DATASHEET

CRITICAL**START**® Security Operations Center (**SOC**)

Human-driven, AI-assisted security operations delivered 24x7x365.

KEY BENEFITS

- ✓ **See more, stop more,** with nuanced, human-driven investigations on top of AI-assisted technology.
- ✓ **Increase your team's productivity** and free up their time to focus on key security objectives by offloading Tier 1 and Tier 2 support.
- ✓ **Driven by highly experienced U.S.-based SOC analysts** with a 90% staff retention rate.
- ✓ **Communicate directly with the Critical Start SOC team** through the CORR portal, MOBILE**SOC**® app, or on the phone for consistent, personalized support and advanced threat mitigation.
- ✓ **Respond faster**, with MDR backed by industry-leading contractual SLAs for every alert, regardless of priority.
- ✓ **Unify support across multi-vendor IT and OT** environments with SOC analysts who understand your technology stack.
- ✓ **See real-time insights into SOC performance**, including analyst engagement, detection coverage, and return on investment (**ROI**) metrics.

Finding and retaining skilled cybersecurity professionals, managing immense volumes of security alerts and data, and tackling sophisticated cyber threats can overwhelm even the most well-equipped security teams. Automated tools can help alleviate some of the burdens, but overreliance on those tools can create costly blind spots and security gaps.

The CRITICAL**START**® Security Operations Center (**SOC**) provides comprehensive services, 24x7x365, including Managed Detection and Response (**MDR**), detection rule and playbook creation, alert responses, and alert reports that alleviate the burden of security management. By providing expert resources, advanced analytics, and continuous monitoring, the Critical Start SOC improves security outcomes to reduce the risk of a breach.

How it works

Critical Start's **U.S.-based SOC teams** build on a shared culture of extreme ownership and full transparency, providing consistent, human-driven detection and response. Our SOC analysts and engineers work within the same Cyber Operations Risk & Response™ (**CORR**) platform used by customers, which means you see exactly what our SOC sees. Whether auto-resolved based on our AI-assisted technology, or escalated in accordance with your tailored investigation procedures, your alert notifications will include full details, response actions at your fingertips, and immediate communication with real people—not bots. With industry-leading contractual SLAs, customizable Response Authorizations, two-person approvals (Quality Assurance) for escalations, and the "Who's on Call" feature that allows our SOC analysts to reach out directly to your team, you'll experience reliable, rapid Median Time to Resolution (**MTTR**) for greater breach prevention.

> **We could not staff a 24x7 SOC, but even if we could, we could not touch the level of service provided by Critical Start. The cost savings are huge for the value that we receive."**
>
> **– CISO, Leading U.S.-based Food Distributor**

CRITICALSTART®

Grounded in Training, Empowered by Experience

Every Critical Start SOC analyst follows the same training path. Starting with an 8-week, 300+ hour intensive training program before they can begin to analyze alerts, our analysts have expertise across a wide array of security tools and with the CORR platform itself. To keep pace with evolving tactics, techniques, and procedures (**TTPs**), we also require even our most experienced analysts to set aside five hours per week for ongoing training.

In addition, our SOC analysts work toward career advancement through a combination of required industry certifications and ongoing in-house training. The dedicated Microsoft MDR, MXDR, and Managed Sentinel SOC teams hold certifications that allow Critical Start to maintain the status criteria for both Microsoft Intelligent Security Association and Microsoft Solutions Partner for Security.

With this continuous training, clear professional growth paths, a mentally stimulating environment, and a strong work/life balance, you benefit from a 90%+ SOC analyst retention rate. That means expertise and support you can trust as you work through issues together.

We Simplify the Complex

Critical Start's SOC relies on AI-assisted and automated technology, including the Trusted Behavior Registry™ (**TBR**), benign true positive detection, and AI-accelerated incident writeups to deliver rapid, detection and response tailored to customer needs and requirements.

But Critical Start's SOC does not leave detection and response to the technology alone. Human nuance catches threats that automated systems often miss.

The Critical Start SOC relies on curated threat intelligence, in-house defined indicators of compromise, detailed playbooks, and two-person integrity reviews on every escalated alert. This high level of service is delivered within Critical Start's industry leading contractual SLAs while significantly reducing the burden of false and redundant alerts.

A True Security Partner for Your Organization

Don't leave your organization's security in the hands of blind automation and frustrating, bot-driven communications. Partner with Critical Start for a SOC team that feels like an extension of your organization and receives the experienced care, complete transparency, and human ingenuity that you should expect from your MDR provider.

Learn More

Book a demo to see how the Critical Start SOC can improve security outcomes for your organization.

CRITICALSTART®