

Industrial Cybersecurity

EOS.ii™ Monitoring and Detection Platform

Intelligent Illumination for IoT Cyber Defense

About Our Practice

SIEMENS energy



Content

08 The Dawn of Industrial IoT

10 The Energy Industry's Digital Revolution

12 The Complexities of Defending an IoT Environment

14 The IoT Monitoring and Detection Imbalance

16 Building a Fusion SOC to Illuminate Industrial IoT

19 Illuminating the Foundation for IoT Visibility and Context

21 Seeing Through the Fog with Monitoring and Detection

23 The Intelligence Behind Eos.ii™

27 Realizing the Vision of a Fusion SOC

Executive Summary

Imbuing useful machines with network connectivity and automated monitoring offers tremendous power. We can envision warehouses and retail stores with instant, automatic inventory. Cities where traffic flows steadily because the lights change when vehicles approach. Pipelines that self-report signs of impending failure. Electric grids that seamlessly shift between renewable sources of energy to provide affordable, reliable power with low or zero emissions during peak demand.

These visions are already just expansions of fundamental changes in our economy, currently underway. The reality of physical industrial equipment seamlessly integrated with the digital world is already here and poised to grow.

Energy and critical infrastructure companies are aggressively building an industrial Internet of Things (IoT) to make operations more automated, more flexible and more efficient by seamlessly linking operational technology (OT) to control physical assets with information technology (IT) applications. Yet without IoT cybersecurity monitoring and detection, these ambitions will fail.

Protecting energy and critical infrastructure sectors run on industrial IoT technology puts Chief Information Security Officers (CISOs) and their existing Security Operations Centers (SOCs) under significant strain. As the IoT business model increasingly integrates physical assets and digital networks, CISOs need entirely different monitoring and detection capabilities to overcome the scale and complexity of securing a hyperconnected world from cyberattacks.

To monitor and secure industrial IoT environments, CISO will need a new platform that can serve as the foundation of their organization's IoT SOC with the capabilities to address today 's vulnerabilities and evolve to meet tomorrow's threats. Leveraging its legacy in engineering and securing energy and critical infrastructure industries for more than 170 years, Siemens Energy has developed a new Security Information and Event Management (SIEM) platform, Eos.ii™.

Eos.ii™ is a scalable and flexible AI-based monitoring and detection platform designed to serve as the foundation for a next-generation fusion IoT SOC. By design, it enables rapid gathering, processing, and prioritizing of actionable intelligence within industrial operating environments. Eos.ii™ is the first SIEM to unify IT and OT monitoring and detection capabilities through machine learning to prioritize high-consequence alerts for human investigation – and enable continuous, site-specific improvement.

Eos.ii™ empowers CISOs and SOCs with the platform and insights needed to scale up security to meet the demands of IoT business models. It offers unmatched capabilities to build and maintain robust, adaptable, and resilient defenses in a fast-moving and competitive IoT future.



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



EOS.ii™
intelligent illumination
by Siemens Energy

An AI-based monitoring and detection platform purpose-built to serve as the foundation of an IOT fusion SOC for energy and critical infrastructure in an era of persistent cyberattacks.



Acronyms & Definitions

AI

Artificial Intelligence is field of computer science that uses algorithms to iteratively learn relationships between variables in large datasets.

Fusion SoC

A Fusion SoC is both a strategic and tactical Security Operations Center (SoC) capable of monitoring, detecting and acting on cyber threat intelligence on IT networks and physical assets controlled by OT systems.

CISO

The Chief Information Security Officer is responsible for assessing cyber risks and defending company assets against cyberattacks. Modern CISOs often have responsibility for digital security of people, devices and data.

IT

Information Technologies are technologies for storing, retrieving, or transmitting information. They include personal computers, servers, and communications networks.

Context

Context is the information necessary to understand the operating status of a device, its relationship to linked systems, and the operating status of those connected systems.

IoT

The Internet of Things is a term used to describe IT and OT devices that are networked together to make an integrated whole, allowing for automated feedback loops between multiple devices, automatic inventory, remote management tools, and many other features.



OT

Operating Technologies include equipment with a mechanical or real-world output – for example a turbine, pump, or robotic arm – often controlled by a computer processor built into the equipment.

Precision Defense™

Precision Defense™ is the use of monitoring to identify the extent of intrusions, enabling effective containment, eradication and recovery with the smallest possible collateral impact on business processes.

PSA

Process Security Analytics is the proprietary methodology Siemens Energy uses to analyze IT and OT data to assess which security events will be consequential.

SIEM

Security Information and Event Management is a category of software platform used to log and analyze data and events relevant to cybersecurity.

SOC

A *Security Operations Center* is the centralized hub of cyberdefenses for an organization. Analysts within a SOC investigate potential threats and take actions to protect assets or recover from attacks.

Unified Threat Stream

A Unified Threat Steam is a data feed that collects information from every monitored component of a system in a centralized and standardized format, translating from disparate source languages and formats as needed.

Visibility

Visibility is the ability of an analyst or security operations center to pull real-time information about a device, its operating status, and its context within the larger system.

The Dawn of Industrial IoT

Seamless Integration of Digital and Physical Worlds

The "internet of things" (IoT) is bringing rapid change to the industrial world – fundamentally and forever shifting all aspects of the economy into digital connectivity.

At its core, IoT is the seamless integration of operational technology (OT) – which is responsible for controlling and commanding physical equipment – with information technology (IT) systems. This integration allows companies to optimize, refine and create efficiency through big data, tailor-made apps and artificial intelligence (AI).

IoT brings big benefits to businesses across industrial sectors – and for cybersecurity, it's also a big change. Previously, digital OT commands running energy assets, heavy machinery or infrastructure facilities were typically sectioned off from network connected IT systems, with a clear divide between IT and OT assets and their respective security procedures. This divide helped protect OT assets from more frequent and easily executed cyberattacks commonly launched against IT networks.

