DATASHEET

CRITICAL**START**®
Managed Detection and Response (**MDR**) Services

Human-driven threat detection, proactive risk mitigation, & full protection for maximum security outcomes.

Key Benefits

- **Eliminate security blind spots** Account for every asset, stop threats from exploiting hidden gaps, and know your SOC is receiving every critical threat signal
- **Detect and respond faster with Direct Integrations** Connect directly to leading security tools for **24x7x365** alert and threat detection for complete, multi-faceted, and faster response
- **On-the-go threat containment** Remediation instantly and anywhere with MOBILE**SOC**®
- **Always available access** to U.S.-based security experts; benefit from nuanced, human-led analysis
- **Reduce alert fatigue** Keep the focus on real threats using business-aware filtering; customize response strategies, and eliminate redundancies and false positives
- **Achieve measurable risk reduction** Contractual SLAs of 10-min notification for Critical alerts and 60-min or less Median Time to Resolution (**MTTR**) for ALL threat alerts
- **Maximize security ROI** Improve detection effectiveness with deep threat intelligence and detection engineering

Validate defenses to mitigate breaches and minimize business disruption.

Traditional Managed Detection and Response (**MDR**) often fails to deliver on its promise — missing signals, limited visibility, and reactive-only approaches leave organizations exposed. Critical Start sets a new standard by combining proactive and reactive security in one comprehensive service.

Our **Cyber Operations Risk & Response**™ (**CORR**) **platform** provides complete signal coverage, 24x7x365 monitoring, and human-led investigation and response. With integrated asset inventory, **visibility into endpoint protection and vulnerability assessment Gaps, and SIEM health monitoring**, we ensure your SOC sees every critical threat signal.

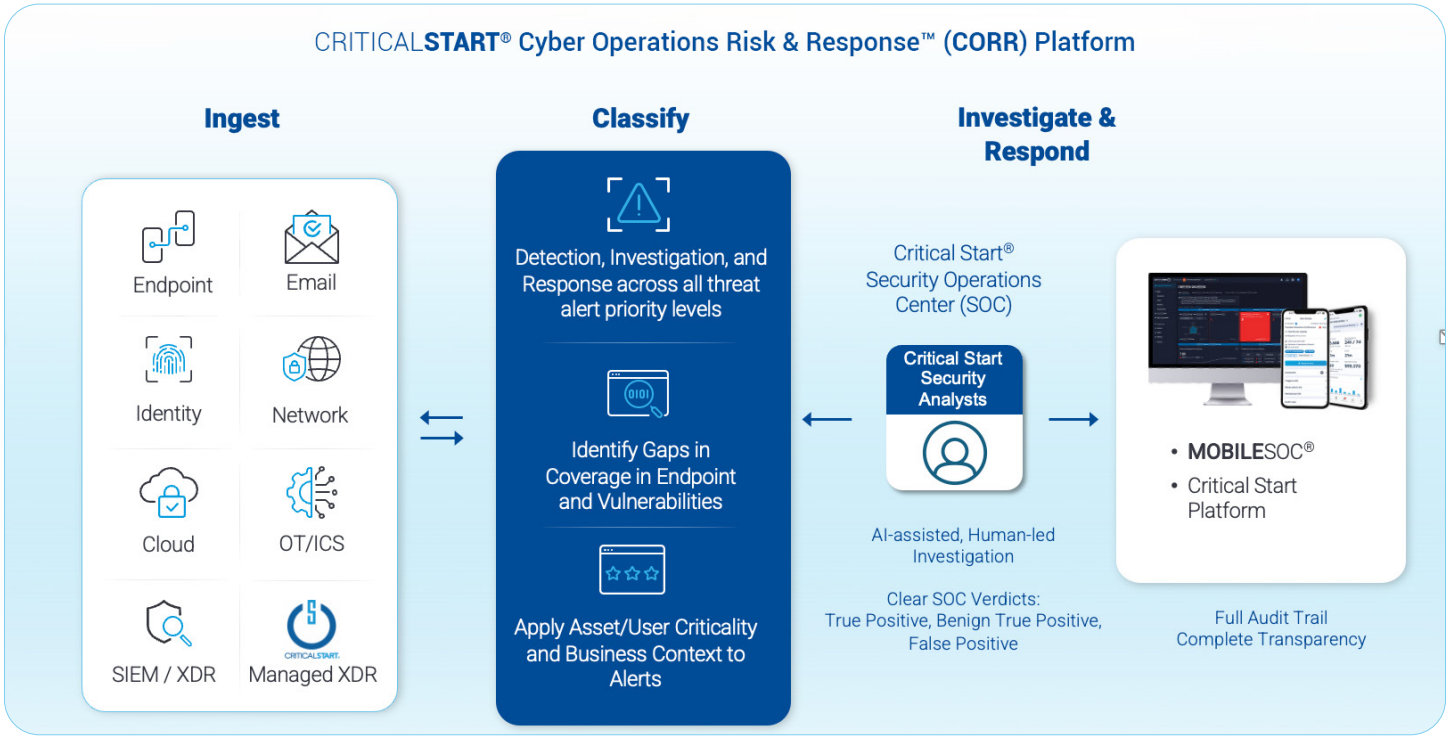
Unlike other MDR providers, we go beyond alerts — mapping risks to MITRE ATT&CK® mitigations and prioritizing based on asset criticality to help you reduce breach risk and maximize security ROI.

