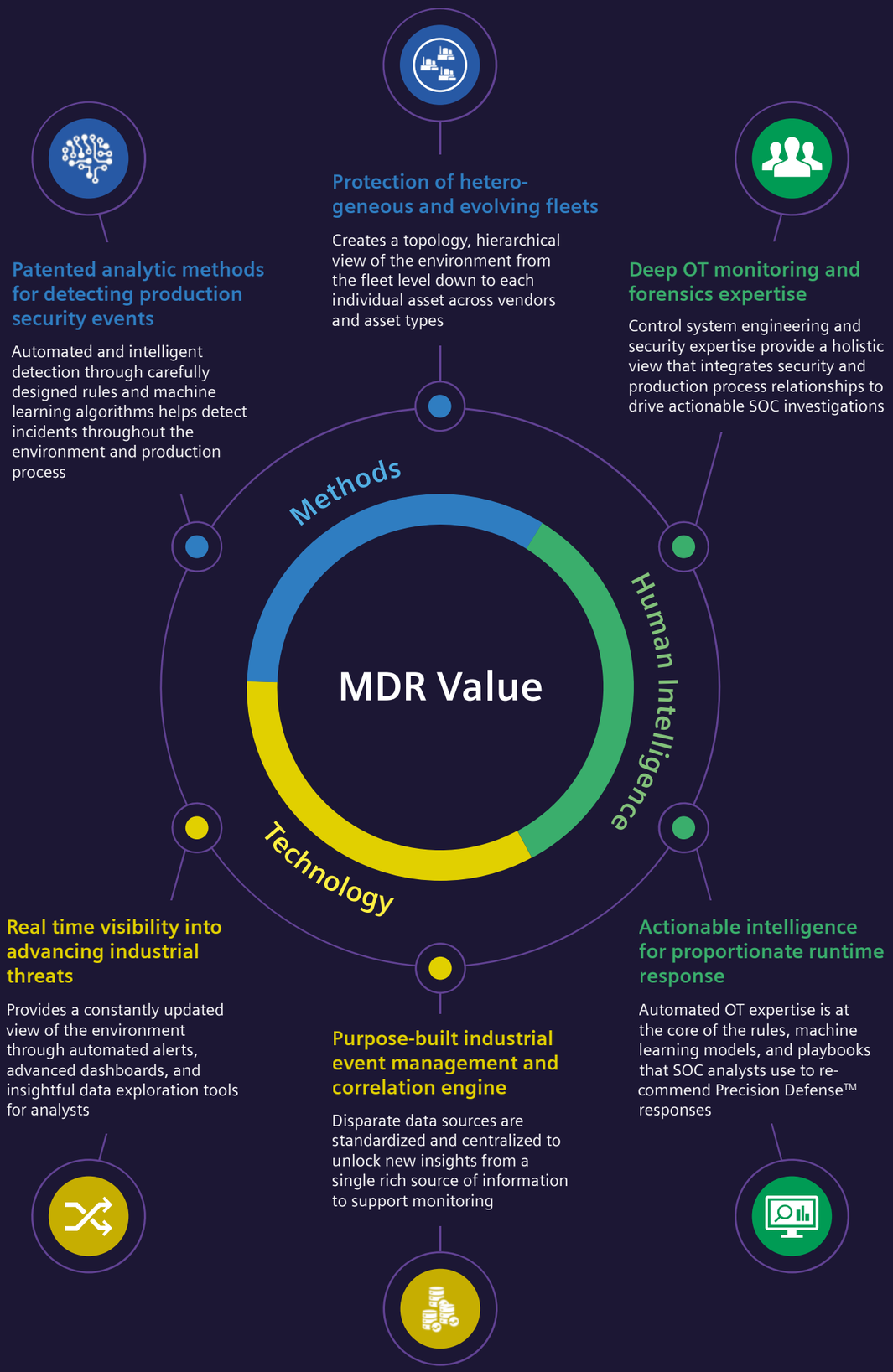
An Accessible Solution to Provide Context and Visibility to Shine a Light on Attackers

Siemens Energy's industrial cybersecurity service, Managed Detection and Response (MDR), powered by Eos.ii™, changes all that – providing the context and visibility to shine a light on attackers before they strike.

