



## **MDR is Built to Find the Hidden Threats. Ok, Prove it.**

It can be a bold claim to say that MDR is capable of finding the threats where other security solutions fall short. But it's a bold claim we prove time and again—even when we're looking at a potential customer's environment for the first time.



# During onboarding engagements we sometimes uncover a cyberattack already in progress.

From day one, as we connect ZTAP to an environment, we can see alerts and evidence of attacks such as malware and ransomware that may already be present prior to MDR. We investigate and advise our new customers of what remediation actions to take and our internal Cyber Incident Response (CIRT) experts come alongside your dedicated Onboarding Team to make sure the problem is solved.

## Here's an example:



We had a new customer inform us during implementation that an endpoint in their environment was displaying a system virus alert. They were unsure if it was an actual attack in progress or not.



Using ZTAP, our Onboarding Team and Incident Response (IR) investigated and found significant freeware/adware on a few customer endpoints. The issue they were seeing was a result of browser add-ons and freeware applications.



The IR team provided a write-up of their findings for the customer, and the Onboarding Team held a working session with the with suggested remediation actions.



The customer took action on recommended remediation steps and resolved the issue resulting in immediate and documented results that they were able to share with their board to prove the value of their new MDR investment.

## How We Do It

The example on the left is just a small glimpse into how we help enterprises face radical, ever-growing and sophisticated multi-vector cyber-attacks. Facing these types of threats may seem hard, but it doesn't have to be. CRITICALSTART simplifies the complexity of cybersecurity by extending your team with a comprehensive and customized enterprise solution of flexible services, exclusive technology and well-trained, seasoned security experts that will deeply understand, adapt, and scale with your organization's unique needs and collaborate with you to detect, investigate, and respond to all alerts. We guarantee the value you receive with contractual Service Licensing Agreements (SLAs) for Time to Detection (TTD) and Median Time to Resolution (MTTR) and 100% transparency into our service.



# Think Simple



At CRITICALSTART, our MDR business is simplifying your business. We deliver managed detection and response that flexes to your business objectives and cybersecurity vision, regardless of the complexity.

We offer unique benefits to enterprise customers who are building and optimizing security operations to be extremely effective and better at stopping breaches.



**Turmoil to tranquility.** Our services integrate with industry-leading security tools and our security experts tamp down the noise and push them to be more effective at detecting and stopping threats.



**X – tended MDR.** Over 40% of our existing customer base relies on us for threat detection and response that leverages multiple endpoint security tools. Our services also expand beyond endpoint to SIEM, identity and cloud.



**Don't build a SOC, buy one.** Our in-house SOC experts tailor our service to your unique needs and become an extension of your team, seeking to deeply understand your environment, helping you make faster, more accurate decisions on which actions to take.



**Simple security, sped up time to value.** Security teams will never scale to keep up with threats. So, we said let's approach the problem differently. We developed the industry's only Trusted Behavior Registry (TBR) within our Zero-Trust Analytics Platform (ZTAP) purpose-built to resolve all alerts. We simplify your life by reducing your volume of alerts by more than 99 percent. We escalate only less than 0.1% of alerts, and never send you the same alert twice. In fact, you can see an 80% reduction in false positives on the first day of production monitoring.



**Life is mobile. Security operations should be, too.**

We simplify your security team's lives with the power to triage and contain alerts from anywhere. Our mobile application, MOBILESOC, provides you with easy, quick interaction with your CRITICALSTART security team.



**Bewilderment to clarity.** Our service is an open book, and we give you the tools to inspect it. From your detection coverage aligned to industry frameworks, to full alert details with enhanced context, and a dashboard proving our contractual service licensing agreements for time to detect (TTD) and median time to resolution (MTTR)—we operate with precision and everything is visible in ZTAP and MOBILESOC.



**Tools change, but your service doesn't have to.** We are on the journey with you as you continuously optimize your program. As you make decisions about the security tools you leverage, we'll be there at your side, scaling with you, still stopping breaches.

Contact CRITICALSTART to learn what simplified—yet highly effective—cybersecurity can mean for your business, and your peace of mind.

