THE INSIGHTCYBER SOLUTION: PROTECTING CYBER-PHYSICAL ENVIRONMENTS WITH A RADICALLY SIMPLE APPROACH

Our AI-powered service can pre-empt devastating cyber-attacks. And that's just the start.

Bridging the OT/IT cyber-security divide

As every enterprise security expert knows, the world of Operational Technology (OT, including IoT and IIoT devices) is quickly converging with the world of Information Technology (IT, including networks, computers, databases, and more). This convergence presents the enormous challenge of protecting OT against cyber-attacks, which is made uniquely difficult because of the foundational differences between the two worlds.

In OT environments that include things like critical infrastructure, manufacturing, and other industrial systems, the primary concern of Operations managers is to ensure *availability*, which has a direct tie to revenue. Plant managers and automation engineers, to guarantee safe and secure operations, are hyper-aware of risks and irregularities that threaten to cause disruptions. Until relatively recently, this mindset did not include cyber-security.

By contrast, the primary concern of IT Operations and IT Security managers is to ensure *confidentiality* and data integrity. Cyber-security has long been a priority in IT, and here the approach is primarily based on understanding and addressing vulnerabilities—e.g., creating logs of known malware and past attacks, monitoring activities, installing patches, controlling access, and so on.

In the past, OT environments were often physically segregated, and operations were either based on non-standard proprietary technology or were not computerized at all. As OT converges with IT, OT environments have shifted to utilizing standard IT systems and Internet Protocol (IP) networking, and are connected to enterprise networks. This shift has not been accompanied by a corresponding focus on cyber-security, which makes OT an easy target for attackers.

Logic might dictate that IT security practices could simply be extended to protect OT. Practice has proven otherwise. The vulnerability-focused approach used in IT is unworkable, since OT devices are generally not patchable and cannot accommodate software agents. More significantly, the telemetry and data generated by OT is fundamentally different from that found in IT systems, and thus cannot be readily processed by existing tools.

InsightCyber bridges the OT/IT gap with a groundbreaking new approach that protects OT by recognizing attacks in their very earliest stages, rather than focusing on vulnerabilities. The service is unobtrusive and cost-effective, and it dovetails seamlessly with existing enterprise security tools and processes.

Continuous monitoring + advanced AI

InsightCyber's AI-powered service works by continuously monitoring an organization's complete OT activity and watching for signs that an attack is either underway or imminent.

The service tracks the functionality, connectivity, and network activity of every single connected asset in near real time and compares observed activity with desired normal behavior. When it detects even the smallest operational anomaly, the service processes the deviation and sends an alert when a problem is confirmed.

In addition to 24/7 monitoring, alerting, and reporting, the service also offers incident and breach response, which is critical to the protection of operations, revenue, and regulatory compliance. In these cases, customers can receive custom alerts based on risk criticality and regulatory controls, with AI-generated playbooks for fast response and remediation.

An original approach to AI for OT

The power of the InsightCyber service comes from an innovative application of AI, built from the ground up with new algorithms designed specifically to work in the OT context. Our approach comprises Neural Networks and Deep Learning, and includes game theory, video game technology, semantic engines, and real-time investigation. It employs self-learning AI, which enhances the service's ability to identify, understand, and respond to new problems as it works with new data.

The InsightCyber team spent three years honing and fine-tuning this new breed of AI, refining the models by working with a vast amount of real-world data generated through development partners. So even though the offering is a new one, it is remarkably well-educated.

SIEM capabilities in an OT context

Within hours of initiating the InsightCyber service, customers are given a view of their operational environments that typically reveals a surprising number of "unknown/rogue" assets, which are undetected or misidentified. In fact, the ability to generate and maintain an up to date, comprehensive inventory of assets is one of the primary benefits of the service.

The greater value is derived from the powerful analytics engine that underlies the service. With a fine-grained understanding of operational data (from our Collector devices as well as OT data streams from other sources), InsightCyber can deliver significant benefits beyond effective cyber-protection in areas such as compliance, risk modeling, and cost management.

Significantly, the InsightCyber service is designed to operate natively within the OT infrastructure, which means it can deliver SIEM-like processing capabilities for pre-analysis of OT security platform data. Combined with powerful new behavioral analytics, the service holds the promise of correlating and

interpreting a broad range of operational data from myriad sources, ultimately becoming a significant source of business intelligence, and enabling faster and better decision-making.

About InsightCyber

InsightCyber is on a mission to keep the world's critical infrastructure, supply chains, and manufacturing operations cyber-safe, preventing attacks that can have catastrophic human and economic impact. The company's AI-powered security service continuously monitors an industrial enterprise's environment, providing insight and protection against a wide range of cyberthreats. To learn more, please visit https://insightcyber.com.

