

CRITICALSTART®

Managed Detection and Response (MDR) Services

Protect your business 24x7 with SLA-backed detection and response across your security stack.

Key Benefits

- ✓ **Achieve measurable risk reduction**
Contractual SLAs: ≤10-min Critical notifications, tiered ≤60-min Time to Respond (TTR)
- ✓ **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 **MOBILESOC®**
- ✓ **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
- ✓ **Maximize security ROI**
Improve detection effectiveness with deep threat intelligence and detection engineering

MDR for organizations that cannot afford uncertainty.

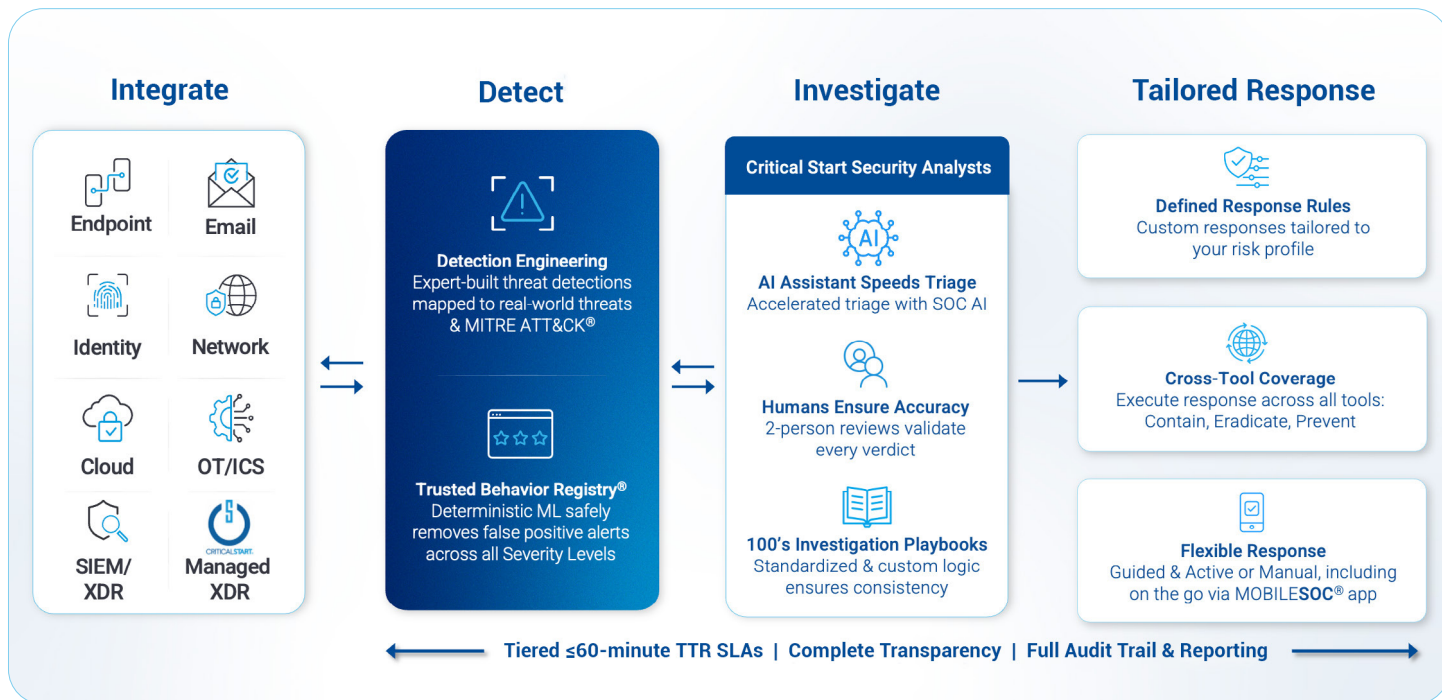
Trust your environment is protected with Managed Detection and Response (MDR) that makes every alert and action *transparent, verifiable, and accountable*. The Critical Start Cyber Operations Risk & Response™ (CORR) platform integrates with your existing tools via direct API — no agents required — to cut noise, accelerate investigations, and deliver verified actions visible in real time through our platform and **MOBILESOC®** app.

AI-accelerated, human-validated response beyond just notifications.

Get the power of automation with the insight of experienced analysts for faster, smarter, and more reliable triage and threat response. Backed by our 24x7x365 SOC, Cyber Research Unit, and Incident Response Team, we deliver context-rich investigations and blast radius analysis that automation alone can't match. With direct access to our analysts through our Platform and **MOBILESOC®** app, your team can contain threats at their desk or on the go, and collaborate in real time wherever they are.



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 XDR**

Abnormal

 **CORTEX[®]**
BY PALO ALTO NETWORKS

 **Microsoft Defender for:**
Office 365 Containers
Identity Cloud
Servers Endpoint

 **Microsoft 365 Defender**

 **SentinelOne[®]**

sumo logic

 **paloalto[®]**
NETWORKS

splunk[>]

 **Microsoft Sentinel**

 **CROWDSTRIKE**

proofpoint.