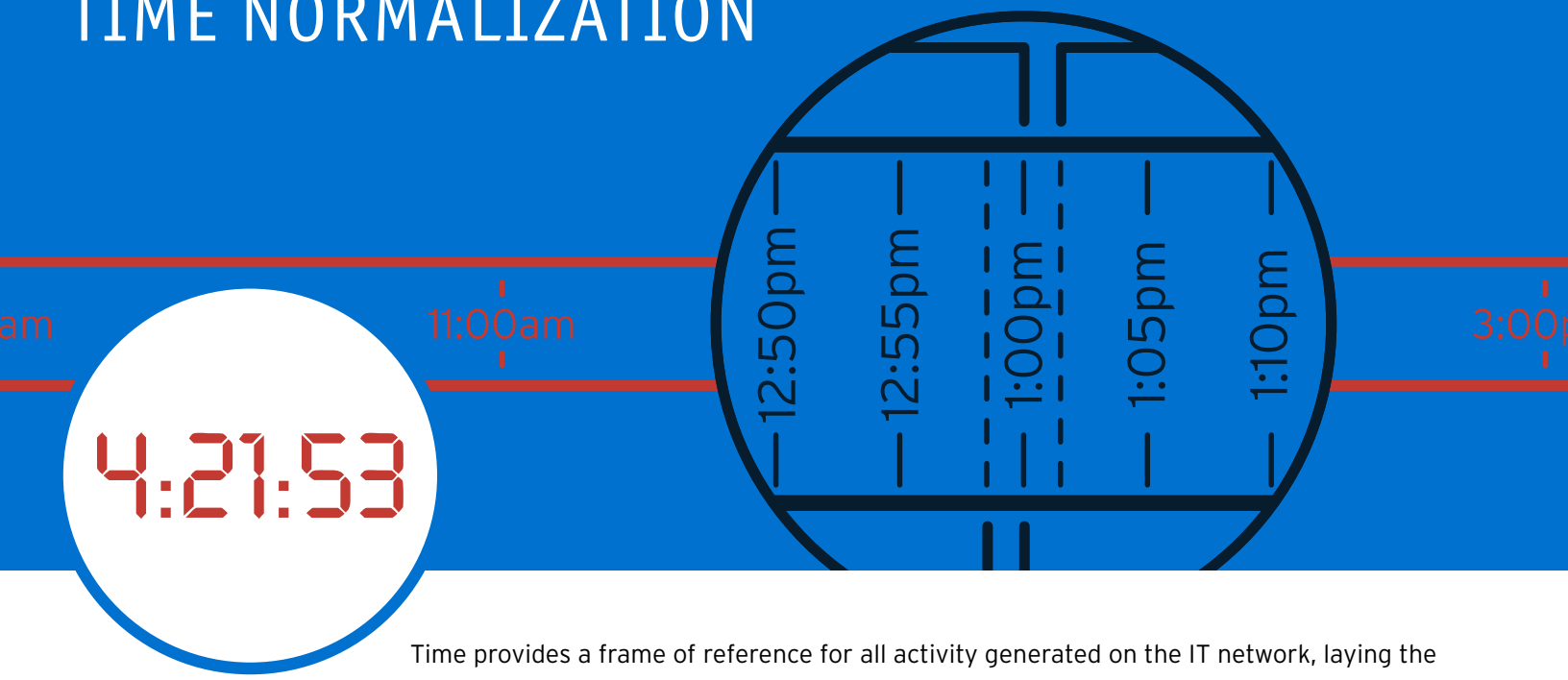
LOGRHYTHM TIME NORMALIZATION

LogRhythm™



Time provides a frame of reference for all activity generated on the IT network, laying the foundation for behavioral modeling and unveiling patterns of suspicious activity. In computing, time variations between disparate data sources can result in inaccurate and incomplete data sets. If security tools are not capturing and analyzing machine data based on the actual time that each event occurs, real-time analytics and event recognition are plagued with blind spots and misinformation resulting in false positive and worse yet, false negatives.

Organizations should not assume that all data generated within their environment is assigned an accurate timestamp relative to the variety of data sources and logging mechanisms across the IT environment. Disparate timestamps can result in data being evaluated out of order which impairs real-time event recognition and response. There are many reasons log and machine data collected for analysis may be attributed to a different time than when the event actually occurred:

- Time Zones: Logs, forensic host and network data collected from geographically dispersed networks introduce time zone disparities that, if not handled properly, result in inaccurate analysis. For example, if a user authenticates to the corporate VPN at 3:00 PM PST and across the country, the same user account authenticates to the web VPN at 6:00 PM EST, real-time analytics need to evaluate these logs against a standardized timeline to recognize that these two logs occurred at the same time and are indicative of compromised credentials [See diagram A].

