Tripwire ExpertOps Industrial Visibility

Managed Services for Industrial Visibility, Threat Detection and Vulnerability Management

Why Managed Services?

"The skills gap doesn't have to be an operational gap. Security teams shouldn't overburden themselves by trying to do everything on their own. They can partner with trusted vendors for managed services or subscribe to service plans where outside experts can act as an extension of the team."

— Tim Erlin, VP of Product Management and Strategy at Tripwire

Industrial automation and process control systems largely run our world. However, cyber risks to industrial networks, endpoints and control systems are on the rise and protecting highly specialized plant environments can be very challenging for industrial businesses and critical infrastructure.

Sometimes finding a powerful set of security solutions to keep your industrial control system (ICS) secure isn't enough on its own. You also need talented cybersecurity professionals who can leverage those tools correctly and have the OT expertise needed to remediate security incidents immediately.

The high demand for recruiting, training and retaining competent cybersecurity personnel with deep OT expertise poses a serious challenge to most organizations. There simply aren't enough experts to fill those roles—and this skills gap leaves organizations vulnerable to attacks because of improper enforcement of OT security best practices.

Addressing the Cybersecurity Skills Gap

In order to manage the shortage of cybersecurity talent on their teams, industrial organizations and agencies often leverage IT security professionals with limited or no OT cybersecurity background into cybersecurity positions that oversee both IT and OT networks.

Operational Challenges

The IT/OT convergence is driving the need for new security capabilities and integrations. The breadth of new OT security tools adds to security teams' already overburdened task of

managing their environment. They often have too many tools to manage and not enough bandwidth to get up to speed in time to meet their compliance needs. When staff transitions, a lack of proficiency with security tools can make for awkward and incomplete hand-offs.

Increased Vulnerability

The skills gap is much more than an HR problem. It pits IT and OT professionals against cyber adversaries using sophisticated and ever-changing plans of attack. Not effectively leveraging the full capabilities of security tools can lead to breaches going undetected for months, costing untold resources in short periods of time.

Tripwire ExpertOps Industrial Visibility

Tripwire® ExpertOps℠ Industrial Visibility is a managed services version of the industry's best industrial visibility solution: Tripwire Industrial Visibility. A single subscription provides personalized consulting from trained experts and hands-on tool management to help you achieve and maintain compliance and critical asset security. It gives stretched security teams an alternative to the difficult process of purchasing, deploying and maintaining products.

Ongoing support: You'll be matched with a designated Tripwire expert who serves as an extension of your team by providing personalized advice, incident assistance and audit support. You'll receive recommendations and organizational grading to maximize the value of Tripwire Industrial Visibility, as well as regular alerts and reports in your inbox.

System transparency: How can your security team prioritize which system changes to address if they don't have deep visibility—let alone a detailed understanding of which changes are relevant? Tripwire ExpertOps Industrial Visibility provides you with detailed and robust security and compliance visibility.

Tripwire ExpertOps Industrial Visibility Features

Extreme visibility for improved security	Discovers asset details across the entire industrial network, profiles all the communications between assets, and generates high-fidelity baselines to detect anomalies, create virtual zones and hunt for threats.
Advanced threat detection	Delivers superior threat intelligence by providing alerts across the full "cyber kill chain"—from early reconnaissance activity to later-stage attacks designed to impact control systems and processes.
Proactive vulnerability monitoring	Enables users to proactively identify issues that can leave networks vulnerable to attack.
Network segmentation—policies and zone management	Groups assets into logical segments based upon their communication patterns, and then generates an ideal virtual segmentation scheme.
Automated foundational cybersecurity controls	Leverages change management, event logging, passive monitoring and active scanning to increase operational efficiency.
Secure cloud capabilities	Aggregates data across customer sites to enable identification of industry-specific threats, tactics and trends.
Attack vector simulation and analysis	Users can highlight a sensitive asset and the system will posit attack vectors that could be executed against it.
Scalable deployment architecture	Supports deployments in environments characterized by a large geographic spread across multiple remote/isolated sites—even in extreme environmental conditions.
Seamless integrations	Leverages your existing investments in technology, process development and training, including network infrastructure, SOC tools and other important IT/OT operational systems.
Modern user interface and dashboards	Helps you quickly visualize the status of the system, including hardware performance, software functionality and data capture sources to address issues and preserve the security of the network in a timely manner.
Designated Tripwire experts	A Tripwire expert acts as an extension of your team by keeping consoles, sensors and all contents (threat definitions, etc.) up to date, prioritizing your work efforts, managing critical escalations, and presenting results to stakeholders.
Custom service plan	Your Tripwire expert will jointly develop a service plan outlining communication practices, escalation practices and any specialized requests.
Expert recommendations	Maximizes automation capabilities for security, including but not limited to baseline evaluation, policy rules, custom alert configurations and system tuning based on reconditions from your Tripwire expert.
CISO and executive review	A quarterly report to your key stakeholders includes deployment health statistics as well as an overview of achievement towards your objectives. The quarterly CISO and Executive review provides insights into ongoing improvement and utility of your Tripwire environment.
Prioritized remediation	Take a practical approach to gap remediation by identifying the areas of greatest impact to organization risk, and opportunities to efficiently improve overall security posture.
Alert/incident response	Your Tripwire expert will conduct initial triage of alerts to identify false positives and the accuracy of alert details, ensuring delivery notifications to your response team.

Licensing

Annual subscription pricing includes a base fee for the service. Tripwire ExpertOps Industrial Visibility offers an advanced subscription service. Tripwire ExpertOps Industrial Visibility Advanced provides day-to-day maintenance of the Tripwire Industrial Visibility console and sensors, ensuring both content and software is up to date. An assigned program coordinator will work with you to develop an operational use plan with best practice recommendations, as well as assistance with alerts configuration, system tuning and prioritization of suggested remediation activities.

Summary

The disparity between security needs and security talent leaves most organizations in a challenging position. Tripwire ExpertOps Industrial Visibility fills the skills gap by equipping your teams with the expert support needed to maximize the full benefits of a best-in-class industrial visibility solution.

Schedule Your Demo Today

Let us take you through a demo of Tripwire ExpertOps Industrial Visibility and answer any of your questions. Learn how Tripwire's suite of security products and services can be customized to your specific industrial security and compliance needs.

Visit **tripwire.com/contact/request-demo**

tripwire®

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. We protect the world's leading organizations against the most damaging cyberattacks, keeping pace with rapidly changing tech complexities to defend against ever-evolving threats for more than 20 years. On-site and in the cloud, our diverse portfolio of solutions find, monitor and mitigate risks to organizations' digital infrastructure—all without disrupting day-to-day operations or productivity. Think of us as the invisible line that keeps systems safe. **Learn more at tripwire.com**

***The State of Security*: News, trends and insights at tripwire.com/blog**
Connect with us on LinkedIn, Twitter and Facebook

CBTXOIV1c 2012