SOLUTION QUICK CARD

CRITICALSTART® Managed Detection & Response Services for CrowdStrike Falcon Endpoint 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 platform, RSOC 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 CrowdStrike security tool, we help you effectively stop breaches.

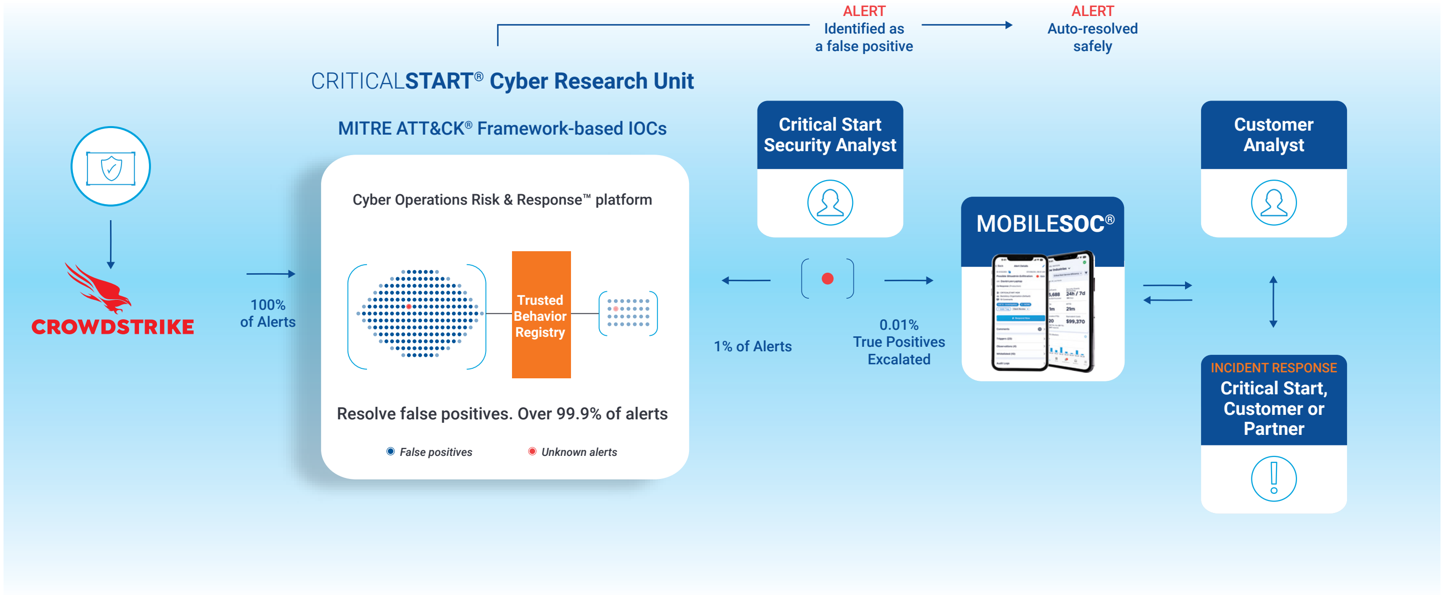
Solution

Critical Start MDR Services for CrowdStrike Falcon Endpoint Platform 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 return on your CrowdStrike investment

How it works

Every alert is ingested from CrowdStrike Falcon Endpoint into the **Cyber Operations Risk & Response™ 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
Cyber Operations Risk & Response™ platform
Trusted Behavior Registry
Resolve false positives. Over 99.9% of alerts
False positives
Unknown alerts
CROWDSTRIKE
100% of Alerts
Critical Start Security Analyst
1% of Alerts
0.01% True Positives Escalated
MOBILESOC®
Customer Analyst
INCIDENT RESPONSE
Critical Start, Customer or Partner

*Based on our platform ingesting 15,000 alerts/customer/day on average

criticalstart.com