Manufacturer Unifies Security Posture, Dramatically Increases Alert Visibility Through CRITICALSTART MDR Services and Palo Alto Cortex XDR™

CASE STUDY

AT A GLANCE

- Major International Manufacturing Organization
- 20 Offices Worldwide
- Shifted 85-90% of Its Office Staff to Remote Work
- Several Acquired Companies Not Yet Unified Under One Security Umbrella

CORE AGENDAS

- Extended Team with Cybersecurity Expertise
- Consolidate Threat Visibility
- Strengthen Security Posture

CRITICALSTART

They're good. We're better.

With over 20 offices worldwide, this manufacturer has multiple unique brands built through acquisitions and partnerships.

But with such strength in diversity also comes security challenges that require constant vigilance. When the North American IT director for this business joined the organization, he uncovered vulnerabilities that he knew needed to be addressed.

"Prior to my arrival, there were these were silos of security, where each division had its own IT representative, and he or she did what they felt was best," he explained. "This resulted in a lack of synergies in areas such as antivirus, where there wasn't a centralized deployment. Symantec, Malwarebytes, and Webroot were all being utilized. I knew the first step was to unify our team, figure out what are the needs for each division, and then come up with a solution. That was my roadmap, but then the unexpected occurred."

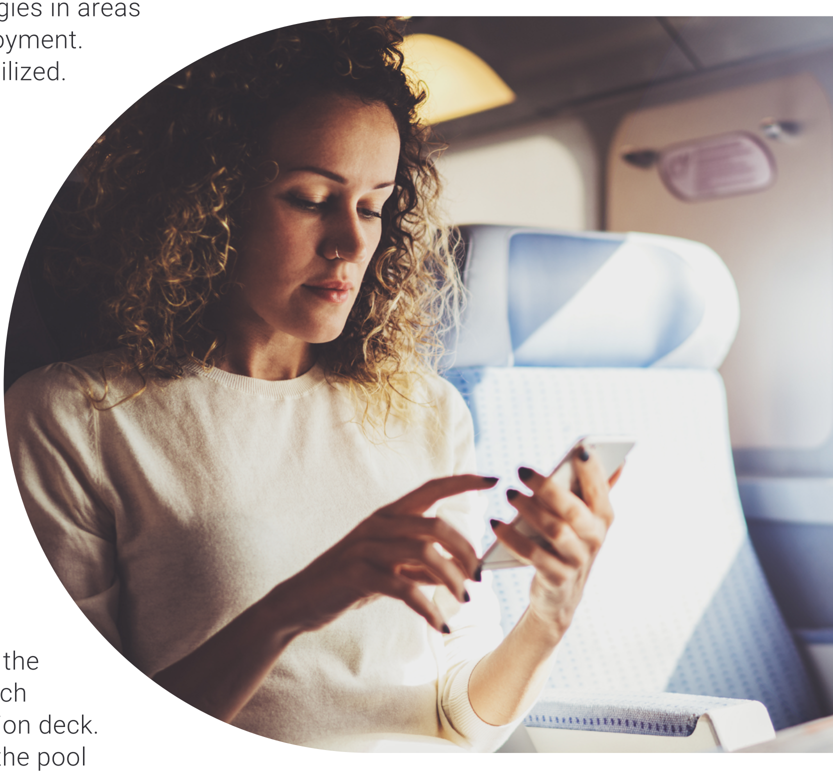
Trial by Fire

An incident occurred at one of the divisions of the manufacturer. A ransomware attack started to spread out like the spokes on a wheel across the organization including databases, VMware, and file servers. As the potential severity of the attack began to set in, a vendor that the manufacturer worked with recommended CRITICALSTART to help the firm respond to this attack in the quickest manner possible. "It was kind of an interesting way to start a partnership," the IT director related. "There was no time to get to know each other, do formal introductions or go through a presentation deck. This was, 'We're going to push you into the deep end of the pool and see if you can swim.' We signed the contract around 1 in the morning."

Manufacturer Profile

Due to the sensitive nature of this account, this customer's name is redacted for security.

But we can say this manufacturer has 6 directly owned plants. And through an extensive wholly owned network of subsidiaries in 40 countries and more than 50 distribution partners in key markets this company distributes in nearly 100,000 selected points of sale worldwide.



