

CASE STUDY

Global Manufacturer Protects Its Business with 24x7 Threat Monitoring

Combined Investment in MDR and Vulnerability Management Strengthens Cyber Defense Strategy



Challenge

For a systems engineer of a European manufacturing organization, a big part of the job is to ensure the company stays safe from malicious activity. It's not easy considering there is a limited team supporting IT and security operations spread out across multiple continents. The systems engineer did not feel they had a single view of all activity across the organization's infrastructure. "We are unable to monitor the whole environment 24x7," they said. "We were afraid that if something happened, for example at night, we would just arrive in the office and notice everything would be encrypted."

It didn't happen to their company, but the systems engineer witnessed the impact of "what if" when one of the company's top suppliers was breached. The resulting disruption in that supplier's business operations lasted for several months, and drove home the importance and necessity of deploying a strong security solution. "When they got breached, our management started to ask how we could avoid ending up in the same situation, and what were we doing to reduce our risk," the systems engineer said.

Challenges

- No single view of what was happening in their environment
- Small team unable to respond if something happened after hours
- Lack of confidence in existing vulnerability management solution
- Concern of impact to business if breached

Solution: Secureworks® Taegis™ ManagedXDR and Taegis VDR

- More robust detection and response capabilities
- Better prevention with vulnerability scanning and contextual prioritization
- Value of having a comprehensive solution from the same vendor

Benefits

- Peace of mind knowing their environment is being monitored 24x7
- More time to focus on strategic initiatives
- Threat detection and response, and vulnerability management from one provider

CASE STUDY

Solution

Secureworks Taegis ManagedXDR provides the manufacturer with a 24x7 managed detection and response (MDR) service built on the Taegis cloud-native security platform. Taegis continuously gathers and interprets telemetry from proprietary and third-party sources, including endpoints, networks, cloud, and identity systems. Secureworks uses this telemetry to help detect and prevent threats, automatically prioritizing the most serious ones to enable faster and more confident responses. ManagedXDR includes 24x7 access to Secureworks security experts, who augment the company's limited in-house resources by monitoring the environment and taking rapid action to investigate and escalate security events. ManagedXDR also includes monthly proactive threat hunting from an expert threat hunter, and incident response capabilities that would enable the company to respond quickly and reduce negative impact should a breach occur.

While a managed solution solves for detection and response, the organization also wanted to strengthen the foundation of their security program with a vulnerability management solution. With too many alerts to chase down and a small team stretched thin, it was impossible to know which vulnerabilities needed the most critical attention. Secureworks Taegis VDR delivers a fully automated, integrated and comprehensive vulnerability management solution that is configuration free. Taegis VDR prioritizes the vulnerabilities that pose the highest risk to the company's environment, looking at both likelihood of attack and impact in context of their environment. VDR automates manual tasks, uses machine learning to improve over time, and provides focus on vulnerabilities that are most meaningful.

A comprehensive, proactive solution that provided both managed detection and response and vulnerability management was the right solution to best protect the organization. The investment in vulnerability management helped prevent attacks by knowing what vulnerabilities to address first, while managed detection and response helps ensure if a threat actor breaks through, early detection and response occurs to avoid an official breach and damage. The validation and market-leadership position Secureworks has from third-party industry analysts helped the business case. "We were convinced in part because Secureworks was cited by leading market analysts," the systems engineer said. "We had to see for ourselves, of course, but the market analysts provided a good starting point in our evaluation process. Working with the same vendor to help us prevent threats by managing vulnerabilities, and also managing threat detection and response, was very appealing to us."

"The chat with a security expert works well. We have used it when we have questions, and we're really impressed by how fast they always answer."

Systems Engineer,
Global Manufacturer

CASE STUDY

Benefits

The systems engineer said one aspect of Secureworks Taegis that has made an immediate impact is the live-chat functionality, and how quickly Secureworks security operations experts respond. With very limited internal security resources, having access to this type of guidance and rapid response is a game changer for the company and uplevels the security skills of their staff. "The chat with a security expert works well," the systems engineer said. "We have used it when we have questions, and we're really impressed by how fast they always answer."

Combining this expertise with the functionality of Taegis frees up time the systems engineer can now spend on more strategic initiatives. As they explained: "In the past, we were analyzing firewall logs ourselves. We had log collectors set up and we were frequently looking and checking for possible threats. Since we have Secureworks in place, we don't even look because we have Secureworks analyzing the logs. If something happens, Secureworks sees it themselves. It saves us a lot of time just from the manual work we did ourselves in the past."

The organization previously had deployed a vulnerability management solution that lacked capabilities beyond light scanning that produced a list of vulnerabilities. The manual nature of trying to know what to work on resulted in lack of adoption and use. With Taegis VDR and its contextual, ongoing prioritization, the manufacturer feels they now possess a much more robust first line of defense against vulnerabilities. "If VDR detects something, it means Secureworks was able to find a hole in our system," the systems engineer explained. "VDR is the first step in making sure no malicious actors get into our network. And if, for some reason, that system failed, then the other Secureworks part – ManagedXDR – would kick in."

It's the confidence of knowing the company has found a trusted security partner, one that provides powerful security solutions delivered in a collaborative nature with expertise available around the clock, that helps the systems engineer and their colleagues rest easy. "We know with Secureworks, we finally have somebody watching over our back to help us out with everything," they said. "We get a good sleep, a good night's rest."

About Secureworks

Secureworks® (NASDAQ: SCWX) is a global cybersecurity leader that protects customer progress with Secureworks® Taegis™, a cloud-native security analytics platform built on 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.

"We know with Secureworks, we finally know that somebody is watching over our back to help us out with everything. We get a good sleep, a good night's rest."

Systems Engineer,
Global Manufacturer



[Learn more](#) about how Secureworks Taegis ManagedXDR improves threat detection and enables rapid response, provides on-demand access to security experts, and reduces operational burden.



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