

The Foundation for Securing Industrial IOT in an Era of Persistent Cyberattacks

Siemens Energy's New AI-based Monitoring and Detection Platform, Eos.ii Provides Intelligent Illumination for IoT Cyber Defense

The digital revolution is the key to unlocking a more innovative, sustainable, connected global economy. This future hinges on transforming the decades-old analogue machines that run the world's energy and industrial sectors into a hyperconnected network of physical and digital assets — an industrial Internet of Things (IoT).

For energy and infrastructure companies, industrial IoT opens new horizons. Innovative business models digitally connect physical assets with operational technology (OT) and information technology (IT) to improve efficiency, enhance safety, and optimize operations by leveraging innovative software applications, big data analytics, advanced sensors, and artificial intelligence (AI). But harnessing the power of industrial IoT is about more than any one company's success — it holds the promise to drive the innovative businesses and professions of tomorrow for communities around the globe.

Above all, IoT is accelerating the energy transition, enabling an all-electric future, and catalyzing new industries only possible with connected infrastructure. Yet a future run on industrial IoT has a glaring Achilles' heel: cybersecurity. Today, defenders lack the capability to secure the energy sector and critical infrastructure from cyberattacks. And criminal enterprises and rival nation-states have already shown that they can hijack or destroy critical infrastructure at the touch of a button. So, if we're going to deliver a more sustainable, accessible, and low-carbon future, we must reimagine how to secure it.

The IoT Monitoring and Detection Imbalance

When it comes to cybersecurity, defenders are overwhelmed by the complexity and relentless change inseparable from the benefits of IoT. As companies digitize both novel and legacy technologies to operate everything in the industrial world — from renewables and electric vehicles to retrofitted smart grids, pipelines, and water treatment facilities — they also make themselves more vulnerable to cyberattacks. Every link between a physical and digital asset enhances a future attacker's ability to hold hostage the energy and critical infrastructure systems of tomorrow. Right now, defenders are behind the curve.

Securing industrial IoT eludes even highly skilled defenders for one simple reason: most companies lack the capabilities to *equally* monitor, detect and act on potential cyberthreats across an operating environment of physical and digital assets. Defenders primarily engineered their Security Operations Centers (SOCs) around the then-contemporary challenge of identifying and preventing cyberattacks on IT systems. These existing capabilities don't match the complex threats now facing IoT networks.

Chief Information Security Officers (CISOs) and their teams of analysts must adjust to meet these threats — not of tomorrow, but of today. Companies relying on industrial IoT business models need defenders with both sophisticated IT and OT technical expertise, and SOC capabilities to secure physical assets from cyberthreats. Not only are these capabilities hard to come by, but no solution exists to level up physical cybersecurity and merge it with well-practiced digital protocols. Without a unified understanding of the industrial IoT threat landscape, defenders will continually lack the visibility to see the operating status of every connected device, let alone analyze the tremendous volume of data produced every minute to spot a potential threat.

Eos.ii – The Foundation for a Fusion SOC to Illuminate Industrial IoT

That’s why Siemens Energy has built Eos.ii — the first AI-based monitoring and detection platform to serve as the foundation of an IOT fusion SOC for energy and critical infrastructure in an era of persistent cyberattacks.

Eos.ii is an intelligent software platform that provides CISOs with an evergreen foundation for industrial IoT cybersecurity. By design, Eos.ii readily adapts to future threats and empowers analysts with actionable insights that bridge the digital and physical divide within a unified SOC. The AI-based monitoring and detection platform automatically unifies and standardizes IoT data flows, so analysts have visibility into every part of an IoT network — and can analyze anomalous behavior that might represent a cyberthreat — in a single pane of glass.

Eos.ii uses machine learning to automatically tailor defenses and prioritize high-consequence events. As new threats emerge, Eos.ii seamlessly integrates their known characteristics into automated defenses, and allows for easy manual updates to its rules-based detection engine. With Eos.ii, defenders spend less time on routine tasks and more time conducting powerful investigations. This marks a powerful shift — instead of reacting to attacks already underway, defenders can disrupt attacks in early stages. Companies can implement precision defenses when confronted with breaches. Instead of all-or-nothing shutdowns, with precision defense, companies under attack can purge exactly the affected systems — no more and no less.

Eos.ii empowers defenders with the insights they need to act quickly and precisely. It’s how we secure the energy revolution against an era of rising threats.

To learn more about how Eos.ii lays the foundation for a secure industrial IoT future, check out our new white paper: [EOS.ii](#)