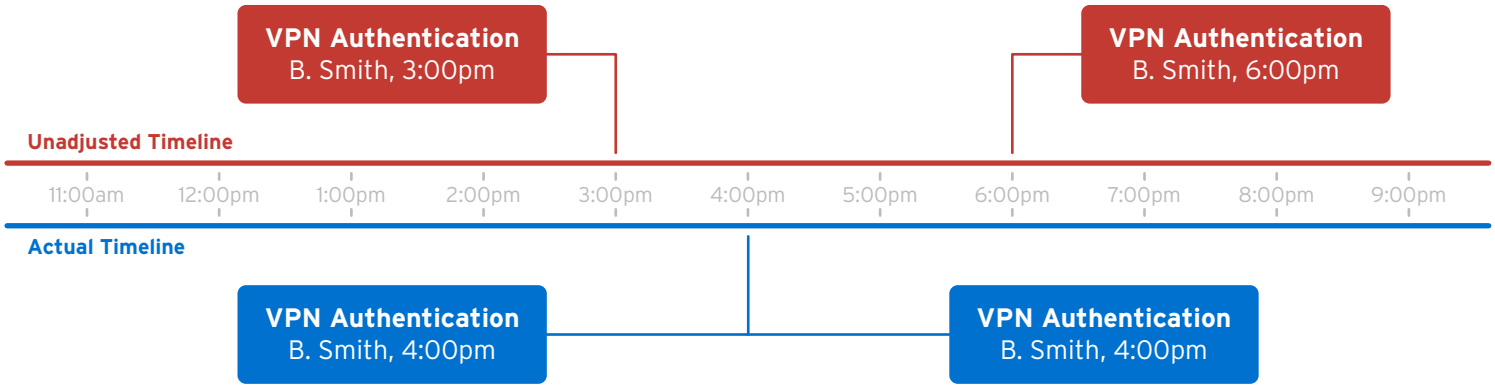


Diagram A – Time Zones

- Desynchronized system clocks: Not all systems within an organization are configured for time synchronization via Network Time Protocol (NTP). And while organizations may have standards for using NTP, there are still situations where new systems are introduced to the network but not assigned NTP servers. Additionally, an organization may only perform an initial sync of system clocks, eventually allowing misalignment in log timestamps. Network outages can also cause systems to become desynchronized with time servers. One example where desynchronized clocks can matter is when data from different sources is received out of order and changes the sequence of events. If an IDS attack signature occurs at 1:00 PM EST and a system configuration change occurs on the same targeted host at 1:01 PM EST, but the system clock is behind by two minutes and records the change at 12:59 PM EST, the events will not be evaluated in the correct order. The true pattern of an IDS attack signature followed by a system configuration change will be missed resulting in a false negative [See diagram B].

