SOLUTION QUICK CARD

Security Coverage Gap Detection

Ensure EDR and vulnerability scanner protection, SIEM data ingestion, and SIEM log health

KEY BENEFITS

- ✓ **Consolidate asset inventories** into a single, useful view that continuously and automatically updates
- ✓ **Determine endpoint protection gaps** in connected EDR tools from CrowdStrike, Sentinel One, Palo Alto, Carbon Black, and many more
- ✓ **Ensure vulnerability scanner coverage** to streamline patching and boost proactive security measures.
- ✓ **Find overlooked SIEM log sources** to ensure you are ingesting all security-relevant telemetry
- ✓ **Detect SIEM log ingestion failures** quickly and restore operations so that you don't miss critical threat signals
- ✓ **Trust your alerts**, knowing that your SOC is expecting all expected signals

You have security tools installed and connected across your network. You know which assets are covered. But can you quickly and easily detect unprotected endpoints? Do you know which SIEM log sources are being overlooked or where interrupted and failed data ingestion are creating blind spots? Are you sure your vulnerability scanner agents are deployed to new hosts? And what about ephemeral assets… are you certain they're protected upon creation?

IT environments move fast. Faster than any team can manually track and update. That's why CRITICAL**START**® Managed Detection and Response (**MDR**) continually scans for coverage gaps across your connected tools. Since you can't protect what you can't see, Critical Start shows you exactly where coverage gaps leave you open to attack.

How it works

The Critical Start Cyber Operations Risk & Response™ (**CORR**™) platform continually curates, de-duplicates, and normalizes asset inventories across all your connected sources. From those sources, it automatically determines assets that lack necessary coverage by endpoint and vulnerability scanner agents.

Additionally, Critical Start monitors SIEM log sources and log ingestion to ensure all relevant log sources are ingested and to monitor for any interrupted ingestion telemetry (referred to as SIEM log health). The latter is compared against pre-determined thresholds, empowering the SOC to alert on log ingestion failures before they cause security gaps.

Endpoint coverage gap detection: Compare configured and integrated EDR endpoint coverage against asset sources to determine assets that lack agents. You can use asset criticality ratings to quickly prioritize remediation to best reduce the risk of a breach across your most vital assets

Vulnerability coverage gap detection: Compare vulnerability scanner deployment across configured asset sources beyond your vulnerability management tool to determine gaps in coverage. For customers will Vulnerability Management Service or Vulnerability Prioritization, you also gain immediate visibility into connected assets that have endpoint coverage gaps.

SIEM detection gaps: Find overlooked SIEM log sources that you have available so you can prioritize them for ingest.

SIEM log health monitoring: Compare SIEM log ingestion data to pre-determined thresholds to see where log monitoring has failed. Use this data to ensure complete SIEM coverage across your IT estate.