



# Exceeding Protective Monitoring Mandates In GPG 13

Enterasys SIEM correlated logs and events for actionable intelligence

---

# Exceeding Protective Monitoring Mandates In GPG 13

## Enterasys SIEM correlated logs and events for actionable intelligence

---

### Executive Overview

Government organizations across the United Kingdom are preparing for the CESG (Communications and Electronic Security Group) Good Practice Guide (GPG 13) on Protective Monitoring. CESG, the UK's National Technical Authority for Information Assurance, developed the guide in an effort to better protect systems from internal and external threats through monitoring practically every component within an organization's IT infrastructure.

Protective Monitoring is defined as a set of business processes, with essential support technology, that need to be put into place in order to oversee how ICT systems are used (or abused) and to assure user accountability for their use of ICT facilities. Within the scope of the Guide, Protective Monitoring is provided by the information security controls of ICT systems (e.g. inspecting firewall logs, investigating operating system security alerts and monitoring an IDS).

Security Information and Event Management (SIEM) and log management are important tools to implement the Protective Monitoring Controls (PMC) identified in GPG 13. The most important functional differentiator among products is the ability, in one solution, to extract contextual information by correlating logs and events for actionable intelligence. The most efficient organizations require a comprehensive platform that enables staff to focus on such actionable information rather than struggle to interpret millions of daily events.

Organizations demanding this efficiency look to Enterasys SIEM to meet GPG 13 requirements and extend their security and compliance operations to protect their information systems for the long term. Enterasys SIEM is one of the Enterasys Advanced Security Solutions. Enterasys security enables enterprises to ensure the confidentiality, integrity and availability of critical resources in support of GPG 13 and other compliance mandates.

### Benefits Summary

- **Compliance:** Ensure ICT systems are operated within the requirements of applicable policies, legislation and regulations, and deter and detect any unlawful activity
- **Risk Management:** Help mitigate risks to the confidentiality, integrity and availability of information assets processed by ICT systems and ensure other countermeasures are operating effectively
- **Reporting and Continuous Improvement:** Contribute to the mandatory reporting elements of the Security Policy Framework (SPF: reference [c]) and provide a rich source of information to feed into IA reviews of ICT systems as part of the "Plan Do Check Act" cycle of continuous improvement mandated by HMG IA Standard
- **Situational Awareness:** Ensure that system owners have real-time information about the status of ICT systems, including activities of threat sources, enabling security incidents to be detected, investigated and effectively remediated
- **Accountability:** Ensure that ICT is used within the parameters that the business defines and is not used for wasteful or unlawful purposes, or in a manner that diverts users from their true job function
- **Network Defense:** Working with other security countermeasures, provide a complete "defense in depth" approach and facilitate automated responses to threats to ICT

### Mapping to GPG 13 PMC's with the Enterasys SIEM

GPG 13's Protective Monitoring Controls require organizations to deploy an efficient technology solution to collect ICT log information and configure ICT logs to demonstrate an audit trail of security relevant events of interest. Given the comprehensive nature of GPG 13's requirements, the capabilities needed will allow teams to detect, respond to and anticipate attacks, meet compliance mandates and ultimately report on activity across users, applications and the network infrastructure.

Security Information and Event Management (SIEM) solutions are designed specifically to meet these demands in enterprise and government environments, and align with the guide's requirements. GPG 13 calls out log management and SIEM solutions within the guide as effective technologies for organizations to comply with the mandate. However, the all-important ability to provide contextual information to administrators and security personnel across a vast network of users, machines, servers, mobile devices and applications differentiates the Enterasys SIEM platform.



- **PMC 3 – Recording related to Suspicious Behavior at a Boundary**

Enterasys uniquely profiles the behavior of systems, applications and users that profiles normal behavior and instantly recognizes anomalies caused by security breaches, policy violations and internal network misuse.

