



Meeting and Exceeding GSI/GCSx Information Security Monitoring Requirements with Enterasys SIEM

The benefits of Enterasys SIEM for protective monitoring of government systems as required by the UK Government Connect (GC) program

Meeting and Exceeding GSI/GCSx Information Security Monitoring Requirements with Enterasys SIEM

Introduction

Effective information security has become a fundamental requirement in the delivery of any networked based service where confidential information is exchanged. Over the last few years the UK government has facilitated extensive network infrastructure, under the Government Connect (GC) program, that allows information exchange amongst connected government agencies. Local government authorities (LAs) that connect to this infrastructure must adhere to strict information security controls, as defined by multiple requirement and guidance documents including the Code of Connection (CoCo) for the Government Secure Intranet (GSI) and the Government Connect Secure Extranet (GCSx), Memorandum Number 22, the IT Health Check Requirements, and ISO/IEC 17799. Specific information security mandates of CoCo, for partial level compliance to Memo 22, include the implementation of comprehensive log and threat management security controls.

The strongest foundation for meeting compliance is applying network security best practices. The fundamental goal of compliance and network security is to protect sensitive data from unauthorized access or modification and ensure that the data is available to authorized users when needed. 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.



Enterasys Advanced Security Solutions - Overview

Enterasys, the network infrastructure and security division of Siemens Enterprise Communications GmbH & Co KG, 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"> Correlate and manage network flow data Provide visibility and reporting 	Security Information and Event Manager (SIEM) Network Access Control (NAC)
Enforcement	<ul style="list-style-type: none"> Enforce role-based least privilege access Control visitor access Enforce location dependent access Enforce time dependent access Protect critical network segments Enforce information compartmentalization Harden servers 	Policy-based Switching Infrastructure NAC
Detection and Response	<ul style="list-style-type: none"> Detect known attacks Respond to attacks Detect server compromise Correlate flow data, event data and log data Detect Zero Day attacks 	SIEM Host Intrusion Detection (HIDS) Distributed Intrusion Prevention (IPS)

This white paper focuses on the key element of visibility and the Enterasys SIEM solution as a critical tool to address the Code of Connection (CoCo) for the Government Secure Intranet (GSI). The Enterasys SIEM solutions are deployed today by numerous government organizations, including local, state, provincial and federal government agencies. This white paper discusses some of the information security challenges UK government agencies face in conjunction with CoCo. It discusses how total security intelligence solutions from Enterasys help local authorities deliver log management and auditing required by government mandates as well as Enterasys' advanced threat detection typically not provided by a stand-alone log management solution.

Challenges for UK government agencies

Organizations that leverage the UK GSX, including local government authorities, face significant challenges protecting the network and control infrastructure used in the delivery of their vital services, including:

- Protecting the environment from an increasing threat of cyber-attack and insider threats
- Collecting, archival and analysis of event log data from a wide variety of data sources including network devices, hosts and servers, security devices and applications
- Protecting critical infrastructure from an existing and emerging landscape of complex vulnerabilities
- Managing a diverse set of vendor products that generate a seemingly overwhelming and unwieldy amount of information
- Meeting a wide variety of existing and emerging information security requirements including those discussed here, but also including the Payment Card Industry Data Security Standard (PCI-DSS) and National Health Services privacy regulations

The solution to these challenges requires a centralized security management solution to enable network visibility; more effectively detect threats and meet specific regulatory guidelines.

Challenge: Improving Security While Reducing Costs

Like almost every other type of business, government agencies are being asked to reduce operational expenses. This cost reduction is particularly challenging to the IT departments because the burden on the organization from both emerging threats to the network and regulatory mandates is not going away. As organizations assess their information security programs, they need to consider solutions that help improve security and meet a broad spectrum of information security mandates, while at the same time reduce overall costs.

Enterasys SIEM for Government Authorities

The Enterasys SIEM solution delivers an improved security management capability that can help better protect systems that connect to the GSX. Enterasys SIEM provides an integrated network security management framework that combines log management, flow-based network and application behavior analysis, and security information and event management (SIEM) functionality to provide organizations with an unparalleled capability to meet IT security objectives. Enterasys SIEM's ability to monitor non-traditional systems provides increased visibility into networked systems to detect vulnerabilities before they impact services. The Enterasys SIEM solution provides comprehensive monitoring, threat detection, threat response, reporting, and auditing capabilities.

Log Management

In addition to the traditional log management capabilities of log collection, storage, and search, Enterasys SIEM provides advanced leverage of all of the information collected through integrated, real-time event correlation, threat detection, and compliance reporting.

Log management is central to meeting the requirements of CoCo - which mandates the monitoring of electronic access to the systems connected to the GSX. Audited records must be retained for 6 months for CoCo, at least a year for PCI-DSS, and potentially longer for other regulations.