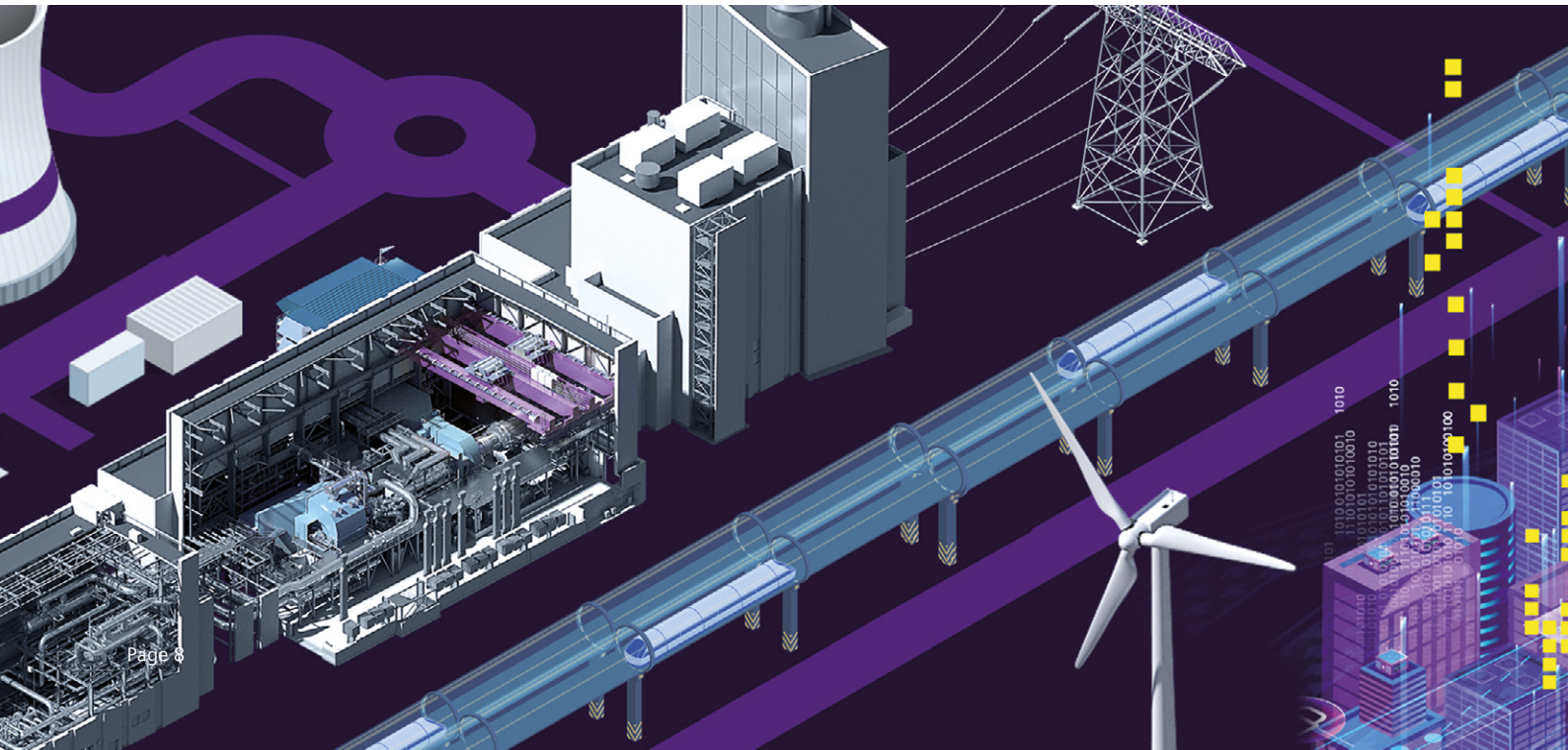
Digitalization's Achilles Heel

IoT is blurring that division. Energy and critical infrastructure companies are intentionally linking IT and OT to make their operations more automated, more flexible, and ready to launch previously impossible products and processes.

Over 8 billion industrial IoT devices are already in use, and more than a billion are expected to be added this year. As organizations bridge the boundaries between the physical and digital worlds, they are also unavoidably exposing new vulnerabilities to physical assets that had previously been protected from many digital attacks.[1]

The confluence of these factors means that industrial IoT gives cyber attackers a pathway – if successful – to cause physical damage that would bring huge and lasting consequences for millions of customers. This makes the energy and critical infrastructure sectors an attractive target for malicious actors, including some backed by nation-states.

1 https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/



Defending in the Dark

It is no secret that cybersecurity teams tasked with defending industrial IoT environments now have more infrastructure to protect against the backdrop of more frequent, more ferocious attacks. The assets in need of protection have also changed as connectivity is now required for previously isolated devices, and mobility and variability are defining features of previously static assets.

It should not be surprising that CISOs and their teams frequently find a mismatch between their current cyber capabilities, their organization's demands to advance innovative IoT business models – and that attackers seek to exploit these gaps.

This forces the question: How does a CISO overcome the technical obstacles and capability gaps needed to secure digital and physical assets from cyberattacks today and in the future?

Hyperconnectivity Here to Stay

Slowing the pace of change isn't an option. Companies have bet their businesses on expanding IoT capabilities for a competitive advantage in the industrial marketplace.

