CASE STUDY

Secureworks® | Taegis™ ManagedXDR

THE KRAFT GROUP ADOPTS TAEGIS MANAGEDXDR AS THEY TRANSFORM THEIR IT ENVIRONMENT

Secureworks led a proactive incident response engagement to review core systems and ended up partnering with The Kraft Group for 24/7 visibility, threat detection, and access to security experts with Taegis ManagedXDR

Name: The Kraft Group
Industry: Entertainment
Country: United States

SOLUTION

The Kraft Group partners with Secureworks® Taegis™ ManagedXDR for 24/7 visibility, threat detection, and closing the skills gap with a team of experienced security experts.

OVERVIEW

The Kraft Group is the holding company for numerous operating units in the sports and entertainment industries. Their scope includes a stadium, professional sports team, and related holdings operating in the United States. They are continuously looking for new ways to engage guests at their sports and entertainment venues.

“Here at Gillette stadium, technology is playing a critical role in changing the way we do business with our guests. One example of that is our point-of-sale environment in which guests now have the ability to purchase right from their seats. To order from their seats, to engage with special views, fancam views, to just interact in different ways that they never have before,” said Michael Israel, CIO of The Kraft Group.

As The Kraft Group was undergoing a transformation across all IT, leadership teams recognized that security needed to evolve at an equal pace and align to the overall IT strategy.

If the company suffered a ransomware attack, the consequences could be devastating. It would negatively impact guest experience and tarnish the company's reputation. However, their cybersecurity team was overwhelmed with alerts from disparate, fragmented point solutions ranging across endpoint, cloud, and network resulting in data spread across multiple dashboards, identity systems, and reports. Without a single view, security analysts were unable to analyze cross-solution telemetry to understand if alerts were white noise or true threats. What good are multi-system notifications if the team was unable to identify threat actors from employee activity?

CHALLENGE

- The Kraft Group needed to avoid ransomware attacks that would impact reputation and guest experience.
- There were not enough on-staff cybersecurity experts to support the business and its rapid expansion and evolution.
- Existing staff were drowning in alerts from point solutions (endpoint, cloud, network (as noted above) that weren't designed to play well together.

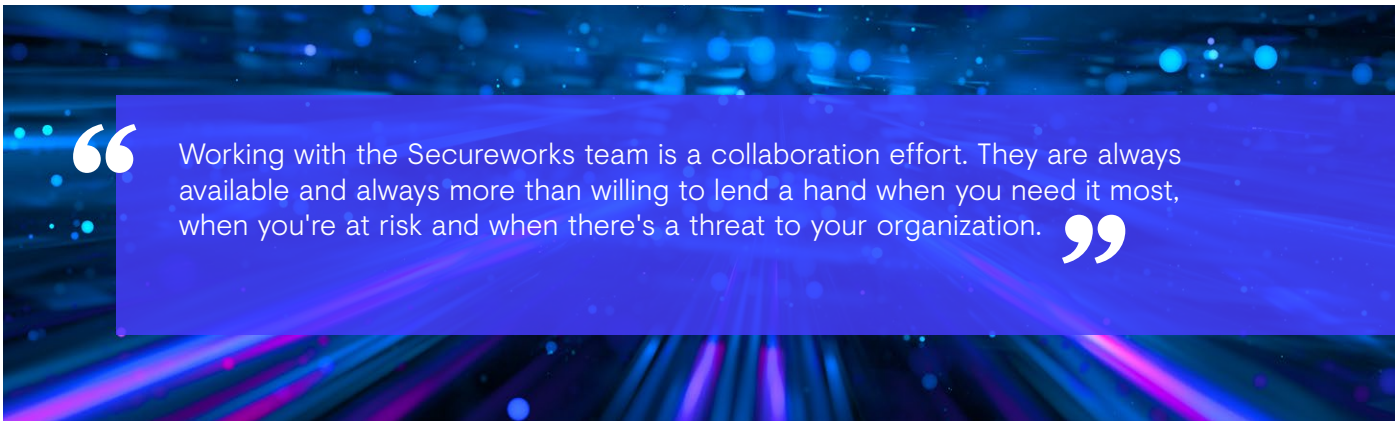
For The Kraft Group to stop threats, they needed to evaluate alerts in real time. With so many external factors, these numerous points of vulnerability required constant monitoring. But the challenges did not stop there. A shortage of cybersecurity talent on staff – coupled with a difficult labor environment for hiring and retaining qualified cybersecurity personnel – meant slower response time. This left The Kraft Group more vulnerable to attack.

