



White Paper:

**Meeting and Exceeding GSI/GCSx Information Security
Monitoring Requirements**

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

Overview

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.

Q1 Labs' QRadar security management product family is 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, and provides an overview of how total security intelligence solutions from Q1 Labs helps local authorities deliver log management and auditing required by government mandates in addition to 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

A critical component that should be considered as part of the solution to these challenges is a centralized security management solution which can greatly improve 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.

QRadar Solution for Government Authorities

QRadar delivers an improved security management capability that can help better protect systems that connect to the GSX. QRadar 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. QRadar's ability to monitor non-traditional systems provides increased visibility into networked systems to detect vulnerabilities before they impact services. The QRadar solution provides comprehensive monitoring, threat detection, threat response, reporting, and auditing capabilities.

Log Management

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

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.

QRadar'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 QRadar 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, QRadar 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 QRadar 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, QRadar provides a flexible architecture to support event logs from unique

event sources, including legacy systems and proprietary applications. QRadar provides a complete log management solution for government authorities tasked with collecting, retaining, and managing event logs in their environment.

Threat Management

“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.”

Fundamental to CoCo is the ability to detect threats and vulnerabilities to the infrastructure. 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. QRadar’s threat management features 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. QRadar takes traditional correlation one step further by helping to connect the dots across the entire infrastructure to deliver to overburdened security operators a manageable set of prioritized security threats that must be addressed along with the information necessary to remediate the situation. (For more information on how Q1 Labs helps organizations detect threats missed by other solutions, please read the white paper titled “A Proactive Approach to Battling Today’s Complex Network Threats” available at www.Q1labs.com.)

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. Unfortunately, the guidance provided by these documents can be confusing and unclear. Recognizing that compliance with a policy or regulation often works on a sliding scale, 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

Although no magic tool exists to enable full compliance, monitoring and management solutions that span the network and security technologies in your environment play a key part in supporting various compliance initiatives. QRadar network security management 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 QRadar helps meet specific requirements of GCSx logging and threat management is provided in Appendix B.

Delivers improved operational efficiency and lowers costs

A critical goal in the development of QRadar is the ongoing delivery of industry-leading security management features that have the lowest cost to acquire, deploy, and maintain. QRadar customers benefit from this philosophy in many ways, as QRadar provides the following benefits for improving operational efficiency and lowering costs:

Converged Solution – QRadar provides — in a single solution — features that historically may be deployed 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 – QRadar provides significant embedded security knowledge which reduces the burden on organizations to understand the complexity of the information provided by the devices on the network. Hundreds of out-of-the-box rules and thousands of report templates that are easily tuned for the business greatly reduces the effort required to turn millions of cryptic events into useful and actionable information.

Ability to Scale – QRadar's appliance-based architecture provides easy deployment and scalability of a security management solution for organizations of any size. Enterprises that deploy QRadar are typically up and running and receiving significant value the first day the product is installed.

Easy to Maintain - Unlike other solutions, QRadar does not require advanced skills to maintain. Core to the solution are simple to follow configuration wizards that minimizes 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. QRadar from Q1 Labs provides government agencies with features to improve overall IT security and to meet specific regulatory mandates through an integrated approach to network security management, which provides unique and differentiated value in the areas of log management, threat management, and compliance management.

Appendix A – Sample Reports for GSI/GCSx

A.1 GSI/GCSx Reporting Overview

QRadar 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.