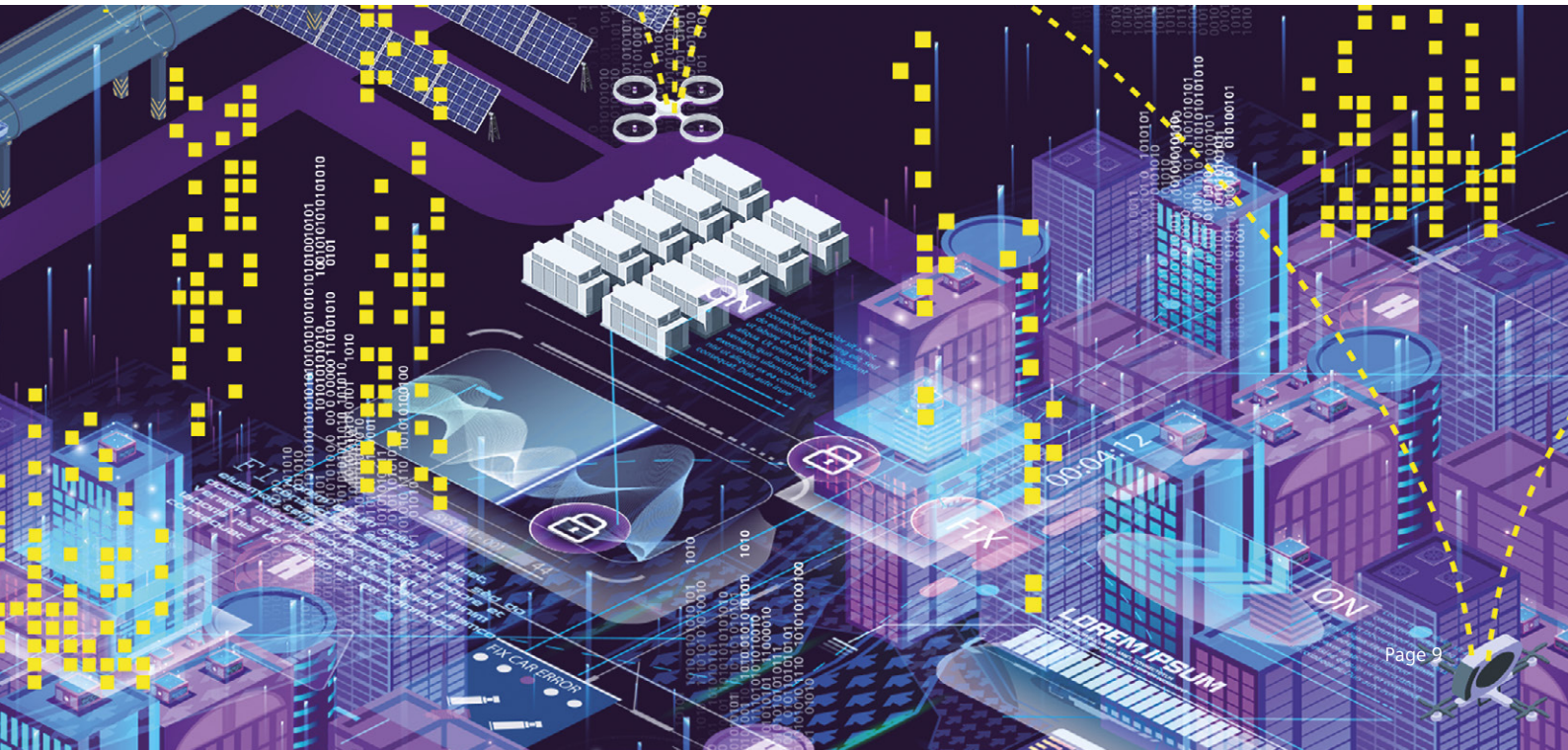
But most CISOs and cybersecurity personnel come from IT backgrounds with a high degree of expertise securing digital networks, and the security of physical equipment was left to engineers in the field.

For CISOs, their businesses, and their ever-changing assets, the future depends on gaining expertise in physical asset security with relatively new OT-specific cybersecurity technologies and methodologies to get IoT cybersecurity right. That means cybersecurity teams need to master IT and OT monitoring and detection equally amid rapid change and increasing complexity.

Illuminating an Ongoing Revolution

IoT cybersecurity relies on a core concept: defenders must gain visibility and context across an operating environment of physical and digital assets to monitor, detect and act on potential cyberthreats before they execute across an interconnected system.

To mitigate cyberattacks against digital and physical assets, defenders need to see into each and every system. And CISOs need to ensure their teams will have that capability no matter what new technologies their companies add in the future.



The Energy Industry's Digital Revolution

Unlocking the Energy Transition

As the energy and critical infrastructure sectors increasingly depend on seamless connections between physical and digital assets, malicious actors are taking advantage of the inherent vulnerabilities in a digitally driven energy ecosystem.

Oil and gas companies are accelerating the digital connections between existing energy assets – such as pipelines and gas turbines – with cutting-edge digital sensors and IT systems to improve safety, performance and reduce emissions. Utilities already accustomed to balancing electric grids in real time are rapidly connecting smart devices and distributed power sources with sophisticated software systems for variable time-of-use pricing and to increase clean energy penetration.

These trends are only expected to increase as major oil and gas players announce plans to shift away from fossil fuels and towards digital energy platforms, and the titan combustion-engine carmakers plan for all-electric futures.

Exploiting Connected Infrastructure

As the energy and critical infrastructure sec-tors increasingly depend on the seamless connection between physical and digital assets, malicious actors are taking advantage of the inherent vulnerabilities in a digitally driven energy ecosystem.

In 2021 – in the United States alone – malicious actors have targeted a major oil and gas pipeline, a wastewater treatment facility, and food, manufacturing and critical infrastructure supply chains.[2] Whether ransomware, supply-chain attacks, denial-of-service or zero-day threats, these attacks are accelerating for a range of reasons – from collateral in broader geopolitical conflict between nations to financial gain.

While motivations differ, criminal gangs and state-supported cyber units understand that vulnerable IoT assets give them the power to not only paralyze entire economies, but also sow chaos for families and businesses across the world.

2 https://cybermagazine.com/top10/10-high-profile-cyber-attacks-2021

A Glimpse Into the Future: The Threat to Critical Infrastructure

How a Cyberattack on an Oil and Gas Pipeline Exposed the World's Vulnerability

In mid-May, millions living up and down the American East Coast experienced the chaos caused by a far-reaching cyberattack targeting critical infrastructure.

A ransomware attack hit a major pipeline company. Unsure if OT or IT systems were compromised, the company feared that malicious actors could gain further access to critical OT control systems. The infrastructure carrying gasoline and jet fuel to nearly a third of the U.S. population was at stake. Rather than operate with uncertainty, the company shut down all operations, stopping all flow of fuel through the pipeline.[3]

As industry leaders and government officials responded to the unfolding crisis, it only took a few hours for panic to set in – gas lines formed, emergency and critical care services further stretched in the midst of a global pandemic, and the economic security threatened millions of businesses and families. The price of gasoline skyrocketed, and filling stations soon ran out of supply. In response, the federal government declared a state of emergency. State governments put in place policies to increase oil and gas supplies by tanker trucks and dissuaded citizens from panic buying fuel.

The pipeline remained shut down for six days while teams of investigators diagnosed the problem and negotiated a ransom. In Congressional testimony, the pipeline company's executives revealed that the cause of the attack was a lack of cyber hygiene – an employee failed to enact two-factor authentication to help protect the company's software.[4]

The ransomware attack successfully breached the organization's IT network, but luckily never infiltrated OT systems or physical energy infrastructure.[5] However, the incident forced the company to shut down all operations on the suspicion that malicious actors had access to sensitive OT infrastructure. The lack of visibility and context into the attack inflicted financial losses in the millions due to the ransomware payment, more than seven days of system-wide downtime and significant reputational damage.

3 https://www.gao.gov/blog/colonial-pipeline-cyberattack-highlights-need-better-federal-and-private-sector-preparedness-infographic

4 https://www.hsgac.senate.gov/hearings/threats-to-critical-infrastructure-examining-the-colonial-pipeline-cyber-attack

5 https://us-cert.cisa.gov/ncas/alerts/aa21-131a



The Complexities of Defending an IoT Environment

Securing A New Nonlinear Frontier

Before the rise of industrial IoT business models, cybersecurity teams mostly knew and understood the threat landscape they were responsible for defending, and built the right capabilities for that task. But the promise of industrial IoT calls for an environment where every piece of equipment and software can connect with any other equipment – and can trust that connection.

