Cortex XDR

Managed Detection and Response (MDR) services from CRITICALSTART powered by Cortex XDR

> CRITICAL**START**™ integrates with Palo Alto Networks products like Cortex XDR to offer a full Managed Detection and Response (MDR) service using CRITICAL**START**'s proprietary MDR platform. By ingesting Cortex XDR endpoint events into the platform, we effectively detect and resolve every alert.

The Key Benefits of the Integration

Take advantage of Cortex XDR as a managed service. The CRITICAL**START** difference (Unprioritize, Trusted Behavior Registry, Human Element, Transparency) combined with Coretex XDR's product capabilities around endpoint detection stops malware, exploits, and ransomware before they can compromise endpoints.

Cortex XDR removes security blind spots by stitching together network, endpoint, and cloud data to deliver monitoring, analysis, and coordinated response across your entire environment. CRITICALSTART monitors this data around the clock with highly-trained analysts who specialize in incident triage, malware analysis, and incident management and response.

Unprioritize

We believe that every alert begins as equal. Because of this, we provide a full investigation of every security alert/incident (vs industry-standard of investigating only a subsegment of critical and high) with response actions.

Trusted Behavior Registry (TBR)

TBR enables a trust-oriented approach that automatically resolves what is known-good and can be safely trusted first – shifting focus to known alerts for triage and quick resolution.

Human Element

24x7x365 monitoring, our highly skilled analysts work in a SOC 2 Type 2 certified Security Operations Center (SOC) to investigate, escalate, contain, and respond to threats – helping to significantly reduce attacker dwell time.

Transparency

Full visibility into every data point collected, every alert resolved or escalated, every playbook. Your team sees the same dashboard as the CRITICAL**START** SOC.

MOBILE**SOC**

CRITICAL**START** offers native iOS and Android apps to give analysts full access to their MDR toolset on the go. Within the fully-featured app, analysts can investigate alerts, communicate with CRITICAL**START** Security Experts, and respond, all without needing a computer.

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

CRITICAL**START**