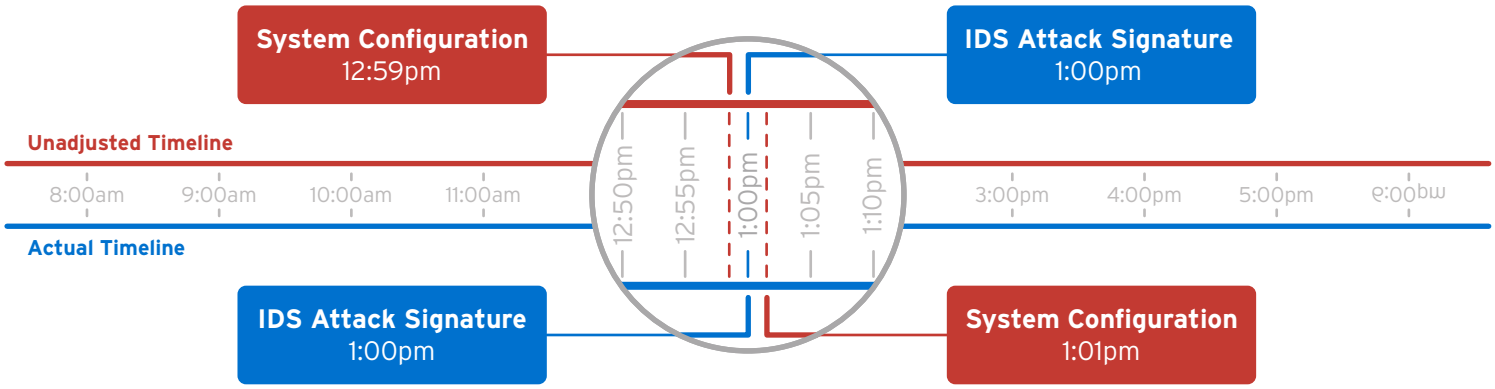


Diagram B – Desynchronized System Clocks

- Timestamps assigned by the collector: If a SIEM or Analytics tool assigns a timestamp when data is collected, the analysis might not take into account delays between the actual occurrence of the event and the time the tool receives the log. There are many reasons for a system to not send log data immediately, such as device reboots/power cycles, processing spikes, and network latency. For example, a switch configuration that is altered at 2:00 PM EST causes a five minute power cycle and the logs describing network allows/denies are delayed until the boot sequence is complete. This delay causes the collector to assign an inaccurate timestamp of 2:05 PM EST to network data, compromising the integrity of the dataset [See diagram C].

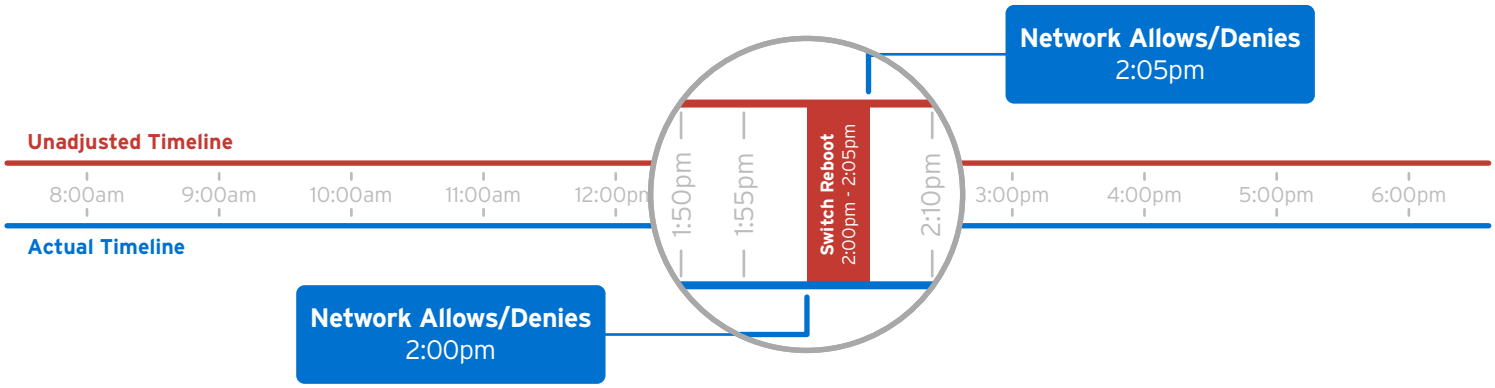


Diagram C – Timestamp at Collection Layer

LogRhythm TrueTime™

Time Normalization is a critical component of security intelligence. LogRhythm's TrueTime™ normalizes data observed in the customer environment to a standardized timeline. This consistent data set allows organizations to understand activities in relation to each other to correctly correlate activity observed on different systems to expose attack patterns, uncover compliance violations, and detect operational issues.

LogRhythm automatically compensates for potential time offsets by applying a universal timestamp to every message as part of initial processing. TrueTime™ synchronizes the timestamps of all log and machine messages to a single 'normal time' which is critical for accurate analysis. The time normalization applied to collected data enhances LogRhythm's real-time machine analytics, enables accurate anomaly detection, improves search accuracy, and allows an analyst to view the true sequence of events during their analysis.

When possible, LogRhythm's collection technology checks the server clock on the original log source and calculates the difference between that time and the universal time used by the LogRhythm deployment. LogRhythm's TrueTime then attributes the difference to the original log time to create a normalized timestamp [See diagram D]. The result is that no matter how frequently the data is received, the time offset is calculated for each individual log. This process ensures that the actual time of occurrence of an activity is recorded and leveraged by LogRhythm's analytical capabilities, regardless of external factors such as an out-of-sync server clock, delayed delivery of a log or differences in time zones.