Enterasys's comprehensive security management framework includes the ability to deliver scalable and secure log management capabilities across all networked systems and applications that are under management. The Enterasys SIEM solution provides integrated storage, and includes features to help guarantee the integrity of collected information from tampering (as required by Memorandum No 22, General Requirement 21). In addition to traditional log management capabilities of log collection, storage, and search, Enterasys SIEM provides advanced leverage of all of the information collected through integrated, real-time event correlation, threat detection, and compliance reporting and auditing. A sample set of reports that support specific GSI/GCSx requirements is provided in Appendix A.

The Enterasys SIEM solution provides scalable log management by enabling distributed log collection across a widely dispersed network of control systems, but with a centralized view of the information. In addition, Enterasys SIEM provides a flexible architecture to support event logs from unique event sources, including legacy systems and proprietary applications. Enterasys SIEM provides a complete log management solution for government authorities tasked with collecting, retaining, and managing event logs in their environment.

Threat Management

Other existing first-generation SIEM and/or log management solutions might turn millions of events into thousands of correlated alerts – unfortunately those alerts still need to be manually analyzed and correlated.

The ability to detect threats and vulnerabilities to the infrastructure is fundamental to CoCo. Like many other organizations, government agencies continue to struggle to stay ahead of the evolving threat landscape. Even after significant investments in a plethora of security solutions, security teams still face an enormous burden trying to extract relevant and actionable information about threats from their IT infrastructure. Traditional SIEM solutions often fall short because they require complex tuning and may not piece together all the information necessary to effectively correlate and detect threats.

To detect more complex threats, it is important to leverage all available information including information that may be segmented across different network and security solutions and across network and security operational teams. The Enterasys SIEM solutions supports advanced threat management features to provide the advanced correlation required to bridge the gap between network and security operations. This broad visibility delivers the requisite surveillance on the network to detect today's more complex and sinister IT-based threats.

Many existing first-generation SIEM and/or log management solutions might turn millions of events into thousands of correlated alerts – unfortunately those alerts still need to be manually analyzed and correlated. Enterasys SIEM takes traditional correlation one step further by helping to connect the dots across the entire infrastructure. It delivers overburdened security operators a manageable set of prioritized security threats that must be addressed along with the information necessary to remediate the situation.

Compliance Management

Unlike many other information security mandates, government agencies have been pointed in the right direction on compliance with multiple supporting information security references from CoCo, including ISO 17799 and Memo 22. Still, the guidance provided by these documents can be confusing and unclear. Gartner and other research firms and security consultants assert that demonstration of compliance initiatives should involve these key factors:

- **Accountability:** Proving who did what and when
- **Transparency:** Providing visibility into the security controls, the business applications, and the assets that are being protected
- **Measurability:** Metrics and reporting around risk within a company or organization

Monitoring and management solutions that span the network and security technologies in the infrastructure play a key part in supporting various compliance initiatives. The Enterasys SIEM brings to enterprises, institutions, and government agencies the accountability, transparency, and measurability that are critical to the success of any IT security program tasked with meeting regulatory mandates.

A checklist of how Enterasys SIEM helps meet specific requirements of GCSx logging and threat management is provided in Appendix B.

Improved operational efficiency and lowers costs

Enterasys SIEM solution delivers industry-leading security management features that have the lowest cost to acquire, deploy, and maintain. Enterasys SIEM customers' benefits include:

- **Converged Solution** – Enterasys SIEM provides – in a single solution – features that historically may be deployed in as many as four separate solutions: log management, network behavior analysis, SIEM, and compliance reporting. Cost savings come from both a significant reduction in acquisition costs and ongoing maintenance expense.
- **Out-of-the-box Intelligence** – Enterasys SIEM provides significant embedded security knowledge. This embedded intelligence reduces the burden on staff to understand the complex information provided by the devices on the network. Hundreds of out-of-the-box rules and thousands of report templates, easily tuned for the specific environment, greatly reduce the effort required to turn millions of cryptic events into useful and actionable information.
- **Ability to Scale** – Enterasys SIEM is an appliance-based solution that provides easy deployment and scalability for organizations of any size. Enterprises that deploy the Enterasys SIEM are typically up and running and receiving significant value the first day the product is installed.
- **Easy to Maintain** - Unlike other solutions, Enterasys SIEM does not require advanced skills to maintain. Simple to follow configuration wizards minimize the time and expertise required to tune the system and extract useful information for individuals at all levels of the organization.

Conclusion

The job of delivering an effective IT security program is not trivial for government agencies. The motivation for improving overall IT security comes from many directions, including operational improvement and compliance, but all lead in the same direction: protecting critical information assets from those that wish to do harm.

Historically, enterprises have invested in many point solutions in an attempt to mitigate specific IT risks.

Moving forward, organizations need to look at ways to capitalize on their existing investments and integrate the value from the information that these solutions already provide. SIEM from Enterasys provides government agencies with features to improve overall IT security and to meet specific regulatory mandates. Its integrated approach to network security management provides unique and differentiated value in the areas of log management, threat management, and compliance management.

