SOLUTION BRIEF

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

KEY BENEFITS

- Accelerate value from Palo Alto Networks Cortex XDR on day one
- Extend your team with threat detection and response expertise
- Reduce risk acceptance
- Speed up investigation and response in one portal
- Reduce attacker dwell time
- Triage and contain alerts from anywhere with MOBILE**SOC**™

MDR up leveled. XDR go beyond. An integrated threat detection and response solution for unrivaled security and operational efficiency that's more than good, *it's better.*

We do what others don't. The CRITICAL**START** Managed Detection and Response (MDR) service integration with Palo Alto Networks Cortex XDR™ delivers a comprehensive combination of experienced analysts and operational process that helps your security team to quickly detect, investigate and respond to every alert, and stop the most advanced attacks while reducing risk, alert fatigue, and analyst burnout. Plus, by simply augmenting in-house security protocols with MDR security experts, the painstaking process of building or refining your own security operations center (SOC) is eliminated.

Why CRITICAL**START**

Resolving alerts is good. Resolving all alerts is better.

- ✓ Our trust-oriented approach leverages the power of the Zero Trust Analytics Platform (ZTAP) and Trusted Behavior Registry (TBR) to address all alerts
- ✓ We auto-resolve more than 99% of alerts
- ✓ We escalate less than 0.1% of alerts – the alerts that really require the attention of your security team

By ingesting Cortex XDR endpoint, network, and cloud data into ZTAP, the TBR quickly establishes what data is a trigger event and what information in the alert is an observation.

Simplify security operations to stay ahead of attackers.

Unlike other managed detection and response services, CRITICAL**START** MDR services for Cortex XDR provides:

	CRITICAL**START** with Cortex XDR Pro	CRITICAL**START** with Cortex XDR Prevent
Quick and easy API integration	●	●
Prevent common malware	●	●
Alert on malware not prevented	●	●
Isolate hosts where malware was not prevented	●	●
PowerShell attack detection	●	
Script attack detection	●	
Identity analytics	●	
Behavior analytics	●	
Continuously update detection rules to catch more attacks	●	
Perform investigations and root cause analysis on compromised machines	●	
XSOAR integration	●	●

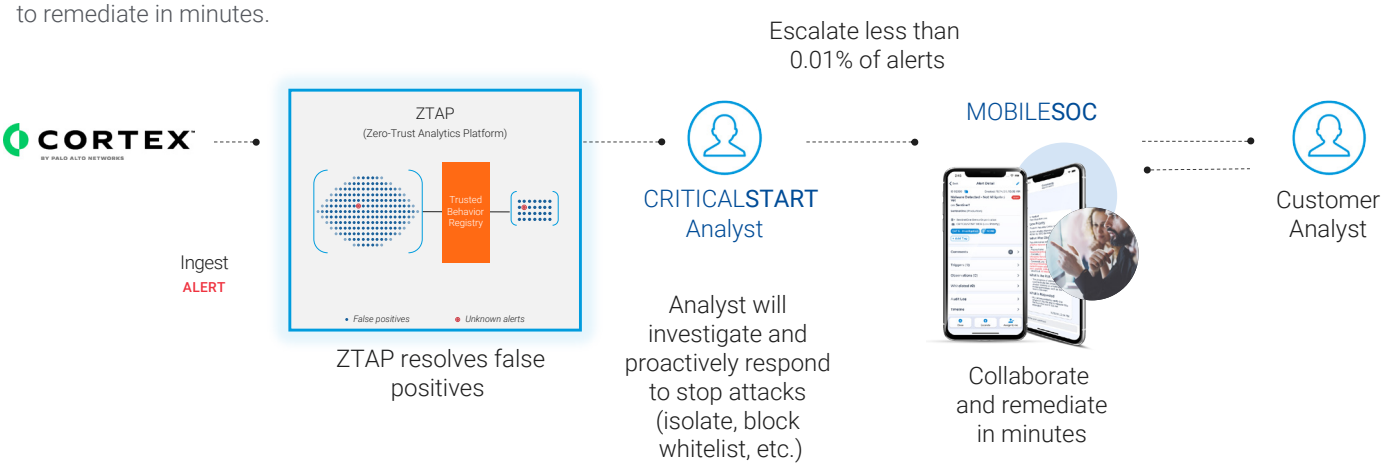
Not more resources. Better ones.

Leverage the collective experience of security experts with backgrounds in threat detection and response and expertise across a broad range of security domains.

