DATASHEET

CRITICALSTART® Risk & Security Operations Center (**RSOC**)

KEY BENEFITS

- ✓ Strengthen your security posture by staying ahead of emerging cyber threats
- ✓ Augment the capabilities of your in-house SOC and free up their time to focus on other priorities by offloading Tier 1 and Tier 2 support
- ✓ Reduce time between detection and response by eliminating false positives, simplifying investigation, and expediting the response process
- ✓ Deliver unmatched scalability paired with consistent, high-quality service to your security team

Critical Start's Risk & Security Operations Centers

We built our U.S.-based Risk and Security Operations Centers (**RSOCs**) with our customers' success in mind. Everything we do—from training to engineering to our **Cyber Operations Risk & Response™ platform**—is focused on reducing risk, maximizing threat detection and response services, and optimizing business outcomes. Our RSOC analysts provide expert, **24x7x365** response to validated threats and are always available on the go through our MOBILE**SOC**® iOS and Android app.

Our analysts are always learning and improving

Our experienced security analysts undergo intensive training, enabling them to provide the highest caliber of support in the industry. They must complete an **8-week**, **300+ hour** intensive training program before they reach the level of expertise Critical Start requires to begin analyzing alerts, and even then we require a **two-person integrity review** on every action to be taken to ensure RSOC orchestration quality control for every customer. To keep pace with evolving tactics, techniques, and procedures (**TTPs**), we also require even our most experienced analysts to set aside ten hours every two weeks for ongoing training.

Critical Start certification requirements

Our RSOC teams are built on the concept of extreme ownership, providing our analysts with a supportive, professionally stimulating environment and a strong work/life balance, which in turn benefits our customers by ensuring they are always working with a consistent, committed crew.

Every analyst has the ability to grow their career after meeting certain prerequisites, including achieving specific certifications required for advanced roles.

ROLE	MINIMUM CERTIFICATION REQUIRED
Senior SOC Engineer	CASP+ Certification or Equivalent/Higher
Lead Analyst	
RSOC Engineer Team Lead	CySA+ Certification or Equivalent/Higher
RSOC Engineer	
Principal RSOC Analyst	
Senior Security Analyst	Security+ Certification or Equivalent/Higher
Analyst	Training Requirement Only

In addition to many of our lead analysts being CompTIA A+, Security+, Network+, Advanced Security Practitioner (**CASP+**), and Cybersecurity Analyst (**CySA+**) certified, we have a dedicated group with in-depth Microsoft expertise, including AZ-500 Azure Security Engineer Associate, SC200 Security Operations Analyst Associate, and SC300 Identity and Access Administrator Associate certifications.

Additional certifications held by our analysts include (but are not limited to):

- Certified Ethical Hacker (**CEH**)
- Offensive Security Certified Professional (**OSCP**)
- Vendor Product Certifications

Organizational attestations include:

- SOC 2 Type II: Statement on Standards for Attestation Engagements 18 (SSAE18)
- PCI-DSS: Payment Card Industry Data Security Standard

© 2024 CRITICALSTART. All rights reserved.

It takes a village

In addition to our dedicated team of analysts, our RSOC also includes supporting teams organized by function to ensure we consistently meet or exceed our contractually obligated **10-minute notification** for Critical alerts and a **60-minute or less** Median Time to Resolution (**MTTR**) SLAs for all alerts, regardless of priority:

- **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
- **Engineering Team:** Develops additional features to enhance the overall benefits of our **Cyber Operations Risk & Response™ platform**, and other integrated solutions and assists our RSOC analysts in their efforts to resolve all alerts. Within this group, our RSOC Engineers also help 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 the Critical Start Cyber Incident Response Team (**CIRT**) to heighten the fidelity of detections in the TBR.

We simplify the complex

Regardless of priority, all unknown alerts that are not auto-resolved by our platform and the TBR are triaged and investigated by our security analysts.

First, our 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 our platform and MobileSOC. 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 RSOC analysts can also use your tools and our platform to contain and respond to alerts on your behalf.

Our platform 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 RSOC escalates only <0.01% of all alerts to our customers.

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 RSOC capabilities, at your service

Whether you are looking to expand the capacity of your SOC, optimize the efficiency of your tools, or mitigate risk, 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, with full-scale, complete alert resolution.

Our RSOC experts tailor our services to your unique needs and become an extension of your team, seeking to understand the complex nuances of your environment to detect and investigate the right threats, helping you make faster, more accurate decisions on which response actions to take so you can stay protected and sleep better at night.

To see how we can help, contact us at criticalstart.com/contact

criticalstart.com

© 2024 CRITICALSTART. All rights reserved.

CRITICALSTART®