SOLUTION BRIEF

Uncover hidden threats and maximize the value of your SIEM investment.

Sharpen risk resilience by maximizing the operating potential of your SIEM.

The strength of your security posture depends on a well-managed SIEM solution. While Security Information and Event Management (**SIEM**) solutions have many advantages, they require technical expertise and can be challenging to deploy, tune, and manage. This results in unused “shelfware” that wastes time and money and creates security awareness gaps. At the same time, the number of people, processes, and technology that need constant coordination and monitoring to protect your organization is directly at odds with the increasing demand for simplified cybersecurity that doesn’t compromise coverage.

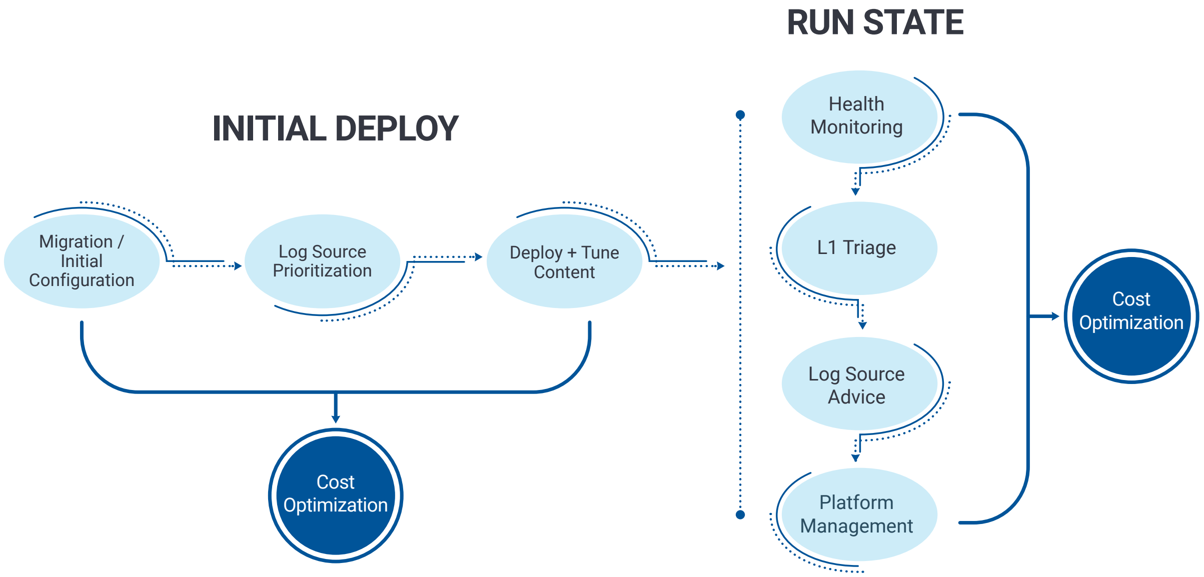
Critical Start Security Services for SIEM helps you derive maximum value from your SIEM investment and holistically improve your security posture by pairing premier MDR defense with experts to manage the maintenance and tuning of your SIEM application.

THE CHALLENGE

Your MDR is only as good as the security signals it receives, so your SIEM can’t just be a “set it and forget it” solution. The lack of dedicated resources to tune, configure, and test the right log files prevents you from getting the greatest security value out of your SIEM. This leads to an increase in false positives and alert saturation that clouds decision-making and hides genuine threats. Without complete visibility, control of your data, access to the latest security intel, and the ability to scale, your organization will struggle to manage risk and strengthen its security posture.

Our approach: Maximizing efficiency without compromising your security posture

With Critical Start Managed SIEM, included with your Managed Detection and Response (**MDR**) for SIEM services purchase, we integrate leading SIEM platforms like **Microsoft® Sentinel**, **Splunk Cloud™**, **Splunk ES**, and **Sumo Logic®** with our purpose-built Trusted Behavior Registry® (**TBR®**), our proprietary **Cyber Operations Risk & Response™ platform**, and human-led expertise. This powerful combination reduces complexity and risk while maximizing the value of your security resources. (*Fig 1*).



