DATASHEET

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

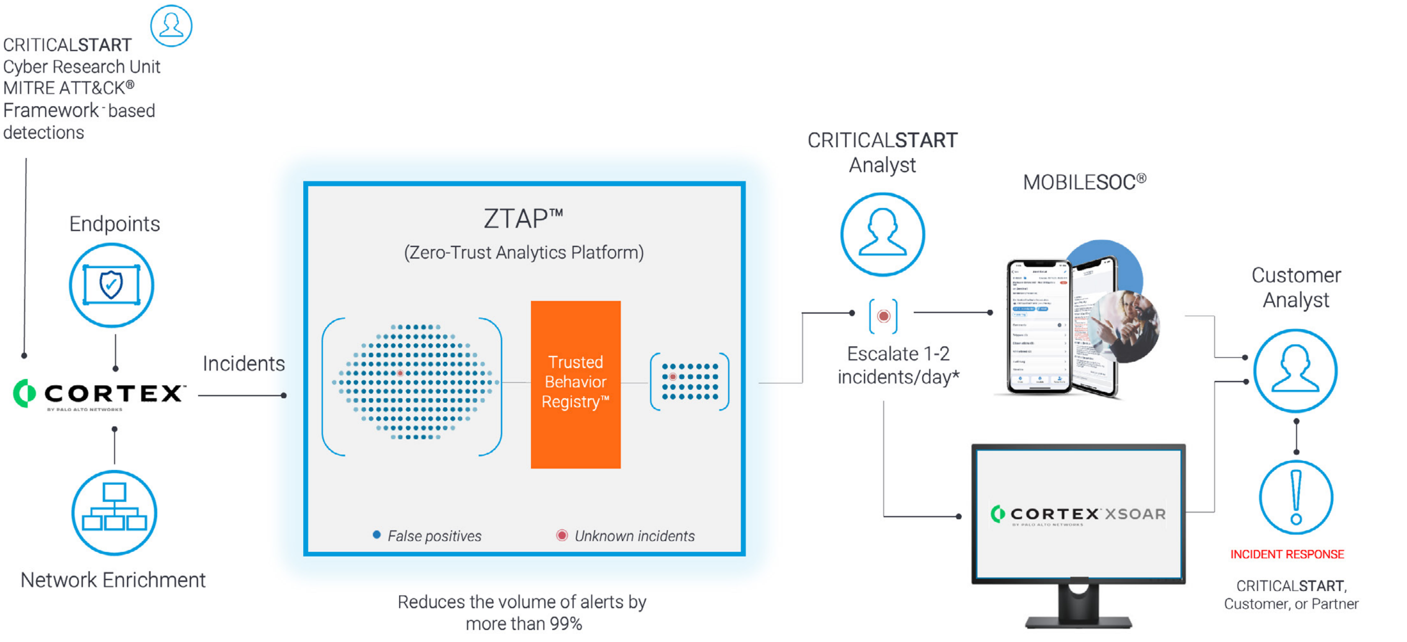
KEY BENEFITS

- ✓ Team expansion with Cortex XDR™ security expertise
- ✓ Every endpoint incident investigated
- ✓ Guaranteed 1-hour SLA for Time-to-Detect and Median-Time-to-Resolution
- ✓ Personalized playbooks and SOC operations
- ✓ 100% consolidated visibility into a single portal
- ✓ Tool configuration and tuning
- ✓ Triage and contain attacks anytime, from anywhere with MOBILE**SOC**®

At CRITICAL**START**®, our managed detection and response (MDR) service is all about simplifying your security. We built our MDR service for Palo Alto Networks Cortex XDR to go beyond monitoring alerts. We help customers see attacks across hybrid device types and operating systems to stop the most advanced attacks, reduce risk exposure, eliminate alert fatigue, and optimize security operations center (SOC) efficiency.

We detect and investigate the right threats.

CRITICAL**START** does this by ingesting every endpoint incident from Cortex XDR into the Zero Trust Analytics Platform™ (ZTAP™), the backbone of our MDR service. We compare alerts 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 for investigation to the SOC where our human-led service helps you make more accurate decisions on which response action to take.



Reduces the volume of alerts by more than 99%

* Based on ZTAP ingesting 15,000 alerts/client/day on average

How we do it
Resolving alerts is good. Resolving all alerts is better.

- ✓ Trust oriented approach leverages the power of ZTAP and TBR to investigate every Cortex XDR Incident when triggered at the endpoint
- ✓ We resolve more than **99%** 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 ZTAP 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 SOC 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 near 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.

Take threat detection and response on-the-go with our MOBILE**SOC** application, an iOS and Android app that puts the power of the ZTAP 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** SOC senior security analysts in-app and can take immediate action with information gathered by tools and in coordination with your MDR team.

Contact Us

Request a Free Assessment

CRITICALSTART®