CASE STUDY

Secureworks® | Taegis™ ManagedXDR

Utility Infrastructure Company Saves Costs and Strengthens Security with Secureworks MDR

Secureworks® Taegis™ solutions deliver $500,000 in cost savings while improving security maturity, reducing alert noise, and providing rapid access to security experts

Industry: Utility Infrastructure
Country: United Kingdom
Employees: 2,500

CHALLENGES

- Too many low-fidelity alerts without context from existing security platform
- Lack of holistic visibility across variety of security tools
- Need for 24/7 investigation and response to threats

SOLUTION

Company selected Secureworks Taegis ManagedXDR and Taegis ManagedXDR Elite to:

- Deliver holistic visibility across company's environment to reduce cyber risk
- Filter out noise to prioritize real security threats
- Enable continuous, proactive threat hunting with bi-weekly meetings

BENEFITS

- Cost savings of $500,000 and lower TCO by avoiding building internal SOC
- Rapid access to security analysts with unlimited support
- Additional vigilance and expertise from continuous threat hunting

CHALLENGE

A leading utility infrastructure company in the United Kingdom had worked to evolve its security program through the years. The Head of Information Security recalled the company going through a cybersecurity review. In response to the findings, the organization added network access controls, antivirus, mail filtering technology, and a security monitoring and notification platform.

While the platform provided the company a higher level of visibility, the Head of Information Security said it generated plenty of alerts that lacked context and often turned out to be false positives. This took time away from working on higher value security projects. The company needed a solution that reduced the noise by investigating the validity of detected alerts while also enabling better visibility by bringing together the various elements of their security environment.

Availability varies by region. ©2023 SecureWorks, Inc. All rights reserved.

"We have a lot of personal data, we run utilities, we're a big target, and we understand there are threats that have impacted organizations like ours," the Head of Information Security said. "We need a proactive solution with 24x7 monitoring so that someone is looking at our environment not just during the 9-to-5 hours when I'm here, but when the office is not open."

SOLUTION

The company sought a unique solution built on superior detection that filters noise to find real threats. They were also looking for unmatched response, driven by security operations experts investigating and performing response actions. Furthermore, the organization needed an open and transparent platform that ingests telemetry from a wide variety of sources, delivering high return on investment and low total cost of ownership by minimizing internal costs for people and tools.

Secureworks® Taegis™ ManagedXDR is a managed detection and response (MDR) solution that reduces risk, maximizes value of existing investments, and helps elevate a customer's security posture. The Taegis platform continuously gathers and interprets telemetry from proprietary and third-party sources throughout a customer's environment, including endpoint, network, cloud, identity, OT, email, and business applications. This MDR solution not only provides 24x7 monitoring, but also offers access within 90 seconds to experienced SOC analysts. Taegis provides access to full-service incident response capabilities, one year of raw telemetry storage, and impactful threat intelligence — all standard on the platform. Taegis is a transparent platform: SOC analysts and customers share the same interface for collaboration, and customers can see all actions taken by Secureworks.

The company also purchased the Taegis ManagedXDR Elite threat hunting add-on, expanding the proactive monthly threat hunting included in the Secureworks MDR solution. Taegis ManagedXDR Elite provided the organization with a designated threat hunter, scouring the company's environment continuously for stealthy threats and meeting with the organization every two weeks to provide updates and insights.

"Having that second pair of eyes always looking at our environment and systems was really important," the Head of Information Security said. "With the experience of the security analysts in the SOC and the level of detail of the threat hunters, they can report on where we are and what we need to do."

BENEFITS

The company considered building out and staffing their own internal SOC, but the Head of Information Security said that approach would be challenging given the global cybersecurity skills shortage and the cost associated with hiring, training, and retaining staff.

"We were looking at a cost of at least $500,000 per year on staffing, or we could spend far less than that to get the Secureworks MDR solution, which includes great security expertise," they said.

"Every time I've contacted Secureworks, the response has been instant. They don't mess around. They answer. It's not like a normal call center where you get put in a queue. If I have a question, I have 100 percent confidence that I can write my question in a chat, and within 90 seconds, I'll have someone online who is answering the question or investigating the answer for me," the Head of Information Security said of their responsive experience with

Availability varies by region. ©2023 SecureWorks, Inc. All rights reserved.

Secureworks®

Secureworks. "They all seem to be at the same level. They know almost instinctively where to start looking. There's someone always there, and that's the real value add to the business."

One of the biggest differences with Taegis is the ease of having one place where the Head of Information Security can look at the vast array of security tools in the company's environment. The Head of Information Security said the company finds great value in the dashboards and reporting functionality within Taegis.

"We don't rely on a single vendor. We use Microsoft Office 365 and Azure. We use Forescout Network Access Control, Zscaler, Mimecast. Logging into these things and looking at them individually would be a real pain," they said. "But with out-of-the box integrations, they all integrate into Taegis and I can go into the platform and see everything. It shows flexibility to support the integrations I have today and in the future."

The company purchased the Taegis ManagedXDR Elite add-on as an additional layer of security and vigilance against stealthy threats. "It's not that much money in comparison," the Head of Information Security said. "I liked the monthly threat hunts but wanted more. We got Taegis ManagedXDR Elite, and I was blown away," said the Head of Information Security. "They went into the most exquisite technical detail about what they did, how they did it, why they did it. It always resonates. The threat hunting team all have the knowledge of a SOC engineer, as well as the knowledge of how to talk to a business."

Secureworks MDR pulls together powerful cybersecurity analysis with vast human intelligence to give customers the best cyber defense, experience, and value.

"We were able to enable a really secure solution and approach with very minimal effort on our part," the Head of Information Security said. "It's like having another department in the company, focused on security, and only more competent because of the level of experience Secureworks brings. We've been able to demonstrate security maturity improvements. We're ahead of where we need to be, and we see having the Secureworks MDR solution as being strategically linked to that goal."

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.

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

Availability varies by region. ©2023 SecureWorks, Inc. All rights reserved.