USE CASE

Enriching Event Data with Geographic Context

LogRhythm

Log Management and SIEM solutions provide numerous tools for automatically identifying and communicating what events are happening on your network. With the increasing globalization of information technology, understanding the geographic details of where an event takes place has become an increasingly critical component of incident identification and response.

Knowing the physical origin or destination of specific communications, whether inside or outside the network, can lend immediate urgency to any event. Being able to geographically isolate operations events such as failing communications devices, or to quickly identify the origin and scope of a security breach, can provide immediate value to enterprise IT organizations. The right data can reduce incident response times while providing better information for an appropriate response.

LogRhythm's automated geolocation capabilities provide important geographic context related to internal and external events impacting IT environments of all sizes.

	Adding Geographic Context	Preventing Unauthorized Access	Enforcing Access Control
CUSTOMER CHALLENGE	With the increasing globalization of information technology, geographic context has become a critical component of IT operations and security. Not knowing the physical location of devices and applications involved in an event can handicap root cause analysis and slow response times.	In large enterprises high-volume communication is common, making it difficult to identify unauthorized or anomalous data transfers to or from rogue destinations. The problem is exacerbated when communication related to an event involves multiple sources.	With today's global workforce, many employees access company networks from different locations around the planet, including many who log in from multiple locations over a given period of time. Identifying improper usage of authorized credentials among thousands of legitimate logins is a difficult task.
LOGRHYTHM SOLUTION	LogRhythm automates the process of adding geographic context to any event data. This adds immediate context for performing root-cause analysis, forensic investigations and recognizing incident propagation.	LogRhythm's intuitive, wizard-based setup for alarms and investigations makes it a simple process to establish blacklists that automatically identify any communication with unauthorized or rogue locations, whether inbound or outbound.	LogRhythm's data management allows geolocation data to be correlated against any field. LogRhythm users can easily create alarms that will send an alert when communications from authorized users is coming from geographic locations that are not on a predefined whitelist.
ADDITIONAL BENEFITS	LogRhythm offers an automated geolocation service that automatically populates unknown geographic context, either from within the network or from external and anonymous IP addresses.	Once a problem has been identified, LogRhythm provides numerous tools for understanding the scope and specific details. From interactive trending and relationship mapping to on-screen keystroke filtering, administrators can immediately zoom in on the relevant context surrounding a significant event.	When an alert is generated, all activity by that user or from that location can be immediately investigated with a simple right-click, providing a complete picture of suspicious behavior patterns tied to specific data points.