INSIGHTCYBER™

THE INSIGHTCYBER PLATFORM:

A New Approach to Protecting Cyber-Physical Environments

An AI-driven solution for real-time proactive protection & risk management for OT/IoT environments

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.

In OT environments, which include things like critical infrastructure, manufacturing, and other industrial systems, the primary concern of Operations managers is ensuring availability as it has a direct tie to revenue. Plant managers and automation engineers are hyper-aware of risks and irregularities that threaten to cause disruptions to safe and secure operations. Until relatively recently, these mindsets did not include cybersecurity.

In contrast, the primary concern of IT Operations and IT Security managers is ensuring confidentiality and data integrity. Cybersecurity 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.

Historically, OT environments were often physically segregated, and operations were either based on non-standard proprietary technology or were not computerized at all. As Operational Technology converges with Informtaion Technology, 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 cybersecurity, making 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's AI-driven platform continuously monitors your organization's entire infrastructure, recognizing and alerting you to the tiny signs that indicate an attack is imminent. It is unobtrusive and cost-effective, and it dovetails seamlessly with existing enterprise security tools and processes.

24/7 monitoring, alerts and reporting

InsightCyber's AI-driven platform works by continuously monitoring OT, IoT & IT environments, instantly spotting the tiny anomalies that signal trouble and delivers solutions on fast remediation, prioritizing risk, and preventing devastating outcomes.

The InsightCyber Platform 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 platform processes the deviation and sends an alert when a problem is confirmed.

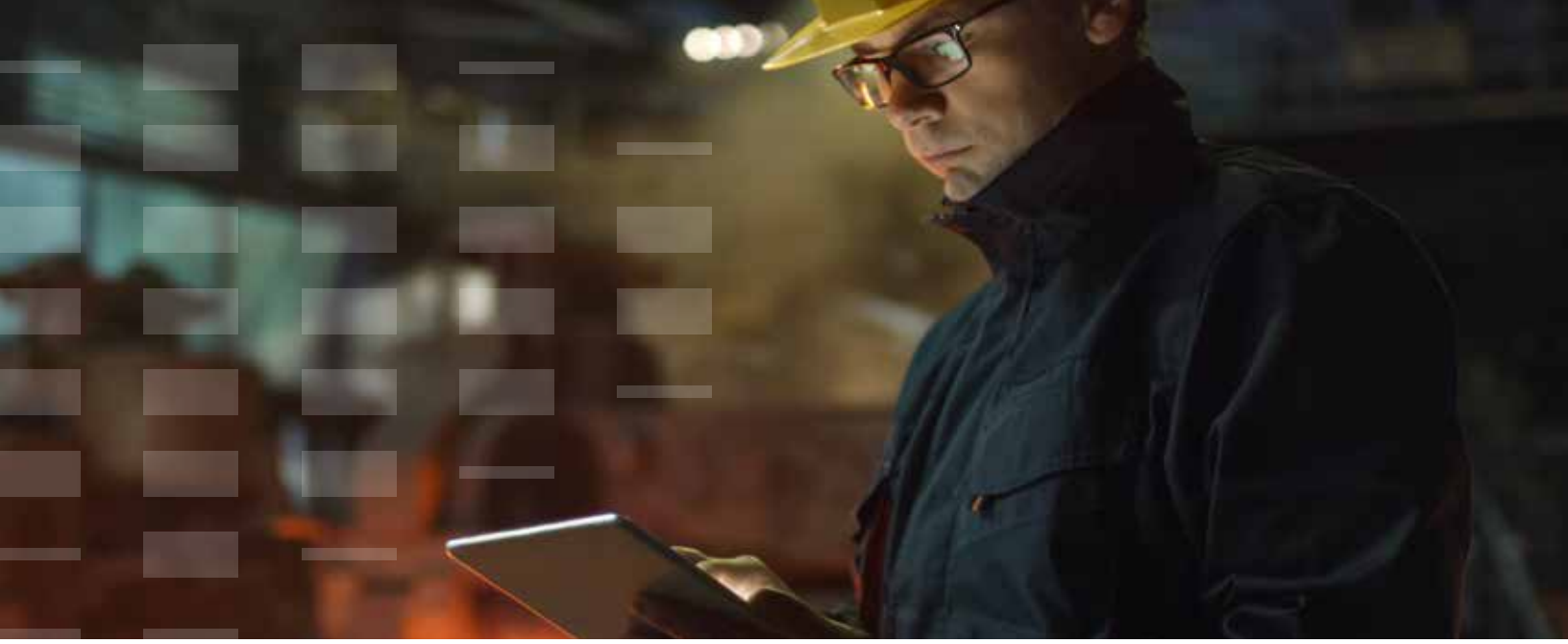
In addition to 24/7 monitoring, alerting, and reporting, the platform offers incident and breach response, which is critical to the protection of operations, revenue, and regulatory compliance. In these cases, customers receive AI-generated playbooks with custom remediation recommendations based on risk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

> InsightCyber's AI-driven platform **continuously monitors** an organization's **complete OT activity**...

An original approach to AI for OT

The power of the InsightCyber Platform comes from an innovative application of Artificial Intelligence, built from the ground up with new algorithms designed specifically to work in the OT context.

InsightCyber's approach to AI 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 platform's ability to identify, understand, and respond to new problems as it works with real-time data from diverse sources, including asset monitors, threat intel and behavioral analyzers. InsightCyber refined the models by working with a vast amount of real-world data generated through development partners, honing and fine-tuning this new breed of AI.



SIEM capabilities in an OT context

Within hours of initiating the InsightCyber Platform, customers have a view of their operational environments, that typically reveals a surprising number of “unknown/rogue” assets which had been undetected or misidentified. The ability to generate and maintain an up-to-date, comprehensive inventory of assets is one of the primary benefits of the platform.

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

The InsightCyber Platform 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 platform holds the promise of correlating and interpreting a broad range of operational data from myriad sources – ultimately becoming a significant source of business intelligence to enable faster and better decision-making.

About InsightCyber

InsightCyber is on a mission to protect critical infrastructure and enhance fiscal outcomes, by using artificial intelligence to identify insights within data, networks & systems, for companies & institutions and empower them to make informed decisions around resilience, risk and revenue. The company’s AI-driven platform continuously monitors an industrial enterprise’s environment, providing insight and protection against a wide range of cyberthreats. To learn more, visit **insightcyber.com**

