DATASHEET

CRITICAL**START**® Managed Detection and Response Services for Palo Alto Networks® Cortex XDR®

KEY BENEFITS

- ✓ Team expansion with Cortex XDR security expertise
- ✓ Identify Endpoint Coverage Gaps to help you reduce the risk of endpoint compromise
- ✓ Every endpoint incident investigated
- ✓ 60-minute or less SLAs for Time to Detect (**TTD**) and Median Time to Resolution (**MTTR**)
- ✓ Personalized playbooks for your unique business needs
- ✓ 100% consolidated visibility into a single portal
- ✓ Accelerate value from your Cortex XDR technology with tool configuration and tooling
- ✓ Triage and contain attacks anytime, from anywhere with MOBILE**SOC**®

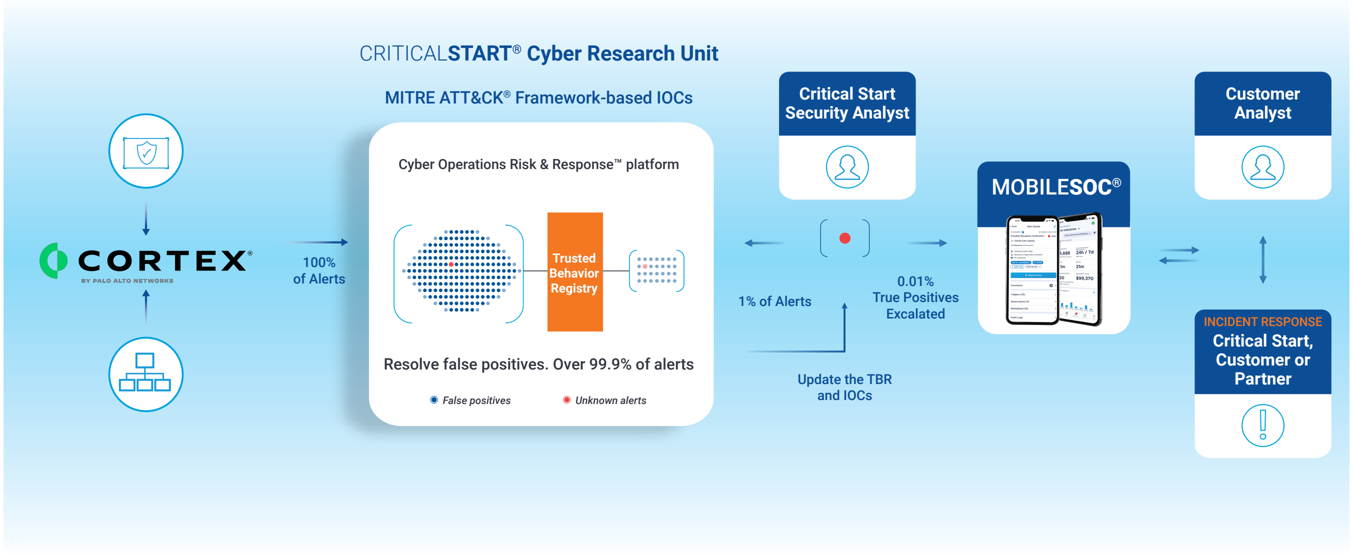
At Critical Start, our risk-based Managed Detection and Response (**MDR**) service is all about streamlining your security and increasing your Return on Investment (**ROI**).

We help you identify threats across hybrid devices and operating systems to stop the most advanced attacks, reduce risk exposure, eliminate alert fatigue, and optimize Security Operations Center (**SOC**) efficiency.

Our MDR service for Palo Alto Networks Cortex XDR goes beyond monitoring alerts by providing you with **24x7x365** expert security analysts at the ready, the only technology in the industry that resolves every alert (regardless of criticality), and additional threat detections and intelligence curated by our Cyber Research Unit (**CRU**) to your Cortex XDR technology.

We detect and investigate the right threats.

Critical Start does this by ingesting every endpoint incident from Cortex XDR into our **Cyber Operations Risk & Response™ platform**, the backbone of our MDR service. We compare alerts against known good behaviors in our Trusted Behavior Registry® (**TBR**®) where playbooks auto-resolve known good alerts. Alerts not identified by the TBR are escalated for investigation to our Risk & Security Operations Center (**RSOC**) where our human-led service helps you make more accurate decisions on which response action to take, helping you mitigate breaches and stop business disruption.


CRITICALSTART® Cyber Research Unit
MITRE ATT&CK® Framework-based IOCs
CORTEX®
BY PALO ALTO NETWORKS
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 Excalated
Update the TBR and IOCs
MOBILESOC®
Customer Analyst
INCIDENT RESPONSE
Critical Start, Customer or Partner

criticalstart.com

HOW WE DO IT

Reduce risk with expanded MDR capabilities.

✓ Critical Start MDR services, delivered through our deep integration with Palo Alto Networks Cortex XDR technology, go beyond a reactive, threat-based approach to provide additional capabilities aligned to proactive security.

✓ These include closing Endpoint control coverage gaps and providing essential **MITRE ATT&CK® Mitigations** recommendations.

Resolving alerts is good. Resolving all alerts is better.

✓ Trust oriented approach leverages the power of our platform and TBR to investigate every Cortex XDR Incident when triggered at the endpoint

✓ We resolve more than **99.9%** of alerts

✓ We escalate less than **0.01%** of alerts—the alerts that really require the attention of your security team

Integration, the better way.

MDR services for Cortex XDR leverage a bi-directional integration

✓ With Palo Alto Networks Cortex XDR Prevent and Pro

✓ Between our platform and Cortex XSOAR that will centralize your data, provide visibility via a synchronized "single pane of glass," and fit right into your existing workflows

Elite RSOC capabilities, at your side, at your service.

Whether you are looking to expand the capacity of your SOC, optimize the efficiency of Cortex XDR, or both, our team of Cortex XDR certified security experts stand ready to extend the detection and response capabilities of you cyber security operations **24x7x365** through real-time monitoring, rapid investigation, and proactive response to endpoint alerts, with full-scale, complete alert resolution.

So long, tedious IOC Management. Hello optimized rules.

A key feature of the MDR service for Cortex XDR is the management, maintenance, curation of:

✓ Cortex XDR out-of-the-box detections and Behavioral Indicators of Compromise (**BIOCs**)

✓ Original and third-party threat intelligence used to develop new detections and Indicators of Compromise (**IOCs**)

✓ **MITRE ATT&CK® Framework**-based Critical Start proprietary detections and Indicators of Compromise (**IOCs**).

Never miss a threat. Or your desk with MobileSOC.

Reduce attacker dwell time when you take threat detection on the go with our Mobile**SOC** application, an iOS and Android app that puts the power of the Our platform in your hands, giving you the ability to triage, escalate, and isolate attacks from your phone. With Mobile**SOC**, you're able to see the full alert data that we see, can communicate directly with Critical Start RSOC senior security analysts in-app, and can take immediate action with information gathered by tools and in coordination with your MDR team.