DATASHEET

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

Breach prevention with SIEM, simplified.

KEY BENEFITS

- ✓ **Accelerate return on your SIEM investment**
  Prioritize data to be ingested to drive threat detection and enrich content needed 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 ZTAP platform, 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.

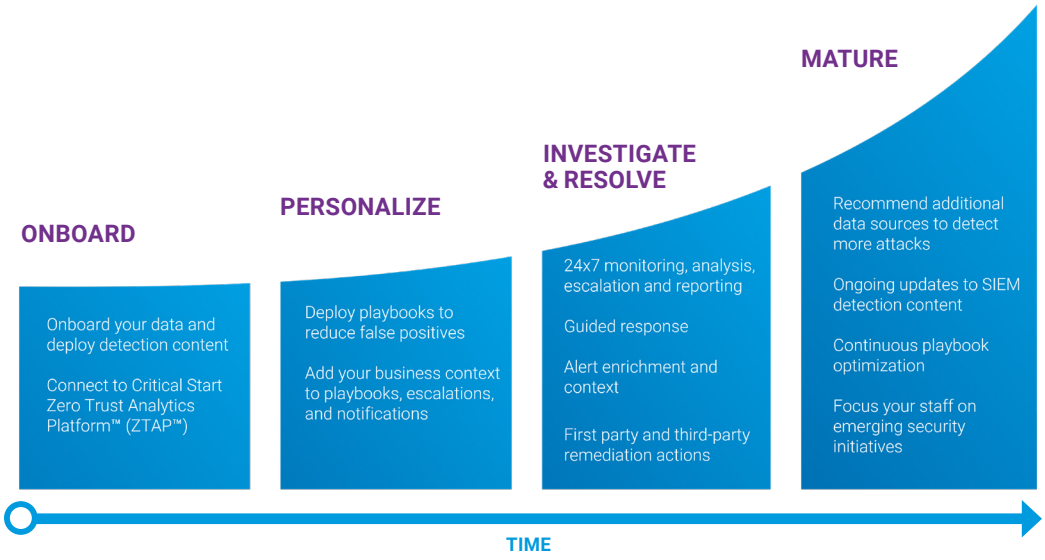
CRITICALSTART® Managed Detection and Response (MDR) services for SIEM simplify the complexity of Security Information and Event Management (SIEM) implementations and give you protection against the latest tactics, techniques and procedures (TTPs). By combining SIEM's flexibility and ability to ingest any vendor's log data with Critical Start's trust-oriented approach to MDR, this solution eliminates false positives at scale to 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 realizing value with any SIEM solution is a journey, and, unfortunately, many businesses do not reach the maturity phase. From the moment you meet with Critical Start, we're with you every step of the way – from Onboarding through Maturity – so your staff can focus on emerging security initiatives.



CRITICALSTART®

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

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

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 Zero Trust Analytics Platform™ (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.

Highly skilled 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.

Unmatched SIEM detection engineering expertise

At Critical Start, simplifying breach prevention with your SIEM means being the most effective at detecting at 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