Siemens Energy's MDR, powered by Eos.ii™, is an affordable artificial intelligence-driven (AI) cybersecurity monitoring service for energy companies to proactively detect and prevent cyberattacks against OT regardless of their fleet size or market share. Combining Siemens Energy's industrial cybersecurity expertise with our proprietary detection technologies, the MDR service collects raw IT and OT data from across a customer's energy operating environment, and then translates – and contextualizes – it in real time.

This provides a unified picture of anomalous behavior with actionable insights for defenders to stop attacks. Until now, this capability was only accessible to the industry's largest operators. MDR's data collection method, technology and Siemen Energy's analysts connect the dots between OT configurations and their real-world consequences – enabling insights that enhance cyber defenses while minimizing impacts on production for small and medium-sized companies. By design, the methods and platforms used are affordable and scalable, making them accessible to companies throughout the energy supply chain. They are also engineered to handle the ever-growing number of digital native and retrofitted assets.

Copyright 2020 Siemens Energy



Patented analytic methods for detecting production security events

Automated and intelligent detection through carefully designed rules and machine learning algorithms helps detect incidents throughout the environment and production process

Protection of heterogeneous and evolving fleets

Creates a topology, hierarchical view of the environment from the fleet level down to each individual asset across vendors and asset types

Deep OT monitoring and forensics expertise

Control system engineering and security expertise provide a holistic view that integrates security and production process relationships to drive actionable SOC investigations

Real time visibility into advancing industrial threats

Provides a constantly updated view of the environment through automated alerts, advanced dashboards, and insightful data exploration tools for analysts

Purpose-built industrial event management and correlation engine

Disparate data sources are standardized and centralized to unlock new insights from a single rich source of information to support monitoring

Actionable intelligence for proportionate runtime response

Automated OT expertise is at the core of the rules, machine learning models, and playbooks that SOC analysts use to recommend Precision Defense™ responses

Copyright 2020 Siemens Energy

A New Day for Cybersecurity Through Affordable AI

Companies that secure their own networks remain affected by the strength or weakness of security practices in the wider energy ecosystem. While some large companies have begun deploying OT cybersecurity solutions, small and mid-sized companies do not have sufficient research and development budgets to pursue new technology in-house, and many struggle to hire or train the expertise needed to pursue such a project. Small and mid-sized companies are getting left behind – and becoming the weak links in the overall energy system.

Achieving a future built on smart infrastructure – like electric vehicles and prosumer business plans – depends on increasing cybersecurity industry-wide and in every link of the value chain. That's why Siemens Energy's MDR service was created as the first industrial cybersecurity solution that brings all organizations access to OT monitoring, detection and cyberattack prevention capabilities, currently only attempted in-house at companies with ample research budgets.

Artificial Intelligence Reveals the Consequential Threats

Siemens MDR service goes beyond conventional monitoring by achieving a deeper understanding of how digital systems relate to the real world. With its unified OT and IT data stream, MDR's Eos.ii™, technology platform uses AI and digital twin technology to compare billions of real-time data points against a correctly functioning asset. This provides context for Siemens' analysts to determine not only which events are anomalous, but which are consequential.

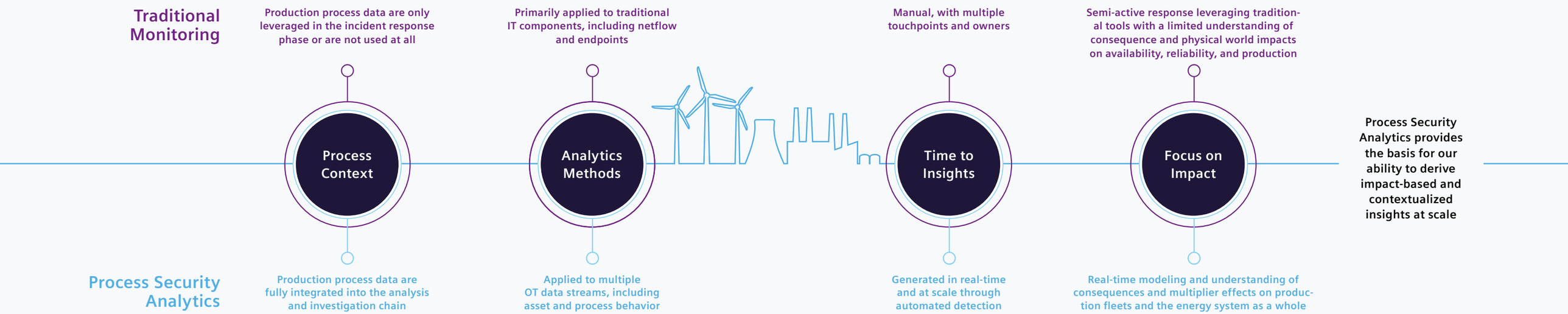
Out of the Darkness: Unifying an IT-OT Threat Stream

