

Protective Monitoring: GPG 13 Compliance

Introduction

Protective Monitoring for HMG ICT Systems is based on CESG's Good Practice Guide no.13 (GPG 13.) It provides a framework for treating risks to systems and includes mechanisms for collecting ICT log information and configuring ICT logs in order to provide an audit trail of security relevant events of interest.

All HMG organisations, whether central or local government, police, fire, health and education authorities are mandated to comply with policy, standard, legislative and regulatory requirements. Protective Monitoring with its levels of log management and reporting can help in forensic readiness, incident management and most importantly, delivering against these regulatory requirements by providing evidence of compliance to the auditors.

A fundamental component of an effective Protective Monitoring strategy is an automated Log and Event Management platform that delivers a repeatable service to all stakeholders.

Requirements

There are 12 Protective Monitoring Controls (PMC) defined by GPG 13 describing specific organisational requirements for monitoring. Each PMC has a Recording Profile which measures the strength of a particular solution.

Information systems must be monitored in real time to ensure compliance with GPG 13 best practices. Investigations, Reports, and Alarm Rules must provide immediate analysis and notification of conditions that are impacting the integrity of the enterprise. Areas of non-compliance should also be identifiable in real-time. When investigating automation of these requirements, key functionality should also be available in the log management solution such that additional reports and alarm rules are available to further augment the usefulness of the log data.

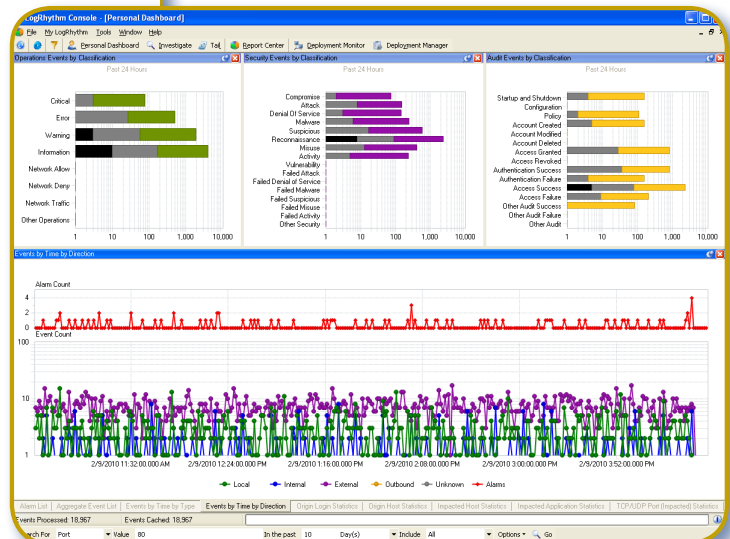
Solution Summary

LogRhythm is deployed with an integral report package developed specifically to address the needs of GPG 13. Using our inbuilt information classification schema to simplify the task of interpreting detailed technical information into logical business and compliance language, LogRhythm's time to value is extremely rapid. Enterprise assets defined within the scope of the Protective Monitoring compliance mandate are categorised by control type and these devices are eligible for inclusion in the report framework. Reports can be generated as needed by the GPG 13 Compliance Officer, and scheduled to run at pre-determined intervals.

Additional benefits to be gained from adopting an automated approach to Protective Monitoring are visibility into your security posture, controlling the cost of demonstrating compliance, and reducing the complexity of managing a heterogeneous IT infrastructure.

LogRhythm Accelerates GPG 13 Support

- o **Demonstrate Compliance**
Ensures ICT systems operate within the requirements of applicable policies, legislation and regulations.
- o **Enhanced Risk Management**
Provides an essential contribution to the mitigation of risks to the confidentiality, integrity and availability of information assets processed by ICT systems.
- o **Reporting and Continuous Improvement**
Contributes to mandatory reporting elements of Security Policy Framework and regulatory controls.
- o **Situational Awareness**
Ensures system owners are provided with a real-time feed of information regarding the status and threats to ICT systems enabling security incidents to be detected, investigated and effectively remediated.
- o **Enables Accountability**
Ensures that ICT is used within the parameters defined and not used for wasteful or unlawful purposes.
- o **Complements Network Defence**
Enhances the value of other security countermeasures to provide a complete "defence in depth" approach and facilitate automated responses to threats to ICT.



GPG 13 Dashboard

The table below shows the 12 Protective Monitoring Controls defined in GPG 13, how LogRhythm demonstrates compliance against the control and the added value benefits gained.

Protective Monitoring Control		Solution	Benefit
PMC1	Accurate time in logs.	LogRhythm collects logs and delivers them to the LogRhythm Mediator Service using best practices for ensuring the integrity of the audit data.	Ensures that all logs have accurate time stamps without compromising the integrity of the original log.
PMC2	Recording relating to suspicious activity at a boundary.	LogRhythm collects logs from boundary security monitoring devices providing unparalleled insight to incidents and threats.	Automated log reviews generates cost savings in trending and real-time attack investigation.
PMC3	Recording of workstation, server or device status.	LogRhythm collects detailed logs from network connected devices and can provide File Integrity Monitoring to extend protection over critical data.	Comprehensive analysis of control system changes reducing risk to organisation.
PMC4	Recording of workstation, server or device status.	LogRhythm collects detailed logs from network connected devices and can provide File Integrity Monitoring to extend protection over critical data.	Comprehensive analysis of control system changes reducing risk to organisation.
PMC5	Recording relating to suspicious internal network activity.	LogRhythm records detected suspicious activity, including misuse and vulnerability exploitation.	Improves investigation ability by being able to track behaviour by user, network identity and application.
PMC6	Recording relating to network connections.	LogRhythm collects logs from network devices, including access control and network flows, to retain details of network activity.	Aids security investigations by identifying crucial systems that frequently change their network identity.
PMC7	Recording of session activity by user and workstation.	LogRhythm collects logs that assist in the recreation of session activities and retains them for forensic analysis.	Preserves evidential trail, and reduces time and cost of forensic investigation.
PMC8	Recording of data backup status.	LogRhythm collects logs from backup systems and reports on successes, failures, as well as operational status that could influence backups.	Supports efficient IT operations by enabling robust archiving systems robust.
PMC9	Alerting critical events.	LogRhythm can alarm on pre-defined conditions that can be displayed on the console or sent via the notification service to e-mail or via SNMP.	LogRhythm minimises an organisation's response time for critical events.
PMC10	Reporting on the status of the audit system.	LogRhythm manages the enterprise audit system.	Saves time and money by simplifying log and audit readiness.
PMC11	Production of sanitised and statistical management reports	LogRhythm supports the generation of reports that omit detail that was used as part of the reports creation.	Custom report enables generation of reports for special needs, including for use by external agencies and management.
PMC12	Providing a legal framework for Protective Monitoring activities.	LogRhythm collects notifications from third party tools that allows for tracking of legal message response or any other custom source.	Industry leading rule building technology saves time and money when handling custom log formats.