SOLUTION QUICK CARD

CRITICAL**START**® Managed Detection and Response Services for Splunk® Cloud

Achieve the full operating potential of your Splunk Cloud investment.

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.

Security Information and Event Management (SIEM) solutions can be complex. You must make choices about what data to ingest based on the value of that data and make adjustments as your needs change. Critical Start MDR for Splunk® Cloud simplifies breach prevention and gives you comprehensive insight into your security coverage. By combining Splunk's flexibility and adaptability to ingest data from across the entire security landscape with Critical Start's trust-oriented approach to MDR, this solution enables full operational threat detection and response.

Solution

Critical Start MDR Services for Splunk allows you to:

- Prioritize the log sources you send to Splunk Cloud
- Apply the right detections to those log sources
- Investigate and respond to threats to prevent breaches

How it works

Critical Start helps you prioritize the data being ingested into Splunk Cloud and applies Critical Start Indicators of Compromise (IOCs) to enhance threat detection. Leveraging our seamless integration with Splunk Cloud, our Zero Trust Analytics Platform™ (ZTAP™) automates the investigation and triage of alerts. ZTAP removes false positives and escalates true positives to the Critical Start Security Operations Center (SOC) for further enrichment and investigation. Throughout the service, we make continuous recommendations on additional data sources and update detection content to uncover more attacks.