DATASHEET

CRITICALSTART® Managed Detection and Response Services for Palo Alto Networks Cortex XSIAM for Endpoint

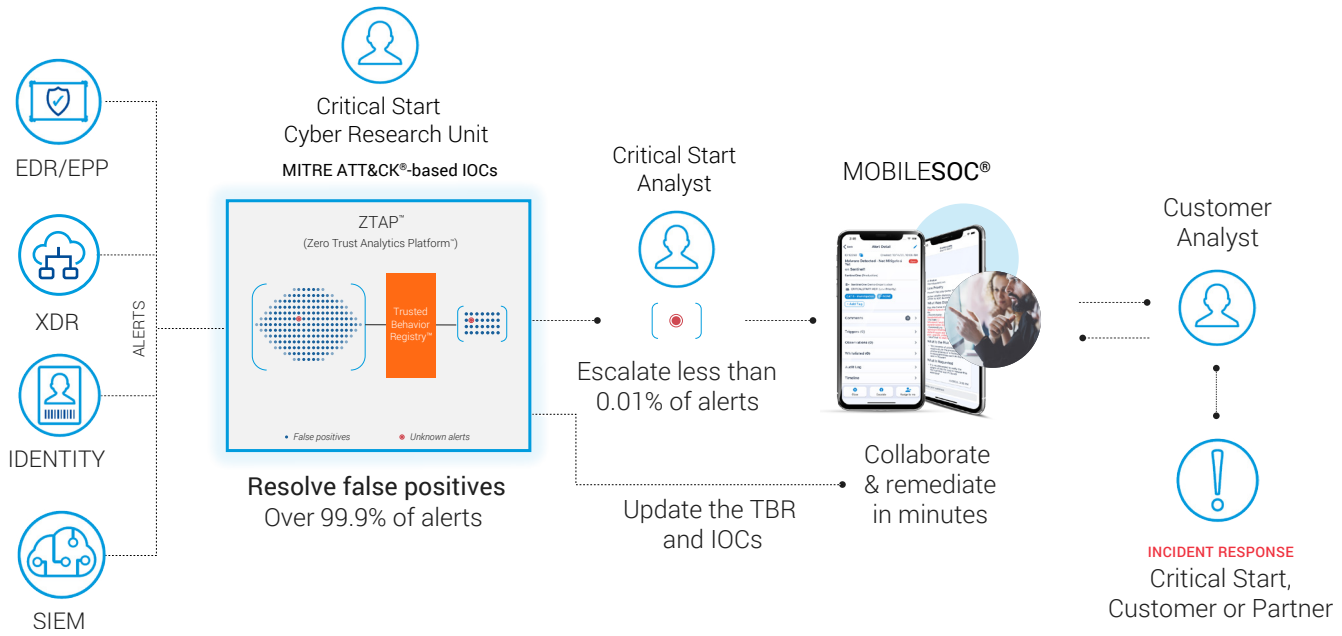
KEY BENEFITS

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

At Critical Start, our managed detection and response (MDR) service is all about simplifying your security and providing across-the-board support to you during your new implementation or migration to Cortex XSIAM. As a Palo Alto Networks® Cortex® XSIAM™ early access design partner, Critical Start worked side-by-side with the Cortex XSIAM Product, Engineering and Go to Market teams, and shadowed Cortex XSIAM customers during their implementation. As a result, Critical Start possesses the infrastructure, firsthand experience, and technical expertise with Cortex XSIAM that few other MDR services possess.

Detect and investigate the right threats.

Critical Start does this by ingesting every endpoint incident from Cortex XSIAM into the Zero Trust Analytics Platform™ (ZTAP™), the backbone of our MDR service. We compare incidents against known good behaviors in the Trusted Behavior Registry™ (TBR) where playbooks auto-resolve known good incidents. Incidents not identified by the TBR are escalated for investigation to the SOC where our experts can help you make more accurate decisions and take response actions on your behalf. Best of all, we stand at your side and work with you until remediation is complete.



CRITICALSTART®

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 XSIAM 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 XSIAM that leverage an integration

- ✓ With Palo Alto Networks Cortex XSIAM

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

Whether you are looking to expand the capacity of your SOC, migrate to or optimize the efficiency of Cortex XSIAM, our team of Cortex 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 incidents, with full-scale, complete alert resolution.

So long, tedious IOC Management. Hello optimized rules.

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

- ✓ Out- of-the-box threat detections and rules and Behavioral Indicators of Compromise (BIOC)
- ✓ Original and third-party threat intelligence, mapped to the MITRE ATT&CK® Framework, are used to develop new detections and BIOCs

Never miss a threat. Or your desk with MOBILESOC.

Take threat detection and response on-the-go with our MobileSOC 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 MobileSOC, 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 team.