Leading Food Service Distributor Realized Maximum Value from Security Program with Tailored MDR from CRITICAL**START®**

A food industry giant improved overall security posture and accelerated detection and response with Critical Start's adaptable, tailored MDR approach.

CASE STUDY

AT A GLANCE

Industry: Food Service Distribution

Number of Employees: 5,600

CORE AGENDAS

Challenge
The organization could not afford to staff a full-time security operations center to handle alert volume, nor could they build robust detection rules and integrations to make the best use of their incumbent tools.

Solution
Critical Start's human-driven MDR provided the coverage they needed to protect, detect, and respond while giving them the power to tailor rules and integrate deeply with the security tools they already owned.

Results
Increased ROI across their security stack, implementation that aligned with risk appetite, deep integration across their incumbent tools, dependable escalations that eliminated alert fatigue and allowed them to focus on key objectives.

Background

Since mid-2022, the Critical Start Managed Detection and Response (**MDR**) service has helped one of the largest food manufacturers and distributors in the United States reduce the risk of security breaches. This company serves major national restaurant chains with reliable food delivery. In the event of service disruption, the cascading effects could impact thousands of stores. The company's Chief Information Security Officer leads a team that has grown from three to six members, including senior engineers and junior to mid-level analysts.

Business Priorities

Before partnering with Critical Start, this food service giant managed their security operations in-house with a small team that couldn't provide 24x7x365 coverage. They faced challenges with blind spots, alert fatigue, and the inability to respond quickly to potential security incidents.

Their CISO noted, "The volume of alerts – up to 50,000 per month – overwhelmed our small team." The team spent significant amounts of time sifting through noise to find genuine threats. Given budget constraints, they could not afford to staff a full-time security operations center (**SOC**) that was robust enough to fully manage their alert volume.

Limited staffing also meant that they lacked round-the-clock monitoring. Any incidents occurring at night went unnoticed until the next day. The potential impact on their own business, as well as the cascading effects on their customers, was beyond their acceptable risk appetite. Something had to change.

The company's CISO chose Critical Start for their Managed Detection and Response (**MDR**) services, including MDR for Cortex XDR, Microsoft 365 Defender, and SIEM.

The CISO and their extended team were also impressed with Critical Start's MOBILE**SOC**® app. Because their team works on-call after hours, the ability to contain threats from anywhere via their mobile devices significantly contributed to their choice of Critical Start MDR.

> **I could not staff a 24x7 SOC, but even if we could, we couldn't touch the level of service provided by Critical Start. The cost savings are huge for the value that we receive.**
>
> **- CISO**

Solution

Since partnering with Critical Start, the company has seen significant improvements in their security operations. The volume of alerts has been drastically reduced with Critical Start resolving all alerts regardless of priority and escalating only real threats. The team has saved a considerable amount of time, allowing them to focus on more strategic tasks.

One notable incident involved an unusual mailbox rule in Microsoft 365 that was quickly escalated by Critical Start. The prompt response helped the company thwart a phishing attempt and ensured no sensitive information was compromised. The team also values Critical Start's responsiveness and the human-driven approach to security operations, which includes personalized recommendations and thorough investigations.

Additionally, this customer is impressed with Critical Start's willingness to listen when it comes to requests for feature enhancements. "Critical Start is very open to developing the product based on customer feedback," said the CISO. "And it's not so they can just charge us more money. Critical Start provides features that are new just because there is value in it, and it will improve the security posture of all their customers."

Outcomes

When asked for specific outcomes, this company's extended team noted:

"Critical Start's responsiveness is excellent. They have been quick to jump when we need them."

"Basically, every after-hours High Alert call we have received has been actionable and on-point."

"There are alerts we would have likely missed on our end, or it would have taken way longer to see them. It could have been too late had Critical Start not been monitoring for us."

"The MOBILE**SOC®** app is a game-changer. We use it daily. It's also cool to pull it out at lunch and show people what we can accomplish from anywhere. Most importantly, in addition to reading alerts, we can also take response actions from our mobile devices without having to login to our computers. This has greatly improved our MTTR and work/life balance."

Overall, this food service giant has benefited from the cost savings, improved security posture, and the ability to leverage Critical Start's expertise for incident response. The partnership has allowed them to maintain a high level of security without the need to staff and budget for a 24x7x365 Security Operations Center (**SOC**).

For more information, contact us at:
https://www.criticalstart.com/contact/