CRITICALSTART | CORTEX XDR BY PALO ALTO NETWORKS

Cortex XDR

Managed Detection and Response Services from CRITICALSTART Powered by Cortex XDR

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. Through our deep bi-directional integration, we ingest Cortex XDR endpoint, network and cloud data into the platform, to quickly detect every event, resolve every alert and stop every breach.

What We Do Is Different

CRITICAL**START** delivers the only MDR service built around a cutting-edge trust-oriented model. Powered by ZTAP, the most advanced analytics and automation platform in the industry, we collect, investigate and resolve all alerts. This trust-oriented approach helps customers eliminate risk acceptance, eliminate alert fatigue, and receive full value on their Cortex XDR investment.

The Key Benefits of the Integration

Eliminate alert fatigue and risk acceptance.

Around the clock, CRITICAL**START** monitors, investigates, and responds to **every** alert regardless of priority, from our U.S. based 24x7x365 Security Operations Center (SOC).

Stop malware, exploits, and ransomware before they compromise endpoints.

Indicators of compromise (IOCs) and continuous threat hunting is built into the service. Utilizing our deep bi-directional application interface protocol (API) with Cortex XDR, we gather comprehensive information upfront for quick and effective triage, investigation, and response.

Accelerate return on Cortex XDR.

Deployment of the MDR service is done in weeks instead of months so you see an immediate reduction in alerts and accelerated return on your Cortex XDR investment.

CRITICALSTART

How We Do It

Every alert begins as equal.

We provide full investigation of **every** security alert/incident. Our trust-oriented approach leverages ZTAP and the Trusted Behavior Registry (TBR) to automatically resolve what is known-good for your organization and can be safely trusted first – shifting focus to unknown alerts for triage and quick resolution by the CRITICAL**START** SOC.

Detection and response in 1-hour or less.

ZTAP enriches our investigation of unknown alerts to ensure the escalation of the alerts that really require the attention of your security team. Contractual Time to Detect (TTD) and Median Time to Respond (MTTR) Service Licensing Agreements (SLAs) ensure effective and quick incident management of every alert, guaranteed in 1-hour. This results in efficient, effective and scalable operations, both for CRITICAL**START** and our customer security teams.

Ongoing security guidance.

CRITICAL**START** provides a named point of contact to ensure continuous success and satisfaction with your security. We offer advisory opportunities to help you build out a security program that stays up-to-date, meets your goals, and keeps your data safe.

Built-in transparency.

CRITICAL**START** MDR services have built-in transparency. Our customers see what our SOC security analysts see so they can continuously monitor and validate the value we deliver.

Threat detection and response in your pocket.

CRITICAL**START** offers native iOS and Android apps to give analysts full access to their MDR toolset on the go. With the fully-featured MOBILE**SOC** application your team can investigate alerts, communicate with CRITICAL**START** security experts, and respond – from anywhere, anytime.

Want more information on CRITICAL**START**?
To see how we can help, contact us at www.criticalstart.com

CRITICALSTART