DATASHEET

CRITICALSTART® Security Operations Center (SOC)

KEY BENEFITS

- ✓ Strengthen your security posture to more effectively defend against cyber threats.
- ✓ Deliver unmatched scalability to your security team.
- ✓ Free up your security team to focus on other projects.

We built our SOC with our customers' success in mind. Everything we do – from training to engineering to our technology platform – is focused on simplifying cybersecurity and optimizing business outcomes.

Our analysts never stop learning and improving.

The Critical Start SOC is staffed with experienced security analysts who have undergone intensive training to enable them to provide the highest caliber of support in the industry. Our security analysts must complete 300 hours of training before they analyze an alert, and even our most experienced analysts set aside ten hours every two weeks for ongoing training.

Our security analysts have MS-500: Microsoft 365 Security Administration, SC200 and AZ-500: Microsoft Security Technologies certifications, and they are also Palo Alto Networks® Cortex® XDR™ certified security experts.

Additional certifications include:

- CompTIA A+, Security+, Network+, Advanced Security Practitioner (CASP+) and Cybersecurity Analyst (CySA+)
- Certified Ethical Hacker (CEH)
- Offensive Security Certified Professional (OSCP)

It takes a village.

In addition to our dedicated team of analysts, our SOC also includes supporting teams organized by function to ensure we consistently meet or exceed our one-hour SLAs for Time to Detection (TTD) and Median Time to Resolution (MTTR):

- Our **Training team** delivers role-specific training to make it easy for our analysts to progress in their careers and increase the quality of the service they provide to our customers.
- Our **Engineering team** develops additional features to enhance the overall benefits of our Zero Trust Analytics Platform™ (ZTAP™) and other integrated solutions and assists our SOC analysts in their efforts to resolve all alerts. Within this group, our Security Orchestration and Response (SOAR) Engineers maintain and grow our Trusted Behavior Registry™ (TBR) and provide quality assurance for entry-level analysts.
- Our highly skilled **Incident team** performs the most advanced investigations and works with our Cyber Incident Response Team (CIRT) to heighten the fidelity of detections in the TBR. This team is constantly testing itself from a non-biased perspective through Threat Hunting and making necessary improvements.

CRITICALSTART®

We simplify the complex.

Critical Start SOC analysts triage and investigate unknown alerts that are not auto resolved by ZTAP and the TBR. First, these analysts determine the scope of the problem to build a full narrative of the threat, and then they communicate and collaborate with your security team through ZTAP and MOBILE**SOC**®, our iOS and Android app. Based on their investigation, they assign a priority to the alert and advise your team on recommended actions, such as removing malicious files, terminating suspicious processes, and blacklisting questionable domains. Depending on mutually agreed-upon rules of engagement, our SOC analysts can also use your tools and our platform to contain and respond to alerts on your behalf.

Zero Trust Analytics Platform (ZTAP) automatically resolves >99.9% of all alerts

On average, we ingest more than 14,000 alerts per customer per day and **escalate only one alert per customer per day.**

CRITICAL**START** SOC escalates only <0.01% of all alerts to our customer

Check out what our customers are saying about us.

"I can go to sleep knowing that someone is watching what's happening in my network"

GLOBAL EXECUTIVE TALENT LEADER

"The value of this far outweighs any cost. And you really can't put a price on the peace of mind you get from knowing you can rely on this level of expertise."

IT DIRECTOR, INTERNATIONAL MANUFACTURING ORGANIZATION

Elite SOC capabilities, at your service.

Whether you are looking to expand the capacity of your SOC, optimize the efficiency of your tools, or both, our team of experts stands ready to extend the detection and response capabilities of your cyber security operations 24x7x365 through real-time monitoring, rapid investigation, and proactive response to alerts, with full-scale, complete alert resolution.

Our SOC experts tailor the service to your unique needs and become an extension of your team, seeking to deeply understand your environment to detect and investigate the right threats, helping you make faster, more accurate decisions on which response actions to take.

Unlike other MDR vendors who struggle with high employee turnover in their SOCs, ours has a retention rate of more than 90%. We provide our SOC analysts with flexible shifts that rotate on a regular basis to promote work/life balance, so you are always working with a consistent, committed crew.