SOLUTION QUICK CARD

CRITICAL**START**® Managed Detection and Response Services for SentinelOne Singularity™ XDR Platform

KEY BENEFITS

- ✓ **Team expansion**
  Threat detection and response security expertise at your side, at your service 24x7
- ✓ **Reduce the noise**
  Fewer false positives over time results in reduced alert fatigue
- ✓ **Improve security posture**
  Expanded detection, mapped to the MITRE ATT&CK® Framework
- ✓ **Increase SOC efficiency & productivity**
  Between our ZTAP platform, SOC and threat intelligence experts, we do all the heavy lifting for you

At CRITICAL**START**®, we take a different approach to managed detection and response by simplifying your operations. With 24x7x365 expert security analysts at the ready, the only technology in the industry that resolves every alert, and threat detections and intelligence from our Cyber Research Unit (CRU) being added to your SentinelOne security tool, we help you effectively stop breaches.

Solution

Critical Start MDR Services for SentinelOne Singularity allows you to:

- Investigate and respond to threats to prevent breaches
- Increase Security Operations Center (SOC) efficiency
- Boost the effectiveness of your security tools to mature your SentinelOne investment

How it works

Every alert is ingested from SentinelOne Singularity into the Zero Trust Analytics Platform™ (ZTAP™), the backbone of our MDR service. Alerts are compared against known good behaviors in the Trusted Behavior Registry™ (TBR) where playbooks auto-resolve known good alerts. Alerts not identified by the TBR are escalated to the Critical Start SOC for further enrichment and investigation enabling you to make a more accurate decision on which response action to take. Critical Start can take response actions on your behalf and we work with you until remediation is complete.