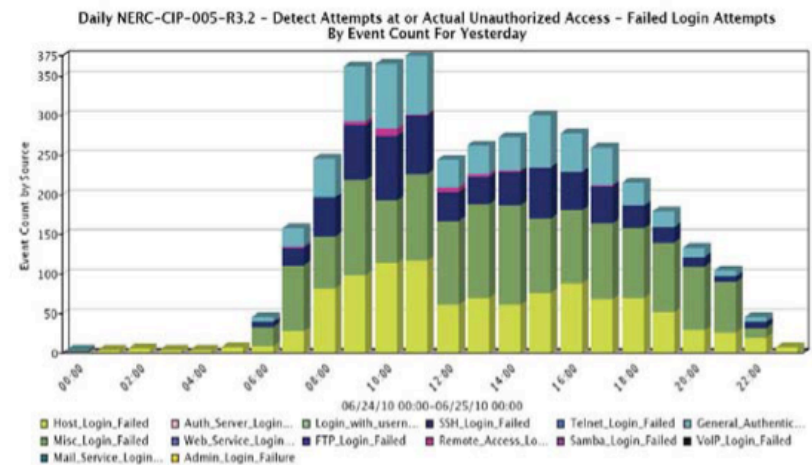
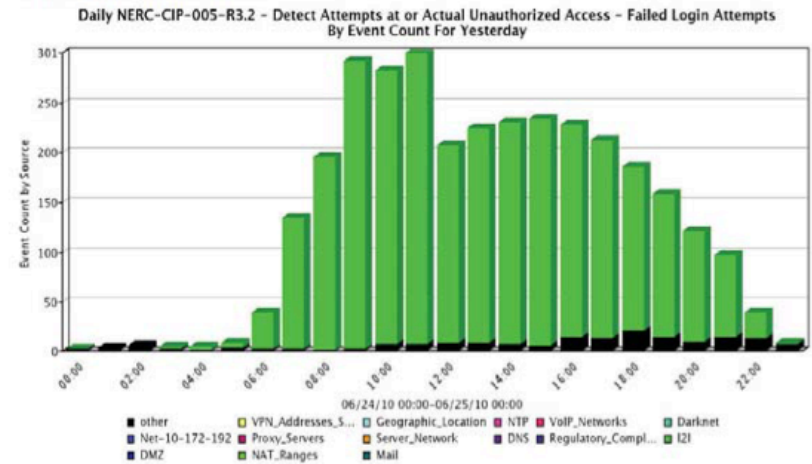
Leveraging advanced behavioral analysis, Enterasys alerts network administrators when an attack begins to propagate, identifies which areas of the entire enterprise are at risk and quickly isolates the threat at its source— preventing further impact to the network, data center and assets in general.

- **PMC 5 – Recording Relating to Suspicious Internal Network Activity**

Enterasys's intelligent surveillance of the network, combined with advanced Network Behavioral Anomaly Detection (NBAD) capabilities, deliver the intelligence needed to detect complex internal-based threats. Additionally, Enterasys can integrate with your company's Identity and Access Management (IAM) solution to develop a comprehensive picture of a user's suspicious behavior and provide a manageable set of prioritized security threats along with the information necessary to quickly identify and alert on threats from internal users.

## Daily GPG13 PMC6 - Detect Attempts at or Actual Unauthorized Access - Failed Attempts

Generated: Jun 25, 2010 8:24:57 PM



## Compliance and Better Security are Driving Technology Adoption

The business drivers for implementing technology to satisfy the Protective Monitoring requirements are audit –related. Organizations are required by GPG 13 to adhere to guidelines set forth in other existing standards, including HMG ICT standards for Information Assurance. These standards require organizations to provide evidence through audit and reporting capabilities to show they are in compliance with the applicable Mandatory Requirements, for example. Organizations should leverage the overall set of best practices in GPG 13 to optimize their security posture and meet all Protective Monitoring components with an intelligent, automated and integrated solution. This will help deliver value to all stakeholders involved.