Visibility in an industrial operating environment is impossible without understanding how the digital world impacts the physical world. To gain this insight, OT and IT data must be collected from each digitally connected energy asset in an organization's operating environment, and then translated into a common language for analysis. This data collection must take place every second of the day, every day of the year. To collect and prepare vast amounts of network data for analysis, Siemens created a proprietary method called Process Security Analytics (PSA) which serves as the backbone of the Eos.ii™ technology platform.

Creating a Unified OT-IT Threat Stream

PSA is a systematic method for unifying OT and IT data streams, revealing anomalous behavior and discovering cyberattacks in an OT environment. Without a methodology to unify this data, it is impossible to assess abnormalities in an energy asset's behavior. Using PSA enables analysts to determine if inconsistencies stem from a physical or digital manipulation that could alter the asset's configuration and cause destruction. That's why PSA's algorithms gather and synthesize information on real-time configuration changes, operational feedback, and human intervention to measure anomalous behavior and compare it against normally functioning energy assets.

Unifying IT and OT data streams enables greater visibility into the interactions of digital and physical assets – and this matters. Where conventional network monitoring would only reveal that network traffic is higher than usual between two devices, MDR's PSA methodology applies advanced and continuously adapting algorithms to its data collection and synthesis process to power AI models for deeper insights.