CRITICALSTART responded quickly. "They determined the exact extent of the infection and which systems were infected," the IT director stated. "They became an extension of my team as if they were right next to us, where we just went back and forth sharing information. Normally, with an event like this, you're talking days of downtime, if not weeks. In our case, the initial word on the breach went down on a Friday afternoon, and yet we were back up and shipping product by Monday around lunch."

With the breach under control, IT director felt that it was time to unify the multiple security teams and infrastructure of his organization to prevent such an attack in the future. One of the first steps was expanding the relationship with CRITICALSTART into areas such as Managed Detection and Response (MDR). "I think the number one point is having everybody on the same coverage," he related. "The way I see it, I have two options: I can develop a team from the ground up, or I can partner with someone who is currently in the field that deals with several different customers and can see a trend across those customers. If I have my own team, I only have visibility to what is internal to me. But if I partner with someone that has visibility to a much greater scope, they can see a trend coming down the pike, perhaps prior to hitting me and I can be alerted. I need someone to basically say, 'Hey, we're seeing this malicious virus that is exploiting this particular vulnerability. Please push this update to all your servers. From a software and a vendor perspective, when one team that sees the entire picture, they're able to connect dots in a much more efficient manner than if you have multiple vendors. This type of visibility is hard to replicate internally, so it makes it essential to work with one strong partner and keep everything under one umbrella."

> **"In our case, the initial word on the breach went down on a Friday afternoon, and yet we were back up and shipping product by Monday around lunch."**

Moving to MDR

As CRITICALSTART started to deploy an MDR security operations center (SOC) and implement the tools necessary to identify, contain and mitigate threats, the IT director liked what he saw.

““CRITICALSTART has a knowledgeable team, so they know exactly what needs to be done,” he shared. “You can tell these guys have done it before. The onboarding went smoothly, and they really provided accurate direction for us. In one instance, we ran into an issue with our threat detection and response platform, Palo Alto Cortex XDR. My company had multiple Palo Alto Cortex XDR accounts, which caused some issues on the initial setup. But I just stood back and let CRITCALSTART, which has a well-established relationship with Palo Alto, work directly with them to straighten everything out. Then they showed how to use the portal, gave us the login information and they created the executables for us to start deploying the agents to all the workstations. We had weekly meetings to see our progress, and once we reached approximately 70-75% saturation of the agent deployment, we started onboarding to the MDR and going live with full monitoring.”

One very important benefit to this IT director was CRITICALSTART’s approach to MDR, especially their Zero Trust Analytics Platform (ZTAP). ZTAP resolves all alerts instead of focusing only on critical or high alerts that—on the surface—would appear to present the greatest threat. CRITICALSTART SOC data shows that of all the alerts that are escalated, only 1% are critical and 4% are high, while 26% are medium and 69% are low. This makes it essential to treat all alerts equally, but that can be a task far beyond the capabilities of an internally run SOC. This is why CRITICALSTART analysts worked with the customer’s team to build out a Trusted Behavioral Registry (TBT) to identify known-good and safely trusted alerts to enable analysts using ZTAP to clearly identify the alerts at any level that can indicate a threat.

“

Having a team that considers the potential threat of a low-priority alert in the same way they treat a critical- or high-alert is a big deal,” the IT director shared.

“No one wants to show their cards up-front. When a business gets attacked, the attackers could have been hiding in the system for months while only leaving low-priority alerts to identify their presence. Having that much higher level of visibility into all alerts played a big part in my decision-making.

”

Defining value

When it comes to the bottom-line value that the IT director has gained from this process, he has a clear answer: “I’m able to sleep at night,” he shared. “It might sound like a joke, but there’s a lot of truth behind it. I can go to sleep knowing that someone is watching what’s happening in my network. And if they see something concerning, they’re not only going to be able to isolate a specific workstation or server, but they’re going to be making phone calls and waking everybody up. It’s this kind of response that provides a priceless peace-of-mind, both to me and ultimately my organization, when it comes to dealing with a ransomware or virus attack.”

> “I can go to sleep knowing that someone is watching what’s happening in my network”

Running the Numbers

If a company with 7,000 endpoints faced a ransomware attack, it would take 6 traditional IT admins 8 days to resolve the alerts and find the attack (assuming 10 minutes per investigation during a typical work week). With a day of downtime typically costing millions, TBT and ZTAP present an alternative, by enabling analysts to quickly move past the 99.94%* of alerts that are actually false positives.