Facilities that used to have centralized controls now use remote access for routine workflows. Physical equipment that was previously air-gapped is now networked. Apps and networked endpoints in the hands of consumers and users must connect to company assets to fulfill their intended functions.

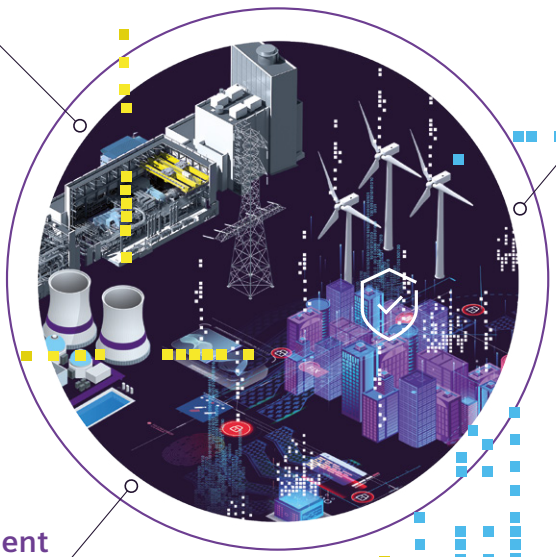
Industrial IoT operating environments now rely on hyperconnectivity, an intermeshed network of connected legacy and digitally native assets, and extreme flexibility to allow network access to non-stationary and intermittent IT and OT technologies owned by a company, used by its customers and integrated with third parties.

These same defining features of powerful IoT business models often leave organizations vulnerable to cyberattacks, and CISOs without the capabilities needed to defend a typical industrial IoT portfolio. As the threat landscape changes dramatically, CISOs need to balance closing the gaps between current capabilities, growing responsibilities to support innovative business models, and countering evolving threats.

A hyperconnected operating environment

Industrial IoT fundamentally changes the need for humans to manage connections between physical and digital assets as connected devices will automatically exchange information to optimize workflows. Market forecasters project 25 billion industrial IoT devices by 2030.[6]

6 www.statista.com/statistics/1183457/iot-connected-devices-worldwide



Mobile and variable assets

Like the move from landlines to cell phones, the IoT future means the devices connected to an industrial network will change from day to day – or even minute by minute. The business benefits of industrial IoT depend on supporting and defending this flexibility.

A mix of legacy and new equipment

Older systems retrofitted for IoT and integrated with newer, digitally native technologies will remain as infrastructure backbones. Both old and new equipment need cutting-edge defenses against evolving threats.



The IoT Monitoring and Detection Imbalance

The foundation of IoT cybersecurity is understanding the two-way relationship between the digital and physical worlds, and then monitoring those relationships to detect and act on threats. For most CISOs using existing SOC capabilities, gaining insight into all physical devices and digital networks that comprise an IoT operating environment is an overwhelmingly complex technical and capability challenge.

Poor Visibility and Unseen Threats Mask Physical and Digital Assets

To monitor and detect threats in time to prevent an attack requires two key elements – visibility and context. Security teams need visibility into every physical and digital node connected to their network.

Then they need to combine billions of data points into a unified threat stream so analysts in a SOC can understand from context whether anomalous behavior poses a threat or is a benign change in production workflow.

Lacking a Unified Threat Stream

Creating a unified threat stream is a significant technical challenge for most IoT SOCs because raw OT and IT data speak separate languages that were never intended to be analyzed together. Yet without unifying these data streams, defenders can't contextualize anomalies between commands sent to OT controlling physical assets and IT software linked to this data – and subsequently will miss attackers who are actively exploring the network in search of vulnerabilities.

Until now, creating a unified threat steam in a hyperconnected environment has not been possible in most SOCs because OT-specific monitoring and detection technologies were too immature and required specialized technical expertise in physical assets. Even as emerging AI-based solutions helped overcome many of these challenges, few have the capability to sync heterogeneous IT and OT data streams.

The result is that most IoT SOCs can't see a complete picture of what's happening in their systems – and can't defend what they can't see.

Fog Surrounds Defenders without Equal Detection Capabilities

Most organizations seeking to expand monitoring and detection in IoT environments suffer from a capability gap when it comes to IT and OT technology deployment and expertise. While even organizations with a business model firmly grounded in owning and operating physical assets struggle with OT security, the vast majority of CISOs struggle to apply IT cybersecurity methodologies to physical equipment in IoT environments.

Imbalanced Maturity

CISOs without a foundation in securing physical assets from cyberattacks often find themselves in one of several technological or capability gaps.

In the least mature organizations, CISOs are asked to expand security for IoT environments without deploying any new OT-specific monitoring capabilities; while others use IT monitoring approaches in the field as a solution to satisfy regulatory requirements or believe that more specialized approaches are too costly or are unnecessary for complete defense.

In more sophisticated organizations, CISOs will monitor IT and OT assets side by side in a SOC built for IT security, and manually analyze data streams. Finally, the most mature organizations have custom monitoring approaches where they analyze physical and digital relationships in a massive data pool, but lack the rigorous methods to effectively apply insights.

While gaps between IT and OT monitoring and detection capabilities leave operating environments exposed to cyberattacks, the true capacity gap most CISOs lack is an ability to equally understand – and act on – threats in both the physical and digital worlds under a unified platform.

Defense Gap Leaves Assets in the Dark

Lacking Equal Expertise in Defending the Physical and Digital Worlds Frequently Leaves IT Networks Protected and OT Assets Exposed

Most organizations seeking to expand monitoring and detection in IoT environments suffer from a capability gap when it comes to IT and OT technology deployment and expertise.