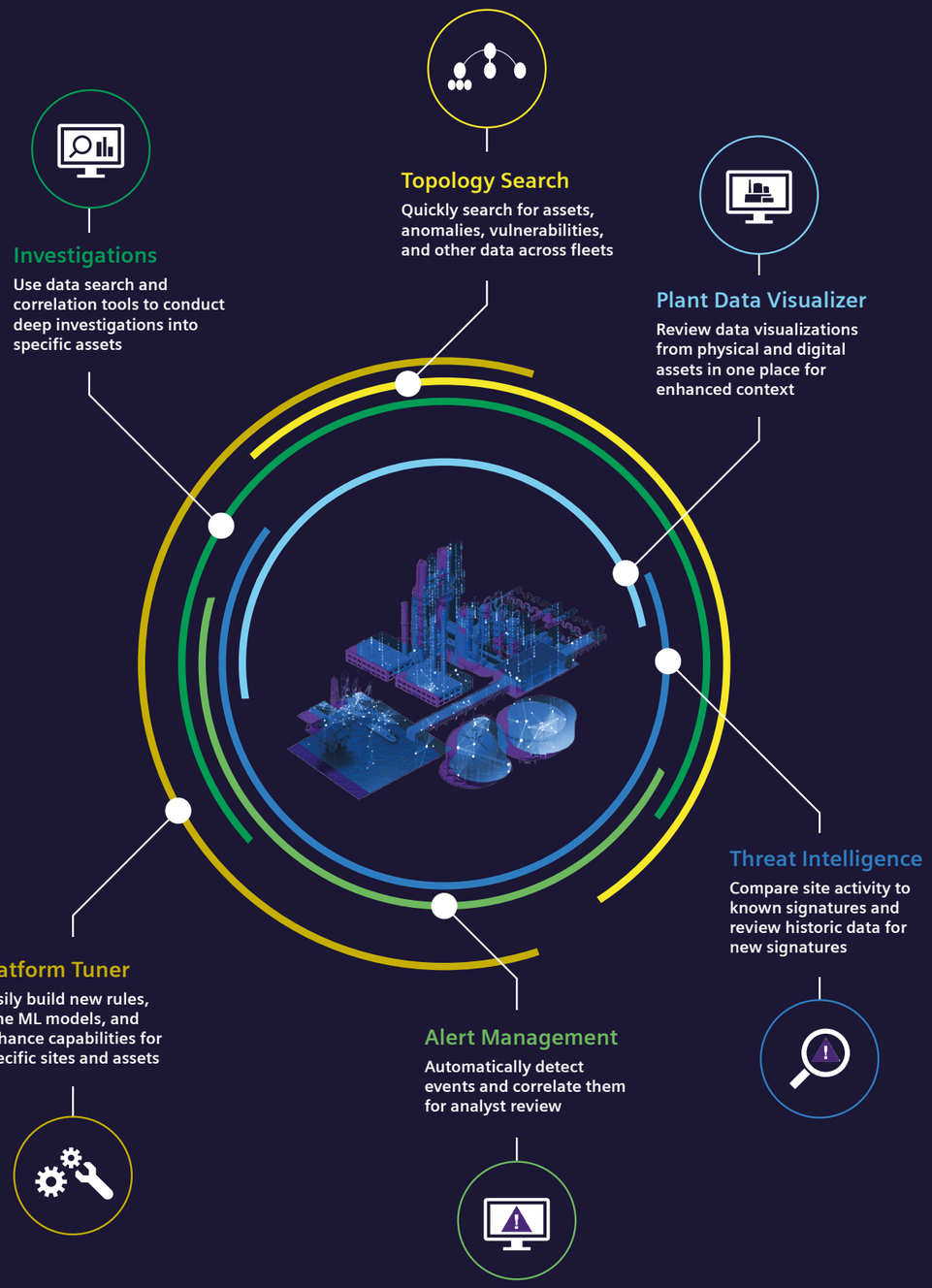


 Copyright 2020 Siemens Energy

Copyright 2020 Siemens Energy

Eos.ii™ Platform

Platform modules provide the backbone to generate insights and drive actionable intelligence



 Copyright 2020 Siemens Energy

Into the Light: Looking Ahead with Digital Twins

While visibility can provide customers insight and intelligent data for detecting anomalous behavior, defenders still require context to stop attacks. This is a core challenge for industrial-scale OT cybersecurity – defenders need to analyze and act on the credible threats embedded in huge flows of IT and OT data every second of the day, every day of the year. The only way to enable rapid human understanding at this scale – leading to decisive actions to stop an attack – is using AI and automated domain expertise to provide context.

The Eos.ii™ Platform Brings Illumination Intelligence to the Industrial Operating Environment

Siemens Energy created Eos.ii™, our Security Incident Event Management system (SIEM), to provide AI-backed speed and scale for automated analysis and exact context. This technology is an interoperable and manufacturer-agnostic platform which takes the aggregated IT and OT data from PSA's threat stream and contextualizes it to understand anomalous behavior.

The platform does this by using algorithms to create a digital twin to compare anomalous behavior against a digital replica modeling normal operations. Any deviations, automatically flagged by our platform rule logic, will indicate an impending cyberthreat that analysts can act on before a malicious command executes in the physical world.

MDR's technology platform also scales to enable efficient in-depth investigation into the anomalies it discovers. The platform was built from real world use cases, leveraging Siemens' domain expertise to develop detection rules from past attacks to model for increasingly sophisticated threats. Our platform leverages proprietary OT threat intelligence datasets tailored to operating environments, such as oil and gas assets, power and electric grid assets, and edge devices – and compatible with any manufacturer.

Copyright 2020 Siemens Energy

Visualizing Insights: The Power of Human Intelligence

MDR's methodology and technology platform empowers defenders with the visibility and context to see where attackers are launching threats and what they are targeting. These highly sophisticated algorithms cut through the complexities of today's energy ecosystem to give defenders actionable intelligence – but data and algorithms can't stop an attack by themselves.

The power of Siemens' MDR solution comes from human intelligence – experts who can seamlessly transition from analyzing intelligence in the digital world to acting in the physical world to stop an attack.

Every Threat Is Consequential: Siemens' OT-SoC Makes the Digital World Real

Armed with our proprietary MDR playbook, and based in our state-of the-art OT-Security Operations Center, Siemens OT cybersecurity experts turn visibility and context into action. Siemens' cyber experts believe in the principle that every threat is consequential, so every alert matters. That's because they've seen the consequences of cyberattacks on critical infrastructure before.

To Stop an Attack, Experts Must Think Like Attackers

Trained in plant operations, they can think – and act – like a hacker to stop an attack; and they remain dedicated to an incident case – from the time it is detected to the time it is neutralized. This means our analysts don't filter potential cyberthreats and raise awareness to others with deep domain expertise after the severity of the attack becomes apparent. Instead, MDR customers start straight away with an expert who has decades long experience in OT cybersecurity to anticipate and pinpoint attacker's every move, and that expert sticks with the case.

Our experts continually maintain the tools and sharpen the algorithms needed to conduct forensic investigations into anomalies, run operations to rapidly discover malicious code and determine the intended consequences early enough to prevent or mitigate damage, and provide customers with actionable intelligence.