Human-driven, AI-assisted for real-world response.

Our MDR services combine the power of automation with the insight of experienced analysts to deliver faster, smarter, and more reliable threat response. Backed by our 24x7x365 SOC, Cyber Research Unit, and Incident Response Team, we go beyond machine-driven triage to deliver context-rich investigations that automation alone can't match. With direct access to our analysts through MOBILE**SOC**®, your team can contain threats remotely and collaborate in real-time. This hybrid approach enhances productivity, reduces risk exposure, and strengthens your security posture, so you're ready for whatever comes next.

CRITICALSTART®

Our Platform and Process



Confidently Reduce Risk, Mitigate Breaches, and Stop Business Disruption

Critical Start goes beyond traditional threat detection by delivering proactive, human-driven, AI-assisted MDR. We help you identify solutions to your challenges and risks, empowering you to confidently mitigate breaches and effectively address a wide-range of alerts including active threats and underlying vulnerabilities within your organization.

License Includes	Essentials	Enterprise	Signature
24/7 Monitoring & Response	✓	✓	✓
Tailored Onboarding	✓	✓	✓
Direct Integrations	✓	✓	✓
Custom Dashboards, Reports & Training	✓	✓	✓
SIEM/XDR Integrations	✗	✓	✓
Custom Data Sources & Detections	✗	✓	✓
Managed SIEM	✗	✓	✓
Executive Sponsor	✗	✗	✓
Relationship Level	Team-Based	Dedicated Partner	White Glove
SIEM/EDR Health Reviews	Quarterly	Monthly	Proactive
Cyber Risk Reviews	Annual	Monthly	Monthly
Security Architecture Review	✗	Annual	Bi-Annual

Available Add-Ons	Essentials	Enterprise	Signature
Advisory SOC Analyst (ASA)	✗	✓	✓
Incident Response	✓	✓	✓

Built to Work With the Tools You Already Have

We support hundreds of log sources and integrate directly with your existing security technologies across **Endpoint, Email, Identity, Network/Firewall, Cloud**, and more. Whether through direct connections or indirect ingestion from your **SIEM, XDR, or OT/ICS** tools, we bring together the signals that matter for complete coverage and trusted results, working closely with you to detect, investigate, and respond to alerts and threats specific to your organization.

- Microsoft Entra ID/ Entra ID Protection
- Microsoft Defender for:
  - Office 365
  - Identity
  - Servers
  - Containers
  - Cloud
  - Endpoint
- Microsoft Defender XDR
- Microsoft 365 Defender
- Microsoft Sentinel
- Abnormal
- CORTEX
- SentinelOne
- sumo logic
- paloalto NETWORKS
- splunk>
- CROWDSTRIKE
- proofpoint.

CRITICALSTART®