FUJ00155413

Document Title: Horizon Event Logging Process for Operational Security

Document Type: *PRD*

Release: *DRAFT*

Abstract: *This document summarises the Operational Security Process for Event logging*

Document Status: WITHDRAWN – REPLACED BY ING-X DOCUMENT SVM/SDM/PRO/0032

Originator & Dept: *William Membery*
Operational Security

Contributors *Deborah Haworth CISO, Mike Conneely, Brian Gallacher Tivoli, Dave Hawood Solutions Architect, Marie Clare Mcoy ISD [illegible], Jo Diffen ISD Unix, Andy Gibson ISD UNIX, Shaun Pinder [illegible], James Gosnold CSA Security, Jo Booth ISD Network*

External Distribution: *(Post Document Management to distribute following approval)*

WITHDRAWN

Approval Authorities: *(See CM/ION/078 for Approval roles)*

Name	Role	Signature	Date
Howard Pritchard	Chief Information Security Officer (CISO)		
Pete Sewell	Operations Security Manager		

FUJ00155413

0.0 Document Control

0.1 Document History

Version No.	Date	Reason for Issue	Associated CP/PEAK/PPRR Reference
0.1	14/12/2007	Process required for Event Logging	
0.2	18/01/2008	Amended following comments	
0.3	03-Feb-2009	WITHDRAWN AND REPLACED BY HNG-X DOCUMENT SVM/SDM/PRO/0032. Bill Membery email of Mon 02/02/2009 16:2	

0.2 Review Details

Review Comments by :	Thursday, 14th January 2008
Review Comments to :	Bill.membery GRO & RMGA Document Management GRO

Mandatory Review	
Role	*Name*
CISO	Howard Pritchard
Service Delivery Manager (Ops)	Ian Cooley
Lead Architect	Sean Kerrin
Operational Security Manager	Peter Sewell
Head of Service Transition and Change	Graham Welsh
SV&I, LST Test Manager, RMGA	Sheila Bamber *
Service Support Manager RMGA	Peter Thompson
CS Network Services	Alex Kemp
CS System Support Centre Manager	Mik Peach *
CS Business & Risk Security Manager	Brian Pinder
SI Technical Designer	Ian Bowen
ISD Team Manager IS Operations (KA)	Adrienne Thompson
ISD POA UNIX Administrator IS Operations KA	Andrew Gibson *
ISD NT Senior Systems Engineer IS Operations KA	Warren Welsh
ISD Practice Head - Implementations North	Dave Jackson
IS Operations Manager	Jerry Acton *
Principal Consultant	Mike Conneely *

WITHDRAWN

FUJ00155413

Optional Review	
Role	*Name*
Principal Security Consultant	Jim Sweeting
SI ASS Designer	Alan Hodgkinson
CS Service Release Manager	John Budworth
SI Test Designer	Peter Robinson
SI Release Manager	James Stanton
CS Business Continuity Manager	Tony Wicks
Design & Development Manager	Roy Birkenshaw
Software Configuration Management (PO)	Tariq Arain
SI Team Leader	Peter Ambrose
SI ASS Designer	Ian Devereux
SI Technical Designer	Chris Beddo
Programme Office Manager	David Cooper
CS Major Release Manager	Sa Payne / Peter Goodwin *
Service Delivery Manager (OBC)	n Ve bles *
Service Management Manager	Liz lrose
Customer Solutions Architect	reth nkins
Technical Design Authority	Da e Tanner
Technical Consultant MSS, SMC	Da e Laker
Solutions Group - Service & Tr sition, In mation Assurance	James Gosnold
Release Controller	John Boston
Lead Test Engineer - MGA	Graham Jennings
Service Definition M ager	Adam Bowe
Problem Mana r	Lionel Higman
Integrati Team eader	Asad Sheikh
Tes ngine ications	Nigel Taylor
Principal ns ltant/SAP Service Delivery Team Leader	Eveline Bunce
Service Delivery Manager - Data File Transfer	Kirsty Gallacher
Product Specialist	Mark Wright
*Issued for Information – **Please restrict this distribution list to a minimum***	
Position	*Name*

WITHDRAWN

FUJ00155413

(*) = Reviewers that returned comment sheets and/or attended a Group Review (Meeting Review)

0.3 Associated Documents

Reference	Version	Date	Title	Source
PA/TEM/001 (DO NOT REMOVE)			Fujitsu Services POA Horizon Programme Document Template	PVCS
			Fujitsu Services Horizon Security and Control Framework (New Document)	PVCS
RS/POL/002			Fujitsu Services Security Policy	PVCS
CS/SER/016			Service Description for the Security Management Service	PVCS
SVM/SDM/PRO/0018			RMGA Customer Service Incident Management Process	Dimensions
FSSL	10.01	24/01/2008	Security Information & Event Management Supported Devices and Standard Reports	Fujitsu Services

Unless a specific version is referred to above, reference should be made to the current approved versions of the documents.