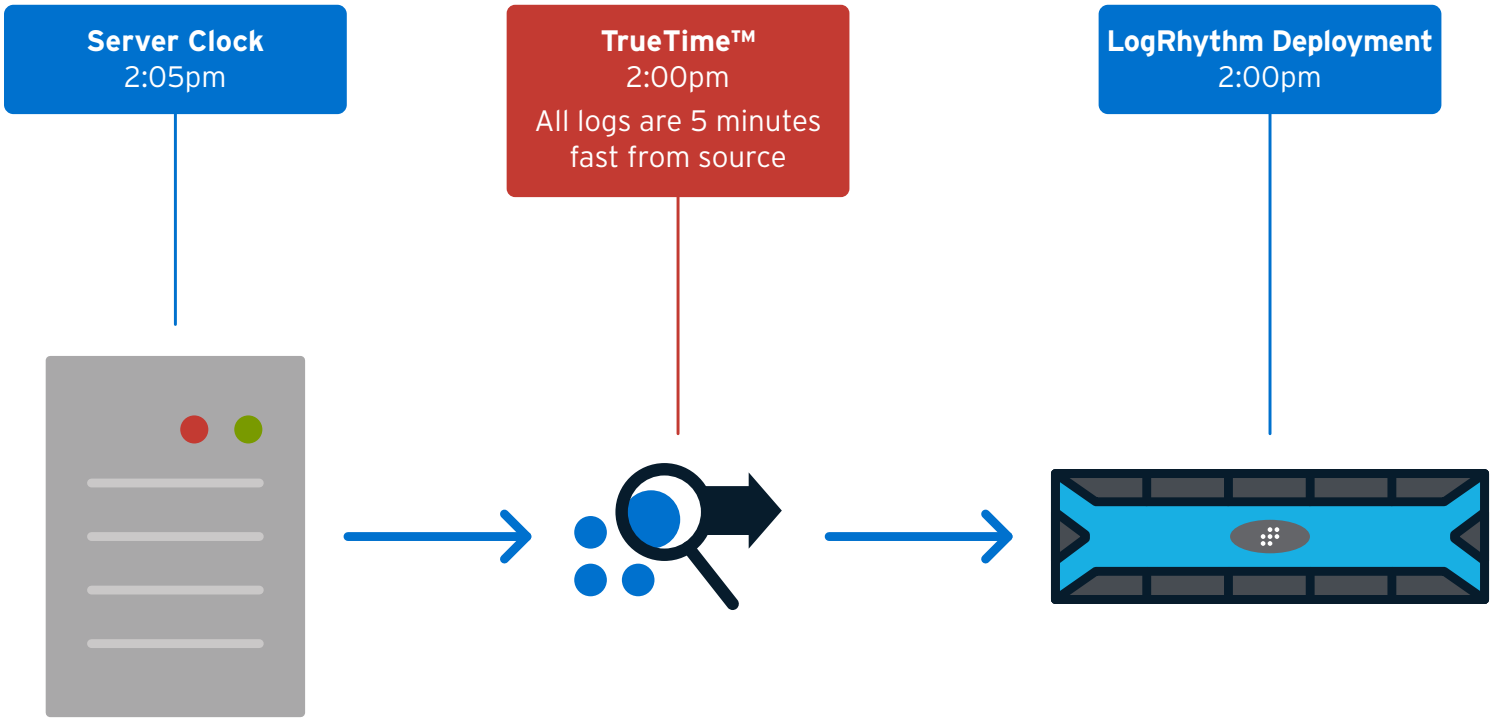


Diagram D - Calculating TrueTime™

LogRhythm Analytics

While many traditional correlation and pattern recognition techniques evaluate data in the order in which it was received, LogRhythm's AI Engine's is able to compensate for data received out of order via the Temporal Chain Normalizer. The Temporal Chain Normalizer is constantly evaluating newly inserted data against in-memory data sets to determine what searches to run based on the combined data set.

LogRhythm's Temporal Chain Normalizer increases the accuracy of advanced analytics in environments with bandwidth constraints and excessive network latency. One instance where network resources are constrained is in organizations with branch offices or remote locations. For example, to ensure that credit cards are processed in a timely manner, many remote retailers with limited connectivity to payment processors will opt to batch collect and then send logs from Point of Sale systems every 30 minutes. This delay in data collection can impact the order in which the data is analyzed and jeopardize the accuracy of event recognition. If a retailer needs to detect external data exfiltration from Point of Sale systems, traditional analysis tools would need to receive the data in the correct order—a VPN authentication, then a file access on a POS system, followed by a firewall allow. Because logs from the POS system are delayed by 30 minutes, the VPN authentication and firewall logs are received well in advance of the file access on the POS system and the criteria for the pattern match is not satisfied, resulting in a false negative. LogRhythm's Temporal Chain Normalizer ensures that advanced analytics are accounting for time offsets in the delivery of data by continuously reevaluating patterns against a dynamic dataset. Once the POS logs are received, the Temporal Chain Normalizer queues the AI Engine to re-run analytics across the new dataset for accurate pattern recognition [See diagram E]. LogRhythm's ability to account for data that is received out-of-order is imperative for organizations that experience both expected and unexpected network delays.