(*Fig 1*) Your entire SIEM program with Critical Start

How we address your core challenges

1. MIGRATION AND IMPLEMENTATION

A SIEM platform is not a one-off technology purchase. We offer assistance with migration from your current SIEM provider(s) and help with implementation, ensuring ongoing development and maturation.

2. CONFIGURATION

Tuning is critical for achieving optimum control over your data and the best possible results from your SIEM. We provide custom configuration, SIEM dashboards, reports, and log sources to support your specific security, risk, compliance, and audit use cases.

3. CONTENT

We help you work more efficiently by automating everyday tasks—such as playbook development—and provide expert guidance on quickly and effectively responding to incidents using your SIEM data. We design and build detection and reporting content and then translate alerts into information you can do something with.

4. OPERATIONAL MONITORING

With Quarterly Service Reviews, Ingest Cost Analysis, and more, we maximize and keep your total cost of ownership predictable and manageable.

5. TECH MANAGEMENT

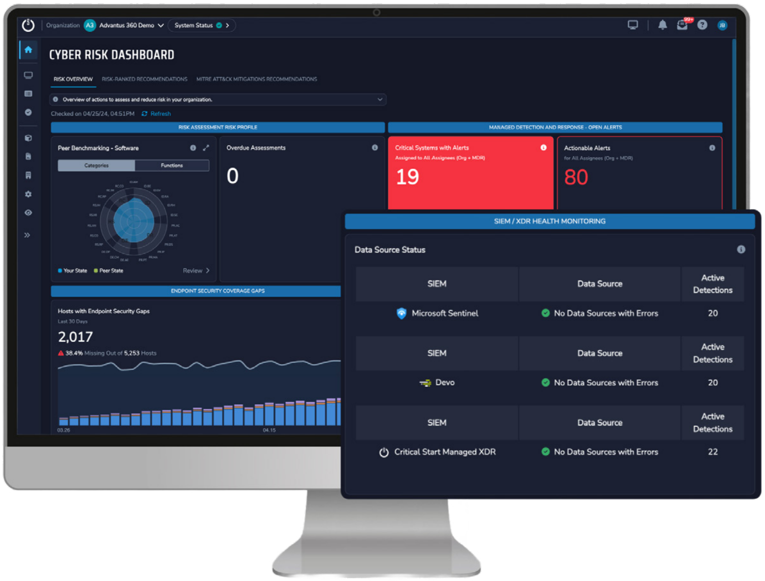
We help simplify resource management and improve team efficiency by staying on top of current changes—even if your SIEM vendor continuously updates your platform. We make sure your SIEM is up-to-date, address hotfixes, and review any out-of-the-box content, allowing your analysts to focus on real and emerging threats.

6. THREAT MONITORING & INVESTIGATION

Critical Start extends your team with skilled security experts who partner with you to detect, investigate, and respond to threats. Powered by our Cyber Operations Risk & Response™ (**CORR**) platform, 24x7x365 expert security analysts, and the Critical Start Cyber Research Unit (**CRU**), we help you respond to alerts quickly and effectively, elevating your efficiency level in orders of magnitude greater than can be achieved through manual effort.

7. PROACTIVE SIEM FEATURES

We've expanded our MDR offering to include features like SIEM log and health monitoring (*Fig 2*) and SIEM Coverage Gaps so you can stay ahead of evolving threats. Watch for anomalies—like Zero-Log Ingestion—from the Cyber Risk Dashboard within CORR to ensure your logs are constantly being reviewed and monitored for any signs of a breach.


