CRITICAL**START** ⏻

MDR for MSP and MSSP

It's Time to Rethink Managed Detection and Response

> Your customers look to you for security that actually mitigates breaches. Through CRITICAL**START**™, you can leverage MDR services to effectively detect and resolve every alert. This can reduce your customer's security events, with zero duplicate events, supported by 100% workflow and decision visibility for your both team and theirs.

Security Shortcomings in Traditional MDR

You need to safeguard your customer's networks. Managed Detection and Response (MDR) is one of the most effective strategies to accomplish that goal. But traditional MDR can still fall short, as most vendors typically take one of two approaches to deal with the sheer volume of alerts:

• They disable detection logic to stop alerts that they feel do not need attention.

• They rank the alerts (critical, high, medium, low or informational) and only focus on the alerts that appear critical, or maybe high if they have the time.

The problem with these strategies is that attackers being detected are often appearing through medium, low and even informational alerts, not just the higher priority notifications. A top-down approach to dealing with alerts is simply not sufficient in today's threat environment.

What Does Your Customer Need Today?

Each company has different technology and business challenges. That's why CRITICALSTART offers a range of professional services to fit your customers' unique technology environments. Through our professional services, we will:

Advise

Our cybersecurity experts will develop a holistic security strategy that encompasses your customers' unique business requirements.

Implement

We'll integrate technical solutions into your customers' environment efficiently and effectively through a blended approach of deep product knowledge and implementation experience.

Assess

We'll identify risks, document the effectiveness of existing controls, and create a roadmap to improve your customers' security posture.

- CRITICAL**START** Security Operations Center (SOC) includes 24x7x365 monitoring, investigation and response with 100% transparency.
- Industry's first MOBILE**SOC** enables alert resolution from mobile devices.
- Analysts work in a SOC 2, Type 2 certified SOC to investigate, escalate, contain and respond to threats—helping to significantly reduce attacker dwell time.
- By resolving every alert without disabling the detection logic, CRITICAL**START** allows customers' security products to reach their full operational potential without accepting risk

CRITICAL**START**

Why Partner with CRITICALSTART?

Partners selling CRITICALSTART's MDR service get multiple benefits:

Gain 17% margin on registered opportunities (Unregistered discount is 5%)

Help customers operationalize their investment – decreasing competition and increasing customer satisfaction

Create stickiness in your accounts with ARR service and full support

Participate in CRITICALSTART's active customer health monitoring

Increase competitive advantage with strategic partners to capture larger market share

Unlimited scaling and ease of use means you can grow your business without draining security resources

Working with CRITICALSTART

Onboarding a customer is easy for both you and your customers. We offer:

- Short, simple sign-up with 2 required documents
- 24x7x365 monitoring means you're always covered
- Professional services including penetration testing and assessment services
- Channel-only model means we don't compete with your business
- Integration across multiple tools
- Fast onboarding process of 6-weeks or less

How to Sell CRITICALSTART

1. Quotes are obtained through distribution
   - Westcon (Synnex)
   - Ingram (Cloud Harmonics)

2. Deal registrations are opportunity-based
   - Submit via CRITICALSTART's Partner Portal

3. Services are added as line items to existing quotes
   - 2 simple SKUs; MDR services and implementation
   - Carbon Black Response and Splunk require CRITICALSTART hosting services

Services Offered
by CRITICALSTART

Beyond MDR, CRITICALSTART provides a range of testing, response and remediation services to lock down your customer's infrastructure and close potential gaps that can exploited by an attacker.

Penetration Testing

CRITICALSTART's TEAMARES use both known public exploits and custom techniques to evaluate a company's security and provide detailed assessments and recommendations for improvement.

Tool Assessment

We provide a cost-benefit analysis for the return on current security tool investments, identify gaps and vulnerabilities, and provide recommendations to improve security and efficiency in the customer's environment.

Adversarial Simulation

The TEAMARES Red Team will employ every legal and in-scope method available to access and assess the client's enterprise and network, simulating the most likely threat actor to potentially attack the customer in a real-world scenario.

Threat Hunting

CRITICALSTART's SOC works with a customer over a 30-day period to identify and escalate malicious files, suspicious script and command line activity, and other indicators of compromise within the environment. At the conclusion of the Threat Hunt, we provide a detailed report of key findings, actions taken and recommended next steps.

Incident Response

CRITICALSTART's SOC will work with a customer's security personnel to identify the scope of a breach and act directly to reduce exposure and minimize the threat. After the breach is contained, we provide a detailed report on how to prevent future compromise.

Customers can prepare now with CRITICALSTART's IR Retainer services. From detection through remediation, customers can choose professional service hours; unused hours may be applied to other IR services.

Products Supported
by CRITICALSTART

CRITICALSTART supports best-of-breed technologies that are likely already in your portfolio.

paloalto NETWORKS

Microsoft Defender ATP

CISCO

splunk>

BlackBerry CYLANCE

vmware Carbon Black.

SentinelOne

CROWDSTRIKE

To learn more about working with CRITICAL**START** and how we can redefine how your clients protect their environments against an ever-evolving threat matrix, contact **Joe Tapias**, National Director for MSPs. **Joe.Tapias@criticalstart.com | 949.874.1003**

CRITICALSTART