SOLUTION QUICK CARD

CRITICAL**START**® Incident Response Monitoring

BENEFITS OF PARTNERSHIP:

- ✓ We take on the most tedious aspects of your security operations **24x7x365**
- ✓ Our solution integrates with existing EDRs so there is no need to rip them out
- ✓ We do the monitoring, so your forensics team doesn't have to
- ✓ Cut down alert frequency by approximately 80-95% within 72 hours, allowing you to concentrate on genuine issues rather than false positives
- ✓ Enables your team to take on more investigations using the same number of staff
- ✓ Referral fees are available for cross-sale into other Critical Start services

Concentrate on what you do best while we handle the rest.

Secure your customers' environment during the critical aftermath of a breach, safeguarding them in their most vulnerable state. Prevent the aftershocks from repeat attacks on the same vulnerabilities.

Critical Start Incident Response Monitoring delivers just that. Our service:

- Harnesses the power of our **Cyber Operations Risk & Response™ platform** 24x7x365 to help identify, contain, and remediate threats
- Leverages global and customized/personalized playbooks and threat intelligence
- Context-based alert prioritization tuned from each customer's threat assessment and business impact analysis
- Delivers optional restoration and data mining services

Key Benefits for YOUR Incident Response Team

- **Reduce risk exposure:** Identify unknown attacker's Tactics, Techniques, and Procedures (**TTPs**) through the application of TTP playbooks and tuning of automated alerts and blocking mechanisms
- **Total immersion:** Direct your attention to crucial aspects of the investigation while we handle the 24x7x365 monitoring responsibilities
- **Protected communications:** Use our MOBILE**SOC**® app for encrypted out-of-band communication to ensure secure communication and efficient alert routing during an investigation
- **Elevated insights:** Utilize threat intelligence obtained from our customer base and conduct peer benchmarking to compare the security posture of your customer against that of similar businesses
- **Multi-EDR integrations**: Our solution sits on top of the customer's EDR, which allows you to handle multiple EDRs in the same environment

Key Benefit for YOUR Customers

- Prevent inevitable repeat attacks on your customer
- Deploy free EDR solution for 30 days at no cost to the customer—we work with Microsoft Defender, CrowdStrike, SentinelOne, and other leading EDR products
- Seamless transition into managed detection and response without additional onboarding or tune-up

CRITICALSTART®