DATASHEET

CRITICAL**START**® Cyber Operations Risk & Response™ Platform

One platform for greater security efficiency and reduced risk of a breach.

KEY BENEFITS

- ✓ **Gain rapid situational awareness** with dashboards that show your recent alerts and activities, systems at-risk, escalations, investigation statuses, and more.
- ✓ **Unify data from all connected asset sources** into a single source of truth to find endpoint and vulnerability scanner coverage gaps.
- ✓ **Quickly create, change, and audit Response Authorizations** for a tailored approach to alert response that meets your organization's unique needs.
- ✓ **See all your alerts,** regardless of priority, with full transparency into true positives, auto-resolved false positives, and benign true positives.
- ✓ **Orchestrate response actions directly from the CORR portal** or from the MOBILE**SOC**® app, including host isolation, user session termination, password reset, and many more, for rapid and precise threat containment.
- ✓ **Integrate Vulnerability Prioritization and Vulnerability Management** into CORR for comprehensive security monitoring under a single pane of glass.
- ✓ **Conduct, store, and compare framework-aligned Risk Assessments** and see how your organization's security posture compares to industry peer organizations.

A platform approach to greater security efficiency

Cybersecurity tools offer critical controls that allow organizations to safeguard against attacks. However, cyber environments often grow so rapidly and include so many tools and consoles that security teams become overwhelmed. Inefficient use of tools and lack of in-house expertise can lead to security gaps, blind spots, and uncertainty in the face of conflicting alerts—which all adds up to cyber risk.

The cloud-native Cyber Operations Risk & Response™ (**CORR**) platform serves as the backbone for CRITICAL**START**® human-driven, flexible Managed Detection and Response (**MDR**) and our associated services that consolidate, streamline, and simplify diverse cyber environments. The CORR platform integrates proactive security intelligence with detection and response capabilities for unmatched security effectiveness. Additionally, the Platform provides real-time views and auditable reports of alerts, escalations, response actions taken, and MDR service metrics so you can see your security efficiency in action.

How it Works

CORR takes flexible security to a new level by integrating 100+ data sources and direct integrations, including Endpoint, Identity, Email, Network, OT, and more. It also provides the means to ingest log sources from SIEM and SOAR tools. Once connected, CORR conducts deep analysis that quickly identifies unprotected assets due to endpoint and vulnerability scanner coverage gaps. Additionally, you can set configurable asset criticality scores so your teams can prioritize remediation to make the greatest impact for risk reduction.

With the security operations center (**SOC**) receiving all expected threat telemetry, you can trust that your tools are being used to their greatest potential. You'll gain an actionable view of attacks in progress across your environment mapped to MITRE ATT&CK® Framework, clearly see the response actions taken by the Critical Start team, and receive clear, actionable response guidance for alerts so you can take swift decisions that reduce the risk of a breach.

Improve Security Outcomes at Every Level of Your Organization

The Critical Start Cyber Operations Risk & Response platform delivers value and efficiency at every level of security ownership, including security analysts, leadership, and the C-suite.

Transparency and Trust for Security Analysts	Tailored Solutions that Empower Security Leadership	Measurable Security Efficacy for Security Executives
• The Trusted Behavior Registry™ (**TBR**) and benign true positive alert verdicts mean you only see true positives escalated. • Auto-resolved alert details are always available, so you know exactly which tools, rules, playbooks, and analysis led to each decision made. • Human-driven analysis and two-person quality assurance reviews ensure accurate, nuanced, and actionable alert escalations. • The Who's on Call feature lets you accelerate time to resolution by allowing Critical Start to reach out directly to the right person on your team at those times when every second counts. • Response orchestration allows you to automatically categorize and resolve security events and review playbooks for events that do not require direct escalation.	• The Cyber Risk Dashboard provides a real-time view of your overall security posture, with Risk-Ranked Recommendations so you can make data-informed decisions. • The Your Team Performance screen lets you see, track, and improve your team's responses to escalated and assigned alerts. • Response Authorizations give you an easy and auditable way to direct the actions taken by Critical Start based on configurable criteria that you set. • Configurable Asset Criticality ratings help you prioritize response based on the potential impact to your organization. • 100+ data sources and direct integrations let you see and manage all your security data in one place, regardless of the tools you use, for greater efficiency and threat detection.	• Framework-aligned Risk Assessments allow security executives to measure and track security posture over time and review game-changing peer benchmarks that demonstrate how the organization compares to industry peers. • Easy-to-read, detailed reports provide relevant facts that demonstrate security effectiveness, team responsiveness, and quantified MDR value. • Regular SOC Review reports and Risk-Ranked Recommendations keep you ahead of relevant trends and changes you can make to proactively improve your organization's security posture.

Intelligence in Action

Many organizations struggle with staying ahead of evolving cyber threats and managing the overwhelming volume of security alerts. The Critical Start CORR platform is backed by a Cyber Threat Intelligence (**CTI**) unit that tackles these challenges for you by conducting in-depth cybersecurity research and threat intelligence analysis. Through CORR, you receive actionable insights that help you proactively identify and mitigate emerging threats and vulnerabilities. With the help of intelligence at your fingertips, you can enhance security posture, conduct reverse engineering malware analysis, and work with Critical Start directly through CORR to tune and tailor your detections, Response Authorizations, and response actions or emerging threats.

Respond to Alerts on the Go

SIEM/XDR Health Monitoring provides centralized observability into the performance of your security data sources. We continuously When a critical alert hits, every second counts. Critical Start MOBILE**SOC®** puts the capabilities of CORR into the palm of your hand so you can receive alerts and contain threats no matter where you are. With MobileSOC, you have the same capabilities that you get through the CORR portal, including full alert triage and analysis details, one-click response actions, direct communication with the Critical Start SOC team, and detailed situational awareness across your entire connected environment. You can also see your MITRE ATT&CK Mitigations and Risk-Ranked Recommendations to continually improve your security posture, and you can read the latest CTI bulletins to stay ahead of the continuously changing threat landscape.

Get Started Today

Schedule a customized demo to see how Critical Start can help you improve security operations and reduce the risk of a breach by consolidating detection, response, and strategic decision making with the CORR platform.