DATASHEET

CRITICALSTART® Cyber Research Unit

Stay ahead of emerging threats with comprehensive cyber defense capabilities.

KEY BENEFITS

- ✓ **Leverage proactive defense**
  Stay ahead of emerging threats with expert-led threat-hunting and advanced detection strategies
- ✓ **Enhance situational awareness**
  Get a comprehensive view of the cyber threat landscape for pre-emptive defense and response prioritization
- ✓ **Accelerate cyber response**
  Protect your org with quick and effective incident response, containment, and recovery
- ✓ **Reduce dwell time**
  Limit threat persistence and inhibit lateral movement with continuous assessments and gap analysis
- ✓ **Optimize defenses**
  Get precise hardening of vulnerabilities and fine-tuning of monitoring capabilities
- ✓ **Maximize analyst proficiency**
  Use contextual alerts and guided workflows to boost team efficiency
- ✓ **Prove ROI**
  Rely on objective intelligence and testing to ensure optimal investment in security controls and technologies

A comprehensive approach to proactive cyber defense

The Critical Start **Cyber Research Unit** (**CRU**) works as an extension of your team to stay ahead of emerging threats and prevent breaches and is comprised of specialists across cyber threat intelligence, threat research, malware analysis, reverse engineering, detection development, and more.

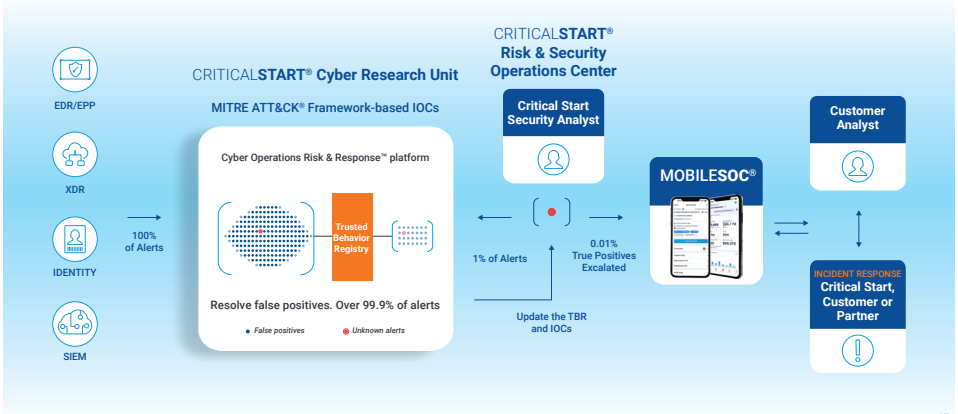
The CRU builds and enriches detections and Indicators of Compromise (**IOCs**) with up-to-the-minute threat intelligence. Our work supports our Managed Detection and Response (**MDR**) services and expanded Managed Cyber Risk Reduction (**MCRR**) offerings delivered **24x7x365** by our U.S.-based analysts, helping them augment defenses with continuous identification, analysis, and mitigation of emerging threats tailored to each organization's environment.

Reduce risk and prevent repeat attacks

We curate threat research on behalf of our Managed Detection and Response (**MDR**) customers and only send you what is actionable, providing you with proactive visibility into new and emerging threats.

Whenever we are notified of a new threat or attack, we map those detections to the industry-leading **MITRE ATT&CK® Framework** to identify gaps in your security solution's detection coverage and ensure you are protected against the latest Tactics, Techniques, and Procedures (**TTPs**) used by threat actors.

By developing and enriching new Detection Chains, verifying the effectiveness of these detections in our **Cyber Operations Risk & Response™ (CORR) platform**, tuning out any false positives, and pushing out new detections to all our customers, we can respond early in the attack cycle and prevent repeat attacks.



CRITICALSTART®

How We Do It

The CRU specializes across multiple areas to bring your team actionable, intelligence-driven information, including:

- **Threat Identification:** Continuous monitoring and analysis to identify and assess emerging risks
- **Vulnerability Intelligence:** In-depth analysis and prioritization of patching based on threat intelligence
- **Exposure Discovery:** Rigorous testing and assessments to validate the effectiveness of security controls
- **Control Validation:** Utilizing analytics and custom detections for enhanced visibility and rapid response
- **Risk Communication:** Providing clear, contextual reporting to stakeholders for informed decision-making

CRU Specializations	What We Do
Cyber Threat Intelligence (**CTI**)	• Gather intelligence from diverse sources like Open Source Intelligence (**OSINT**), commercial databases, and dark web monitoring • Collaborate with our CORR platform and RSOC analysts for integrated threat intelligence and response
Threat Hunting	• Proactively searching for hidden threats within the network • Leverage intelligence to identify and mitigate potential security breaches before they escalate
Threat Research	• Conduct in-depth analysis of emerging threats and their implications • Provide actionable insights and strategic recommendations to fortify defenses
Malware Analysis	• Analyze and understand malware behavior and propagation methods • Reverse engineering malware to extract IOCs and understand attacker TTPs
Reverse Engineering	• Dismante and analyze sophisticated malware and cyberattack mechanisms • Provide crucial insights into attacker methodologies and potential vulnerabilities
Detection Development	• Develop advanced detection mechanisms based on the latest threat intelligence • Continuously updating and refining detection strategies to respond to evolving cyber threats

Managed Threat Intelligence (MTI) for a heightened tactical advantage

The CRU also offers an add-on Managed Threat Intelligence (**MTI**) service for MDR customers looking to amplify their ability to effectively manage risk and mitigate threats with in-depth, actionable insights and expert guidance in:

- Premium Threat Intelligence
- Dark Web Monitoring
- Specialized Requests for Intelligence (**RFIs**)

To learn more about the Critical Start CRU and how we help you stay ahead of emerging threats with comprehensive cyber defense capabilities, contact us at criticalstart.com/contact

criticalstart.com