Organization
A3 Advantus 360 Demo
System Status
99+
JB
CYBER RISK DASHBOARD
RISK OVERVIEW
RISK-RANKED RECOMMENDATIONS
MITRE ATT&CK MITIGATIONS RECOMMENDATIONS
Overview of actions to assess and reduce risk in your organization.
Checked on 04/25/24, 04:51PM
Refresh
RISK ASSESSMENT RISK PROFILE
Peer Benchmarking - Software
Categories
Functions
Your State
Peer State
Review
Overdue Assessments
0
MANAGED DETECTION AND RESPONSE - OPEN ALERTS
Critical Systems with Alerts
Assigned to All Assignees (Org + MDR)
19
Actionable Alerts
for All Assignees (Org + MDR)
80
ENDPOINT SECURITY COVERAGE GAPS
Hosts with Endpoint Security Gaps
Last 30 Days
2,017
38.4% Missing Out of 5,253 Hosts
03.26
04.15
SIEM / XDR HEALTH MONITORING
Data Source Status

SIEM	Data Source	Active Detections
Microsoft Sentinel	No Data Sources with Errors	20

SIEM	Data Source	Active Detections
Devo	No Data Sources with Errors	20

SIEM	Data Source	Active Detections
Critical Start Managed XDR	No Data Sources with Errors	22

(*Fig 2*) SIEM Health Monitoring from the Cyber Risk Dashboard

KEY OUTCOMES

Maximize the productivity of your team

Our security experts handle the heavy lifting around your SIEM implementation and management. Let us optimize your SIEM with dedicated operational services, including functional updates and version upgrades, so your team can focus on other priorities.

Optimize financial stewardship & simplify resource management

We ensure you ingest the right security data to maximize the value of your threat-detection use cases (*Fig 3*). Critical Start helps you efficiently allocate resources, such as understanding the best type of log storage for your business. This reduces your in-house requirements and leads to more effective financial stewardship.

Quickly access data relevant to your specific use cases

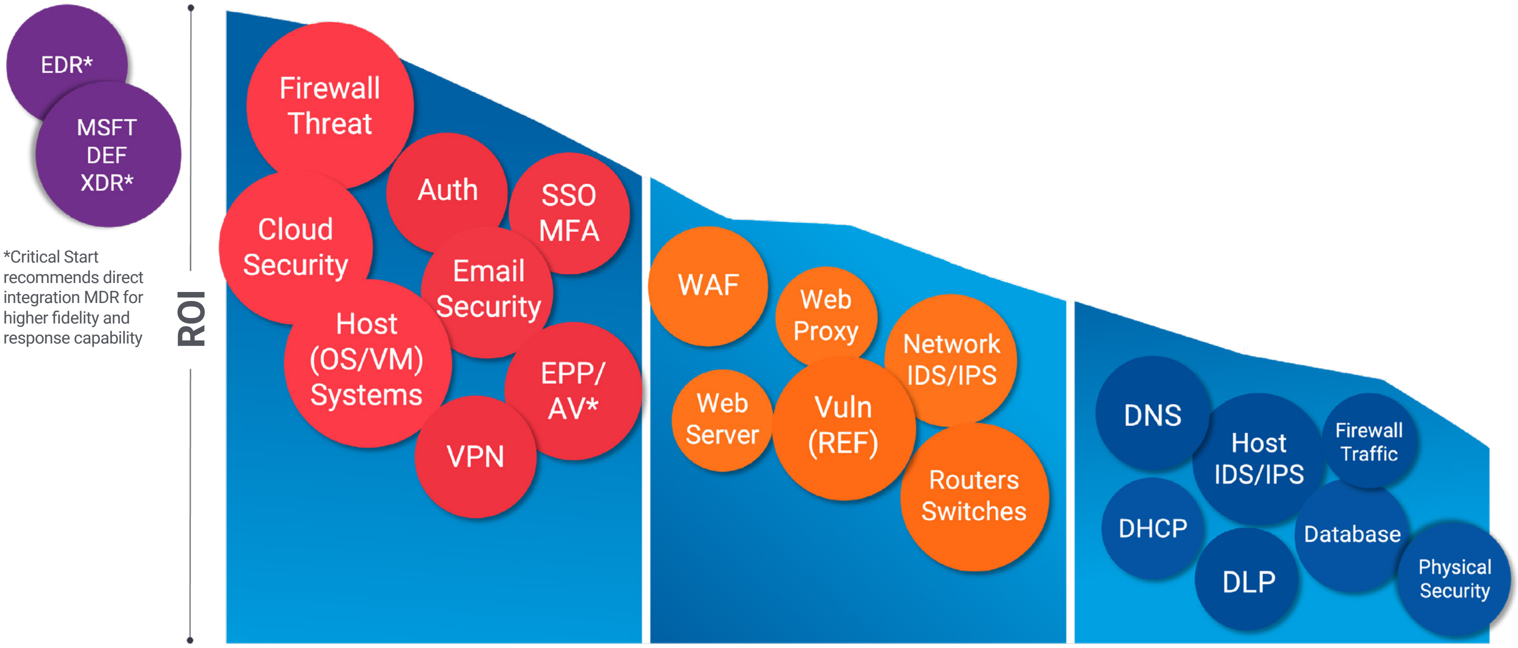
Configure and personalize your SIEM with customized dashboards, reports, and log sources to support your specific security, risk, compliance, and audit use cases to prove the value of your SIEM to your executive team.

