Chronicle vs. LogRhythm

The number of SIEM tools your organization must scrutinize before deciding which solution is the best fit are numerous. Every SIEM offering has its pros and cons which complicates the decision-making process. Here, we reduce the complexities of choice by comparing two of the best SIEM solutions available to you.

Chronicle and LogRhythm are two of the more popular IT security solutions organizations rely on to meet threat detection and response needs. Both offer excellent features for discovering threats, log management, security analytics, and incident response features which we will use to compare and contrast both solutions.

Chronicle vs. LogRhythm: threat intelligence

LogRhythm is a next-gen SIEM platform that supports rapid and accurate threat detection process through the collection of relevant data through your IT infrastructures endpoints and analyzes them in real-time. LogRhythm utilizes machine analytics and search analytics to eliminate noise and prevent the proliferation of false alarms. The extensive analytics LogRhythm offer ensure you gain visibility into every aspect of your organization's IT environment to detect security incidents. LogRhythm offers its solution as a single plane of glass to simplify the process of threat detection and intelligence.

Chronicle is a powerful SIEM tool backed by Google. It leverages Google's extensive malware database to pinpoint security incidents and provide insight into the threats within an IT environment. Chronicle collects security telemetry within enterprise networks and automatically analyzes captured logs to discover discrepancies or security incidents. Chronicle provides extensive visibility into security incidents by discovering and highlighting every activity related to a security incident. The contextual information Chronicle provides into threat-related activities eases the detection process for security teams.

Chronicle and LogRhythm were built for mid-range and large enterprises that intend to rely upon or complement IT security efforts with a SIEM tool. According to Gartner's Peer Review, LogRhythm threat intelligence capabilities is rated 4.2/5. Chronicle gets a rating of 4.5 for its analytics dashboard and threat detection capabilities.

Chronicle vs. LogRhythm: security analytics

Chronicle is built on Google's core infrastructure. This gives Chronicle the support required for ingesting large data sets from cloud infrastructure to analyze. Chronicle delivers exceptionally quick analysis that provides security incident reports in seconds. Chronicle's high-performing analytics ensure near real-time abilities to gain insight into security incidents and to fashion a response in seconds.

LogRhythm guarantees real-time data collection and aggregation across cloud and on-premise infrastructure to run its security analysis. LogRhythm applies machine learning in its analytics to map out threats and gain insight into the behavioral patterns of threat agents.

LogRhythm is rated highly for its security analytics capabilities by users. According to Gartner Peer Reviews, enterprises using LogRhythm rates its analytics features 4.5/5. Chronicle also gets a rating of 4.5 for its security analytics features.

Chronicle vs. LogRhythm: ease of use

Security teams that use Chronicle agree that its easy deployment procedures and interactive dashboard simplifies its use. Chronicle rules engine for orchestrating and automating threat detection and response for advanced security incidents. The rules engine can be quickly and easily configured by security teams to built response rules that support real-time monitoring and ensures a quick response.

The use cases security teams intend to apply LogRhythm to determine how advanced its deployment process is. LogRhythm offers multiple products such as its SOAR product and the Behavioral Analytics product within its platform. To take advantage of these products security teams must deploy each solution to meet specific needs. LogRhythm offers a searchable and interactive dashboard to simplify the threat detection and response process when securing extensive IT networks.

Gartner Peer Review gives a rating of 4.3 for its ease of use and the process of deploying LogRhythm to secure enterprise networks. Chronicle is rated 4.7 for its ease of use features and deployment process.