SOLUTION BRIEF

Achieve full operating potential with Critical Start Managed SIEM

Get the services you need to reach security maturity

Security Information and Event Management (**SIEM**) solutions have many advantages, but they can be challenging to deploy, tune, and manage, resulting in unused "shelfware" that wastes time and money and creates security awareness gaps. Critical Start Managed SIEM services simplify the architecture and deployment of SIEM. We help you derive maximum value from your SIEM investment and holistically improve your security posture by managing back-end components and maintenance of your SIEM application, including version updates and application performance.

Our Approach

Critical Start Managed SIEM is included with your purchase of our Managed Detection and Response (**MDR**) for SIEM services. By integrating 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, Critical Start reduces complexity and risk while maximizing the value of your security resources, allowing us to provide you with dedicated expertise from planning and rollout to threat protection.

Your success is our success, which is why our team stays with you throughout every step of your Managed SIEM journey. We help you identify and continuously analyze your log sources and deliver value-added services that exceed industry requirements. These services include configuration and customization of dashboards, reports, and log sources to support your specific security, risk, compliance, and audit use cases and provide the proof points you need to prove the value of your SIEM to your executive team. *(Fig 1)*

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 business priorities.

Optimize financial stewardship & simplify resource management

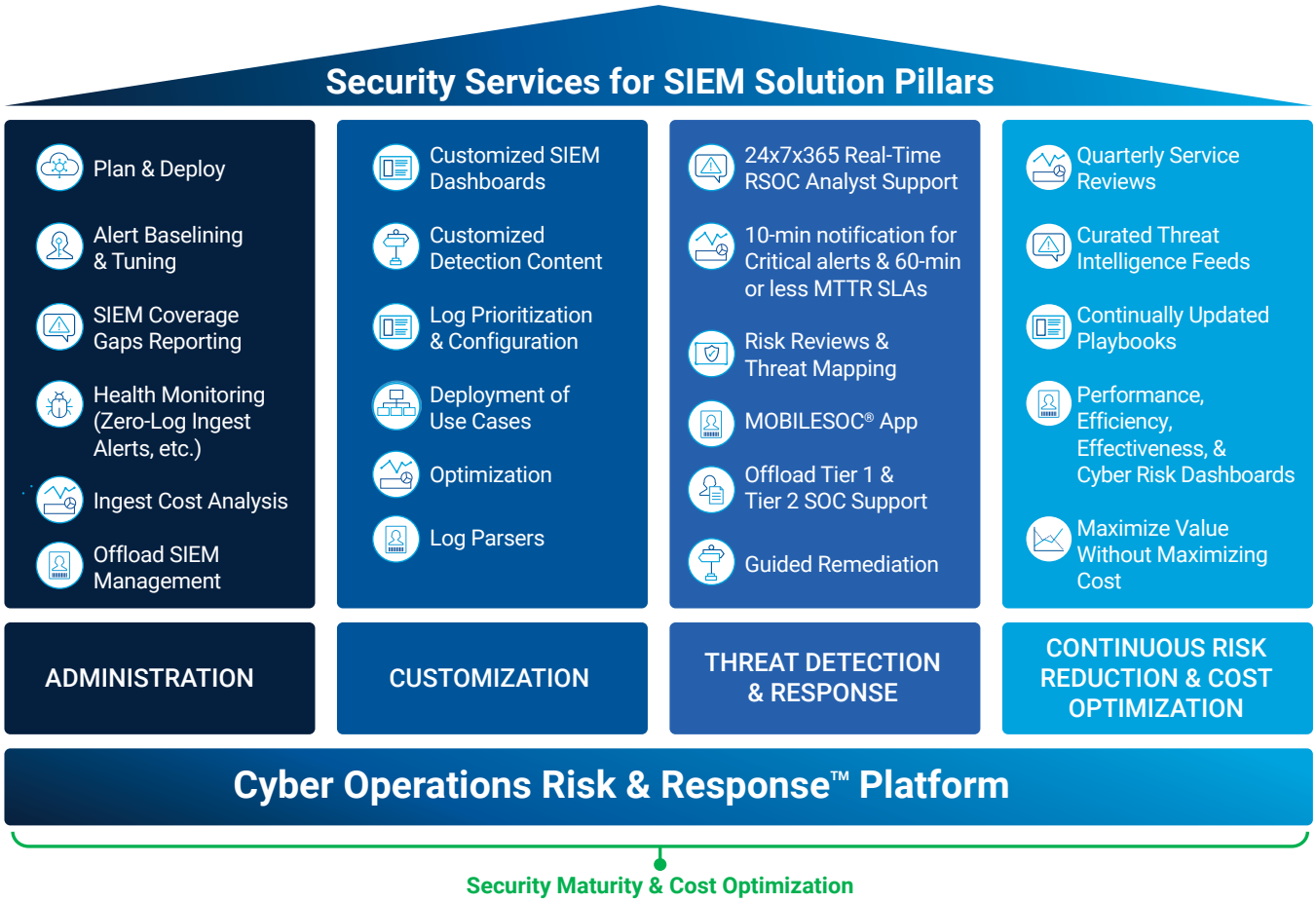
We help manage your operating costs for SIEM by ensuring you are ingesting the right security data to get the most value from your threat-detection use cases. Critical Start helps you efficiently allocate resources—like understanding what type of log storage is best for your business—which decreases your in-house requirements and results in lower costs for your business.

Data when and where you need it

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

Enhance your detection coverage & security posture

We provide **NIST CST** reporting and map your threat detection content to the industry standard **MITRE ATT&CK® Framework** for the foundation you need to help you achieve optimal MDR coverage and outcomes. We help you keep up with new threats and compliance requirements by ensuring that your data is being properly ingested, guiding you in applying the right detection content to your log sources and preventing misconfigurations.



(Fig 1) Managed SIEM and MDR together for cost-effective risk reduction

KEY SOLUTION FEATURES

From cybersecurity effectiveness and efficiency to addressing a staffing shortage or lack of in-house expertise to optimizing your total cost of ownership (**TCO**), Critical Start proactively addresses your pain points with solutions tailored to your needs.

Configuration and customization

We provide a custom User Interface (**UI**) for your SIEM tool by configuring and customizing up to five dashboards and five data sources to help enable queries for each year of your contract, as well as reports to support your specific security, risk, compliance, and audit use cases.

Quarterly Service Reviews

Optimize your detection coverage with our in-depth, quarterly report for constant assurance that the security-relevant log sources necessary for detecting threats are being ingested. Get complete visibility into how your SIEM is performing to help control costs and enhance security outcomes. For **Microsoft® Sentinel** and **Sumo Logic®** customers, this includes an **Ingest Cost Analysis** to analyze billing vs. ingest for specific data sources based on the customer's security products and licenses.

Health Monitoring

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

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**.

SIEM Coverage Gaps

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

Contact us for more information about Critical Start Managed SIEM and other SIEM solutions and services, or schedule a demo at:

www.criticalstart.com/contact/request-a-demo/