Enhance your detection coverage & security posture

We map your threat detection content to the **MITRE ATT&CK® Framework**, helping you achieve optimal MDR coverage and outcomes, keep up with new threats and compliance requirements, and strengthen your security posture.

Identify and mitigate risks

SIEM Coverage Gaps, log and health monitoring, and **MITRE ATT&CK® Mitigations Recommendations** provide actionable insights to identify and address potential security risks before they escalate. These insights empower you to remediate the highest-risk gaps, giving you more control over your environment's security.



*Critical Start recommends direct integration MDR for higher fidelity and response capability

(*Fig 3*) Log prioritization for better security value

KEY SOLUTION FEATURES

Configuration and customization

We configure and customize your dashboards, reports, and log sources to support your specific security, risk, compliance, and audit use cases.

Quarterly Service Reviews: Optimizing your detection coverage

Use our in-depth, quarterly report for constant assurance that your log sources coming in are accurate and necessary for detecting threats. Get complete visibility into what logs you are ingesting and how your SIEM is performing to help you control costs and increase security outcomes.

(Microsoft Sentinel™ customers receive an ingest cost analysis to analyze billing vs. ingest for specific Microsoft data sources based on your security products and licenses.)

Health monitoring: Keep your SIEM running at optimal capacity

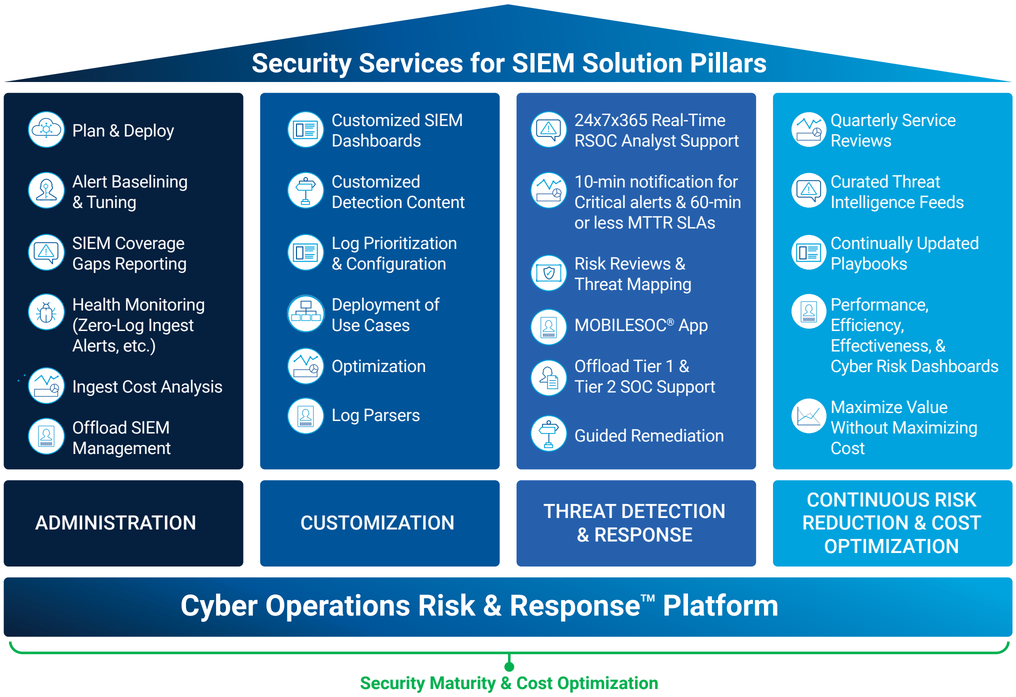
Keep your SIEM running at optimal capacity with log source performance, Zero-Log Ingest Alerts, and availability and capacity monitoring to identify potential log ingestion issues and avoid any misconfigurations.