For additional security protection, Enterasys provides a completely integrated suite of advanced security applications:

- Enterasys IPS – advanced prevention, detection and response capabilities for network, host-based and wireless deployment
- Wireless Intrusion Prevention (WIPS) – continuous scanning, threat detection, classification and prevention for rogue APs, ad-hoc mis-association and next gen threats
- Enterasys Network Access Control (NAC) – a flexible inline or out-of-band solution for pre-connect post-connect network access control
- Enterasys Network Management Suite (NMS) – centralized visibility and control for large multi-vendor networks to streamline administrative tasks.

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.

Appendix A – Sample Reports for GSI/GCSx

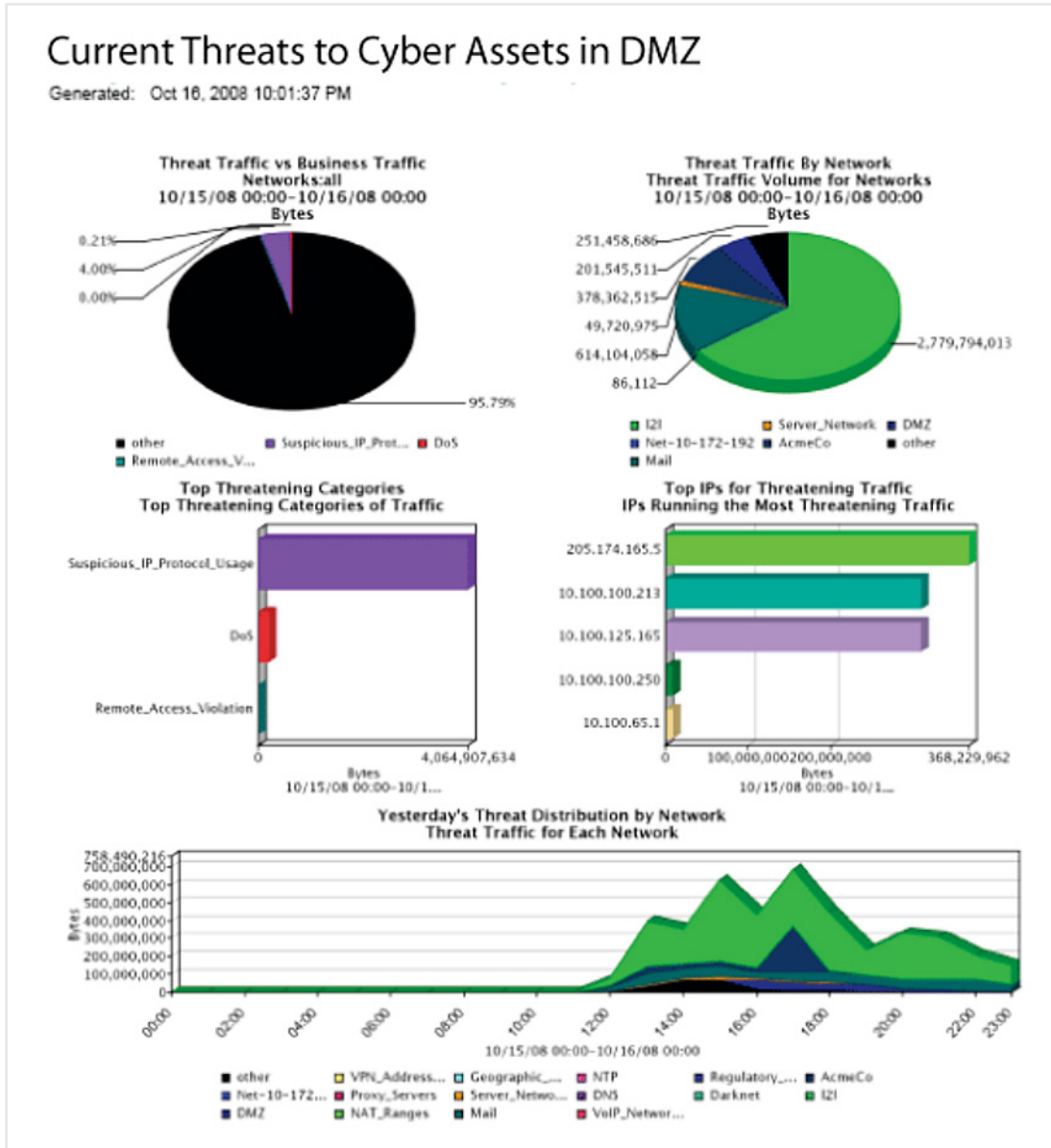
A.1 GSI/GCSx Reporting Overview

Enterasys SIEM ships with over one thousand report templates. A few sample templates are provided below as they relate to specific requirements of GCS/GCSx. This is just a small sample of the reports available.

