



WHY CRITICAL START?

- Zero Trust security model ensures all threats are filtered, categorized and investigated
- Mobile interaction model - access detailed security information from anywhere via mobile device
- Patent-pending event orchestration platform allows customization for each customer
- Highly trained CyberSOC security analysts perform investigations, reducing the number of escalated alerts
- Transparent deployment and configuration lets customers view everything our CyberSOC team sees

MOBILE SOC™ PRODUCTIVITY ON THE GO

Critical Start has revolutionized the interaction model between managed security services provider (MSSP) and customer. Now you can investigate, escalate, and remediate security incidents from anywhere using the Mobile SOC™ app, only available from Critical Start.

criticalstart.com/mobile-soc

Zero Trust MSSP

Comprehensive Cybersecurity Coverage

Critical Start provides an effective, fully managed security operations center complete with security event management, security orchestration, incident response workflow, SOC reporting, and best-of-breed security controls that are fully operationalized and automated.

NO GOOD THREATS

Powered by an advanced Alert Classification Engine, Critical Start's unique approach to MSSP uses a "Zero Trust" security model to boost the effectiveness of our threat hunting. Rather than assuming any events are known good, our Zero Trust approach assumes every unknown or uncategorized security event is considered anomalous and should be investigated.

COMPLETE & EFFECTIVE

Some legacy MSSPs turn off log sources or lower alert thresholds to limit incident "noise." But these tactics also limit visibility. Others bombard customers by escalating an

overwhelming number of unfiltered or unnecessary alerts.

At Critical Start, we can handle the noise without taxing our customers or missing critical events. Our orchestration model accepts all of your data, then sorts, categorizes, and eliminates security events so that only unknown or anomalous events are produced. The result? Security monitoring that's more efficient, effective and comprehensive.

CUSTOM EVENT ORCHESTRATION

Our advanced event orchestration model enables us to tune and adjust our MSSP tools to adapt to customer networks and environment and in turn reduce the number of false positives. We tailor our deployment architecture, maintenance, updates and configurations to suit individual customer needs. Our approach includes building customized playbooks. We build filters and establish a known good baseline for the environment.

Not all MSSPs are created equal.

Discover a new standard for service, quality and coverage.

MANAGED SECURITY SERVICES

THE NETWORK EFFECT

We view every incident as an opportunity to use supervised learning to improve baselines. Our cloud-based multi-tenant system uses crowd sourcing that enables us to share common alert classification data across the systems we monitor. This approach creates a network effect, multiplying knowledge, machine learning and ultimately, security effectiveness.

SOC IN THE CLOUD

By leveraging a cloud-based architecture, we can offer maximum speed and agility, as well as maintain our distance from your on-prem systems, ensuring our security monitoring activities do not interfere with your day-to-day operations.

24X7 CYBERSOC MONITORING

For customers who want comprehensive, around-the-clock monitoring and investigation, we offer the Critical Start **CyberSOC**, our dedicated team of experienced and highly trained security analysts who perform 90% of incident investigations. With CyberSOC as an extension of your team, you'll see a significant reduction in the number of escalated incidents that require your attention.

TRANSPARENT OPERATIONS

Our entire process is completely transparent to our customers. You have access to the same consoles, dashboards and reports as our analysts. No smoke and mirrors or hidden, magic codes behind the curtain. See your security solutions at work, anytime, anywhere.

BEST-OF-BREED TOOLS

Our MSSP technology stack includes solutions for SIEM, endpoint detection and response, network security and vulnerability management. For maximum flexibility, our approach enables us to change and adapt to new or different technologies, as market and customer needs evolve.

START NOW

Ready to experience a new standard for Managed Security Services? Contact us today at **877.684.2077** or email info@criticalstart.com.

MSSP SERVICE OPTIONS

Managed SIEM with Splunk

Continuous Cyber Exposure Monitoring with Tenable.io

IDS and Full Packet Capture with ProtectWise

Managed EDR with Carbon Black Response

Carbon Black Defense

CylancePROTECT

CylanceOPTICS

Vulnerability Management with Tenable.io

Phishing and Training Services

Managed DNS Firewall – Cisco Umbrella (OpenDNS)

Palo Alto Networks Firewall Monitoring

Web Application Firewall (WAF)

Cloud Infrastructure Security Monitoring with RedLock.io

Cyberthreat intelligence and incident mitigation with Intsigths

CyberSOC support with 24x7 monitoring and investigation of all security events

Critical Start is a cybersecurity company committed to using a strategy-based approach to improve the security capabilities of our clients. We're 100% owned by employees who are passionate about cybersecurity, customer success and doing the right thing. For more on what sets us apart, visit www.criticalstart.com

STRATEGY | ASSESSMENTS | IMPLEMENTATION | MSSP | TRAINING



6100 Tennyson Pkwy, Suite 250
Plano, Texas 75024
Phone: 877-684-2077
info@criticalstart.com
criticalstart.com