SOLUTION QUICK CARD

CRITICAL**START**® Managed Detection and Response Services for Microsoft Sentinel™

Achieve the full operating potential of your Microsoft Sentinel 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 Microsoft Sentinel™ simplifies breach prevention and gives you comprehensive insight into your security coverage. Critical Start's trust-oriented approach to MDR combined with the cloud-native scalability of Microsoft Sentinel provides fully optimized threat detection and response for maximized operating potential. We bring our security expertise together with Microsoft tools and adherence to Microsoft Security Best Practices and our Microsoft-certified security staff to deliver end-to-end monitoring, increased efficiency and productivity gains for your security operations team.

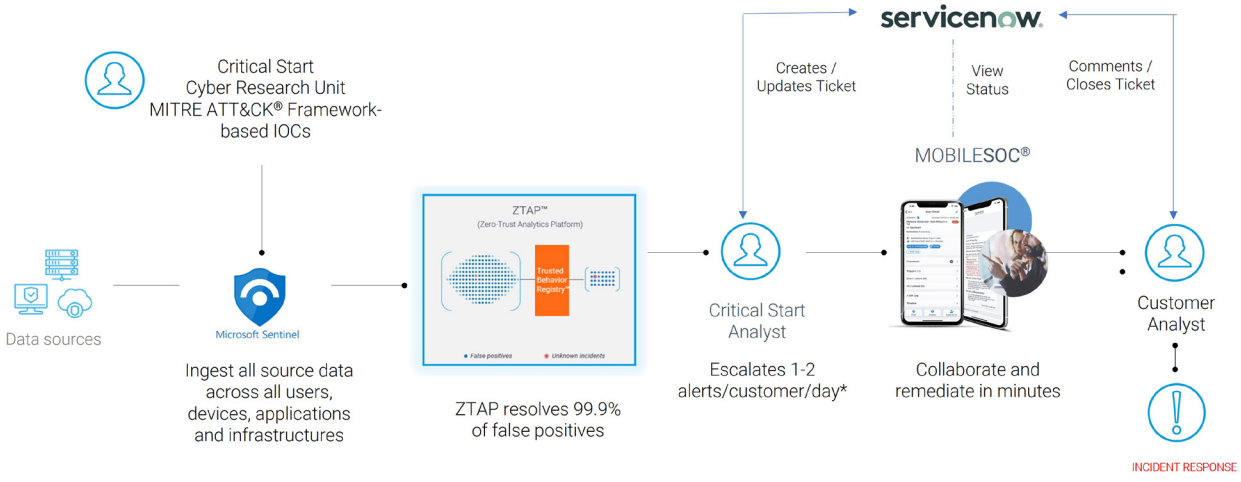
Solution

Critical Start MDR Services for Microsoft Sentinel allows you to:

- Prioritize the log sources you send to Sentinel
- 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 Sentinel and applies Critical Start Indicators of Compromise (IOCs) to enhance threat detection. Leveraging our seamless integration with Sentinel, 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.



*Based on an average of 15,000 alerts ingested into ZTAP per customer/per day