GPG 13 (UK) Compliance Guide **OVERVIEW**

Huntsman®
Defence-Grade Security Platform

GPG13 (UK) Compliance

Compliance mapping using Huntsman®

INTRODUCTION

Her Majesty's Government (HMG) organisations and agencies face a number of obligations concerning the safe-keeping of information and the security of ICT systems. The Communications-Electronics Security Group (CESG) Good Practice Guide No. 13 (GPG13) lays out these obligations, and contains a series of measures designed to assist HMG bodies to implement and sustain appropriate Information Assurance (IA) and security capabilities. The guidance within GPG13, 'Protective Monitoring for HMG ICT Systems' supersedes the CESG's 2002 Memo 22 which set the previous standard for government organisations and private organisations handling government data.

Huntsman® is particularly well-suited to organisations that need to comply with GPG13 (or other similar protective monitoring guidelines) as it features a unique combination of mandated features such as log audit, forensic analysis and rule based intrusion detection, as well as real-time behavioural analysis.

GPG13 COMPLIANCE WITH A SINGLE TECHNOLOGY

Huntsman® is a holistic monitoring system that captures, analyses and reports on events as they occur. Its patented design enables it to identify suspicious activity, human or IT, within any dataset. Huntsman® monitors activity at the boundary and what's happening on the inside, such that for protectively monitored environments, it becomes the focal point for alert notification and forensic "who, what, when and where" investigations.

Huntsman® is not just another Security Information Event Management (SIEM) product, but a unique automated behavioural analysis engine. As well as incorporating all the functionality associated with SIEM, it uses behavioural technology to establish a baseline of normal activity across the enterprise and then immediately identifies and alerts on events that diverge from the recorded baseline.

The net result is that a single product can meet the ensemble of technology requirements for protective monitoring.

RAPID IMPLEMENTATION, EASY TO USE

The Huntsman® technology ships with built-in support for most commonly found devices, and offers straightforward log collection for bespoke applications via the user interface. As Huntsman® can automatically identify threats across any environment or system without the need to predefine them, it can significantly reduce both implementation effort and ongoing operational resource costs.

The ease of use offered by Huntsman® allows analysts and investigators to quickly drill down and analyse root cause, enabling the interception of a breach before damage can occur. A library of GPG13-specific reports provides additional support for protective monitoring activities.

PROVEN TRACK RECORD

Huntsman® is proven in mission-critical environments and protects defence, government and corporate environments worldwide. It is the technology underpinning Memo22 and now GPG13 accreditation in many UK organisations. As well as meeting all the requirements of GPG13 today, Huntsman® has the inherent flexibility to meet the future demands of a changing threat landscape.

The Good Practice Guide references other government standards including the mandatory audit requirements expressed in HMG Security Policy Framework (SPF). As a technology provider, Huntsman Security is primarily focused on meeting the requirements for Protective Monitoring presented in Appendix B of GPG13, as detailed below. Note that, before considering these requirements, each participating organisation will need to undergo a risk assessment process to establish the likelihood and impact levels (ILs) of the risks concerned.

Control ID	Protective Monitoring Control
PMC1	**Accurate time in logs.**
Huntsman® provides accurate, consistent and independent time synchronisation across all collected accounting data, and detects abnormal patterns such as clock time adjustment, both back and forwards.	
PMC2	**Recording of business traffic crossing a boundary.**
Huntsman® analyses network events and combines accounting data from other boundary devices to establish a record of all cross-boundary imports and exports. Raw accounting data is checked against applicable policy in real time, and alerts and reports are generated if any policy breaches or other malicious activities are detected.	
PMC3	**Recording relating to suspicious activity at the boundary.**
Huntsman® analyses the behaviour of boundary traffic and immediately identifies any suspicious or unusual traffic. Alerts are generated and distributed in real time and all raw data is made available for data mining and forensic analysis.	
PMC4	**Recording on internal workstation, server or device status.**
Workstation, server and other device accounting data is collected and analysed by Huntsman® in real time. Huntsman® automatically detects when suspicious activity occurs such as configuration changes; privileged access and unauthorised escalation; unexpected system and application restarts; software installation and patch failures; removable media insertion and removal; sensitive file access and more.	
PMC5	**Recording relating to suspicious internal network activity.**
Huntsman® constantly monitors the behaviour of users, networks, machines and applications. Alerts are generated in real-time whenever any suspicious activity is detected, to indicate an external breach has occurred or an insider(s) is acting maliciously.	

PMC6	Recording relating to network connections.

All connections made to a network are analysed by Huntsman® including Wireless, VPN and dial up.

Huntsman® automatically detects and alerts on any suspicious activity such as attempts to gain remote access or wireless network hacking attempts.

PMC7	Recording on session activity by user and workstation.

Huntsman® monitors user activity across the network including data access and communications.

Huntsman® ensures that any security policy breaches or suspicious patterns of behaviour are identified and alerted on in real time. The raw accounting data is also available in Huntsman® for reporting and ad-hoc analysis purposes.

PMC8	Recording on data backup status.

Accounting data relating to the status and operation of backup and restore processes is monitored by Huntsman®. Huntsman® can identify and generate alerts should an error in the backup and restore process occur, such as a failure to complete a backup/restore, data corruption or deletion.

PMC9	Alerting critical events.

Huntsman® categorises and prioritises all the alerts it generates. Alerts can be viewed centrally via the Huntsman® console, using SOC-styled dashboard views as well as distributed to remote users via SNMP traps, email and third party programs and applications.

PMC10	Reporting on the status of the audit system.

A comprehensive self-auditing feature is included as standard functionality in the Huntsman® system.

This enables all aspects of the audit process from data collection to viewing, alerts and reporting to be independently tracked and audited.

PMC11	Production of sanitised and statistical management reports.

Huntsman® ships with hundreds of compliance and security status and management reports, for example, number of failed logons, number and type of intruders detected, average time to resolve a security incident etc. The reporting function is highly configurable, existing reports can be amended or new ones written simply through the interface.

PMC12	Providing a legal framework for Protective Monitoring activities.

Huntsman® is deployed and configured in accordance with the guidance recommend as a part of the overall risk management process. Throughout the accounting data collection process Huntsman® ensures that all data collected and analysed is forensically valid.

Huntsman | Tier-3 Pty Ltd

Asia Pacific

t: +61 2 9419 3200
e: info@huntsmansecurity.com

Level 2, 11 Help Street
Chatswood NSW 2067

EMEA

t: +44 845 222 2010
e: ukinfo@huntsmansecurity.com

100 Pall Mall, St James
London SW1Y 5NQ

North Asia

t: +81 3 5809 3188
e: info@huntsmansecurity.com

TUC Bldg. 7F, 2-16-5 Iwamoto-cho,
Chiyoda-ku, Tokyo 101-0032

Americas

toll free: 1-415-655-6807
e: usinfo@huntsmansecurity.com

Suite 400, 71 Stevenson Street
San Francisco California 94105

huntsmansecurity.com

linkedin.com/company/tier-3-pty-ltd

twitter.com/Tier3huntsman