Building a Fusion SOC to Illuminate Industrial IoT

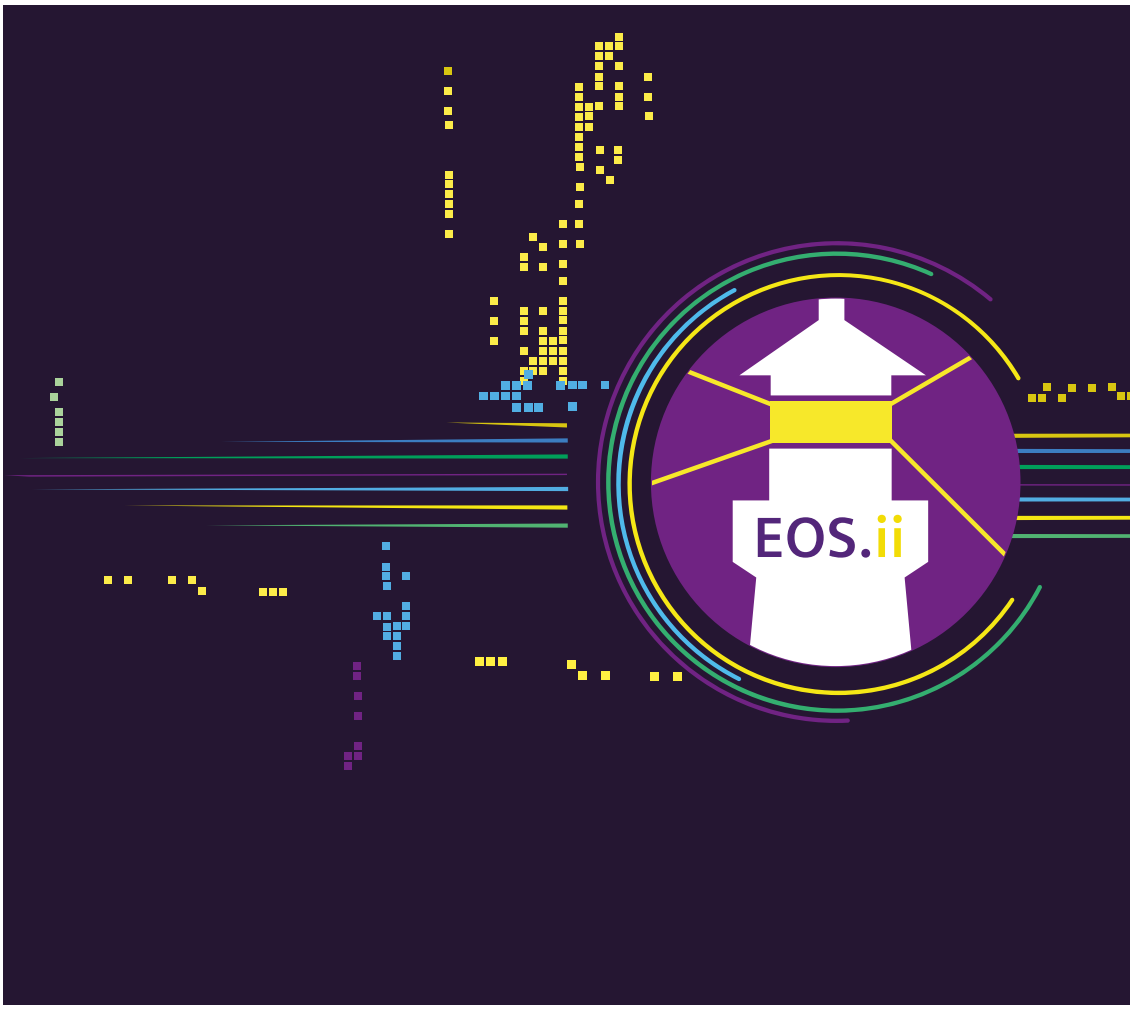
To overcome the obstacles of building robust IoT monitoring, CISOs need to understand if any singular command – out of billions occurring between a given physical and digital asset – represents a cyberattack.

This type of real-time protection requires solving several interlocking challenges simultaneously, including synthesizing heterogeneous data flows into a unified threat stream, equal expertise in IT and OT systems to rapidly draw insight, and acting on threat intelligence in the SOC and in the field.

Analyzing Threats Under a Single Pane of Glass

For CISOs, building a single-pane-of-glass system to monitor and detect threats across their enterprise will require reimagining their existing SOCs.

A CISO can expect the assets and environments under their defensive umbrellas to change frequently as the digital revolution speeds along its exponential growth curve. Threats aiming to exploit this progress will



undergo similar rapid changes to adeptly maneuver around more sophisticated defenses. Rather than trying to adopt the latest cyber solution each time threats evolve, defenders need a platform that can serve as an enduring foundation for IoT security.

Any approach to IoT cybersecurity must integrate IT and OT monitoring and detection within a fusion SOC. That means bringing together otherwise incompatible data sources, empowering analysts to defend each layer of their organization's technology stack within a constantly evolving threat detection engine capable of accomplishing these tasks with speed and accuracy amid constant change.

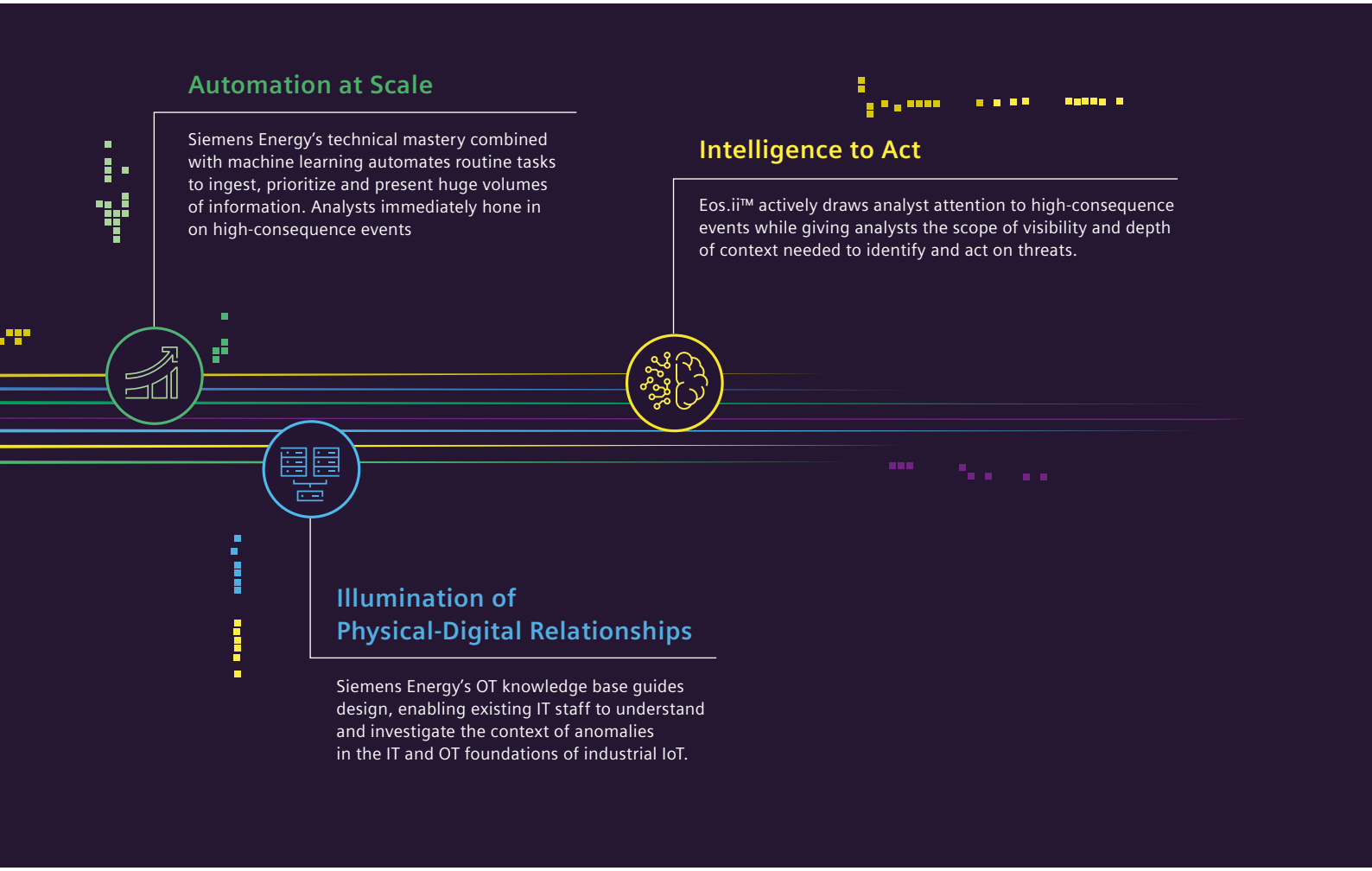
Fusion SOCs will bring together IT and OT cyber capabilities to provide human analysts with efficient and powerful tools to investigate and act on threats in ways that minimize disruption to operations and adapt to evolving threat environments.