"The shortage of talent is critical. With the volume of alerts that come in on any given day, the team that we have just can't evaluate all of these things in real time to be effective. The use of Secureworks and having the Secureworks team behind us allows us to essentially expand our team beyond its reach. We would never be able to expand to the level of what Secureworks is providing us," said Israel.

Among the company's most recent challenges was the increased rise of ransomware attacks. If the company was successfully breached by one of the thousands of ransomware attacks that occur daily, it would have devastating consequences for their reputation and their customer experience.

The Kraft Group evaluated vendors for an extended detection response (XDR) platform that would best fit the needs of their organization. To reduce the load on their staff, they wanted a partner that no longer delivered the platform to prevent, detect and respond to threats but one that coupled 24/7 security monitoring to proactively manage risk.

Secureworks offers Taegis ManagedXDR, which offers 24/7 security monitoring with its open XDR platform. With Taegis ManagedXDR, The Kraft Group has the ability to prevent, detect, and respond to continuously evolving and diversifying threats.



Secureworks

SOLUTION

While The Kraft Group decided on a more long-term solution for their security operations and the right platform to move forward with, they called Secureworks to engage in an initial threat hunt. The Secureworks Counter Threat Unit led a Proactive Incident Response team to review core systems and determine if a threat was lingering in their environment. The goal was to ensure as they onboarded a solution, their systems were clean without known vulnerabilities and active threats in their system.

In working with Secureworks, The Kraft Group team was pleased with the proactive incident response work and ultimately decided to partner beyond this exercise, implementing Secureworks® Taegis™ ManagedXDR for 24/7 visibility, threat detection, and access to security experts. This way, the internal team was free to work on other strategic projects, and the need for new hires was eliminated.

With the customer's unique challenges in mind, Secureworks went to work on a customized plan for mitigating their security concerns. The first key step was to reduce the noise from siloed point solutions that were throwing out far too many alerts, and instead bring alerts into a single view. Secureworks integrated easily into the existing infrastructure, extending the value of existing systems and eliminating the need to rip and replace expensive security tools. This way, the company could have a "single pane of glass" view, providing comprehensive visibility and ensuring that the most critical alerts were prioritized for response.

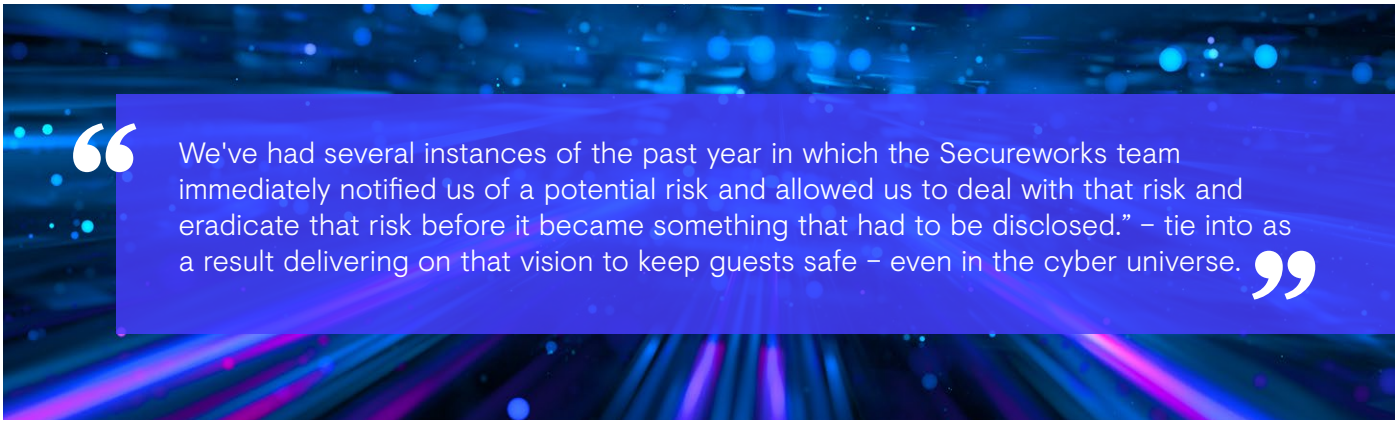
"Our experience with Secureworks Taegis ManagedXDR has been world class. Having the Secureworks global SOC available 24/7 as an extension to our security team along with around-the-clock monitoring of our alerting has drastically improved our response capabilities," said John Gonsalves, IT Security Lead at The Kraft Group.

