USE CASE

Continuous Monitoring - A Cornerstone for Risk Management

LogRhythm™

The implementation of continuous monitoring is a critical step in any successful risk management strategy, particularly for larger enterprises and government organizations. It establishes the ongoing collection and automated analysis of all log and event data, looking at all records of activity and performing real-time advanced correlation and pattern recognition. Continuous monitoring can alert on individual and broader malicious event sequences simplifying remediation and helping mitigate risk.

Continuous monitoring is one of six steps in the Risk Management Framework (RMF) outlined in NIST Special Publication 800-37, Revision 1 and is a major component for validating the Recommended Security Controls for Federal Information Systems and Organizations outlined in NIST Special Publication 800-53, Revision 3. It is also critical for maintaining organizational risk management strategies related to commercial regulations, such as Sarbanes-Oxley, by providing information required to establish sufficient internal security controls for ongoing compliance assurance.

Continuous monitoring combines process and technology, detecting and alerting on operational and security issues related to a wide range of compliance and risk concerns.

Lowering TCO	Establishing Compliance	Advanced Persistent Threats
CUSTOMER CHALLENGE		
Many solutions for continuous monitoring require extensive time to configure, operate and manage, relying too much on manual or overly complex processes. Without effective automation and usability, continuous monitoring strategies are cost-prohibitive, inefficient and produce inconsistent results.	Establishing a continuous monitoring program is necessary, but regulations and best-practices for risk management policies require 3rd party security authorization of the program. This frequently involves extensive manual processes or implementation of a secondary tool to provide auditors with validation information.	Large enterprises and government organizations in particular are increasingly targeted by Advanced Persistent Threats (APTs.) The complex nature and extensive backing behind APTs makes it difficult to adapt quickly to new, highly sophisticated malware and rapidly changing malicious behavior.
LOGRHYTHM SOLUTION		
LogRhythm is easy to deploy, manage and operate. Monitoring, analysis, alerting and reporting are automated, delivering consistent real-time results without burdening operations and security staff with extensive overhead.	LogRhythm provides out-of-the-box compliance packages, including FISMA, SOX, HIPAA, NERC-CIP and PCI to provide automated compliance assurance. Packages include automated compliance reporting packages, best-practice oriented forensic investigation templates, and extensive prepackaged rules for advanced correlation and pattern recognition.	LogRhythm's AI Engine delivers continuous monitoring with automatic analysis of all log data, maintaining constant vigilance for multiple attack vectors that, when combined, may indicate an APT-style attack. Access to underlying forensic data is immediately available, for rapid understanding.
ADDITIONAL BENEFITS		
LogRhythm employs common controls, allowing it to be leveraged by multiple departments. By analyzing all log and event data and creating a consistent look and feel with wizard-based and fully interactive visualization, LogRhythm can provide value to any operations, security or compliance staff.	Reports, templates and advanced correlation rules can be easily adapted to fit new security and operations scenarios and to meet updated or new regulations.	LogRhythm's SmartResponse delivers out-of-the-box automated remediation with an option for up to 3 levels of required authorization. It delivers effective responses to real issues based on a complete set of operations, compliance and security data.