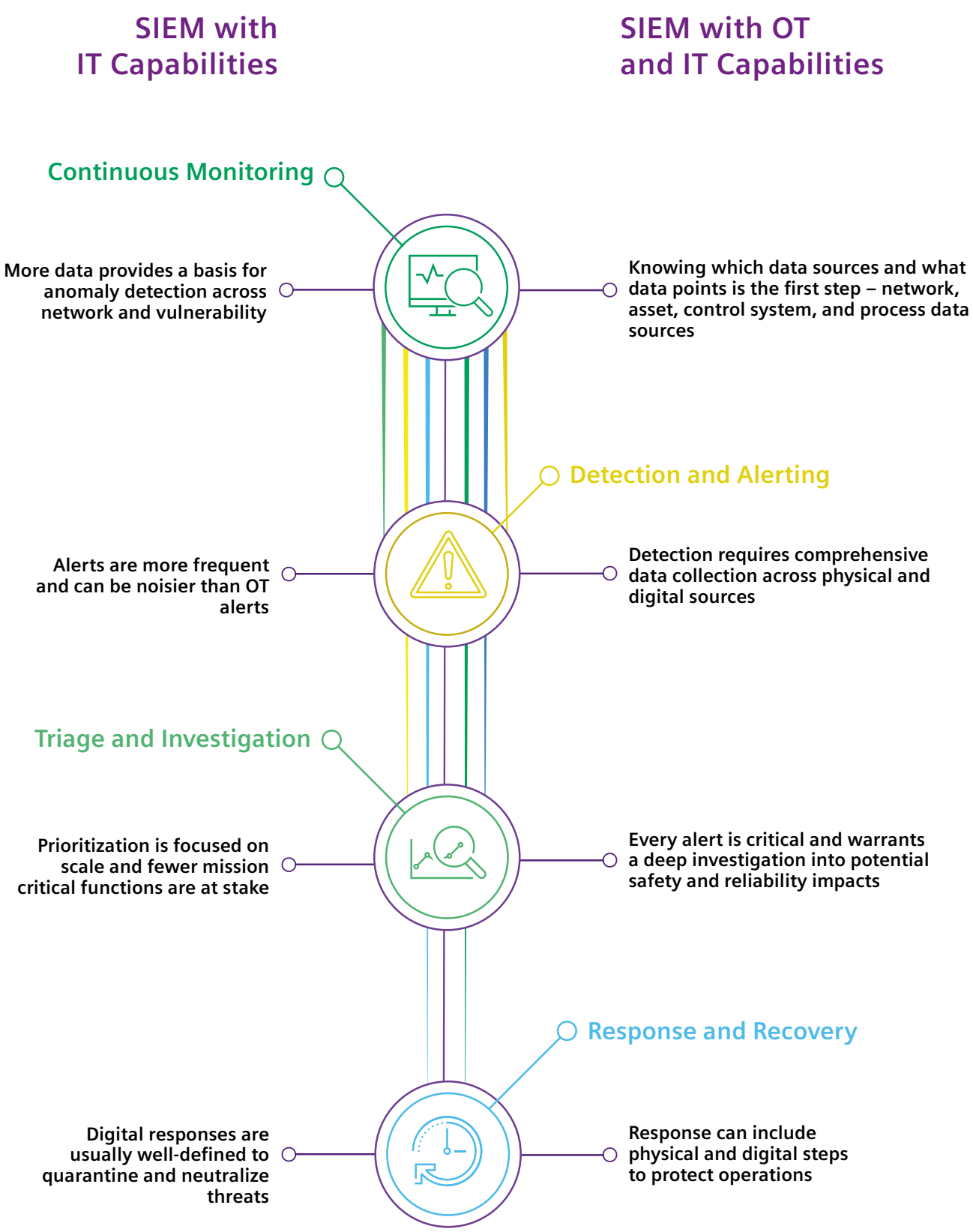
The Intelligent SIEM to Illuminate IoT Cyberattacks

Siemens Energy's Eos.ii™ industrial cyber-defense platform enables CISOs to bridge this physical – digital divide, and illuminate the IoT operating environment so defenders can act on threats before they execute.

Eos.ii™ is a scalable AI-driven Security Information and Event Management (SIEM) platform that serves as the foundation for a Fusion SOC, providing defenders with complete monitoring and detection capabilities through a single-pane-of-glass interface that provides clear and in-depth insights to take action against cyberattacks.

This gives CISOs and cyber analysts working in a fusion SOC the power needed to investigate suspicious events, and permanently bolster defenses for their unique IoT operating environments.