Copyright 2020 Siemens Energy

Human Intelligence at Work

Analyst-customer interlock to deliver richer insights



Sharpening tools and algorithms

MDR's technology platform is self-learning, but it requires OT-specific insight to continually sharpen algorithms and build up new rules to eliminate attacks before they cause damage.

To ensure Siemens OT-SoC stays agile and ahead of attackers Siemens Energy uses OT hackathons to keep our analysts in the mindset of a hacker as they defend operating environments. Siemens control engineers get to work on use cases for specific assets and practice breaching defenses based on the latest threat intelligence.

Running operations

For Siemens OT-SoC analysts, every alert matters; our analysts work based on the potential physical and financial damage of an attack using digital twin technology to map impact across a customer's operating environment.

In the OT-SoC, workflow is determined by playbooks of attack / use case, rather than the importance of escalation path. Instead of passing a potential cyberattack case up an escalation chain, our experts follow the ICS kill chain for every alert. That means our analysts remain with their customers from opening a new case to eradicating an attack. Customers can expect prioritization based on expected operational impacts, a clear assessment of an unfolding attack, and targeted recommendations for how it should be fixed.

Acting on intelligence

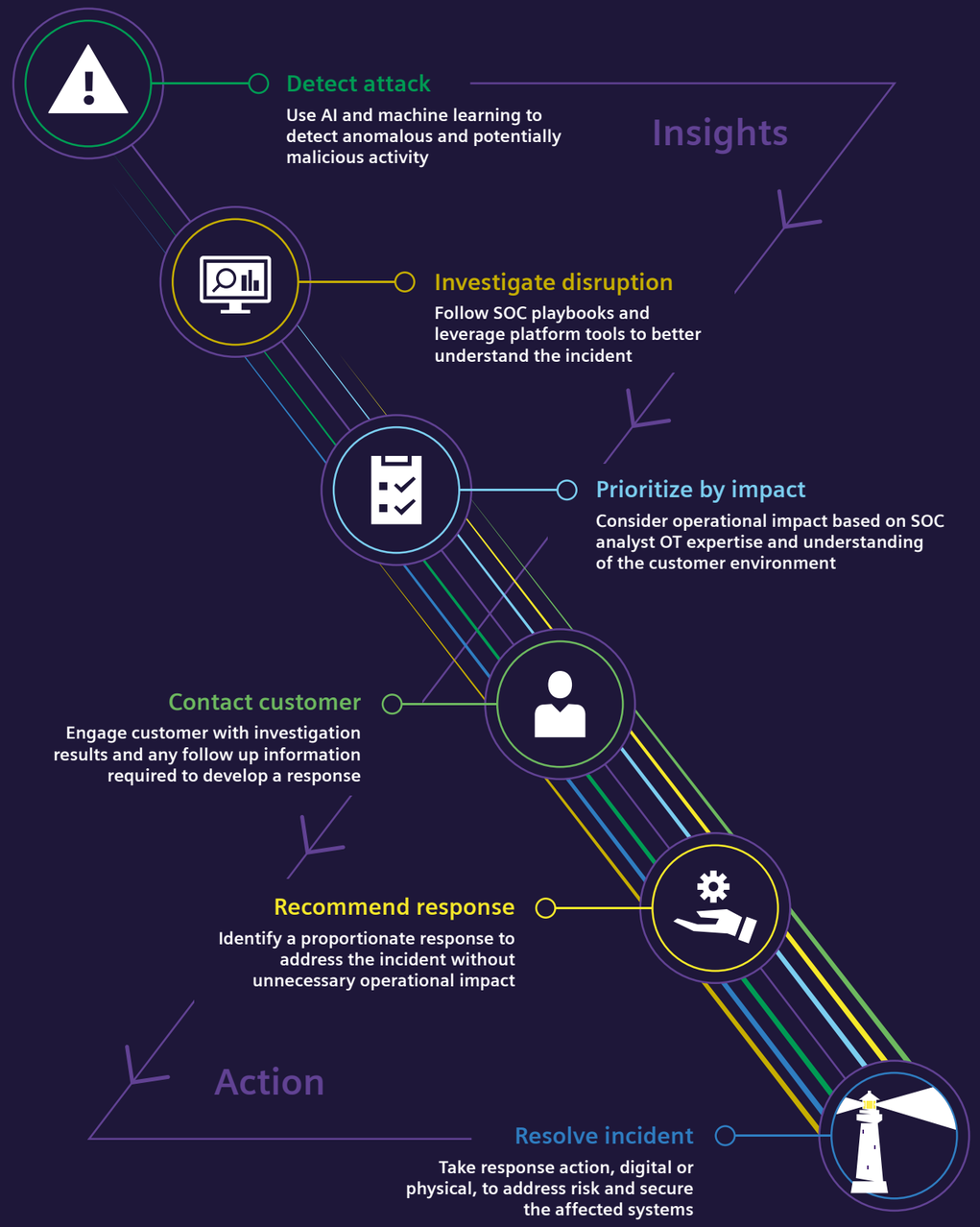
Our customers value operational integrity and security because their businesses depend on minute-by-minute reliability.