A2 Sample reports supporting

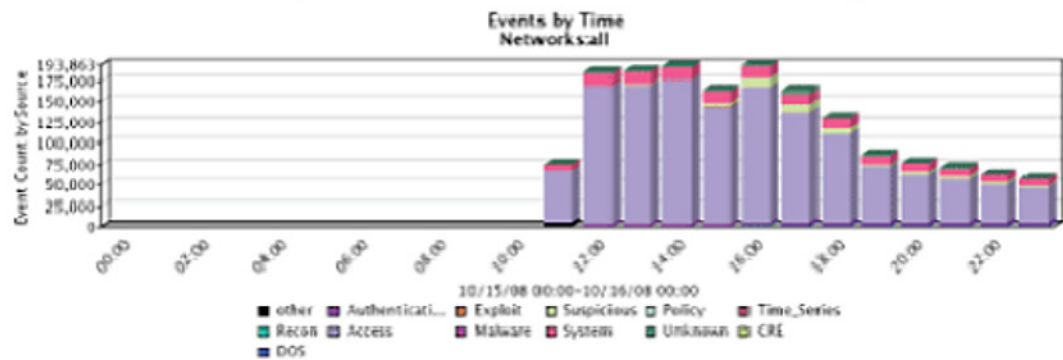
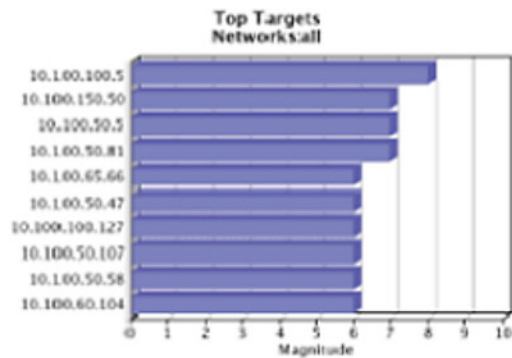
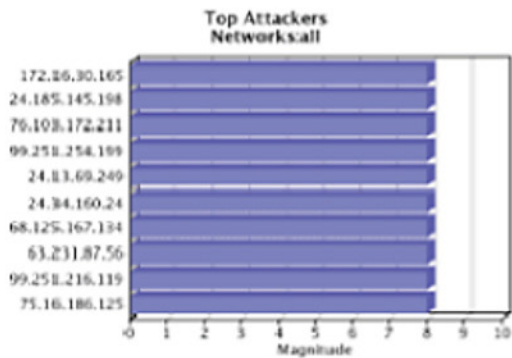
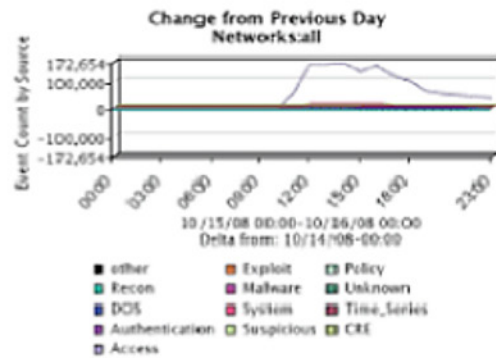
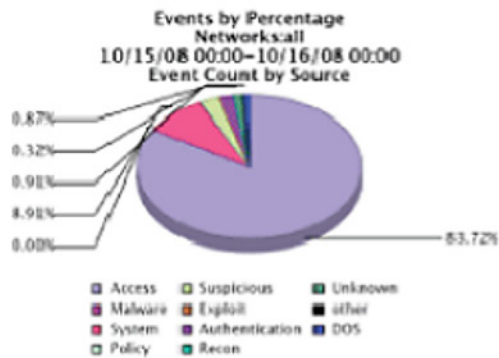
- Memorandum No. 22, T1 – “Unauthorized breach to the boundary of a domain”

Sample Report A.2.1 – Top threats to the security perimeter



Top Events Across Security Perimeter

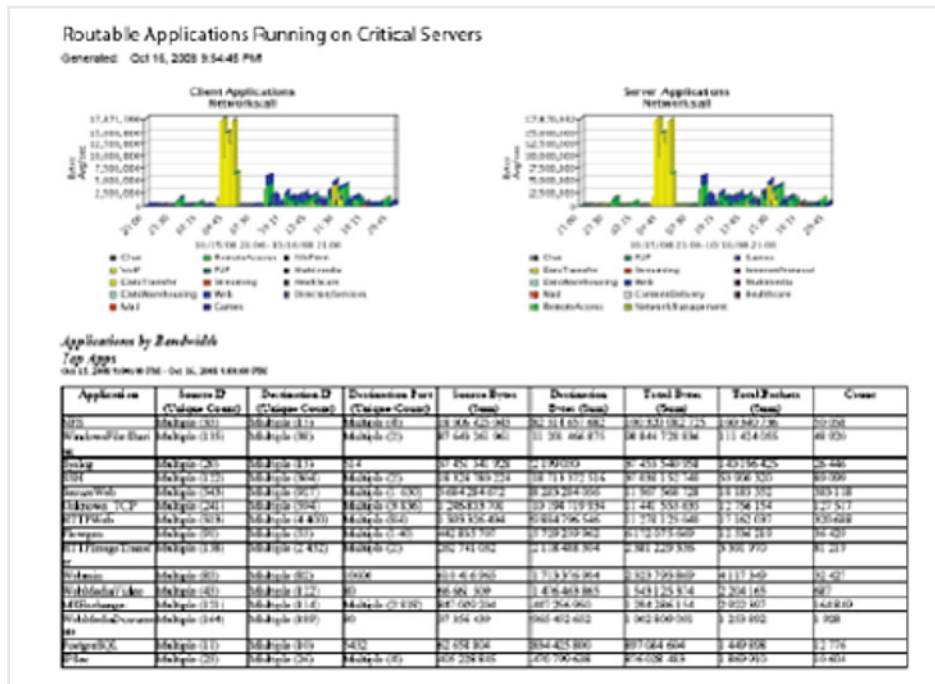
Generated: Oct 16, 2008 1:11:21 AM



A.3 Sample reports supporting

- Memorandum No. 22, T3 – “Unauthorized Export of Information”