- ✓ Cortex XDR experts' setup and manage the environment in weeks, not months
- ✓ Security analysts are rigorously trained: Complete 200 hours of training during onboarding and another 40-80 hours annually
- ✓ Provide 24x7x365 end-to-end monitoring, investigation, and response

How we do it

We take every alert from Cortex XDR into ZTAP and match it against known good patterns in the TBR. If there is a match, the alert is automatically resolved and incorporated into the TBR. If there is no match, the CRITICAL**START** Security Operations Center (SOC) investigates and proactively responds to stop the attack on your behalf. Our analysts then collaborate with you to remediate in minutes.



Automate, Collaborate and Standardize Incident Management.

A powerful bi-directional integration between CRITICAL**START** ZTAP and Cortex XSOAR will centralize your data, provide visibility via a "single pane of glass," and fit right into your existing workflows. Key features of the XSOAR integration include:

- ✓ When an alert is escalated, a XSOAR incident is created with all event details
- ✓ Direct linking to the alert/incident in Cortex XDR for additional investigation
- ✓ You can take direct action in XSOAR that is synchronized with ZTAP like:
  - ⇢ Add a comment, re-escalate back to CRITICALSTART
  - ⇢ Add a comment to the incident

Built-in transparency.

Unlike traditional MDRs that take a "black box" approach to monitoring, CRITICALSTART is transparent by design. The ZTAP dashboard lets you see what our SOC analysts see.

- ✓ You have complete visibility and access to every alert with full investigative details, every action taken – all of which can be audited and reported on
- ✓ Beyond visibility into the service, you have visibility across your security ecosystem. You can better understand how your security tools are performing and confirm the return on these investments plus your MDR service
- ✓ We prove the effectiveness of ZTAP with contractual SLAs for Time to Detect (TTD) and Median Time to Resolution (MTTR). Our guarantee is that we will triage every alert in minutes, with a 1-hour SLA

So long, tedious IOC Management. Hello optimized rules.

- ✓ A key feature of the MDR service for Cortex XDR is IOC management. IOCs are constantly published and updated. The process of publication and application of additional detections can be hard to manage and a full-time job, so we added this feature in the service for no ***added*** cost. The CRITICAL**START** Threat Detection and Engineering team enhances out-of-the box detection capabilities by developing and adding proprietary IOCs and behavioral detections from curated threat intelligence, previous SOC investigations and external threat intelligence feeds.

Never miss a threat. Or your desk.

Take threat detection and response on-the-go with our MOBILE**SOC**™ application. An industry-leading first, MOBILE**SOC** puts the power of our ZTAP platform in your hands, allowing you to contain breaches right from your phone. Our iOS and Android app features 100% transparency, with full alert detail and a timeline of all actions taken.

Capability Comparison

● COMPLETE OFFERING
◐ PARTIAL OFFERING
✕ NO OFFERING

	CRITICAL**START** powered by Palo Alto Networks Cortex XDR	Other MDR Providers
24x7x365 monitoring, investigation, and response by security analysts	●	●
Contractually guaranteed Service Level Agreement for Time to Detect and Median Time to Resolution for all alerts, regardless of priority level	●	✕
Native iOS and Android applications for alert investigation, collaboration, and response	●	✕
Customer and vendor work from the same platform and see the same information	●	◐
Custom Indicator of Attack (IOA) Monitoring	●	✕
Two-person integrity review process that provides quality control of SOC orchestration for every customer	●	✕
Manage and maintain cross-ecosystem Indicators of Compromise (IOCs)	●	✕
Continuous threat hunting	●	◐
Perform configuration, deployment, and health checks without requiring additional professional services	●	●
Alert notifications that include both security event data and expert analysis	●	◐
Analyst will proactively respond to stop attacks (isolate, block, whitelist, etc.)	●	●
Managed response, policy tuning, and updating of agents	●	●
Investigate all operating systems without agent deployment	●	✕
IOCs for Windows, Mac, and Linux	●	✕
PowerShell Live Response library	●	✕
Multi-Tenant so customer can have multiple organizations with N-level hierarchy	●	✕
Bi-directional integration with Cortex XSOAR	●	◐

DIAMOND

paloalto® NETWORKS

Goodbye, alert fatigue. Hello, CRITICALSTART**.**

Contact Us

Request a Free Assessment

CRITICAL**START**
They're good. We're better.