DATASHEET

CRITICALSTART® Managed Detection and Response (MDR) Services for SIEM

Breach prevention with SIEM, simplified.

KEY BENEFITS

✓ Accelerate return on your SIEM investment
Prioritize ingest data for enhanced threat detection and increased context for investigations.

✓ Reduce the noise
See fewer false positives over time while still being able to add more log source feeds.

✓ Improve security posture
Continuously validate **MITRE ATT&CK® Framework** coverage so you can strategically add data sources to address new security initiatives.

✓ Increase SOC efficiency & productivity
Between our **Zero-Trust Analytics Platform®** (**ZTAP®**), SOC and Threat Detection Engineering team, we do all the heavy lifting for you.

Achieve the full operating potential of your SIEM investment for the most effective threat detection

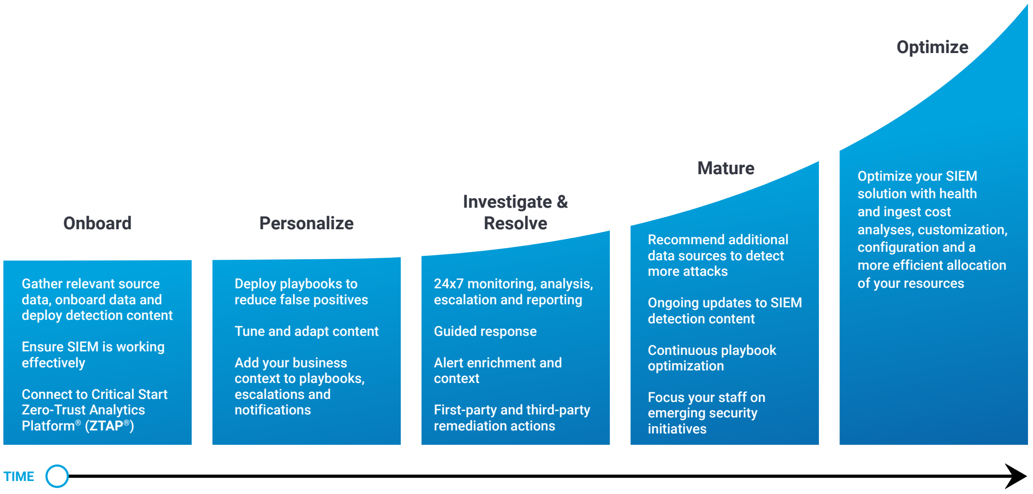
Critical Start Managed Detection and Response (**MDR**) services for SIEM simplify the complexity of your Security Information and Event Management (**SIEM**) system and give you protection against the latest tactics, techniques and procedures (**TTPs**). By combining the flexibility of your SIEM and its ability to ingest any vendor's log data with Critical Start's trust-oriented approach to MDR, we can eliminate false positives at scale and streamline the investigation and response process.

Critical Start MDR services for SIEM allow you to:

- Prioritize the logs you send to the SIEM
- Apply the right detections to those log sources
- Investigate and respond to threats to stop breaches before they disrupt your business

Taking the journey with you

Implementing and managing a SIEM solution takes time and dedication, and unfortunately, many businesses hit roadblocks that prevent them from maturing their SIEM and realizing a return on investment (**ROI**). From onboarding to optimization, Critical Start is with you every step of the way on your security journey, freeing up your staff to focus on what matters most to your business.



Onboard

Gather relevant source data, onboard data and deploy detection content

Ensure SIEM is working effectively

Connect to Critical Start Zero-Trust Analytics Platform® (ZTAP®)

Personalize

Deploy playbooks to reduce false positives

Tune and adapt content

Add your business context to playbooks, escalations and notifications

Investigate & Resolve

24x7 monitoring, analysis, escalation and reporting

Guided response

Alert enrichment and context

First-party and third-party remediation actions

Mature

Recommend additional data sources to detect more attacks

Ongoing updates to SIEM detection content

Continuous playbook optimization

Focus your staff on emerging security initiatives

Optimize

Optimize your SIEM solution with health and ingest cost analyses, customization, configuration and a more efficient allocation of your resources

How We Do It

Prioritizing data ingested into SIEM

To effectively drive threat detection and enrich content needed for investigations, you must make choices about what you want to ingest into the SIEM platform and manage that against the value those data sources provide to your security mission.

Critical Start helps you prioritize your data onboarding by separating it into three tiers:

1. Threat Detection Sources rich in threat detection value and contain actionable signals. Examples include Firewall Threat and Network and Host Intrusion Detection System (**IDS**)/Intrusion Prevention System (**IPS**) logs.

2. Investigation Sources that contain information about what is happening in your environment (used as the primary data corpus for investigations when threats are detected) and select targeted detections. Examples include Sysmon, Domain Name System (**DNS**) and Web Proxy Log.

3. Enrichment Sources that help provide more context to threat detections and investigations but have limited security value. This includes sources such as Dynamic Host Configuration Protocol (**DHCP**) and Network Access Control (**NAC**) logs.

Investigation and response to disrupt attacks beyond the endpoint

Leveraging our seamless integration with your SIEM platform, our ZTAP automates the investigation and triage of alerts across all users, devices, applications and infrastructure. ZTAP removes false positives and escalates true positives to the Critical Start Security Operations Center (**SOC**) for further enrichment and investigation.

Experienced security analysts quickly investigate escalated alerts and help you make more accurate decisions on which response actions to take through 24x7x365 monitoring, rapid investigation and continuous threat hunting.

All of this is backed by our 100% transparency approach—our service is an open book, completely accessible to all our customers, all the time—and our guaranteed 1-hour or less Service Level Agreements for Time to Detection (**TTD**) and Median Time to Resolution (**MTTR**).”

Unmatched SIEM detection engineering expertise

At Critical Start, simplifying breach prevention with your SIEM means being the most effective at detecting and responding to cyberattacks. We accomplish this through:

- ✓ Our dedicated Cyber Research Unit (**CRU**), with a collective 100+ years of experience curating content across multiple industries to ensure that our detections are working properly

- ✓ Leveraging the Critical Start Threat Navigator to manage, maintain and curate out-of-box detections and Indicators of Compromise (**IOCs**)

- ✓ Continuously mapping detection content to the industry-approved **MITRE ATT&CK® Framework**

- ✓ Leveraging Critical Start proprietary detections and IOCs

Contact Us **Request a Free Assessment**