Sample Report A.3.1 – Supports Memorandum No. 22 – SR5/SR6/SR8/SR11 – Application Level Monitoring



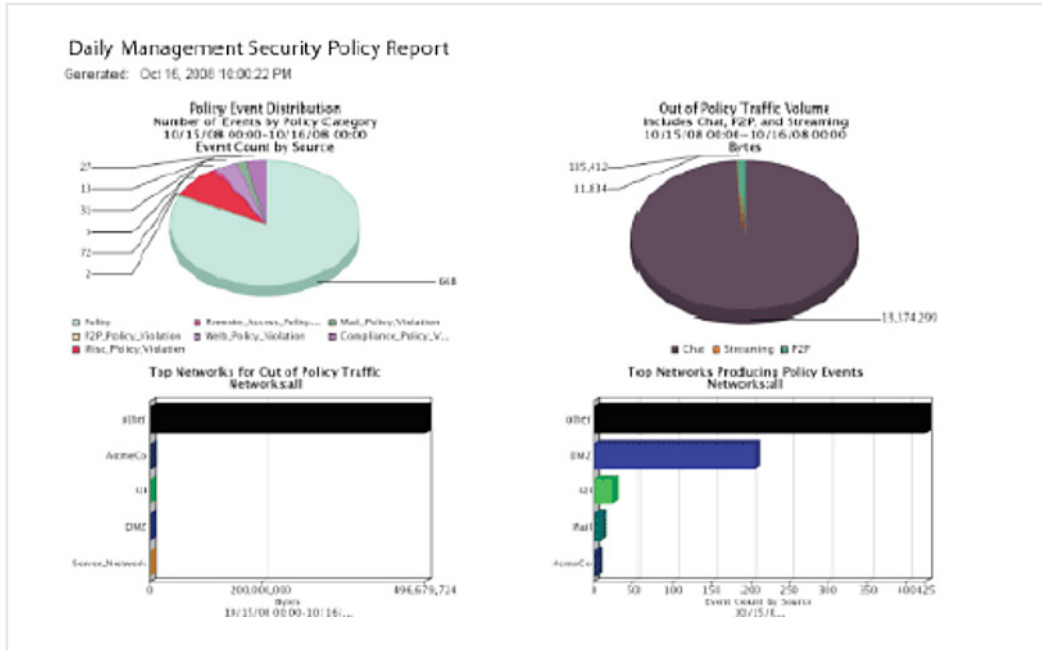
Additional useful report templates for these requirements include:

- Network connectivity report (by source and/or destination)
- Network use by risky or trusted protocol
- Network activity by network and/or user group
- Application activity for specific application (e.g. database, web, mail)
- Denied network activity
- VPN activity
- Network activity by international geography
- Failed and successful authentication (by application)
- Open/closed sessions

A. 4 Sample reports supporting

- Memorandum No. 22, T4 – “Unauthorized import of information into a domain”
- Memorandum No. 22, T5 - “Breach of Integrity of Information”

Sample Report A.4.1 – Management Security Policy Exception Report – External Policy Violations



