SOLUTION QUICK CARD

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

## KEY BENEFITS

✓ **Increase team efficacy**
Rely on 24x7x365 threat detection and response security expertise at your side or on the go with our MOBILE**SOC**® app

✓ **Guaranteed quick response**
Contractual SLAs of 10-minute notification for Critical alerts and a 60-minute or less Median Time to Resolution (**MTTR**) for all alerts, regardless of criticality

✓ **Ensure security controls are in place and working**
Endpoint Coverage Gaps ensures all expected threat signals are received

✓ **Focus only on true-positives**
Fewer false positives over time results in reduced alert fatigue and enables your team to prioritize true-positive alerts

✓ **Reduce risk & improve security posture**
Expanded detection, mapped to the **MITRE ATT&CK® Framework**

✓ **Increase in-house SOC efficiency & productivity**
Between our CORR platform, Risk & Security Operations Cente (**RSOC**) analysts, and threat intelligence experts, we do all the heavy lifting for you

At Critical Start we take a risk-based approach to Managed Detection and Response (**MDR**) to prevent breaches and stop business disruption. With **24x7x365** expert security analysts at the ready, the only technology in the industry that resolves every alert regardless of criticality, and threat detections and intelligence from our Cyber Research Unit (**CRU**) continuously added to your SentinelOne security tool, we help you reduce cyber risk and increase your security posture.

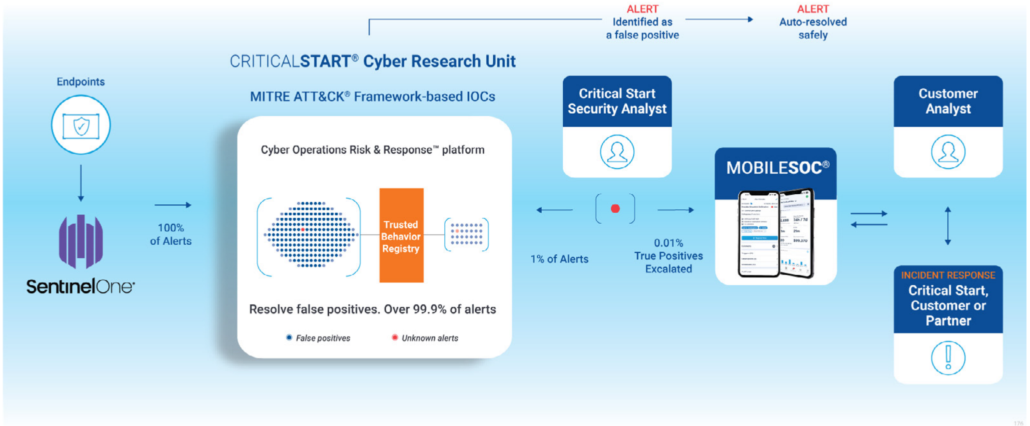
## Solution

**Critical Start MDR Services for SentinelOne Singularity allows you to:**

- Ensure security controls are in place and working as expected
- 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 our **Cyber Operations Risk & Response™ (CORR) platform**, 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 Risk & Security Operations Center (**RSOC**) 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.


ALERT
Identified as a false positive
ALERT
Auto-resolved safely
CRITICALSTART® Cyber Research Unit
MITRE ATT&CK® Framework-based IOCs
Endpoints
SentinelOne
100% of Alerts
Cyber Operations Risk & Response™ platform
Trusted Behavior Registry
Resolve false positives. Over 99.9% of alerts
False positives
Unknown alerts
Critical Start Security Analyst
1% of Alerts
0.01% True Positives Escalated
MOBILESOC®
Customer Analyst
INCIDENT RESPONSE
Critical Start, Customer or Partner

criticalstart.com