Secureworks®

Global Pharmaceutical Company Deploys Secureworks Taegis for Holistic Security

Large organization gains complete visibility, powerful threat detection and response, and impactful security expertise to lower cyber risk

Challenge

A global pharmaceutical company found itself looking for a more centralized security solution that could scale across a dispersed and complex environment. When the CISO for the company's European region arrived in 2018, there wasn't a clear strategy in place, as security mostly consisted of checking log data and alerts.

"We were completely lacking a holistic approach," they said. "That lead to slow reaction or no reaction at all if we received an alert."

The CISO entered the process of looking for a more comprehensive solution with a thought in mind, illustrated by the codename he gave the project. "Operation Light Switch," they recalled. "Every vendor I talked to, I told them it was time to turn on the lights, because it's dark and we can't see if there are threats in our environment."

A critical requirement in the search for a security provider was a 24x7 Security Operations Center to investigate and respond to detected

Industry: Pharmaceutical

Countries: Europe

Employees: 3,000

CHALLENGES

- Lack of visibility across entirety of the company's environment
- Inability to scale security activities beyond checking logs
- Need for around-the-clock monitoring, investigation, and response

SOLUTION

This customer selected Secureworks Taegis ManagedXDR to:

- Provide holistic visibility across their dispersed systems
- Deliver 24/7 monitoring, detection, investigation and response
- Get direct, rapid access to security experts

BENEFITS

- Reduced risk with complete visibility
- Augmented in-house resources with 24/7 monitoring, threat hunts, and response
- Improved endpoint detection capabilities
- Avoided time intensive hiring process to build in-house capacities

alerts. The CISO felt strongly that this around-the-clock vigilance was required, and with only a few employees in the company dedicated to security, trying to operate a SOC with in-house resources was not feasible.

"When it comes to monitoring for security events, it doesn't make sense to just have coverage from 9 to 5," they said. "And, when it comes to internal resources and the possibility of trying to build a SOC internally, there was no way I wanted to take that approach."

Solution

The CISO partnered with an external organization specializing in security strategy to get recommendations on what to look for in a security provider, and reviewed leading third-party analyst reports. They sent out an RFP to several leading providers, and cut down a broader list to three finalists. The CISO said one of the finalists proposed what they described as an old-fashioned approach that required the company to purchase of a substantial amount of third-party licenses to try and stitch together a more complete view of their environment.

Instead, they decided to look for a managed detection and response (MDR) solution to provide a powerful technology foundation and leading threat intelligence combined with security experts available 24/7 to investigate threats. Secureworks Taegis ManagedXDR is an MDR solution built on the Taegis XDR cloud-native platform, which continuously gathers and interprets telemetry from proprietary and third-party sources throughout customer environments, including endpoints, networks, cloud, identity, and other business systems.

Taegis ManagedXDR delivers 24/7 holistic visibility needed across the company's dispersed operations, along with direct access to Secureworks security operations experts. Secureworks studies, learns, and analyses adversaries' tactics and techniques by investigating and responding to real-world security incidents, using detectors and machine learning plus comprehensive threat intelligence and advanced analytics to ensure customers remain protected from the latest cyberthreats.

"Secureworks has a very mature MDR product that is well developed and continues to evolve," the CISO said in describing the Taegis platform. "For onboarding, Secureworks has a very straightforward and easy approach. The technical support was great, easily getting us up and

You have a much better feeling when you go on vacation because Secureworks is looking after your environment.

CISO

Secureworks has a very mature MDR product that is well developed and continues to evolve.

CISO

running quickly. We decided to buy the Premium Onboarding package, which was of great help. We received a very high level of technical expertise, as well as project management expertise. Your dedicated project team met with us and provided us great technical expertise in how we thought about our overall cybersecurity program and how to integrate the solution into our environment."

Benefits

Taegis supports a wide variety of third-party endpoint agents in addition to the Secureworks Taegis agent, helping customers protect their existing technology investments. The company had previously deployed Microsoft Defender for its user endpoints throughout its environment. It didn't take long for Secureworks to show the value of the threat intelligence infused into Taegis when Microsoft Defender detected suspicious activity and categorized the alert as medium.

"The Secureworks Taegis agent categorized it as a high alert, identified it as a true positive, and confirmed it was the Raspberry Robin malware," the CISO recalled. "This is a real-time event we experienced. This same alert Microsoft categorized as medium instead was a very new malware that was starting to spread. Secureworks Taegis and its threat intelligence had already identified the activity as the Raspberry Robin malware."

The CISO had started the process of finding a security vendor by looking for a 24x7 SOC service, only to discover the Secureworks MDR solution delivers much more. Secureworks includes access to security analysts in the SOC within 90 seconds via the live chat functionality in Taegis, one full year of data retention, and proactive threat hunting. Customers are assigned a Customer Success Manager who works with customers to set and meet goals for success, and a Threat Engagement Manager who meets with customers every quarter to review overall security posture and areas to improve to reduce overall risk.

"With Secureworks, we not only get a very mature product in Taegis, but we get the added value of teams that have all this expertise," the CISO said. "We have direct access to the security analysts in the SOC, plus threat hunting, access to the incident response team, and the other groups who provide support in case of an incident. That's very nice to have and is valuable."

Having a solution that can provide visibility across the company's entire environment – one dispersed across multiple countries in Europe – was important to the CISO. So too was having that vigilance no matter the time of year. "You have a much better feeling when you go on vacation because Secureworks is looking after your environment," they said.

"Coming back to codename 'Operation Light Switch,' we now have the visibility we needed. In no way can you compare where we are now to where we were when I took over this role. It's having the visibility, a holistic view, plus the expertise that Secureworks provides. This solution from Secureworks changed everything for us."

Secureworks®

Secureworks (NASDAQ: SCWX) is a global cybersecurity leader that secures human progress with Secureworks® Taegis™, a SaaS-based, open XDR platform built on 20+ years of real-world detection data, security operations expertise, and threat intelligence and research. Taegis is embedded in the security operations of thousands of organizations around the world who use its advanced, AI-driven capabilities 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