GOOD PRACTICE GUIDE 13 (GPG13)

GPG13 - AT A GLANCE

- Protective Monitoring (PM) is based on Good Practice Guide 13
- Comprises of 12 sections called Proactive Monitoring Controls 1-12
- Based on four Recording Profiles; Aware, Deter, Detect/Resist and Defend.
- Protective Monitoring and GPG 13 names are sometimes used interchangeably.
- GPG 13 is a framework of people, businesses and processes
- Designed to reduce risk
- Strong recommendation for all HMG ICT Systems and compulsory for systems that store high impact level data.
- Goal is provide an operational insight of IT use and abuse
- PM / GPG 13 is mandated by the Security Policy Framework which is published by the UK Cabinet Office

Background

In order to gain access and share information that resides on the Government Connect Secure Extranet (GCSX), all public sector organisations are required to comply with published standards that have existed for many years. These organisations include both central government departments and local authorities. For example, the most well-known compliance requirement that local authorities must demonstrate is adherence to Code of Connection (CoCo) which came into effect in 2009. CESG, the Government's National Technical Authority for Information Assurance, added 35 guides as part of CoCo. These guides are widely known as Good Practice Guides and were created to help organisations manage risk effectively in areas many areas including remote working, offshoring, virtualisation and forensics.

What is GPG13?

Of the 35 guides the Good Practice Guide 13 (GPG13) defines requirements for 12 Protective Monitoring Controls (PMC) which comprise of tasks such as event log management and use of intrusion detection and prevention systems. Local authorities are required to conform to GPG13 in order to prevent accidental or malicious data loss. As connection to GCSX encompasses access to sensitive and confidential data, compliance with GPG13 is imperative for protecting privacy and preventing data breaches. GPG13 It is imperative that log is collected from systems that provide the security mechanisms.

GPG13 has four Recording Profiles that roughly map to the HMG Information Assurance Standard Segmentation Model which has four hierarchical segments; **Aware, Deter, Detect/Resist** and **Defend.** The necessary controls are all related to all aspects logging, recording, reporting of network traffic flows, critical events and activities as defined below.

Aware	Obligation to be **Aware** of public domain threats, common attack vectors and known vulnerabilities.
Deter	Obligation to **Deter** an attack from a skilled hacker. Appropriate controls should be in place to Deter such an attack.
Detect/Resist	Obligation to both **Detect** the attack and **Resist** the attack from a sophisticated attacker.
Defend	Obligation to **Defend** against an attack from a sophisticated attacker.

GPG13 Guidelines for Log Management

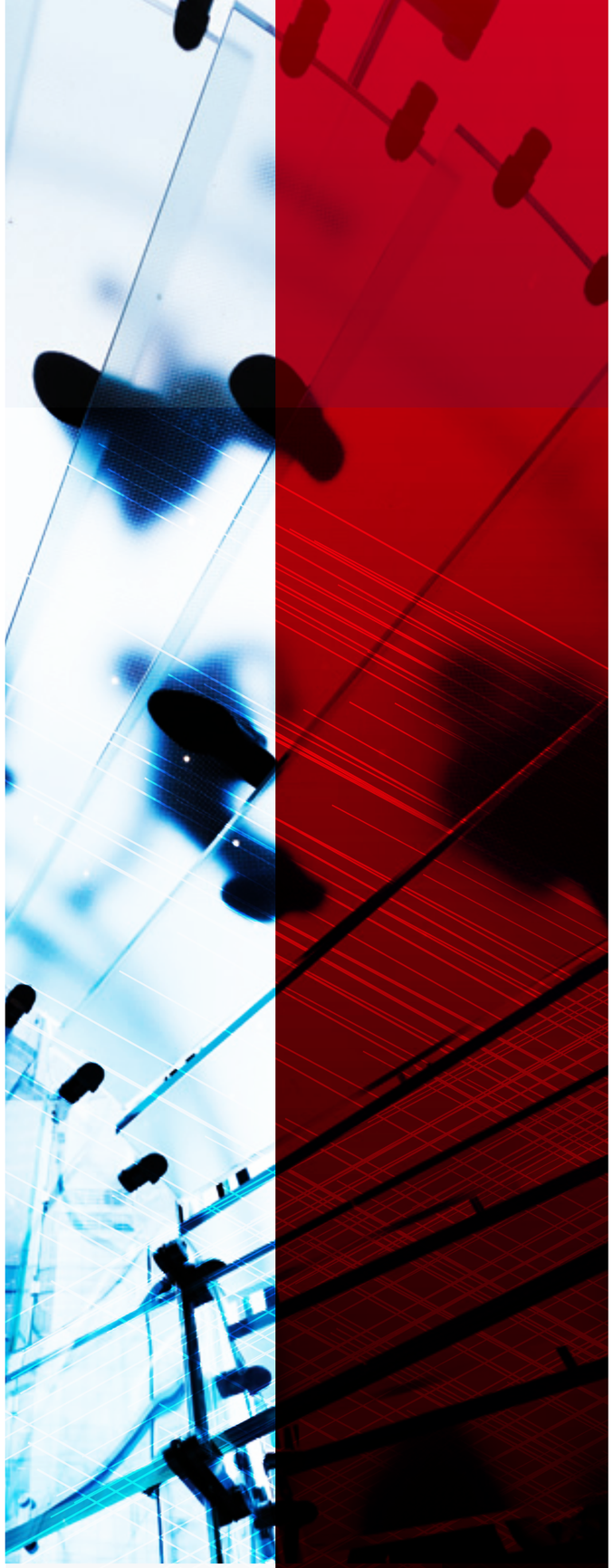
Log management is the key and mandatory component for government departments to achieve GPG13 compliance. Networks nowadays produce millions of logs from across the entire infrastructure that are required to be captured, analysed, alerted upon and stored daily. This is an enormous task that IT staff has to endure in developing and managing log data efficiently to help solve complex compliance challenges. Data required for GPG 13 is collected from systems that are in place to secure organisations and includes firewall logs, intrusion systems and alerts from operating systems. As part of meeting GPG13 requirements, the guidelines below must be followed.

