

CRITICALSTART Managed Detection & Response (MDR) Services



Benefits Overview:

- ✓ Reduce risk acceptance
- ✓ Increase SOC efficiency & productivity
- ✓ Validate value of security investments
- ✓ Report on security posture

Detect all events. Resolve all alerts. Stop breaches.

Today's reality is daunting. And no one needs to tell you that your job is getting harder. You're navigating a maze of security challenges—from staffing, to lack of visibility across disparate security tools, to an increase in sophisticated threats which are triggering massive volumes of alerts.

What if we told you there is a better way to approach threat detection and response? A better way that truly reduces risk acceptance, increases Security Operations Center (SOC) productivity, and helps you validate return on your security investments.

All MDRs are not all created equal.

Traditional threat detection and response services are designed to rank or suppress alerts, addressing only critical and high-priority alerts. Service providers often force customers to accept risk in the form of medium and low-priority alerts. However, **devastating breaches can arise from even low-level alerts.**



MDR Methodology

Input-Oriented

Prioritization

CRITICALSTART



How it Works

- ✓ Disables inputs or alters correlation logic that generates alerts to control false positives
- ✓ Only focuses on critical and high alerts, leaving most alerts untouched
- ✓ Assumes every alert is bad until it can be proved good. Resolves 99% of alarms automatically and investigates remaining 1%



What It Means to You

- ✓ Acceptance of unquantified risk and decreased SOC effectiveness
- ✓ Acceptance of quantified risk
- ✓ Elimination of false positives at scale and optimal SOC team efficiency

We resolve
99%
of alerts

We escalate
0.1%
of alerts

We reduce customer
investigation time by
an average of

99.3%*

*Assumption of workload based on average of 7-minute CRITICALSTART alert investigation time. Customer workload with ZTAP and MDR is 22 hours/week. For the same volume of alert resolution without CRITICALSTART MDR service and ZTAP platform, it would take 3,179 hours/week.

© 2021 CRITICALSTART. All rights reserved.

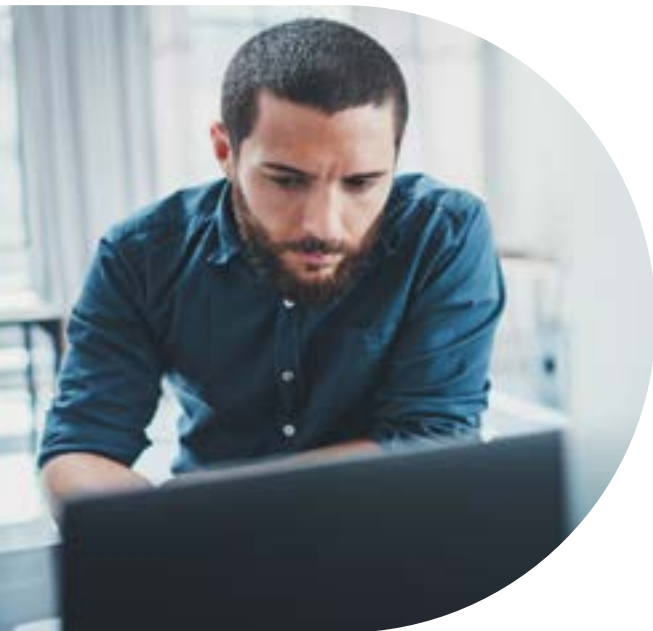
What sets us apart?



Resolving alerts is good. Resolving all alerts is better.

Our unique trust-oriented model is based on resolving every alert. CRITICALSTART MDR is driven by ZTAP, the Zero Trust Analytics Platform. ZTAP features the Trusted Behavior Registry (TBR), the largest registry of known good alerts (false positives), delivering the scalability to resolve every alert.

We take every alert from your security tools into ZTAP and match it against known good alerts in the TBR. If there is a match, the alert is automatically resolved. If there is no match, the CRITICALSTART SOC investigates the alert.



Built-in transparency

Unlike traditional MDRs that take a “black box” approach to monitoring, CRITICALSTART is transparent by design. Our ZTAP dashboard lets you see exactly what our SOC analysts see.

- ✓ You have complete visibility and access to every alert with full investigation details, every action taken – all of it can be audited and reported on.
- ✓ Beyond visibility into the service, you have visibility across your security ecosystem. You can better understand how your security tools are performing and validate the return these investments plus your MDR service.
- ✓ We can prove it with contractual SLAs for Time to Detect (TTD) and Median Time to Resolution (MTTR). Our guarantee is that we will triage every alert in minutes with a 1-hour SLA.

Not more resources. Better ones.

Leverage the collective experience of security experts with backgrounds in SIEM engineering and expertise across a broad range of security domains.

- ✓ 24x7x365 human-led investigation and response by highly skilled analysts who work in a U.S.-based SOC 2 Type 2 certified Security Operations Center (SOC).
- ✓ Rigorous training program—Every analyst completes 200 hours of training during onboarding and another 40-80 hours annually.

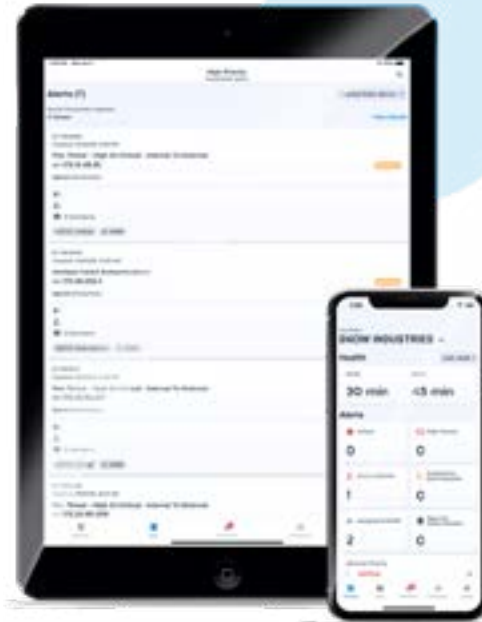




Never miss a threat. Or your desk.

Take threat detection and response on-the-go with the MOBILESOC application.

- ✓ Puts the power of ZTAP in your hands, via iOS or Android app.
- ✓ Provides on-the-go visibility and interactivity with direct communication with analysts, in-app responses and full details around the investigation – and has full parity to web.
- ✓ Allows you to contain breaches right from your phone.



We take the journey with you.

Our commitment to your security doesn't end with your deployment. We assign each new customer their own Customer Success Manager—a dedicated point of contact who is devoted to providing regular communications and concierge services, including custom reporting, feature requests, and Executive Briefing Center (EB)/roadmap reviews.

Unparalleled partnerships

CRITICALSTART integrates with best-in-breed technologies across Endpoint, SIEM, Identity, Cloud and more, to create a comprehensive security strategy with the tools you already use or that best fit your environment.

Goodbye, alert fatigue. **Hello, CRITICALSTART.**

[Contact Us](#)

[Request a Free Assessment](#)