

CRITICALSTART®

Human-driven, Technology Enabled MDR

Proactive + Reactive Security to Reduce the Risk of a Breach

CRITICALSTART® Managed Detection and Response (MDR) redefines expectations in cybersecurity with human-driven, AI-assisted expertise delivering tailored threat detection and response across IT and OT environments.

Our human-driven MDR services are backed by 24x7x365 U.S.-based Security Operations Centers (SOC), Cyber Research Unit, and Cyber Incident Response Team, and gives you rapid threat containment and response across multi-vendor environments through our portal and MOBILESOC® app. This unmatched approach enhances your security operation's productivity, reducing risk exposure and ultimately strengthening your organization's security posture in response to emerging threats and changing business needs.

Effective MDR Requires Proactive + Reactive Security



Tailor MDR to Your Environment

When it comes to MDR, one size does not fit all. Improve security outcomes with tailored onboarding and response strategies that adapt to your critical business context, seamlessly accommodating multi-vendor solutions, IT and OT threat types, and hundreds of log sources.



Trust Your Security Coverage

You can't protect what you can't see. Ensure your SOC receives all expected threat telemetry with **endpoint and vulnerability scanner coverage gap detection** and log ingestion monitoring.



Rely on Accurate Alert Triage

Automation is necessary, especially at scale, but it can't replace nuanced human analysis. Rely on swift, accurate threat resolution with **human-driven analysis** and two-person integrity verification, backed by contractual SLAs and delivered 24x7x365.



Respond with Confidence

Stop guessing and respond based on data. Maintain an **accurate inventory of critical assets** and prioritize security efforts based on potential business impact.

Critical Start MDR is Strengthened by an Integrated Suite of Products and Services

Contain Threats from Anywhere

Contain threats and incidents from your phone via MOBILESOC®.

Turnkey Vulnerability Management

Identify & manage vulnerabilities and put an end to patching guesswork.

Vulnerability Prioritization

Easily identify critical assets that are at risk for ransomware, botnets, and advanced persistent threats (APTs).

U.S.-based SOC's

Multiple SOC's with 90% retention rates and 300 hours of training or every SOC analyst.

Prevent Repeat Attacks

MITRE ATT&CK® Mitigation recommendations built into the platform.

Reduce Alert Fatigue

Every alert is actioned, with trusted behaviors and benign true positives recognized and resolved.

Conduct Regular Risk Assessments

Security-framework-aligned, platform-driven risk assessments with peer benchmarks.

Professional Services

Regular guidance tailored to your business needs and expert support to continually improve your security.

A Revolutionary Approach to MDR

Cybersecurity threats are more sophisticated and frequent than ever before. One-size-fits-all MDR that over-relies on automation doesn't provide the agility and critical thinking needed to reduce the risk of a breach.

Critical Start's Managed Detection and Response (MDR) service is designed to meet the dynamic needs of today's enterprises, ensuring comprehensive threat detection, investigation, and response across IT and OT environments. Leveraging our Cyber Operations Risk & Response™ (CORR) platform, you gain human-driven, nuanced analysis of alerts, along with advanced security intelligence, comprehensive asset inventories, coverage gap detection, asset criticality assessments, and MITRE ATT&CK® Mitigation recommendations to achieve unmatched security effectiveness.

With Critical Start MDR, you can:

- ✓ Focus resources on critical business by offloading security workloads.
- ✓ Identify and respond to true threats to minimize potential impact.
- ✓ Proactively identify vulnerabilities and exposures to shrink your attack surface.
- ✓ Extend MDR across complex environments, including IT and OT infrastructure.

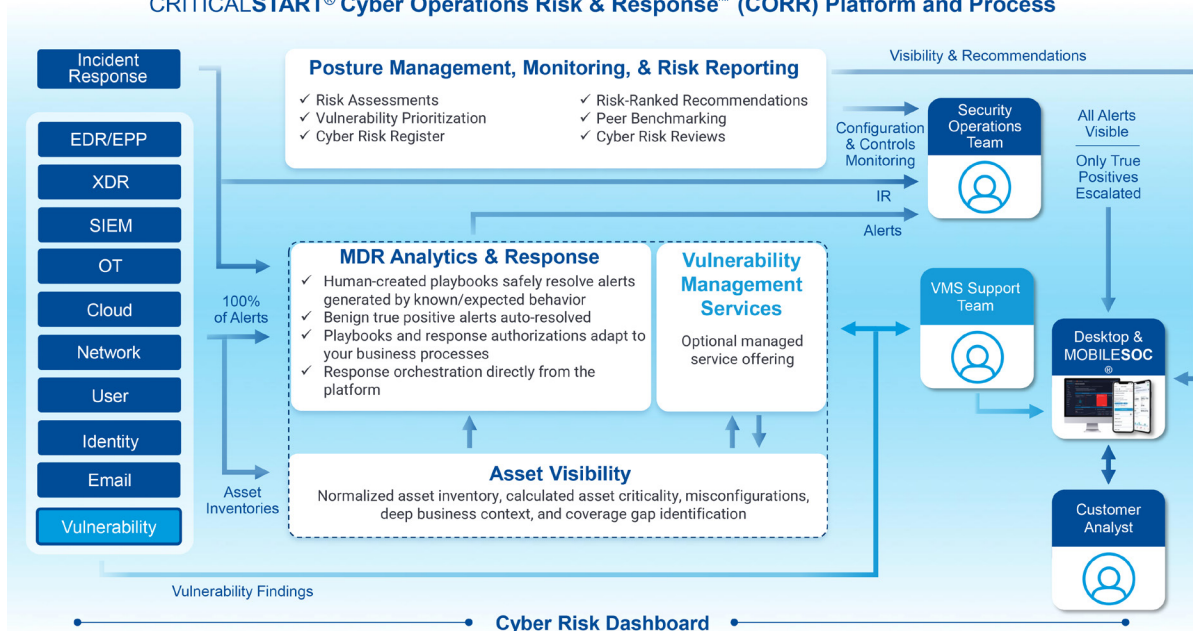
Get More from Your Security Stack

We directly integrate with, fortify, and monitor hundreds of technologies that are crucial to your business and security operations, including endpoint monitoring tools, SIEM tools, user and identity platforms, notification and ticketing systems, and a wide array of technologies for managed XDR/SIEM. Some available integrations* include:



*Talk to us to learn about all available integrations and to discuss your unique needs.

CRITICALSTART® Cyber Operations Risk & Response™ (CORR) Platform and Process



Talk to an Expert

Ready to see how Critical Start can help you manage and reduce risk? Contact one of our experts to request a demo.
www.criticalstart.com/contact/

