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

CORTEX XDR BY PALO ALTO NETWORKS

CRITICAL**START** integrates with Palo Alto Networks Cortex XDR™ Prevent and Pro to offer a 24x7x365 Managed Detection and Response (MDR) service using our proprietary automation and analytics platform, ZTAP. By ingesting Cortex XDR endpoint, network, and cloud data into the platform, the Trusted Behavior Registry quickly establishes what data is a trigger event, and what information in the alert is an observation. Context and data are united together with Cortex XDR but leveraged differently in investigations.

MDR up leveled. Endpoint security up leveled. An integrated threat detection and response solution for the modern enterprise that's more than good, ***it's better.***

What sets us apart?

We do what others don't. Endpoint data is good, but not enough to investigate all alerts. CRITICAL**START** MDR services integrate with Palo Alto Cortex XDR to quickly detect every event, resolve every alert, and respond to breaches. This trust-oriented approach helps customers reduce risk acceptance, eliminate alert fatigue, and demonstrate value from their Cortex XDR investment – on day one.

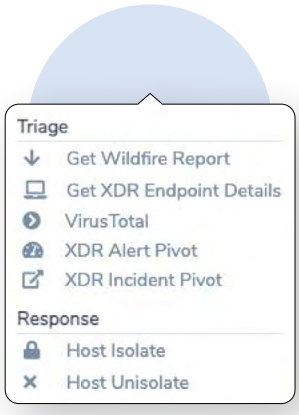
How we do it.

There are lots of security companies with decent people and a decent approach. And when it comes to the security of a company, we admit, they're good. ***We're just better.*** Don't choose between seeing endpoint or network data. Choose both. Don't choose between showing analysts triggers from endpoints and observations from firewalls—show both. Trust shouldn't be easy. Every event and every investigation demands as much context as possible.

Integration, the better way.

Unlike other managed detection and response services, CRITICALSTART** MDR services powered by Cortex XDR leverage:**

- ✓ Incident investigations with endpoint, network, and Wildfire events
- ✓ Security Assertion Mark-up Language (SAML)/Single Sign-On (SSO) authentication for users
- ✓ Additional Behavioral Indicators of Compromise (BIOCs) curated by CRITICAL**START**



Acceptable risk shouldn't be.

Our unique trust-oriented model is based on *resolving every alert.* CRITICAL**START** MDR is driven by the Zero Trust Analytics Platform (ZTAP). The platform features the Trusted Behavior Registry (TBR), the largest registry of known good alerts (false positives), delivering the scalability to resolve every alert.

We take every alert from Cortex XDR into ZTAP and match it against known good alerts in the TBR. If there is a match, the alert is automatically resolved. If there is no match, the CRITICAL**START** Security Operations Center (SOC) investigates the alert.

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.

- ✓ Palo Alto Networks Cortex XDR experts setup and manage the environment in weeks, not months
- ✓ Rigorous training program--Every analyst completes 200 hours of training during onboarding and another 40-80 hours annually

DID YOU KNOW?

CRITICAL**START** is one of a select group of Palo Alto Networks Certified Professional Service Providers (CPSP) in North and South America. Our team is among the elite group of professionals who possess the expertise, tools and ongoing training and resources in Palo Alto Networks solutions.

CRITICALSTART
They're good. We're better.

Built-in transparency.

Unlike traditional MDRs that take a "black box" approach to monitoring, CRITICAL**START** is transparent by design. The ZTAP dashboard lets you see exactly 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 validate the return on these investments plus your MDR service.
- ✓ We can prove ZTAP's effectiveness 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.

Never miss a threat. Or your desk.

Take threat detection and response on-the-go with the MOBILE**SOC** application.

- ✓ Puts the power of ZTAP in your hands, via IOS or Android app
- ✓ Provides on-the-go visibility and interactivity with direct communication with analysts, in-app responses, and full details around the investigation – and has full parity to web
- ✓ Allows you to contain breaches right from your phone

KEY BENEFITS OF THE INTEGRATION

- ✓ Extend your team's capabilities with threat detection and response expertise, 24x7x365, from a U.S.-based SOC.
- ✓ Eliminate alert fatigue and reduce risk acceptance with monitoring, investigation, and rapid--and more importantly, accurate response to every alert.
- ✓ Accelerate value from your Cortex XDR investment with deployment in weeks instead of months.

CRITICALSTART
They're good. We're better.

Capability Comparison

● COMPLETE OFFERING
◐ PARTIAL OFFERING
✕ NO OFFERING

	CRITICAL**START** MDR powered by Palo Alto Networks Cortex XDR	**Other MDR Providers**
Trusted Behavior Registry that resolves 100% of alerts	●	✕
Native iOS and Android applications for alert investigation, collaboration, and response	●	✕
Multi-Tenant so client can have multiple organizations with N-level hierarchy	●	✕
Automated SOC review process that provides quality control of analyst investigations and is available to the customer	●	✕
Contractually guaranteed Service Level Agreement for analyst Time to Detect and Respond to Alert *(as compared to SLO)*	●	✕
Alert notifications that include both security event data and expert analysis	●	◐
Customer and vendor work from the same platform and see the same information for security event analysis *(Transparent view to all rules, comments, audit logs, and metrics)*	●	◐
Behavioral Indicator of Compromise BIOC Monitoring	●	●
24x7 monitoring, investigation, and response by security analysts	●	●
Advanced Threat Detection and Hunting	●	●
Analyst will proactively respond to stop attacks *(isolate, block whitelist, etc.)*	●	●
Managed response, policy tuning, and updating of agents	●	●
Incident Response	●	●
SSAE 18 SOC 2 (TYPE 2) Certified	●	●

Goodbye, alert fatigue. Hello, CRITICAL**START.**

Contact Us **Request a Free Assessment**

CRITICALSTART
They're good. We're better.