DATASHEET

CRITICAL**START** Managed Detection and Response VS Incident Response

CRITICAL**START**™ Managed Detection and Response (MDR) and Incident Response (IR) services are two distinct cybersecurity disciplines addressing two different use cases. They are complimentary services that increase the capabilities we deliver to our clients.

CRITICAL**START** is leading the way in Managed Detection and Response (MDR) services. Our Trusted Behavior Registry reviews every alert to determine if it was generated by known-good behavior versus unknown behaviors that need to be investigated by our analysts. This allows us to resolve every alert and stop accepting risk – leveraging our transparent platform and native iOS and Android mobile apps.

CRITICAL**START** MDR delivers 24/7/365 security monitoring. The service monitors alerts from security tools, including EPP, EDR, XDR 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 clients to:

- ✓ Contain true-positive threats using the isolation capabilities of endpoint protection tools, as defined by client 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** Incident Response 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.

CRITICAL**START's** Incident Response team works with our MDR team and our clients 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 Incident Response 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 ensure a seamless transition between to resolve security events efficiently and effectively.

Goodbye, alert fatigue. Hello, CRITICALSTART.

Contact Us

Request a Free Assessment

CRITICALSTART
They're good. We're better.