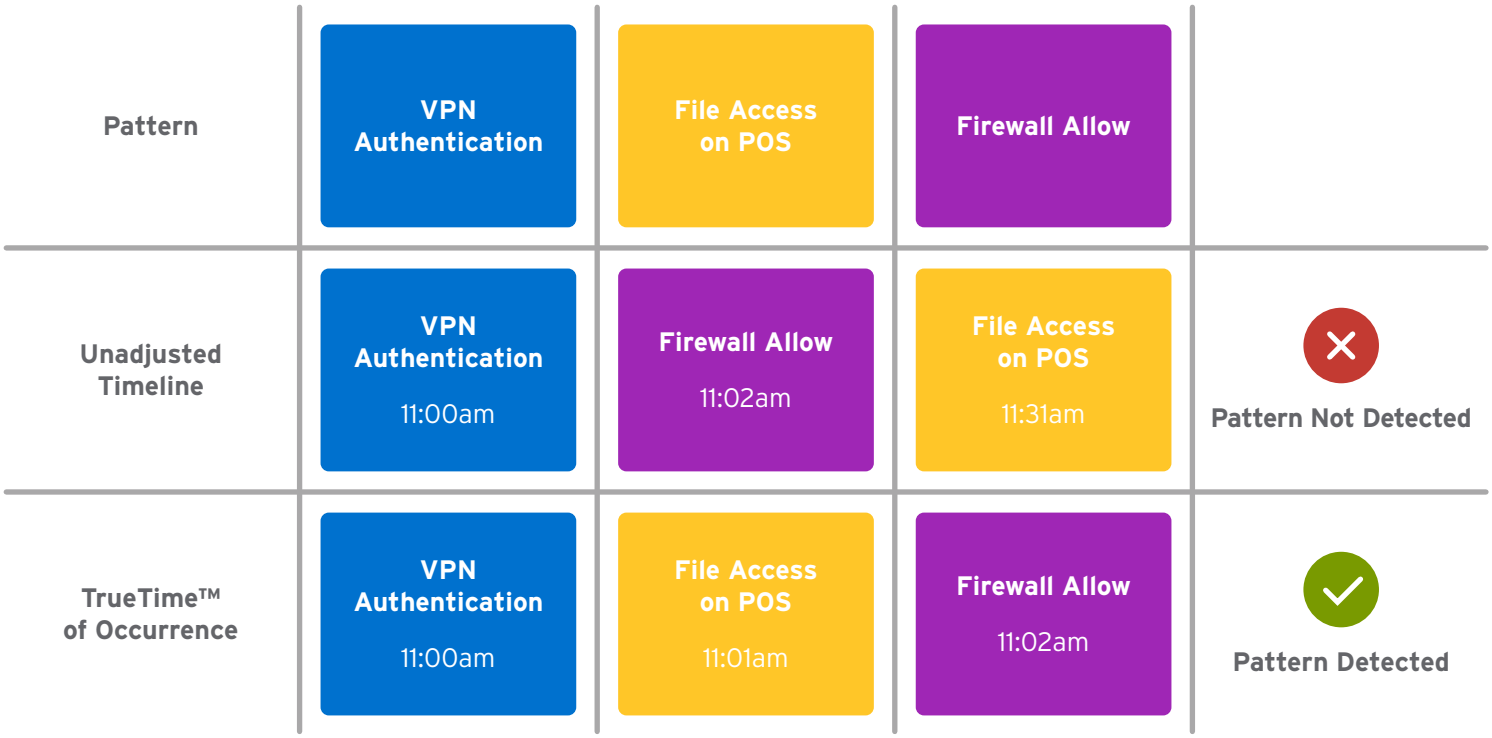


Diagram E - LogRhythm Temporal Chain Normalizer

Analytics that are unable to account for temporal inaccuracies between disparate systems are unreliable and subject to error. LogRhythm's Security Intelligence Platform delivers a unique and patented approach to time normalization via TrueTime™ and the Temporal Chain Normalizer. These capabilities help accurately sequence data to increases the precision of advanced analytics for real-time event recognition and response.