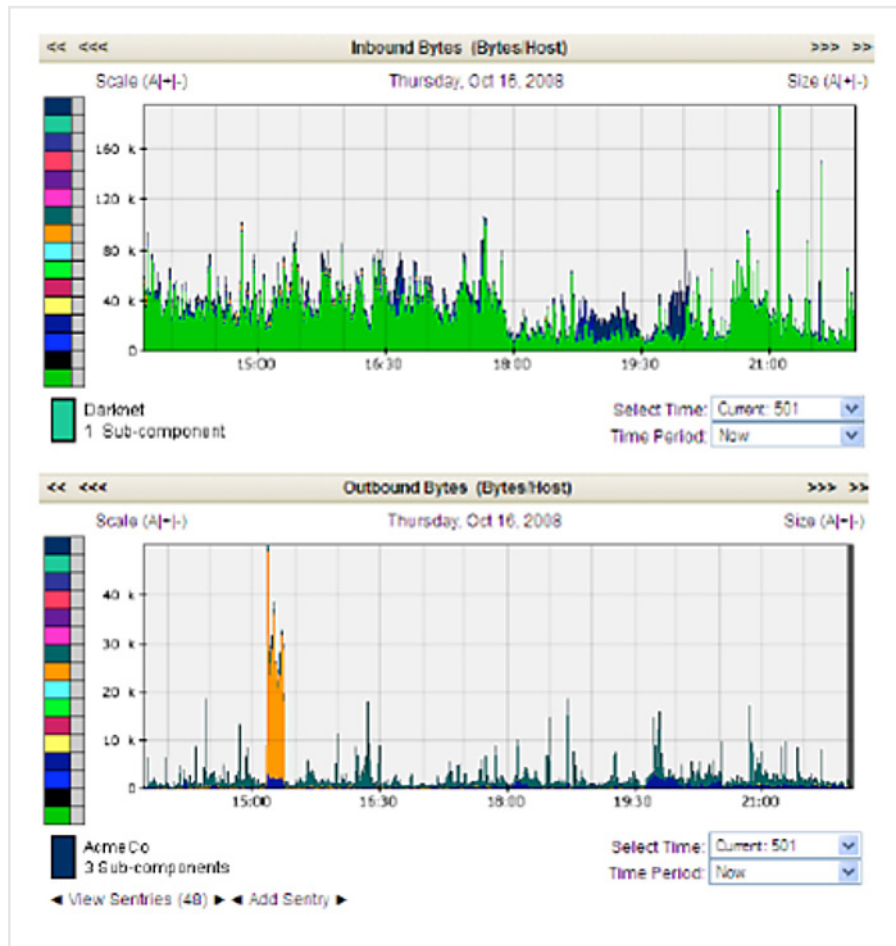
Additional useful report templates for this requirement include:

- Executive level threat report
- Executive level network activity report
- Executive level network health report
- Event summary by severity
- Anti-virus reports
- User activity reports
- IDS/IPS reports
- Network flow/activity reports, including reports by port and protocol
- VPN activity reports
- Voice over IP security reports
- Security offense detail reports, including vulnerability assessment

A.5 Sample reports supporting

- Memorandum No. 22, T6 – “Breach of Availability of Information or Services”

Sample Report A.5.1 – Supports Memorandum No. 22 – SR16 – “bandwidth or performance” incident



A.6 Sample reports supporting

- T7 – “Repudiation of action or responsibility”

Sample Report A.6.1 – Security Incident Report

All Offenses Offense 159 (Summary)									
Magnitude				Relevance	2	Severity	6	Credibility	1
Description	Malware - External - Communication with BOT Control Channel containing Potential Botnet connection - QRadar Classify Flow			Event count	5 events in 1 categories				
Attacker Src	10.100.50.72			Start	2008-10-16 17:21:33				
Target(s) Dest	Remote (3)			Duration	40s				
Network(s)	q1bar			Assigned to	Not assigned				
Notes	Host communicating with a known BOTNET control channel based on the ShadowServer project.								
Attacker Summary Details				Top 5 Categories Categories					
Magnitude		User		Name	Magnitude	Local Target Count	Events	Last Event	
Description	10.100.50.72	MAC	00:0D:60:77:41:C3	Potential Botnet connection		0	5	10-16 17:22:13	
Vulnerabilities	0	Asset Weight	0						
Location	AcmeCo_Europe_Europe/All								
Top 10 Events Events									
Event Name	Magnitude	Device	Category	Destination	Dst Port	Time			
Potential Botnet connection - QRadar...		Flow Classification Engine-5 : DEMO.q1labs.inc	Potential Botnet connection	128.241.236.105	80	10-16 17:21:33			
Potential Botnet connection - QRadar...		Flow Classification Engine-5 : DEMO.q1labs.inc	Potential Botnet connection	128.39.2.28	80	10-16 17:21:48			
Potential Botnet connection - QRadar...		Flow Classification Engine-5 : DEMO.q1labs.inc	Potential Botnet connection	128.241.236.105	80	10-16 17:21:34			
Potential Botnet connection - QRadar...		Flow Classification Engine-5 : DEMO.q1labs.inc	Potential Botnet connection	129.81.183.128	80	10-16 17:22:00			
Potential Botnet connection - QRadar...		Flow Classification Engine-5 : DEMO.q1labs.inc	Potential Botnet connection	129.81.183.128	80	10-16 17:22:13			