SIEM with IT Capabilities
SIEM with OT and IT Capabilities
Continuous Monitoring
More data provides a basis for anomaly detection across network and vulnerability
Knowing which data sources and what data points is the first step – network, asset, control system, and process data sources
Detection and Alerting
Alerts are more frequent and can be noisier than OT alerts
Detection requires comprehensive data collection across physical and digital sources
Triage and Investigation
Prioritization is focused on scale and fewer mission critical functions are at stake
Every alert is critical and warrants a deep investigation into potential safety and reliability impacts
Response and Recovery
Digital responses are usually well-defined to quarantine and neutralize threats
Response can include physical and digital steps to protect operations

Illuminating the Foundation for IoT Visibility and Context

Creating Visibility in a Hybrid Environment

The immediate need in most SOCs is to close the gap in OT capabilities, and then bring together OT and IT visibility and context within a fusion SOC to identify and evaluate anomalies. Unlike operating environments that rely on either IT or OT expertise, a fusion SOC must communicate in terms accessible to the people who need to take action on both the physical and digital realms.

Eos.ii™ provides the needed foundation for an IoT SOC, starting by mastering the daunting technical feat of creating a unified threat stream. A unified threat stream illuminates OT and IT data sources, giving analysts visibility into the full chain of cause and effect when IoT assets interact. While gathering and processing data for IT and OT goes through similar stages, the mechanics of these workflows differ and require analysis through separate algorithms before defenders can fully understand the collated data.

Using a proprietary method called Process Security Analytics (PSA), Siemens Energy systematically standardizes, collates, and analyzes OT and IT data to reveal anomalous behaviors and patterns that match known cyberattacks.

PSA methodology allows defenders to use context to differentiate between normal fluctuations and active threats, even when signals cut across hybrid environments. Workflows can draw on unified and expanded IoT visibility to prioritize high-consequence events for human investigation.

Each action attackers take to probe the IoT network offers signals about what that attacker intends. In a fully successful IoT SOC personnel can recognize these signals, correctly predict how the attack will unfold, assess its potential impacts and – if needed – take action fast enough to block those impacts.

Intelligence to Act with a Unified Threat Stream

Eos.ii™ gives analysts the scope of visibility and depth of context needed to identify and act on threats





Seeing Through the Fog with Monitoring and Detection

Moving from Visibility and Context to Monitoring and Detection

Monitoring and detecting threats requires understanding current conditions, and then comparing them against past threats and normal baselines to illuminate what's suspicious.

Comparing historical and current asset conditions requires a built-for-purpose platform that uses AI, ML and predictive analytics to identify anomalies within seconds of detection. Eos.ii™ illuminates both the depth and breadth of an install base, bringing together automation with the incisiveness of human intelligence to hunt for any trace of malware.

The Power of the Eos.ii™ Detection Engine

With AI at its core, Eos.ii™ is designed to make sense of billions of data points that comprise physical and digital relationships in industrial environments, correlating abnormalities that would be otherwise imperceptible to cyber analysts.

In one real-world example, a SOC analyst using Eos.ii™ detected a problem with firewall hardware at a power plant. The hardware was rated for 55 degrees Celsius, but running above 70 degrees. This made the power plant's control system vulnerable to crashes when the firewall overheated. If this system failed during power production, the company would not be eligible for payment – a potential loss of millions of dollars per hour. Eos.ii™ helped analysts determine this was not an attack, and prompted corrective maintenance that strengthened ongoing cyber readiness.

Built to Adapt to Emerging Threats

When new threats are identified anywhere in the world, the Eos.ii™ detection engine automatically evaluates the vulnerability of an organization's install base and can anticipate anomalous behavior. When these threat signatures – known or novel – are detected, Eos.ii™ can identify asset exposure within an operating environment and generate an alert for human attention.

Eos.ii™ Platform

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

Topology Search

Quickly search for assets, anomalies, vulnerabilities, and other data across fleets

Investigations

Use data search and correlation tools to conduct deep investigations into specific assets

Plant Data Visualizer

Review data visualizations from physical and digital assets in one place for enhanced context



Platform Tuner

Easily build new rules, tune ML models, and enhance capabilities for specific sites and assets

Threat Intelligence

Compare site activity to known signatures and review historic data for new signatures

Alert Management

Automatically detect events and correlate them for analyst review

The Intelligence Behind Eos.ii™

Eos.ii™ brings together key capabilities in an integrated platform. Automation detects events, prioritizes potential threats and alerts analysts to investigate the most consequential anomalies.

Combined, these modules make it easy for analysts to perform quick, deep analyses, relate their findings to the big picture, and adjust defenses to perform the same analysis automatically going forward. Each advances the state of the art for industrial IoT monitoring and detection – and like IoT, the combination is even more powerful than any single feature.

Eos.ii™ enables analysts in a IoT fusion SOC to move seamlessly from discovering a new threat to confirming its absence in protected networks to updating automated defenses. Its powerful detection engine and easy adaptability offer unprecedented ability to stay on top of changing circumstances – from new assets to new threats.

Automation on Scale

Manage alert prioritization to improve alert response time and avoid alert fatigue.
Tailoring new rules – including machine learning rules – continuously strengthens defenses.

Intelligence to Act

Automate proactive decision making with intelligence, domain specific playbooks and threat hunting workflows. Context driven intelligence means active threat hunting becomes a larger share of analyst time.

Illumination of Physical-Digital Relationships

Quickly search and understand the relationships between devices – their location in the plant, and how they link up physically and digitally. Search by time and attribute lets analysts immediately scrutinize relevant devices when new threats are discovered.

The Detection Engine for Industrial IoT

Although most alerts don't require cybersecurity responses, defenders need to quickly home in on those that do. SOC analysts can rely on Eos.ii™ to automatically sift through volumes of security events and alerts that occur in industrial IoT systems, using its library of asset attributes, topology, and known threat profiles to assess which events will be high consequence. This means Eos.ii™ can distinguish between similar alerts – giving low priority to a single wind turbine wearing out its bearings, but high priority to a wind farm inadvertently infested with malware during a site visit.

AI Insights and Tuning

The core of Eos.ii™ is a rules-based detection engine drawn from OT knowledge and sophisticated machine learning. Pre-built rules leverage generations of Siemens Energy engineering knowledge to alert SOC personnel of suspicious or dangerous OT conditions. Meanwhile, Eos.ii's machine learning detection engine teaches itself the normal pattern of relationships between variables based on real-world operating data, automatically tailoring anomaly detection to the specific sites and assets under protection.