Siemens MDR optimizes for both risk reduction and our customers' commitments to energy availability and safety. Resolving attacks with the minimum disruption to operations requires taking proportionate action – and that's the philosophy Siemens Energy takes with our Precision Defense™ method.

Copyright 2020 Siemens Energy

Precision Defense™

Rapid and proportionate response to stop attacks before they occur



 Copyright 2020 Siemens Energy

Insights into Action: Precision Defense™

While most IT systems can physically withstand a no-notice shutdown, things aren't so simple in OT. In OT environments, pulling the plug is an expensive proposition and a last resort. Any defensive action to protect equipment has to account for its physical state, safety consequences, and the physical connections to other systems. Poorly thought out actions may cause irreparable damage. That's why Siemens Energy developed Precision Defense™.

Precision Defense™ is a response method with the goal of deploying appropriate, targeted, and proportionate measures to correct and recover from a cybersecurity incident. Defenders contain an attack by addressing exactly the affected systems – no more and no less. Correctly implemented, it results in fully effective containment and eradication of the threat, with the minimum possible disruption to production. Precision Defense™ is impossible without accurate insights into the extent of an intrusion.

Implementing the Precision Defense™ Playbook

The Precision Defense™ playbook used with Siemens Energy's MDR draws on 30 years of real-world experience and leadership in leading national and multi-national Computer Emergency Response Teams (CERTs). The MDR playbook contains scenarios and associated decision trees for the appropriate level of action in a specific asset stack. For example, the containment steps will differ widely between an outage caused by environmental damage, a safety threat or a mega attack like WannaCry. Playbook recommendations are not only digital but also physical – sometimes reconfiguring a gauge or turning a valve can be as effective as electronically isolating malware.

Copyright 2020 Siemens Energy

Giving Defenders the Advantage

Energy companies can reasonably expect that attacks like the one covered by Wall Street Journal will recur and continue. If – or more likely when – a similar attack targets a Siemens Energy MDR customer, the hackers will risk detection at multiple stages of the attack. The advantage is flipped. Now the defender is empowered with insights to stay ahead of attackers. Instead of an unaware compromised company continuously at risk of disruption, it's the intruders who are continuously at risk of discovery.

The complexity of industrial cyber monitoring has made many companies slow to address the issue, and led some companies to determine the risk-reward proposition isn't worth the investment. Yet the same technology changes driving digitalization and increasing complexity for defenders will continue to raise the stakes for monitoring and detection in the energy industry.

Cutting-Edge Cyber Monitoring and Detection for the Many, Not Just the Few

Siemens Energy's tailored deployment model can change the paradigm without loss of operational control. Instead of flying blind, companies using Siemens Energy MDR have 24/7 visibility across their OT assets and digital control systems. Energy companies gain greater confidence that their leadership will be able to make informed decisions on cybersecurity. Siemens Energy MDR will swiftly identify cyberattacks, and advise how to respond proportionally.

Advances like built-for-purpose OT cybersecurity monitoring and detection will help the energy sector mature and strengthen weak links in the energy value chain. Adopting and deploying better monitoring systems will make critical infrastructure more mature, and importantly, will enable companies to unlock the full potential of digitalization and the next wave of smart technologies. It's how we can all work to secure a better future.

Copyright 2020 Siemens Energy



Copyright 2020 Siemens Energy

Published by

Siemens Energy Inc.

15375 Memorial Drive
Houston, TX 77079
United States

https://www.siemens-energy.com/global/en/offerings/services/digital-services/cybersecurity.html

For further information:

Calvin Hunt
Global Portfolio Lead
Calvin.hunt@siemens.com

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.

Siemens Energy is a registered trademark licensed by Siemens AG.