Appendix B: GCSx Compliance Requirements supported by Enterasys SIEM

GSI Code of Connection (CoCo)	
Requirement	Enterasys SIEM Support
Information Security Standard	The GSI CoCo document is relatively vague as to the security controls required by the government authority. It does, however defer to ISO/IEC 27002 (formerly 17799) which provides numerous controls that organizations should implement as part of the security management program. An overview of how Enterasys SIEM supports the ISO controls is provided in the next section of this table.
IEC/ISO 27702 (formerly ISO 17799)	
Requirement	Enterasys SIEM Support
Information Security Standard	The GSI CoCo document is relatively vague as to the security controls required by the government authority. It does, however defer to ISO/IEC 27002 (formerly 17799) which provides numerous controls that organizations should implement as part of the security management program. An overview of how Enterasys SIEM supports the ISO controls is provided in the next section of this table.
Section 5 - Defining a security policy	Fundamental to any security policy is having the visibility necessary to monitor and assess the effectiveness of the policy. Enterasys SIEM provides enterprise security intelligence that should be considered as part of any security policy.
Section 7 – Asset management <ul style="list-style-type: none"> 7.1.1 Discovery and inventory of assets 7.1.3 Acceptable use of assets 7.2.1 Classification 	Maintaining an accurate assessment of networked systems is nearly impossible without a tool that proactively monitors the network and builds a database of asset profiles. Core to Enterasys SIEM is its ability to collect a broad spectrum of information from all networked systems to build a comprehensive database of assets and a detailed profile of those assets.
Section 10 Communications and operations management <ul style="list-style-type: none"> 10.4.1 Protection against malicious code 10.8.1 Information exchange policies and procedures 10.10 Monitoring <ul style="list-style-type: none"> 10.10.1 Audit logging 10.10.2 Monitoring system use 10.10.3 Protection of log information 10.10.5 Fault logging 	<p>Enterasys SIEM provides significant value in improving the security of networked communications. One high level overview how Enterasys SIEM addresses specific ISO requirements is provided below.</p> <ul style="list-style-type: none"> 10.4.1 Protection against malicious code Enterasys SIEM has many features that quickly isolates and detects threats to the network, including malicious attacks including denial of service, botnets, Trojans, and worms. Through integrated visibility, Enterasys SIEM is capable of detecting threats not found by other security applications. 10.10 Monitoring Fundamental to Enterasys SIEM is its ability to monitor and analyze security events in real-time. 10.10.1 Audit logging Enterasys SIEM provides organizations a centralized log management solution that provides an easy to use data management that supports both real time and historical collection and analysis of log data. 10.10.2 Monitoring system use Enterasys SIEM can collect and analyze a wide variety of access control information including, but not limited to logs from hosts, servers, VPNs, firewalls, and identity systems. Integrated together a comprehensive view of access to systems can be obtained. Utilizing this information important access level audits can be performed on events including, but not limited to: failed and successful login attempts, privilege escalation events, failed and successful administrative login attempts, account lockout events, account creation events, successful and failed service requests (e.g. firewall port denied) 10.10.3 Protection of log information Enterasys SIEM provides the ability to maintain a checksum (or hash) for log files as they are collected to help guarantee the integrity of the log data. Enterasys SIEM also provides the ability to encrypt information transfer across a distributed log management deployment. 10.10.5 Fault logging Enterasys SIEM helps bridge the gap between network and security management. Fundamental to the solution is to understand network activity by bandwidth to quickly detect service interruptions/faults caused by a security incident.
Section 11.1.1 Access control Policy	Enterasys SIEM can collect and analyze a wide variety of access control information including, but not limited to logs from: hosts, servers, VPNs, firewalls, and identity systems. Integrated together a comprehensive view of access to systems can be obtained. Utilizing this information important access level audits can be performed on events including, but not limited to: failed and successful login attempts, privilege escalation events, failed and successful administrative login attempts, account lockout events, account creation events, successful and failed service requests (e.g. firewall port denied).
Section 11.5.1 Secure log-on procedures	
Section 13.1.1 Reporting information security events and weaknesses	One of the most unique features of Enterasys SIEM is its ability to prioritize information for security teams so that they can properly take action while at the same time optimize their time. Many log management solutions will turn millions of events into 1000's of correlated alerts – that unfortunately must still be manually analyzed. Enterasys SIEM reduces this burden by connecting the dots across the entire infrastructure –delivering to security operators a comprehensive understanding of the most significant risk to the network along with sufficient information to remediate.
Section 13.2 Management of information security incidents	

