USE CASE

Protective Monitoring – A Platform for Risk Management

LogRhythm

The implementation of Protective Monitoring is a critical step in any successful risk management strategy, particularly for larger enterprises and government organisations. 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. Protective Monitoring can alert on individual and broader malicious event sequences simplifying remediation and helping mitigate risk.

Protective Monitoring within the scope of the UK government's CESG Good Practice Guide 13 (GPG 13), is a major component for providing essential oversight of ICT systems. It is also critical for maintaining organisational risk management strategies related to commercial regulations, such as PCI DSS, by providing information required to establish sufficient internal security controls for ongoing compliance assurance.

Protective 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

CUSTOMER CHALLENGE

Many solutions for Protective Monitoring require extensive time to configure, operate and manage, relying too much on manual or overly complex processes. Without effective automation and usability, Protective Monitoring strategies are cost-prohibitive, inefficient and produce inconsistent results.

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.

ADDITIONAL BENEFITS

LogRhythm employs common controls, allowing it to be leveraged by multiple departments. By analysing all log and event data and creating a consistent look and feel with wizard-based and fully interactive visualisation, LogRhythm can provide value to any operations, security or compliance staff.

Establishing Compliance

Establishing a Protective Monitoring program is necessary, but regulations and best-practices for risk management policies require 3rd party security authorisation of the program. This frequently involves extensive manual processes or implementation of a secondary tool to provide auditors with validation information.

LogRhythm provides out-of-the-box compliance packages, including GPG 13, SOX, HIPAA, GCSX and PCI DSS 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.

Reports, templates and advanced correlation rules can be easily adapted to fit new security and operations scenarios and to meet updated or new regulations.

Advanced Persistent Threats

Large enterprises and government organisations in particular are increasingly targeted by Advanced Persistent Threats (APT). 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's Advanced Intelligence Engine delivers Protective 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.

LogRhythm's SmartResponse provides out-of-the-box automated remediation with an option for up to 3 levels of required authorisation. It delivers intelligent, immediate responses to real threats based on advanced analysis of comprehensive operations, compliance and security data.