SIEM Coverage Gaps

Know that you are ingesting the most security-relevant log sources and that they are working correctly. Get actionable insights to remediate the highest risk gaps for the quickest way to make your environment more secure.

Risk reduction reviews

If you are considering adding more log sources or detection content, we can analyze the potential impact on your coverage under the industry-standard **MITRE ATT&CK® Framework**.



Security Services for SIEM Solution Pillars

ADMINISTRATION	CUSTOMIZATION	THREAT DETECTION & RESPONSE	CONTINUOUS RISK REDUCTION & COST OPTIMIZATION
Plan & Deploy	Customized SIEM Dashboards	24x7x365 Real-Time RSOC Analyst Support	Quarterly Service Reviews
Alert Baselining & Tuning	Customized Detection Content	10-min notification for Critical alerts & 60-min or less MTTR SLAs	Curated Threat Intelligence Feeds
SIEM Coverage Gaps Reporting	Log Prioritization & Configuration	Risk Reviews & Threat Mapping	Continually Updated Playbooks
Health Monitoring (Zero-Log Ingest Alerts, etc.)	Deployment of Use Cases	MOBILESOC® App	Performance, Efficiency, Effectiveness, & Cyber Risk Dashboards
Ingest Cost Analysis	Optimization	Offload Tier 1 & Tier 2 SOC Support	Maximize Value Without Maximizing Cost
Offload SIEM Management	Log Parsers	Guided Remediation	

Cyber Operations Risk & Response™ Platform

Security Maturity & Cost Optimization

CONCLUSION

Using a risk-based approach, Critical Start pairs managed SIEM with our expanded MDR services to provide a comprehensive solution backed by industry-leading methodologies, processes, and technologies. By assisting in advancing your cybersecurity capabilities over time (based on your risk profile), we empower organizations like yours to balance cost and risk mitigation to achieve your desired maturity level. We are passionate about our work, committed to your success, and proud to provide you with results backed by our contractual Service Level Agreements (**SLAs**) of 10-minute notification of Critical alerts and 60-minute or less for Time to Detection (**TTD**) and Median Time to Resolution (**MTTR**) and enhanced by the convenience of our MOBILESOC® app.

CRITICALSTART®
Don’t Fear Risk. Manage It.

Contact us for more information about Critical Start Security Services for SIEM or schedule a demo at: www.criticalstart.com/contact/request-a-demo/

About Critical Start

Organizations today face the challenge of aligning their cyber protection measures with their risk appetite. CRITICALSTART®, a pioneer of the industry’s first Managed Cyber Risk Reduction solutions, provides holistic cyber risk monitoring via its Cyber Operations Risk & Response™ platform, paired with a human-led risk and security operations team, combined with over 8 years of award-winning Managed Detection and Response (MDR) services. By continuously monitoring and mitigating cyber risks, Critical Start enables businesses to proactively protect their critical assets with a measurable ROI. The company’s platform provides maturity assessments, peer benchmarking, posture and event analytics, and response capabilities. Its risk and security operations team evaluates and actions threats, risks, vulnerabilities, and performs comprehensive threat intelligence research. Critical Start enables organizations to achieve the highest level of cyber risk reduction for every dollar invested, allowing them to confidently reach their desired levels of risk tolerance.

Follow Critical Start on LinkedIn, X, Facebook, Instagram.