"Taegis gives us the ability to work in the same console as the Secureworks analysts with access to query our data and telemetry unfiltered. Investigations are collaborative, sharing searches and alert triage workflows all within a unified user interface. When we evaluated other XDR providers they simply ingested your telemetry into their back-end solutions, only to provide a front-end customer portal of alerts to review with no investigation help," said Gonsalves.

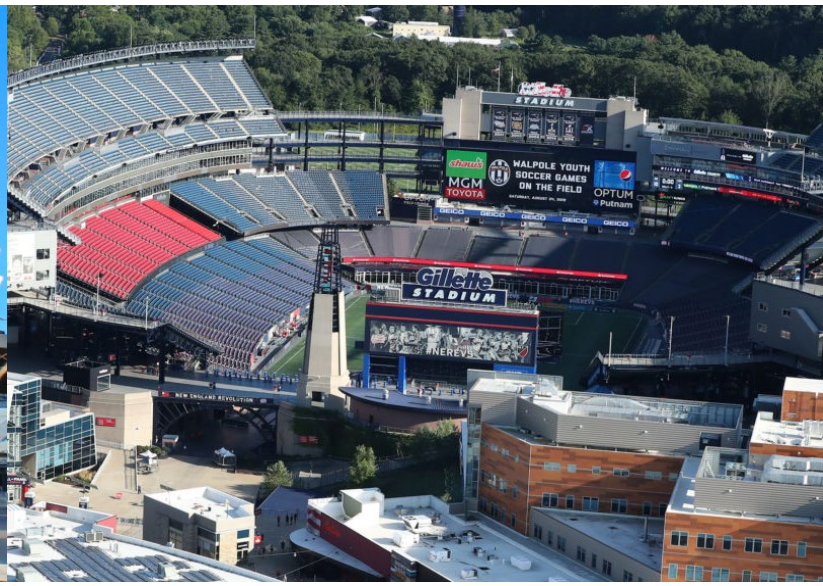
"We've had several instances of the past year in which the Secureworks team immediately notified us of a potential risk and allowed us to deal with that risk and eradicate that risk before it became something that had to be disclosed," said Israel.

With that kind of quick response from the Secureworks Incident Response practice, The Kraft Group could address and ultimately eradicate the risk before it could cause physical, virtual, or reputational damage.

All in all, Secureworks is focused on reducing The Kraft Group's cyber risk while its security team focuses on strategic IT initiatives to maximize guest convenience and engagement.



Secureworks®



BENEFITS

Since The Kraft Group partnered with Secureworks, they have enjoyed 24/7 security monitoring, enabling their team to focus energy on other projects to support business goals. Secureworks promptly notifies the security team of potential risks, ensuring the customer can take timely action – and have the additional support they would have previously needed to recruit, hire, and train – before they suffer a ransomware attack.

“Working with the Secureworks team is a collaboration effort. They are always available and always more than willing to lend a hand when you need it most, when you're at risk and when there's a threat to your organization,” said Israel.

For The Kraft Group, the return on investment is unmatched. Secureworks solved The Kraft Group’s staffing and skills gap while providing active threat prevention, detection, and response across their entire IT environment.

“With Taegis, we have 24/7 access to security experts providing guidance on any event or alert that is captured within the console and aid in any investigations that result. Pair all of this with an extensive list of out-of-the-box integrations with leading solutions in endpoint, cloud, network and email security that are easy to configure and manage, giving customers unmatched time to value and return on investment,” said Gonsalves.

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