Segment (Risk Level)	Log Retention Period	Log Checks	Console Manning	Compliance Review Period
Aware (Medium)	Up to 3 months	At least once a month	Not always but alerts form critical conditions must be managed	At least annually
Deter (Medium-High)	3 to 6 months	At least once a week	Only during core business hours	
Detect/Resist (High)	6 to 12 months	At least once a day	Always manned	At least every 6 months
Defend (Very High)	More than 12 months	At least once every hour		At least every quarter

GPG13 Guidelines for Incident Response

Any alerts generated require a response and depending on the severity service level agreements need to be established as outlined below:

Segment (Risk Level)	Preliminary Response	Analysis Instigated
Aware (Medium)	Less than 1 day	No Guidance
Deter (Medium-High)	Less than 4 hours	Within 2 days
Detect/Resist (High)	Less than 1 hour	Within 1 day
Defend (Very High)	Less than 30 minutes	Within 4 hours

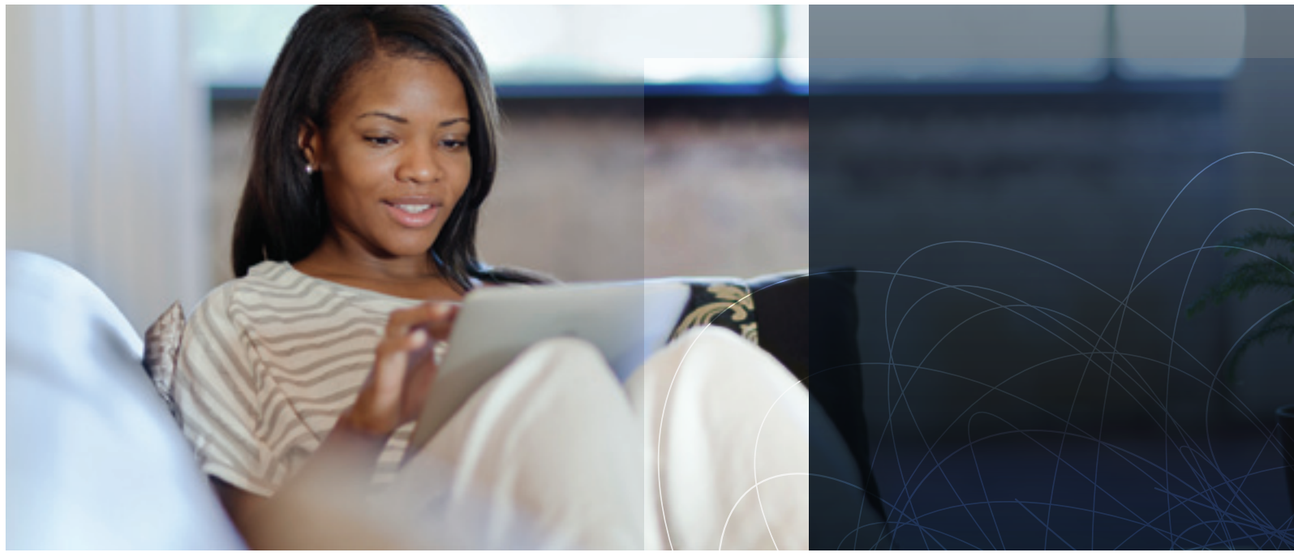


Achieving GPG 13 Compliance with McAfee

To help organisations meet GPG13 compliance, the SIEM (Security Information Event Management) solution from McAfee forms the essential component that delivers data monitoring and collection requirements at all the 12 Protective Monitoring Control levels. McAfee SIEM is complimented by additional McAfee technologies that is a combination of perimeter security, intrusion detection/ prevention systems, end point protection and two-factor authentication all of which are integrated to form the Security Connected framework. The amalgamation of different solutions ensure system activity logs, real time file integrity control, privileged identity activity and critical application session data seamlessly fall under the SIEM reporting umbrella.