Appendix B: GCSx Compliance Requirements supported by Enterasys SIEM

Communications Electronic Security Group (CESG) Info Security Memorandum No. 22	
Requirement	Enterasys SIEM Support
General Requirement #21 – Log File Integrity	Enterasys SIEM provides the ability to maintain a checksum (or hash) for log files as they are collected to help guarantee the integrity of the log data. Enterasys SIEM also provides the ability to encrypt information transfer across a distributed log management deployment.
General Requirement #22 – Log Retention	<p>Enterasys SIEM provides organizations a centralized log management solution that provides an easy to use data management that supports both real time and historical collection and analysis of log data. The solution provides embedded storage with automated management of log data file including 3 possible states:</p> <ul style="list-style-type: none"> • Uncompressed data that is stored on-line for quick access to information • Compressed data that is stored on-line for less frequent request to information, but does not require restoring from external storage • Off-line data which can be stored on external storage for archival purposes <p>Enterasys SIEM can support a wide variety of data retention policies depending on individual business and compliance requirements.</p>
General Requirement #23 – Audit Frequency	Enterasys SIEM supports both real-time and historical profiling of events. Powerful real-time correlation is provided to support real-time audit requirements. Historical profiling is provided for longer term forensics analysis and event search.
General Requirement #24 – Vulnerability Assessment	<p>Enterasys SIEM provides a rich set of vulnerability assessment features. Enterasys SIEM provides the ability to collect information from a wide variety of vulnerability scanners, including Nessus which is mentioned specifically by CoCo.</p> <p>http://www.govconnect.gov.uk/implementation/coco-faqs.php</p> <p>Enterasys SIEM integrates vulnerability assessment data with a wide variety of other information sources to improve the accuracy of how vulnerabilities are presented to information security teams.</p>
General Requirement #25 – protective measures against threats	Unlike traditional log management solutions that typically only provide event collection and rudimentary correlation, Enterasys SIEM provides advanced correlation that provides unrivaled data reduction and prioritization resulting in the detection of threats missed by other solutions.
Security Requirement #1 (SR1) – Clock synchronization	Enterasys SIEM provides the ability to synchronize time across all architectural components using a standards based NTP server.
Security Requirement #2 (SR2) – Unique Identification	Enterasys SIEM provides multiple methods for identifying the source of a networked activity. Identity signatures include source/destination IP address, source/destination port, MAC address, and username. Understanding that IP addresses and identities change over time, Enterasys SIEM provides advanced asset profiling that helps determine access to a system at any given time.
Security Requirement #3 (SR3) – Managing date/time of an event	All events collected by Enterasys SIEM are maintained and indexed by a normalized date/time stamp so all events can be accurately analyzed. Events can be filtered and reported based on the date and time the event was collected.
Security Requirement #4 (SR4) – Identify the physical and logical address	When available in the event data, Enterasys SIEM maintains, as part of an assets profile, both its logical IP address and its physical MAC address. In addition, other logical and physical attributes can be collected and analyzed including, but not limited to, port, protocol, and interface.
Security Requirement #5 (SR5) – Identify source and destination	All network based events can be collected, stored and analyzed by Enterasys SIEM based on both the perceived source and destination IP address.
Security Requirement #6 (SR6) – Reveal the type of service	<p>Enterasys SIEM provides in depth analysis of a wide variety events that span the network, hosts and servers, security devices, and applications. A wealth of information can be obtained from this analysis including, but not limited to: failed and successful login attempts, privilege escalation events, failed and successful administrative login attempts, account lockout events, account creation events, successful and failed service requests (e.g. firewall port denied).</p> <p>Enterasys SIEM integrated network and security reporting provides organizations in depth analysis that looks at the collected information across many angles to quickly pinpoint important trends and isolate security issues that should be of concern. For example, reports can be generated that look at user activity for specific applications, whether they are trusted (e.g. web or email) or un-trusted (e.g. peer-to-peer or file transfer applications).</p>
Security Requirement #7 (SR7) – Identify privileged commands	As mentioned in SR6 above, Enterasys SIEM can provide a detailed audit of privileged (administrative) access to systems. In addition, Enterasys SIEM's unique layer 7 flow information can provide content capture to detect specific security incidents not detected by other applications (e.g. unencrypted passwords, default passwords, etc.).
Security Requirement #8 (SR8) – Identify unauthorized applications	Enterasys SIEM provides a wealth of knowledge of protocols and applications running on the network. Automated correlation rules can be defined to quickly detect and notify security operators any suspicious or un-trusted protocol or applications.
Security Requirement #10 (SR10) – Analyze content of objects	As mentioned in SR7 above, Enterasys SIEM's layer 7 analysis provides the ability to analyze packet payload to detect specific activities including illegal file transfers.
Security Requirement #11 (SR11) – Reveal data export methods	See SR6, SR7, and SR10 above.
Security Requirement #13 (SR13) – Reveal untypical gaps in accounting logs	Enterasys SIEM provides detailed logging of activities internal to the solution. Correlation rules can be utilized to detect systems that have stopped sending event logs for analysis.

Appendix B: GCSx Compliance Requirements supported by Enterasys SIEM

Communications Electronic Security Group (CESG) Info Security Memorandum No. 22	
Requirement	Enterasys SIEM Support
Security Requirement #15 (SR15) – Reveal changes to any executables and/ or configuration files	Enterasys SIEM supports the collection of information from a wide variety of 3rd party network and security solutions including, but not limited to, configuration and file management systems. When collected information from these systems can be analyzed and correlated with all collected information, providing unique visibility into the systems under management.
Security Requirement #16 (SR16) – Bandwidth and performance	Enterasys SIEM helps bridge the gap between network and security management. Fundamental to the solution is to understand network activity by bandwidth to quickly detect service interruptions caused by a security incident.
T7 – Repudiation of action or responsibility	<p>One of the most unique features of Enterasys SIEM is its ability to prioritize information for security teams so that they can properly take action while at the same time optimize their time. Many log management solutions will turn millions of events into 1000's of correlated alerts – that unfortunately must still be manually analyzed. Enterasys SIEM reduces this burden by connecting the dots across the entire infrastructure – delivering to security operators a comprehensive understanding of the most significant risk to the network along with sufficient information to remediate.</p> <p>To help organizations repudiate an incident, Enterasys SIEM provides workflow features to effectively manage security incidents. These features include the ability to assign an incident to a user, annotate an incident, or close an incident. In addition, security incidents detected within Enterasys SIEM can be sent to other 3rd party ticketing systems for resolution.</p>

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



© 2010 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.