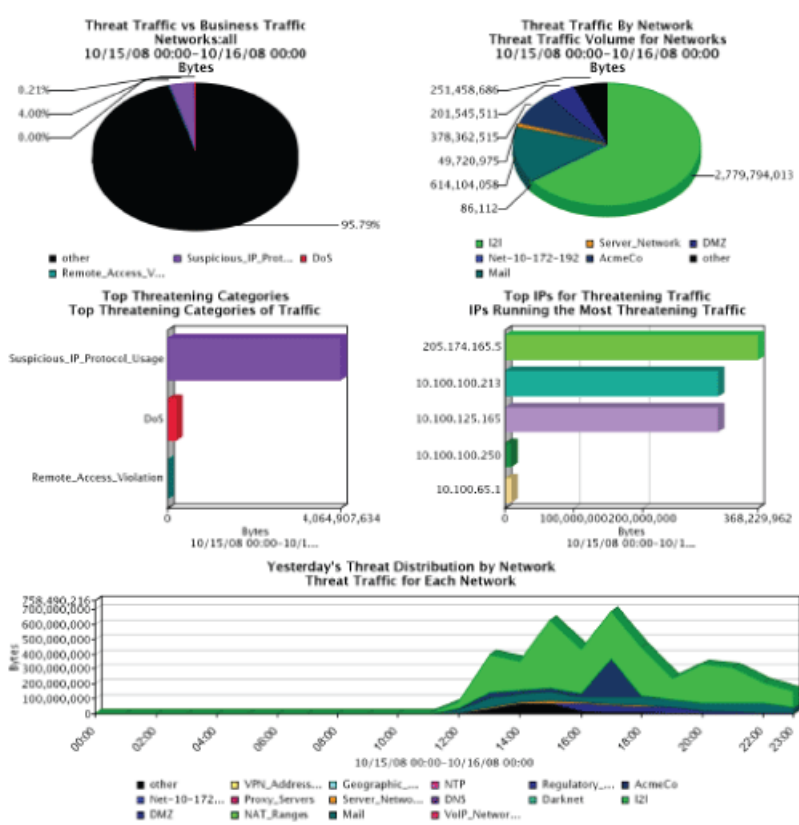
A2. Sample reports supporting:

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

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

Current Threats to Cyber Assets in DMZ

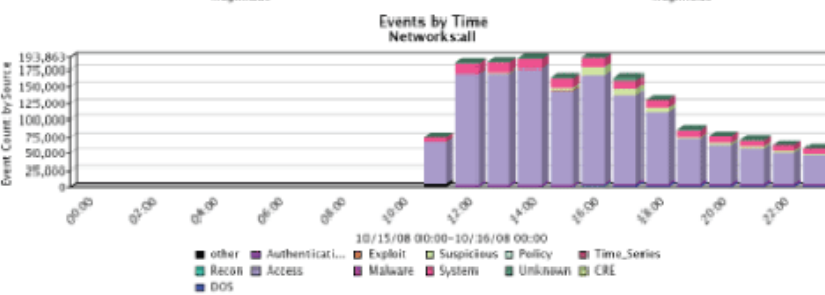
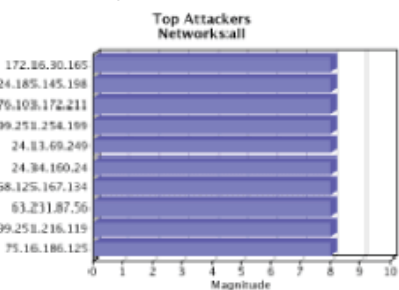
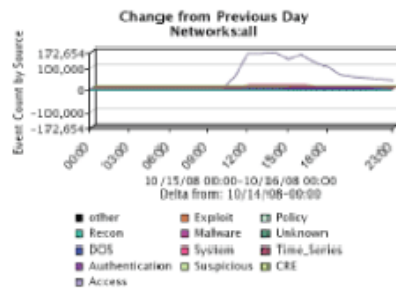
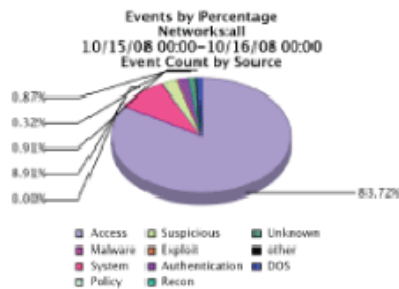
Generated: Oct 16, 2008 10:01:37 PM



