CASE STUDY

Secureworks® | Taegis™ ManagedXDR

COUNTY BOLSTERS CYBER DEFENSE APPROACH TO BETTER PROTECT ITS CONSTITUENTS

One of Largest Counties in U.S. Uses Taegis™ ManagedXDR to Accelerate Threat Detection and Security Effectiveness

CHALLENGE

Being in charge of cyber operations for a large county government and its various departments presents its own unique set of complexities. Every department, while sharing the goal of serving citizens, has different requirements, different levels of security maturity, and their own individual mission to fulfill. Every asset, regardless of where it connects from or who it belongs to, must be protected from malicious threat actors. The county needed a solution to meet the varying needs of its many departments. An audit of the county's cyber defenses showed there were too many security gaps, and one department indeed experienced a cyberattack. The county realized that effective cyberdefense required a high level of investment – from people, technology, and processes – and restructured its approach to establish one branch that would focus exclusively on cybersecurity.

The county now employs a sophisticated approach to security, including security analysts on staff, and five areas of focus: endpoints, access, data center, private cloud, and analytics. The head of cyber operations said the county felt their previous security provider had shortcomings in coverage and visibility, and displayed a lack of automated response capabilities. With so many different technologies in their security stack, building a large number of custom integrations proved problematic. After adding layers of security tools to address concerns in the past, the county needed to partner with the right security provider

Industry:	Government
Country:	United States

CHALLENGES

- Better protecting constituents who leverage county resources
- Future-proofing strategy as point solutions transition in and out
- Safeguarding a large number of devices

SOLUTION

- Secureworks Taegis ManagedXDR
- Increase telemetry ingestion and visibility for faster and more holistic threat detection
- Work with vendor-agnostic platform to support current and future integrations
- Gain on-demand access to security experts to augment existing team

BENEFITS

- Additional layers of defense across all departments
- Rapid detection and response to threats
- Flexibility with integrations

to help maximize not just those current investments, but investments that would be made in the future. “We needed a future-proof solution,” the head of cyber operations explained. “Just because we have ‘X’ technology solution today, it might be ‘Y’ tomorrow, and we have to stay away from locking in with any one vendor.”

SOLUTION

Taegis ManagedXDR is a 24x7x365 managed detection and response (MDR) service that helps reduce customer risk, optimizes existing investments in security technology, and addresses in-house talent gaps. Secureworks experts monitor customer environments across endpoint, network, cloud, identity, and other business systems, and take rapid action to triage and escalate security incidents. Taegis ManagedXDR also features monthly threat hunting and incident response services, incorporating threat research and incident response engagement findings into the Taegis platform. Taegis ManagedXDR also provides access to security operations experts in as little as 60 seconds via the live chat functionality within the platform. Even with a government organization featuring numerous entities and plenty of complexity, Taegis ManagedXDR delivers rapid threat detection and response, and access to security expertise, all while protecting the county’s existing security investments.

The Secureworks solution scales to meet the county’s challenges of having a large security infrastructure with many endpoints and users across the various departments. Having different departments with different agendas could make wide deployment of a solution challenging, but there was immediate buy-in to Taegis ManagedXDR. Secureworks endpoint agents were deployed ahead of schedule across many of the departments, and provided immediate dividends by alerting the county to threats faster than the previous solution.

“It has been a valuable change; everyone wanted to do it,” the head of cyber operations said. “We’re eight months in, and we’re probably eight months ahead of where we were at that time with our previous provider.”

BENEFITS

Taegis features ingestion of telemetry from a wide array of sources across endpoint, network, cloud, and business applications, helping the county reduce the amount of custom integrations that was required with their previous provider. That flexibility also eases the county’s concerns about the types of technology they bring into their stack. This is important, since the county is a public entity, and required to bid out contracts when an existing contract expires.

More importantly, having access to security operations experts gives the head of cyber operations value reassurance. No matter what time of day, no matter the type of alert, Secureworks security staff works with the county’s security teams to help keep all of its departments and users safe. The expertise gained from threat intelligence research, incident response findings, and monitoring customer environments of all sizes across all major industries provides a level of confidence the county welcomes. “The expertise of the folks doing the work, the ones up at night, doing the analysis and detecting and preventing is reassuring to us,” the head of

> “The expertise of the folks doing the work, the ones up at night, doing the analysis and detecting and preventing is reassuring to us. We didn’t want a team of network engineers. We wanted to partner with a team of experienced, dedicated cybersecurity experts.
>
> **HEAD OF CYBER OPERATIONS,** COUNTY GOVERNMENT”

cyber operations said. “We didn’t want a team of network engineers. We wanted to partner with a team of experienced, dedicated cybersecurity experts.”

The head of cyber operations recalled a county employee, who was on vacation overseas, logged in to check their email. The Taegis platform detected the activity and Secureworks security experts opened an investigation. The login was credible – it was done by a county employee using their work credentials – but the location certainly warranted taking a closer look. It’s a capability the county did not have previously. “It’s showing enhanced visibility, year over year,” the head of cyber operations said. “Last year, we couldn’t detect these things, or show what outcome it produced.”

One of the many aspects of Taegis ManagedXDR that the head of cyber operations appreciates is how Secureworks tracks the mean time to resolve escalated security events. It’s evidence of just how important it is for a security vendor to not just provide a service, but to truly partner with customers – even a customer as sophisticated and well-versed in cybersecurity as the county. “You track mean time to hand off an investigation, and you track the time our team takes to acknowledge it and the time to close. It’s not just, ‘hand it over to you guys and good luck.’ You hold us accountable, too. It’s a good partnership. We are in this together.”

> “It’s not just, ‘hand it over to you guys and good luck.’ You hold us accountable, too. It’s a good partnership. We are in this together.
>
> **HEAD OF CYBER OPERATIONS,** COUNTY GOVERNMENT”

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

Secureworks®