In the event that a company is hit with a completely novel attack that does not match known IT signatures, Eos.ii's automatic detection engine would alert human investigators as soon as the attack begins to affect OT assets – and would aid analysts in diagnosing the events.

The combination of powerful investigative tools, prioritized alerts, and automated, scalable tuning reduces the number of SOC staff needed and exposure to alert fatigue, while enhancing the expertise and capabilities of analysts on the detection team.

Threat-Hunting – Getting Ahead of Attackers

Defenders equipped with a detailed and constantly updating understanding of their systems get to shift from a reactive stance to a predictive, prescriptive stance. Instead of waiting for an attack where the impacts are unmistakable, defenders can hunt for subtle signs of intrusions underway. Defenders can use Eos.ii™ to identify the intent of a probing attacker earlier in their attack process, when a SOC has more options to limit the extent of intrusions and strengthen preventive measures.

Eos.ii™ Makes Threat-hunting Faster and More Powerful

Instead of needing to log into several systems or call OT workers to check on conditions, analysts can examine all the attributes and status of assets within a single pane of glass. Visualizations and easy navigation allow analysts to rapidly toggle between deep-dive investigations and their big-picture implications.

With Eos.ii, the previously difficult process of correlating security, process, and control system data becomes easy. Along with IT forensics and signature-based detection, Eos.ii™ enables a digital twin comparison – comparing a virtual model of the worksite against real-world data.


eventA
Then
result.add
eventA

Insights into Action with Precision Defense™

Stopping Threats Before They Execute

The value of an AI-powered detection engine is its ability to provide actionable intelligence in time for defenders to get ahead of attackers. This means analysts get to act on threats they have discovered, interrupt attacks underway and adapt defenses in real time.



Realizing the Vision of a Fusion SOC

Acting on Intelligence

The pipeline ransomware attack described earlier forced a tough choice on the company moving nearly half of fuel needed to power the eastern United States. Unsure whether the attack had spread from its IT networks to affect pipeline infrastructure and controls, the company chose to halt fuel deliveries, leading to gas-pump shortages.

This attack illustrates the need for Precision Defense™ capabilities. Monitoring and detection that can determine the extent of a breach can guide narrowly targeted responses. Without such capabilities, companies are left blind. Leaders end up being forced to choose between doing nothing – leaving worker safety and critical equipment exposed to ongoing malicious actions – or deploying brute-force solutions like a sweeping shutdown.

The value of an AI-powered detection engine is its ability to provide actionable intelligence in time for defenders to get ahead of attackers. This means analysts get to act on threats they have discovered, interrupt attacks underway and adapt defenses in real time. With each threat mitigated, the fusion SOC becomes better prepared to block attacks.

Precision Defense™ for Right-Sized Interventions

The unparalleled ability to investigate IoT with visibility into both OT and IT subsystems enables greater precision for threat detection – and the insights needed for proportionate action.

Determining the source and scope of a problem is a key step in selecting a corrective response in IoT systems. Unlike IT systems, which readily withstand abrupt shutdowns, pulling the plug on physical assets is typically a costly measure reserved for last resort. A precision defense approach seeks to address exactly the affected systems – no more and no less. If an intrusion reached only one pumping station, or only breached a sales database, there's no need to shut down an entire pipeline.

Rapid Responses and Perpetual Improvements

In these investigations, speed and quality both matter. Rapid, early detection can limit intrusions to a few isolated systems. Thorough, high-quality monitoring gives leaders the confidence that small, precise interventions will strike the right balance between eradicating threats and minimizing operational disruption.

Eos.ii™ empowers analysts to rapidly detect and understand an attack anywhere in the IoT portfolio, mapping its scope and tracing the timing and attack vector – the information needed for high-confidence precision defense.

Eos.ii™ immediate adaptability – to novel attacks, to threats observed elsewhere, and to site-specific equipment – means that SOC personnel can take prescriptive, preventive action to block future attacks and scour systems looking for intrusions previously overlooked.

Full visibility and forward modeling of digital-physical interactions turn IoT complexity into a home-field advantage for defenders. When SOC personnel analyze the real-time status and logged histories of any aspect of the digital or physical assets under their protection, attackers have nowhere to hide.

A SOC Greater than the Sum of its Parts

Eos.ii™ transforms the interlocking challenges of industrial IoT cybersecurity into core strengths. It tames the tangle of mismatched languages, provides visibility into obscure corners of OT, and illuminates the meaning of OT data for IT analysts.

Automating routine tasks and prioritizing alerts based on expected consequences leverages human analyst time. Eos.ii™ adapts readily to new asset bases and ever-evolving threats. With Eos.ii™, CISOs can build a fusion SOC, overcome the challenges of today, and create the stable foundation needed for IoT industrial cybersecurity in the future.

Done well, robust industrial IoT cybersecurity builds trust with other parts of the organization. Instead of constantly bothering OT personnel for assistance, the SOC adds value by accurately flagging maintenance concerns.

The SOC gains credibility and the reputation for accuracy needed to call for – and get – sudden shutdowns when a true crisis occurs. With a mature IoT SOC, CISOs can better quantify the magnitude of threats and vulnerabilities the SOC discovers, can better demonstrate the value their teams add to the business, and can better keep up with the changes needed to secure the modern energy sector.

Eos.ii™ provides CISOs with the foundation needed to begin building a predictive SOC, and to strive for continuous improvement. As Eos.ii™ learns the baselines for work sites, and as IT staff become proficient in understanding IoT interactions and diagnosing attacker intent, defenders will be increasingly able to predict the behavior of assets and attackers alike.

Companies that deploy Eos.ii™ will enjoy reduced cyber risk, at a lower cost than hiring expertise or developing solutions in-house, and with support to keep Eos.ii™ current. Forward planning can proceed with better cost-benefit assessments, and crisis response can more precisely tailor eradication and recovery efforts when breaches occur.

For the energy sector, securing the IoT is an essential step in ensuring that innovation can continue without sacrificing reliability. Siemens Energy's Eos.ii™ will help organizations of all sizes address their IoT security needs – strengthening the overall energy sector by hardening more links in the value chain.

Industrial IoT is clearly part of the energy sector's future. At Siemens Energy, we're committed to giving CISOs and SOCs the tools they need to make IoT a source of strength, not a hidden liability.







Published by

Siemens Energy Inc.

15375 Memorial Drive
Houston, TX 77079
United States

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 trademark licensed by Siemens AG.