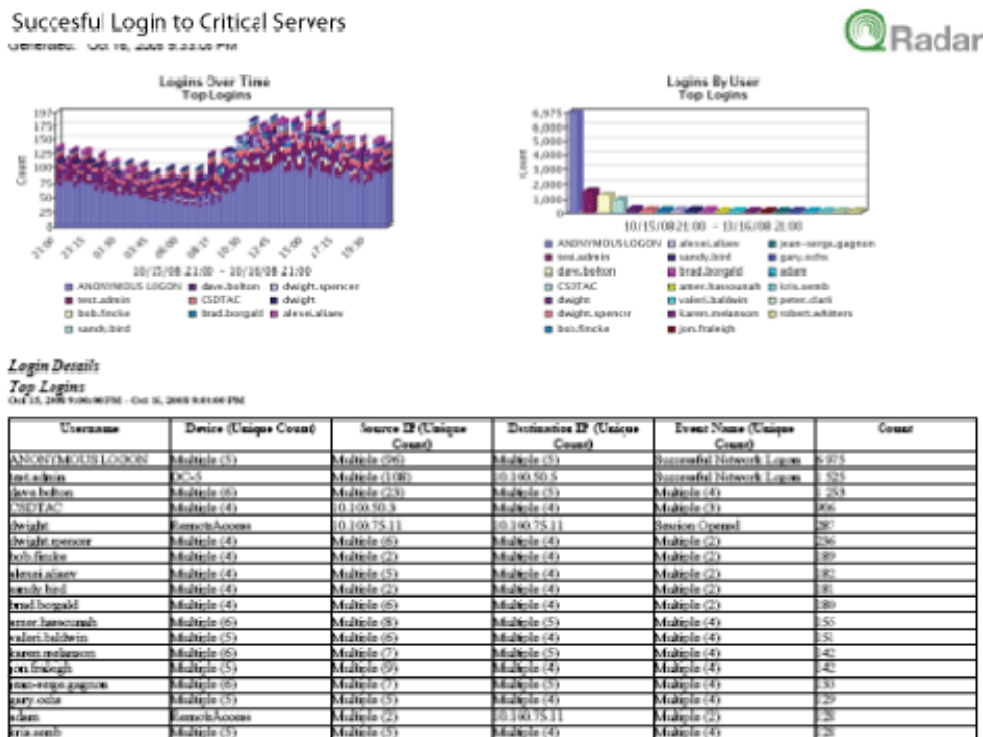
Sample Report A.2.2 – Top Critical Events Across the Security Perimeter

Top Events Across Security Perimeter

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



Sample Report A.2.3 – Memorandum No 22, SR6 – “Logon or Logoff” Activity & SR7 “Execution of Privileged Commands”



Additional useful report templates for these requirements include:

- Network connectivity report (by source and/or destination)
- Network use by user and application
- Network activity by network and/or user group
- Network use by traffic levels
- 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
- Account changes
- Logins to privileged or admin accounts
- Server backup activity

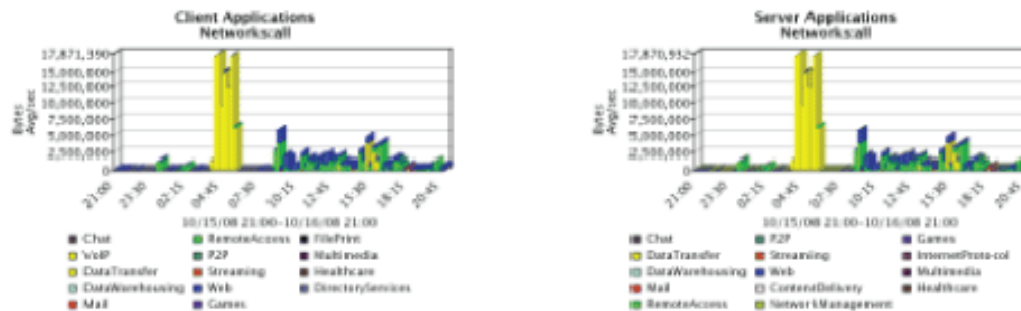
A.3 Sample reports supporting:

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

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

Routable Applications Running on Critical Servers

Generated: Oct 16, 2008 9:54:48 PM



Applications by Bandwidth

Top Apps

Oct 15, 2008 19:00:00 PM - Oct 16, 2008 00:00:00 PM

Application	Source IP (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Source Bytes (Sum)	Destination Bytes (Sum)	Total Bytes (Sum)	Total Packets (Sum)	Count
NFS	Multiple (83)	Multiple (15)	Multiple (4)	8 005 425 043	62 314 657 682	70 320 082 725	660 340 736	50 058
WindowsFileShare	Multiple (135)	Multiple (38)	Multiple (2)	87 643 261 961	11 201 466 875	98 844 728 836	111 424 055	48 920
Snmp	Multiple (20)	Multiple (13)	514	57 451 340 928	2 199 030	57 453 540 958	1 40 196 425	26 446
SSH	Multiple (122)	Multiple (304)	Multiple (2)	18 324 780 224	18 713 372 516	37 038 152 740	53 900 320	80 009
SecureWeb	Multiple (543)	Multiple (927)	Multiple (1 690)	4 684 284 872	8 283 284 095	12 967 568 967	18 183 352	183 118
Unknown TCP	Multiple (241)	Multiple (394)	Multiple (9 836)	1 248 833 700	10 194 719 934	11 443 553 635	12 756 154	127 517
HTTPWeb	Multiple (313)	Multiple (4 400)	Multiple (64)	1 303 328 404	9 884 795 546	11 178 123 950	17 162 037	120 688
Flowgram	Multiple (91)	Multiple (33)	Multiple (1 40)	442 833 707	3 729 239 962	4 172 073 669	12 536 219	16 429
HTTPImageTransfer	Multiple (158)	Multiple (2 452)	Multiple (2)	582 741 082	2 118 488 304	2 701 229 386	3 301 970	81 219
Webman	Multiple (83)	Multiple (82)	0000	610 416 965	1 713 576 904	2 323 993 869	4 117 349	52 427
WebMediaVoice	Multiple (43)	Multiple (122)	80	66 661 509	1 476 463 863	1 543 125 372	2 204 165	287
MSExchange	Multiple (121)	Multiple (114)	Multiple (2 818)	847 029 204	447 256 950	1 294 286 154	2 922 397	164 840
WebMediaDocument	Multiple (164)	Multiple (189)	80	37 356 439	965 452 652	1 002 809 091	1 253 892	1 928
ForeignSQL	Multiple (11)	Multiple (10)	5432	62 658 804	834 425 800	897 084 604	1 449 898	12 776
FSoc	Multiple (23)	Multiple (26)	Multiple (4)	405 228 845	440 799 638	846 028 483	1 889 910	10 604

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

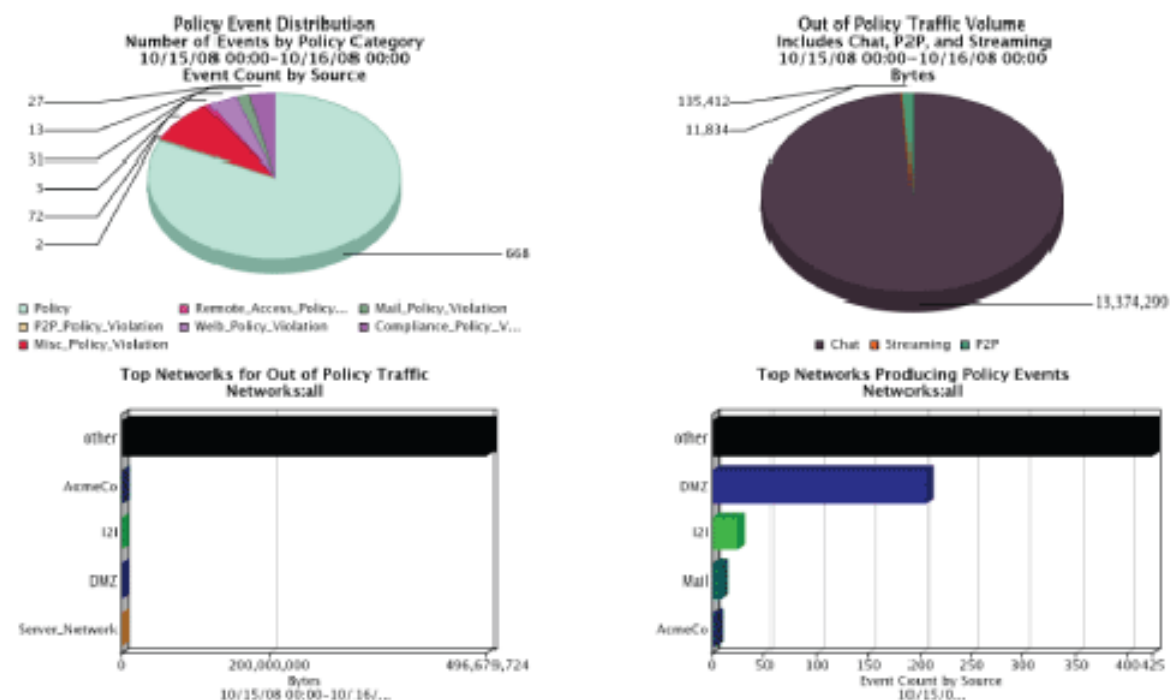
A.4 Sample reports supporting:

- 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

Daily Management Security Policy Report

Generated: Oct 16, 2008 10:00:22 PM



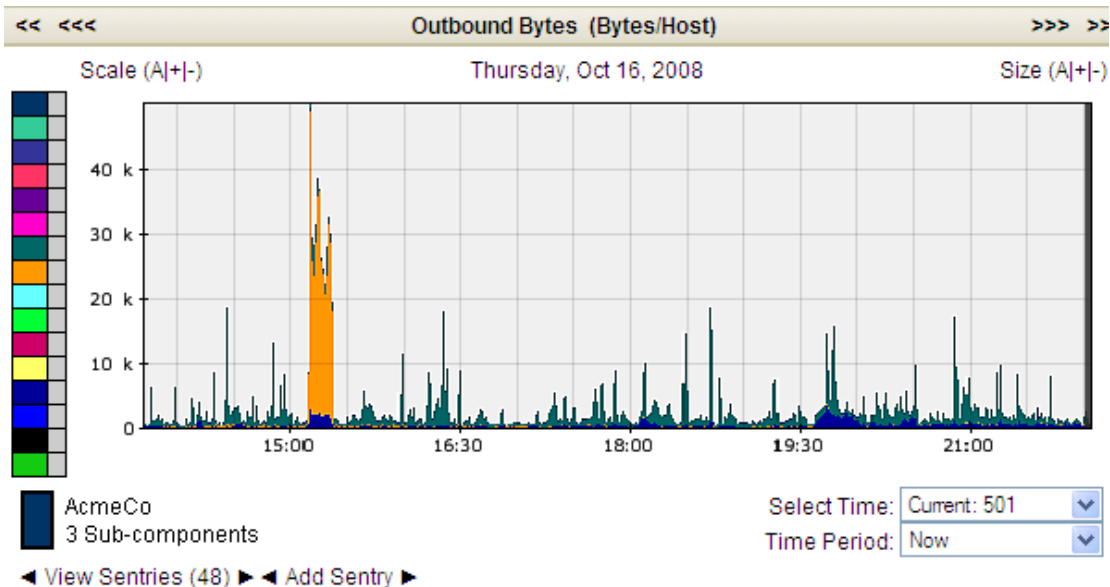
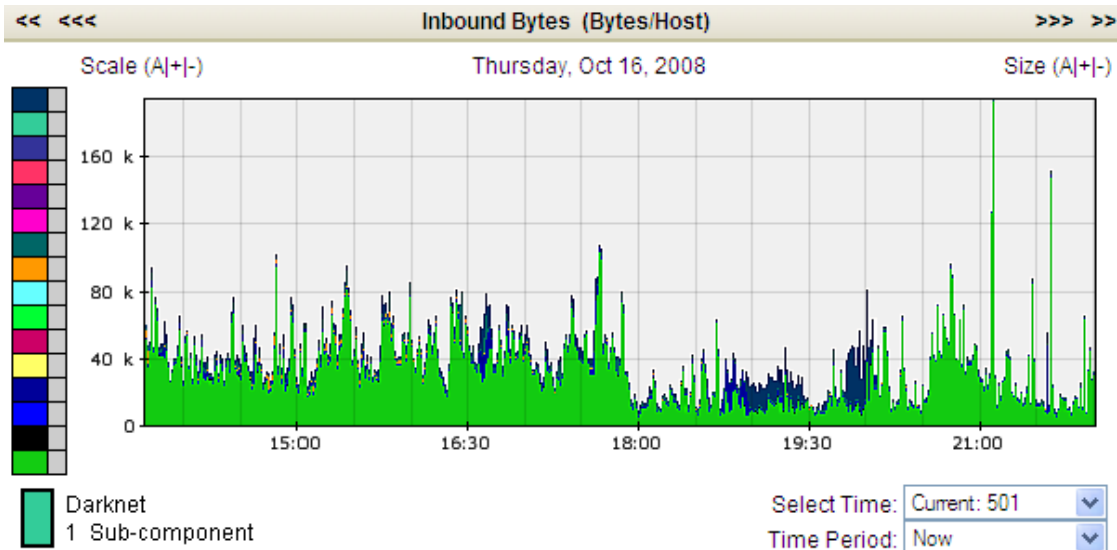
Additional useful report templates for this requirement include:

