Secureworks
a SOPHOS company

Secureworks Taegis MDR for OT

Secureworks MDR solution on the Taegis XDR platform helps organizations prevent, detect, and respond to threats across IT and OT environments

Defend cyber threats across IT and OT assets with Managed Detection and Response (MDR) through Secureworks® Taegis™ MDR for OT. Protect enterprise and operational technology, bringing threat monitoring, detection, and collaborative response to an organization's entire environment. Employ rapid access to security experts, advanced analytics, and vast insights into the global threat landscape to raise cyber resiliency and lower risk.

Reasons for Organizations to Secure Their Environments

Operational disruption: Companies rely on their IT and OT systems to maintain production schedules and ensure product quality. A cybersecurity attack could disrupt these systems, resulting in costly downtime, production delays, and potential safety risks. For example, unplanned downtime alone costs manufacturers around $9,000 a minute—or $540,000 per hour.

Protection of sensitive data: Organizations store sensitive data such as intellectual property, financial information and customer data in their IT and OT systems. A cybersecurity breach could result in the theft of this information, which could cause irreparable damage to the company's reputation and financial stability.

BENEFITS

Provide threat monitoring, detection, investigation, and collaborative response for organizations with both IT and OT environments

Reduce risk of production downtime, and damage to reputation and profits due to cyberattack

Fill internal cybersecurity talent gaps from the absence of cyber resources and the historic lack of security focus on OT

Compliance: Companies must comply with increasingly stringent regulatory requirements that govern data protection and cybersecurity. Failure to comply with these regulations could result in fines, legal action and damage to the company's reputation.

Supply chain risk: Organizations often work within a network of suppliers and partners who may have access to their IT and OT systems. A cybersecurity breach in one part of the supply chain could affect the entire operation, causing significant financial and reputational damage.

Manufacturing Cybersecurity Challenges

Manufacturing companies depend on their operational technology (OT) to power their operations, generate revenue, and enable their business to compete and innovate. However, the increasing digitization of industrial processes and convergence of information technology (IT) and OT has also made these systems more vulnerable to cybersecurity threats.

Digital transformation has converged several cybersecurity trends. Consider these statistics:

70% Gartner reports that by 2025, 70% of asset-intensive organizations will have converged their security functions across both enterprise and operational environments.[1]

23% Manufacturing is the most targeted industry for cyberattacks according to Gartner, making up 23.2% of all attacks.[2]

65% Deloitte's Manufacturing Industry Outlook reports 65% of firms focusing on manufacturing, oil and gas, utilities and mining see cybersecurity as their highest priority for proper governance.[3]

Overall, securing IT and OT environments is crucial for manufacturing companies to ensure business continuity, protect sensitive data, and maintain regulatory compliance. By implementing robust cybersecurity measures, manufacturers can minimize the risk of cyberattacks and defend against cyber threats for their entire operations.

1 Gartner Market Guide for OT, August 2022
2 Gartner Product Leaders Insight, March 2022
3 Deloitte's 2022 Manufacturing Industry Outlook

Introducing MDR for OT Delivered on Taegis XDR

Secureworks Taegis MDR for OT is a holistic managed detection and response solution based on the powerful combination of the Taegis XDR platform and vast human expertise and intelligence, designed to protect organizations from cyberattacks targeting IT and OT environments.

Taegis is a cloud-native security platform that processes more than 5 trillion events weekly across thousands of customers. The platform features hundreds of integrations—including leading OT tools from Dragos, SCADAfence, Claroty, and Nozomi—that are normalized and analyzed, along with Secureworks own proprietary data and global threat intelligence generated by our Counter Threat Unit™ (CTU) research team.

Taegis is backed by vast security experts available to customers at every turn. Security analysts staff our SOC 24/7, and OT experts help investigate and provide remediation guidance for threats targeting operational assets. CTU™ findings, plus insight from thousands of incident response and adversarial testing engagements Secureworks conducts annually, are fed into Taegis. Customers also receive regular reviews of threat activity and guidance to boost cyber resiliency.

SECUREWORKS MDR FOR OT INCLUDES:

- Taegis MDR for OT, our managed detection and response (MDR) solution delivering threat monitoring, detection, investigation, and collaborative response
- 24/7 unlimited, rapid access to security experts within 90 seconds
- OT-focused security experts who investigate OT-specific threats and provide collaborative response guidance
- Integration with customer OT toolsets (including Dragos, SCADAfence, Claroty, and Nozomi)
- Collaborative build out of IT and OT escalation processes, playbooks, and reporting
- Onboarding support, monthly threat hunting, and regular security reviews
- Access to proactive services to improve cyber resiliency

KEY FEATURES	BENEFITS
Threat monitoring and detection	The Taegis platform provides around the clock vigilance for signs of malicious behavior throughout your IT and OT environments, including endpoints, network, cloud, OT, identity, and more.
Monitoring of OT traffic	Taegis integrations and Secureworks Taegis NDR watch your OT traffic and alert on anomalous activity.
Investigation of suspicious activity	Security experts staff our SOC and dig into potential threats in your IT and OT environment, determining if an alert represents a true threat. SOC security analysts are available within 90 seconds via live chat functionality in Taegis.
Collaborative response	Collaborate with security experts to coordinate the right response for threats discovered in OT.
Monthly threat hunting	Threat hunting playbooks executed across data collected from IT and OT environments.
Integration with customer OT toolset	Ingestion of Dragos, SCADAfence, Claroty, and Nozomi including hands-on-access, as needed, to platform consoles by our OT experts.
Proactive services	Secureworks Service Units included for use on broad catalog of proactive services to improve cyber resiliency.

WHY SECUREWORKS?

Superior Detection: We filter the most noise from the most IT and OT sources to find real threats.

Unmatched Response: Ensure any incident is fully remediated before impact, with unlimited around-the-clock access to our SOC to investigate discovered threats and provide collaborative response.

Open Without Compromise: An open architecture with hundreds of integrations that avoids vendor lock-in, helping future-proof organizations as tools change and grow.

Higher ROI: Low total cost of ownership by minimizing costs to hire additional security resources and purchase tools, while reducing risk and maximizing investments that matter most.

Vast Security Expertise: SOC analysts, threat researchers, incident responders, threat hunters, and customer success personnel all working together to deliver the right security outcomes for customers.

The Right Solutions from an Industry Leader: No matter where you are in your security journey, Secureworks has the solutions, the technology, and the people to reduce your risk, protect your investments, and fill your talent gaps.

Secureworks®
a **SOPHOS** company

Secureworks, a Sophos company, is a global cybersecurity leader that protects customer progress with Taegis™, an AI-native security analytics platform built on more than 20 years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

For more information, call **1-877-838-7947** to speak to a Secureworks security specialist.
secureworks.com