The following table illustrates a direct one-one mapping of the PM Controls to the McAfee solutions where SIEM is the integral constituent.

	Aware	Deter	Detect/Resist	Defend
PMC #1- Accurate time in logs Time stamps compared to thresholds to look for discrepancies and compliment with external time source.	• SIEM • ePO • Policy Auditor	• SIEM • ePO • Policy Auditor	• SIEM • ePO • Policy Auditor	• SIEM • ePO • Policy Auditor
PMC #2- Recording relating to business traffic crossing a boundary Collection and analyses of logs from perimeter security, end point security and asset database all collected centrally.	• SIEM • Firewall • Web GW • ePO	• SIEM • Firewall • Web GW • ePO	• SIEM • Firewall • Web GW • ePO	• SIEM • Firewall • Web GW • ePO
PMC #3- Recording relating to suspicious activity at a boundary Collection and analyses of logs from firewalls. IDS/IPS, authentication controls, end point protection and other systems used at the boundary.	• SIEM • Firewall • Web GW	• SIEM • Firewall • Web GW • IDS/IPS	• SIEM • Firewall • Web GW • IDS/IPS	• SIEM • Firewall • Web GW • IDS/IPS
PMC #4- Recording of workstation, server or device status Collection and analyses of logs from workstation. Servers, network devices, security devices, databases and applications.	• SIEM • ePO • Anti-Virus • Database Security	• SIEM • ePO • Anti-Virus • Database Security	• SIEM • ePO • Anti-Virus • Database Security	• SIEM • ePO • Anti-Virus • Database Security
PMC #5- Recording relating to suspicious internal network Collection and analyses of logs from diverse systems such as authentication systems, networks services (DNS, DHCP, WINS), firewalls, databases and network traffic.	• SIEM • Firewall	• SIEM • Firewall	• SIEM • Firewall • ePO • File Integrity	• SIEM • Firewall • ePO • File Integrity
PMC #6- Recording relating to network connections Collection and analyses of logs from diverse systems such as authentication systems, networks services (DNS, DHCP, WINS), firewalls, databases and network traffic.	• SIEM	• SIEM	• SIEM • IDS/IPS	• SIEM • IDS/IPS
PMC #7- Recording of session activity by user and Workstation Import users and workstations from provisioning systems such as Active Directory. McAfee collects logs centrally for auditing, analyses and alerting.	• SIEM • Database Security	• SIEM • Database Security	• SIEM • Database Security • Change Control	• SIEM • Database Security • Change Control
PMC #8- Recording of data backup status Collect logs from external backup systems.	• SIEM • Backup	• SIEM • Backup	• SIEM • Backup	• SIEM • Backup
PMC #9- Alerting critical events McAfee is able send critical alerts to third party service management systems such as BMC and HP.	• SIEM	• SIEM	• SIEM	• SIEM
PMC #10- Reporting on the status of the audit system The system is able to alert on its health for any failures and thresholds.	• SIEM	• SIEM	• SIEM	• SIEM
PMC #11- Production of sanitised and statistical management reports McAfee provides high-level reports and dashboards out of the box. Report data can be exported to PDF, XML, CSV and HTML.	• SIEM	• SIEM	• SIEM	• SIEM
PMC #12- Providing a legal framework for Protective Monitoring activities Collected logs are normalised for management and auditing purposes by McAfee SIEM. In addition logs are stored and retained in original/raw format for forensics and legal requirements.	• SIEM	• SIEM	• SIEM	• SIEM



McAFEE VALUE FOR GPG 13 COMPLIANCE

Key benefits

- McAfee SIEM is positioned as a Leader by Gartner for completeness of vision and ability to execute
- Experienced and trained McAfee Professional Services can work with organisations to achieve GPG 13 requirements
- McAfee SIEM provides GPG 13 out of the box and does not require additional licenses as some other vendors.
- Built-in capability to collect log data from over 300 data sources with ability to create additional as required.
- GPG 13 reports and dashboards are pre-built with options to create custom as required
- The Security Connected approach provides a framework for cost effective management where multiple technologies are integrated seamlessly.
- Log management solutions are complex and costly. McAfee SIEM can be set-up quickly and easily with minimum effort.

Operational benefits

- Global view of the security countermeasures and insight into the security landscape.
- Minimum administration overhead as McAfee SIEM is designed to with specifically for log management.
- Log data views can be changed from years to seconds instantaneously
- Reduces overhead in identifying threats from days to seconds with the integration into GTI.
- Reduced deployment cost with “out of the box” functionality
- Integration into the complete McAfee management platform with feeds from GTI (Global Threat Intelligence)
- Unparalleled performance and scalability with log collection capability of 300,000 EPS
- Fully context and content awareness to ascertain risk levels
- Collected log data stored in two places ; original format for forensics and secondly correlation

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), is the world's largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by its unrivaled global threat intelligence, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. McAfee is relentlessly focused on constantly finding new ways to keep our customers safe. http://www.mcafee.com

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com