CRITICALSTART

Managed Detection and Response

For Channel Partners

Grow business by partnering with CRITICAL**START**™ **Managed Detection and Response (MDR) services.**

We leverage best-of-breed endpoint and SIEM technologies within our proprietary platform to effectively detect and resolve every alert.

The Limitations of Traditional MDR Services

To handle the sheer volume of alerts, most MDR vendors typically use one of two approaches:

Priority-Oriented

Ranking alerts (high, medium, low) and only focusing on the alerts that seem critical.

Input-Oriented

Disable detection logic that generates alerts – turning off the ability to see some alerts that might not seem necessary.

> These approaches might reduce the number of alerts that the team sees, but it is not effectively resolving alerts. In other words, these approaches are accepting risk.

The CRITICAL**START** Difference

CRITICAL**START** does not believe in playing the odds.

We use a **Trust-Oriented** approach to handling alerts at scale. Unlike our competitors, we “unprioritize.” In other words, we believe that every security event begins as equal. Our **Trusted Behavior Registry (TBR)** enables us to put our trust-oriented approach into action by automatically resolving what is known-good and can be safely trusted first – shifting focus to known alerts for triage and quick resolution.

24x7x365 Monitoring

Our highly skilled analysts work in a SOC 2 Type 2 certified Security Operations Center (SOC) to investigate, escalate, contain and respond to threats – helping to significantly reduce attacker dwell time.

Maintaining Operations

By resolving every alert without disabling the detection logic, CRITICAL**START** allows customers’ security products to reach their full operational potential without accepting risk.

CRITICALSTART

Products Supported by CRITICAL**START**

CRITICAL**START** supports best-of-breed technologies that are likely already in your portfolio.

paloalto NETWORKS | Windows Defender ATP | cisco | splunk>

CYLANCE | vmware Carbon Black. | SentinelOne

Why Partner with CRITICAL**START?**

Partners selling CRITICAL**START's** MDR service get multiple benefits:

- Gain 17% margin on registered opportunities*
- Create stickiness in your accounts with ARR service
- Align with key manufacturers to tell a holistic story
- Help customers operationalize their investment – decreasing competition and increasing customer satisfaction
- Participate in CRITICAL**START's** customer success team's active customer health monitoring
- Increase your competitive advantage with strategic partners

* Unregistered discount is only 5%

CRITICAL**START**

How Can I Sell with CRITICAL**START**?

1

Quotes are obtained through distribution

- Westcon (Synnex)
- Ingram (Cloud Harmonics)

2

Deal registrations are opportunity-based

- Submit via CRITICAL**START'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 CRITICAL**START** hosting services

Additional Services

> CRITICAL**START** offers other security-related services in addition to MDR. From penetration testing and security posture assessments to incident response and remediation, our security experts are here to help.

Penetration Testing

CRITICAL**START's** TEAM**ARES** use both known public exploits and custom techniques to evaluate a company's security and provide detailed assessments and recommendations for improvement.

Tool Assessment

CRITICAL**START's** security experts inventory a customer's current security products, deployment, and operational status. We provide a cost-benefit analysis for the return on current security tool investments, identify gaps, and provide recommendations to improve security and efficiency in the customer's environment.

Adversarial Simulation

The TEAM**ARES** Red Team will employ every legal and in-scope method available to access and assess the client's enterprise and network, in order to simulate the customer's most likely threat actor.

Threat Hunting

CRITICAL**START's** CYBER**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

CRITICAL**START's** CYBER**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 CRITICAL**START's** IR Retainer services. From detection through remediation, customers can choose professional service hours; unused hours may be applied to other IR services.

Become a CRITICAL**START channel partner,**
visit www.criticalstart.com

CRITICAL**START**