## Why Enterasys SIEM?

The over-arching value of the Enterasys SIEM is the ability to tie intelligence from the network to the broader set of data collected from the entire enterprise infrastructure. This ability provides collection, analysis and correlation across a broad spectrum of systems including networked solutions, security solutions, servers, hosts, operating systems, and applications. The end result is intelligence that provides a meaningful context for security professionals while radically reducing operational complexity across multiple systems. Centralizing security and compliance operations on a technical level while gaining the intelligence necessary to optimize security decision making is what will help organizations implement GPG 13. However, organizations should use GPG 13 guidelines as a catalyst to develop a proactive, comprehensive security program that extends security, risk and compliance to meet business objectives. Government bodies and local authorities can access the detailed nature of these recommendations and sub controls by contacting The National Technical Authority for Information Assurance. Security Intelligence addresses the spectrum of the security lifecycle, centralizing data from disparate silos, normalizing it and running automated analysis. This enables organizations to prioritize risk and cost-effectively deploy security resources for detection, prevention, response and remediation.

## Enterasys Advanced Security Solutions

The strongest foundation for comprehensive security is to apply network security best practices. Applying well-understood network security concepts and tools enables enterprises to cost effectively satisfy both compliance and security mandates. There are three key elements to address for overall network security: network visibility, policy enforcement, and intrusion or anomaly detection and response – all based on the organization's security policies.



## Conclusion

Enterasys, a Siemens Enterprise Communications company, is a leading global provider of Ethernet switching and routing solutions as well as advanced network security solutions. The complete suite of Enterasys products delivers the underlying network security framework that is the key to meeting compliance mandates. (See also [Enabling Compliance – A Network Approach.](#)) With more than 25 years of experience providing networking and security products, the company's innovative technology and solutions reduce complexity through leading wired/wireless integration, protect investments with long technology life cycles and provide built-in security. Table 1 summarizes the key network security elements, the required functions and the solutions delivered by Enterasys.

Table 1: Network security, functions and solutions

Network Security Element	Functions	Solutions
Visibility	<ul style="list-style-type: none"> <li>• Correlate and manage network flow data</li> <li>• Provide visibility and reporting</li> </ul>	Security Information and Event Manager (SIEM) Network Access Control (NAC)
Enforcement	<ul style="list-style-type: none"> <li>• Enforce role-based least privilege access</li> <li>• Control visitor access</li> <li>• Enforce location dependent access</li> <li>• Enforce time dependent access</li> <li>• Protect critical network segments</li> <li>• Enforce information compartmentalization</li> <li>• Harden servers</li> </ul>	Policy-based Switching Infrastructure NAC
Detection and Response	<ul style="list-style-type: none"> <li>• Detect known attacks</li> <li>• Respond to attacks</li> <li>• Detect server compromise</li> <li>• Correlate flow data, event data and log data</li> <li>• Detect Zero Day attacks</li> </ul>	SIEM Host Intrusion Detection (HIDS) Intrusion Prevention (IPS) Distributed IPS

The Enterasys SIEM and other advanced security solutions are deployed today by numerous government organizations, including local, state, provincial and federal government agencies. Enterasys SIEM, in combination with these other security applications, provides comprehensive threat detection and dynamic threat removal for LAN, WAN, wireless networks, host and server systems. Deployment of Enterasys solutions results in the capability to secure any network from any vendor and the ability to meet compliance mandates.

Resources:

- [Enterasys SIEM](#)
- [Enabling Compliance – A Network Approach](#)
- [GSI/GCSx Compliance](#)

## Contact Us

For more information, call Enterasys Networks toll free at **1-877-801-7082**, or +1-978-684-1000 and visit us on the Web at [enterasys.com](http://enterasys.com)



© 2011 Enterasys Networks, Inc. All rights reserved. Enterasys Networks reserves the right to change specifications without notice. Please contact your representative to confirm current specifications. Please visit <http://www.enterasys.com/company/trademarks.aspx> for trademark information.

