CrowdStrike EDR

Managed Detection and Response (MDR) services from CRITICALSTART powered by CrowdStrike Falcon

CRITICAL**START**™ integrates with CrowdStrike Falcon to offer a full Managed Detection and Response (MDR) service using CRITICAL**START**'s proprietary MDR platform. By ingesting CrowdStrike endpoint detection events into the platform, we effectively detect and resolve every alert generated.

The Key Benefits of the Integration

The CRITICAL**START** difference (Unprioritize, Trusted Behavior Registry, Human Element, Transparency) combined with CrowdStrike's full feature product capabilities around endpoint detection is unparalleled and unbeatable in the marketplace.

For customers already using CrowdStrike MDR, CRITICAL**START** can additionally deliver fully integrated CRITICAL**START** MDR SIEM services along with CrowdStrike Falcon Complete in our MDR platform.

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.

CRITICAL**START**

Capability Comparison

	CRITICALSTART MDR + Falcon	CrowdStrike Falcon Complete	CrowdStrike Falcon Pro
Trusted Behavior Registry with SOAR Platform 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	●	✖	✖
Manage and report on all alerts from SIEM and EDR in one platform	●	✖	✖
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)	●	○	✖
Custom Indications of Attack (IOA) Monitoring	●	●	✖
24x7 monitoring by Cybersecurity Analysts (Security Alert Investigation and Notification performed 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	●	●	○
Privacy Shield Certified	●	●	●
SSAE 18 SOC 2 (TYPE 2) Certified	●	●	●

● Complete Offering   ○ Partial Offering   ✖ No offering

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

CRITICALSTART