DATASHEET

CRITICAL**START** Managed Detection and Response vs. Cyber Incident Response Team (CIRT)

CRITICAL**START**® Managed Detection and Response (MDR) and Cyber Incident Response Team (CIRT) services are two complementary cybersecurity disciplines that address two different use cases, to enhance the value we bring to our customers.

Why CRITICAL**START?**

To simplify, we first embrace the complex. CRITICALSTART is the only managed detection and response services provider on the market today who dared to approach the problem differently. While others are focused on finding bad, we focus on finding good. While others prioritize or suppress alerts, we resolve all alerts. We bring you a team of skilled security experts who will deeply understand your environment to adapt and scale with your organization's needs and partner with you to detect, investigate and respond to threats specific to your organization. **That's how we define simple for our customers.**

CRITICAL**START**® MDR delivers **24x7x365** security monitoring. This service monitors alerts from security tools, including EDR/ EPP, XDR, Identity, and SIEM, and uses the tools' capabilities to investigate and respond to alerts and contain threats as they happen.

CRITICAL**START's MDR Service partners with our customers to:**

- ✓ Contain true-positive threats using the isolation capabilities of endpoint protection tools, as defined by the customer's rules of engagement.
- ✓ Identify indicators on true-positive assets.
- ✓ Threat hunt true-positive indicators to identify other compromised devices.
- ✓ Escalate alerts for business-critical assets where direct response options are not authorized.

CRITICAL**START's** Cyber Incident Response Team (CIRT) service manages the aftermath of a security breach, employing additional tools to perform forensics that identify the source of the attack and help restore the organization to resume business operations.

Our CIRT team works with our MDR team and our customers to:

- ✓ Act on incidents involving business-critical assets.
- ✓ Perform memory and hard disk forensics and copying.
- ✓ Hunt for issues discovered during the forensics process and identify net-new issues that could be a part of the breach.
- ✓ Provide recommendations and expert testimony for incidents involving litigation.
- ✓ Provide compliance disclosure guidance.

CRITICAL**START** MDR and and CIRT services can be used together to protect critical assets and business operations from catastrophic breaches, ransomware, and other malicious activity. Incident Response picks up where MDR ends. Our teams work together to detect the right threats, respond with the right actions, and provide agility and adaptability.

Contact Us

Request a Free Assessment

CRITICALSTART®