- 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)	other			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.EuropeAll							

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 QRadar

GSI Code of Connection (CoCo)	
Requirement	QRadar 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 QRadar supports the ISO controls is provided in the next section of this table.
IEC/ISO 27702 (formerly ISO 17799)	
Requirement	QRadar Support
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. QRadar 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 guidelines 	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 QRadar 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 ➤ 10.10.1 Audit logging ➤ 10.10.2 Monitoring system use ➤ 10.10.3 Protection of log information ➤ 10.10.5 Fault logging 	<p>QRadar provides significant value in improving the security of networked communications. one high level overview how QRadar addresses specific ISO requirements is provided below.</p> <p>10.4.1 Protection against malicious code</p> <p>QRadar 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 QRadar is capable of detecting threats not found by other security applications.</p> <p>10.10 Monitoring</p> <p>Fundamental to QRadar is its ability to monitor and analyze security events in real-time.</p> <p>10.10.1 Audit logging</p> <p>QRadar 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.</p> <p>10.10.2 Monitoring system use</p> <p>QRadar can collect and analyze a wide variety of access control information including, but not limited to logs from:</p>

	<p>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).</p> <p>10.10.3 Protection of log information</p> <p>QRadar 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. QRadar also provides the ability to encrypt information transfer across a distributed log management deployment.</p> <p>10.10.5 Fault logging</p> <p>QRadar 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.</p>
<p>Section 11.1.1 Access control policy Section 11.5.1 Secure log-on procedures</p>	<p>QRadar 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).</p>
<p>Section 13.1.1 Reporting information security events and weaknesses Section 13.2 Management of information security incidents</p>	<p>One of the most unique features of QRadar 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. QRadar 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>
Communications Electronic Security Group (CESG) Info Security Memorandum No. 22	
Requirement	QRadar Support
<p>General Requirement #21 – Log File Integrity</p>	<p>QRadar 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. QRadar also provides the ability to encrypt information transfer across a distributed log management deployment.</p>
<p>General Requirement #22 – Log Retention</p>	<p>QRadar 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

	<p>information</p> <ul style="list-style-type: none"> 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>QRadar can support a wide variety of data retention policies depending on individual business and compliance requirements.</p>
General Requirement #23 – Audit Frequency	QRadar 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	QRadar provides a rich set of vulnerability assessment features. QRadar provides the ability to collect information from a wide variety of vulnerability scanners, including Nessus which is mentioned specifically by CoCo. http://www.govconnect.gov.uk/implementation/coco-faqs.php QRadar 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.
General Requirement #25 – protective measures against threats	Unlike traditional log management solutions that typically only provide event collection and rudimentary correlation, QRadar 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	QRadar provides the ability to synchronize time across all architectural components using a standards based NTP server.
Security Requirement #2 (SR2) – Unique Identification	QRadar 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, QRadar 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 QRadar 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, QRadar 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 QRadar based on both the perceived source and destination IP address.
Security Requirement #6 (SR6) – Reveal the type of service	QRadar 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).
	QRadars 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).
Security Requirement #7 (SR7) – Identify privileged commands	As mentioned in SR6 above, QRadar can provide a detailed audit of privileged (administrative) access to systems. In addition, QRadars 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	QRadar 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, QRadars 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	QRadar 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.
Security Requirement #15 (SR15) – Reveal changes to any executables and/or configuration files	QRadar supports the collection of information from a wide variety of 3 rd 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	QRadar 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 QRadar 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. QRadar 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, QRadar 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 QRadar can be sent to other 3rd party ticketing systems for resolution.</p>

Corporate Headquarters:

Q1 Labs, Inc.
890 Winter Street
Suite 230
Waltham, MA 02451
781-250-5800
info@Q1Labs.com

WP012709A