Protective Monitoring

GPG 13 Compliance with Assuria Log Manager

Log Management. Analysis & Alerting. Protective Monitoring.
Forensic Readiness. CESG CCTM Accredited

CESG's Good Practice Guide No.13 (GPG 13) Protective Monitoring framework has been created for HMG ICT Systems to provide guidance on how to monitor their infrastructure. GPG13 contains 12 Protective Monitoring Controls (PMCs) that align to levels of risk and how these should be treated.

GPG13 is a guide and not a standard. Assuria will work with accreditors in order to ensure and satisfy the GPG13 protective monitoring and customers own requirements.

Assuria Log Manager (ALM) our Forensic Log Management / SIEM solution has built-in analysis rules, alerts and reports which meet the GPG13 PMC requirements at Aware, Deter, Detect and Resist and Defend levels. ALM is a proven GPG13 solution, and is deployed and fully operational in UK classified projects up to the highest levels of classification. ALM provides built-in GPG13 analysis, alerting and reporting features through the optional ALM GPG13 Content Pack.

Assuria provides documentation, advice and support on configuration of audit and collection policy to ensure that the relevant devices, applications etc. generate the appropriate audit events in logs, and that ALM collects the relevant logs and events to meet GPG13 Protective Monitoring Controls.

TABLE. How ALM assists with GPG 13 Compliance:

Protective Monitoring Control	Assuria Log Manager (ALM) Supporting Information
PMC1 - Accurate time in logs	Assuria ALM collects logs in datasets, each consisting of a log (".evt") file and a metadata file ("metafile"). The metafile contains, amongst other things: • A UTC timestamp stating when the dataset was created (with respect to the agent machine's clock). • The time zone offset from UTC of the agent's clock. • SHA256 (.evt file). • A number of digital signatures, depending on configuration. Each ALM dataset therefore has a digitally signed timestamp provided by the agent, and ALM digitally-signs any/all timestamps within the log data. ALM Agents and Collectors compare their current time when they communicate, if their clocks diverge by more than a configurable threshold then the Collector logs a warning and can be configured to generate an alert.

Assuria Ltd. Reading Enterprise Centre, The University of Reading, Reading, Berkshire RG6 6BU U.K.
W: www.assuria.com E: info@assuria.com Tel: +44 118 935 7395

Protective Monitoring
GPG 13 Compliance

assuria

Log Management. Analysis & Alerting. Protective Monitoring.
Forensic Readiness. CESG CCTM Accredited

Protective Monitoring Control	Assuria Log Manager (ALM) Supporting Information
PMC2 - Recording relating to business traffic crossing a boundary	ALM has an asset database that is used to define device characteristics. For example devices can be given the characteristic of "boundary" via the ALM user interface or populated from a Configuration Management Database (CMDB). ALM allows simplified management of assets which can help with environments that change on a regular basis.
PMC3 - Recording relating to suspicious activity at firewall or IDS at the boundary	ALM collects, alerts, analyses and reports on events from firewalls, IDS / IPS and many different network security devices used at the boundary.
PMC4 - Recording of workstation, server or device status	ALM collects, alerts, analyses and reports on events from workstations and servers spanning many different platforms.
PMC5 - Recording relating to suspicious internal network activity	ALM collects, alerts, analyses and reports on events from the customers own detection systems and can help capture malware detection whilst utilising existing resources to help reduce the overall cost and complexity. Out of the box ALM provides alerts and reports for suspicious network activity and in addition Assuria will work with customers to define specific internal attack definitions.
PMC6 - Recording relating to network connections	ALM collects, alerts, analyses and reports on events including various IP address allocation tracking functions such as DHCP, DNS, Netflow and VPN logs including device configuration and or rule changes.

Assuria Ltd. Reading Enterprise Centre, The University of Reading, Reading, Berkshire RG6 6BU U.K.
W: www.assuria.com E: info@assuria.com Tel: +44 118 935 7395

Protective Monitoring
GPG 13 Compliance

Log Management. Analysis & Alerting. Protective Monitoring. Forensic Readiness. CESG CCTM Accredited

Protective Monitoring Control	Assuria Log Manager (ALM) Supporting Information
PMC7 - Recording of session activity by user and workstation	This is standard product functionality for ALM. ALM provides standard reports which include aggregation by user name hostname and event details The ALM Console view shows all login activity which can be selected by a number of criteria, including username, hostname and reason amongst others ALM's Searcher tool allows fast and extensive log interrogation using 'Google like' simple queries or more complex queries with full regex support
PMC8 - Recording of data backup status	ALM collects, alerts, analyses and reports on events from logs collected from backup software.
PMC9 - Alerting upon critical events	ALM can be configured to send alerts to external systems, such as via SNMP to HP OpenView or the alerts are processed within ALM and displayed in the ALM console The alerting can be configured to prevent unnecessary multiple alerts. ALM includes Role Based Authentication (RBAC), and it is possible to provide the User with a defined Dashboard view. ALM enables temporary suspension of selected events.

Assuria Ltd. Reading Enterprise Centre, The University of Reading, Reading, Berkshire RG6 6BU U.K.
W: www.assuria.com E: info@assuria.com Tel: +44 118 935 7395

Protective Monitoring
GPG 13 Compliance

assuria

Log Management. Analysis & Alerting. Protective Monitoring.
Forensic Readiness. CESG CCTM Accredited

Protective Monitoring Control	Assuria Log Manager (ALM) Supporting Information
PMC10 - Reporting on the status of the audit system	ALM includes features for monitoring its status including logs collected, events analysed, database size, available log store space. A Monitor email which summarises the status of the ALM system can optionally be configured to be sent at pre-determined intervals. Assuria recommend an Agent based rather than a remote collection approach such as syslog forwarding or WMI-based remote Windows event log collection One function of the ALM Agent is to monitor the relevant logs to ensure that thresholds, e.g. maximum size, are not reached. The ALM agent can store logs locally if it is unable to forward a log to the ALM collectors
PMC11 - Production of sanitized and statistical management reports	ALM provides support for the production of sanitized and statistical management reports. ALM provides the ability to customise the standard reports via the user interface, e.g. reporting period, content. Further customisation of report format and style are possible via the facilities provided within the ALM Software Development Kit (SDK).
PMC12 - Providing a legal framework for Protective Monitoring activities	Unlike most SIEM solutions that collect selected events and normalise them into a proprietary format, ALM retains forensic integrity by storing the collected logs in their original format. This ensures that no data is lost and future forensic investigations can inspect actual log data collected. To do this, ALM does not normalise log data at source. Instead, all logs are retained, digitally signed, at their original form. For example, this enables a Windows event log, collected by ALM, to be opened in Windows Event Viewer, or a Solaris audit log to be viewed with 'praudit' ALM collects, digitally signs and retains all logs in their original form not raw form. Additionally ALM provides several mechanisms for exporting log data in its original format or in a variety of other formats including Syslog and CEF.

Assuria Ltd. Reading Enterprise Centre, The University of Reading, Reading, Berkshire RG6 6BU U.K.
W: www.assuria.com **E:** info@assuria.com **Tel: +44 118 935 7395**