N.B. Printed versions of this document are not under change control.

WITHDRAWN

FUJ00155413

0.4 Abbreviations/Definitions

Abbreviation	Definition
ARQ	Audit Request – this is a service provided by RMGA Security to PO Ltd.
Athene	Metro's Performance Management, Capacity Planning and Capacity Forecasting software specialist tool for Unix
Centera	EMC Secure Storage Solution
Cisco Works	Cisco's Network Management Tool
CISO	Chief Information Security Officer
CP	Change Proposal
DNS	Domain Name Server – way of translating names to IP addresses
HNG-X	Horizon Next Generation – the new developing Solution for Post Office Ltd
Horizon	Royal Mail Groups Current Solution for Post Office Limited
HP Openview	Hewlett Packard's Network Management Tool
Insight Manager	Compaq's Fault and Performance Management Tool used on Compaq Windows Platforms in RMGA
ISO	International Standards Organisation
KMA Logs	Logs produced by the Key Management Administration System
Maestro	Tivoli's Scheduling Tool
NHS	Fujitsu's National Health Service Account
NMS	Network Management Server
NNM	Network Node Manager
OLA	Operational Level Agreement – agreement defining what is required from the Operational part of an organisation providing a service
OOH	Out of Hours Access Solution for Support Teams
Oracle	Relational Database Management System
Patrol	Software Innovations Unix Applications Monitoring Tool
PO Ltd	Post Office Ltd
Radius	Remote Authentication Dial in User Service
RMGA	Royal Mail Group Account
RSA Tokens	Tokens used for ensuring two factor authentication prior to access to systems

WITHDRAWN

Rules of Evidence	Rules required by the Courts to ensure that any evidence used in prosecution is admissible
SAS	Secure Access Servers – used for remote access logging
Sawmill	Flowerfires Log Analysis Tool
SDU	Service Delivery Unit - unit of an organisation delivering a service
ServerView	Fujitsu's Fault and performance Management Tool used on Fujitsu Windows Platforms
SIEM	Security Incident and Event Monitoring Tool
SI	Fujitsu Systems Integration Group
SLA	Service Level Agreement – agreement defining what level of service is expected
SLT's	Service Level Targets
SMC	Systems Management Centre
Sophos	Anti Virus and Anti Spam product
SSH	Secure Shell – a network protocol that ensures data is exchanged between two computers over a secure channel
syslog	Standard for forwarding log messages in an IP Network
TACACS+	Cisco's Accounting, Authentication and Audit Tool
Tivoli	IBM Event Monitoring and Configuration Tool
VPN	Virtual Private Network

WITHDRAWN

FUJ00155413

0.5 Changes Expected

Changes
Expect changes following the definition of PO Ltd requirements
Expect changes following review process.
Expect changes following production of Fujitsu Services Security and Control Framework
Expect changes once SIEM tools are agreed and finalised
Expect changes following SI Designs
Expect changes once asset details requiring log analysis are available
Expect changes once Event test Criterion are agreed

WITHDRAWN

FUJ00155413
FUJ00155413

0.6 Table of Contents

1.0 SCOPE OF DOCUMENT 5
1.1 POLITICAL BACKGROUND 5
1.2 TECHNICAL BACKGROUND 5
1.2.1 Tivoli 5
1.2.2 Networks NMS and Syslog Server 5
1.2.3 Service Delivery Unit Analyses 5
2.0 DEPENDENCIES 5
3.0 PROCESS FLOW 5
3.1 HORIZON SECURITY AND CONTROL FRAMEWORK 5
3.2 EVENT AUDIT SECURITY CONTROL AND FRAMEWORK REQUIREMENTS 5
3.3 EVENT AUDIT FRAMEWORK AND CURRENT VIEW 5
3.4 OPERATIONAL SECURITY FRAMEWORK IMPLEMENTATION. 5
3.5 TESTS 5
3.6 REPORTS 5
3.6.1 Summary Reports 5
3.6.2 Compliance Report 5
3.6.3 Operational Security Management and adhoc Reports 5
3.7 SAWMILL PROCESS 5
4.0 AUDIT 5
5.0 APPENDIX A 5
5.1 TIVOLI EVENT LOG SUMMARY BY SAWMILL 5
5.1.1 Summary 5
5.1.2 Overview 5
5.1.3 Years/months/days 5
5.1.4 Days 5
5.1.5 Days of weeks 5
5.1.6 Hour of days 5
5.1.7 Console hostnames 5
5.1.8 Log sources 5
5.1.9 Log source types 5
5.1.10 Event origins 5
5.1.11 Hostnames 5
5.1.12 Severities 5
5.1.13 Event codes 5
5.1.14 Actions 5
5.1.15 Usernames 5
5.1.16 Domains 5
5.1.17 Login ids 5
5.1.18 Login types 5
5.1.19 Auth pkgs 5
5.1.20 File names 5
5.1.21 Messages 5

WITHDRAWN

FUJ00155413
FUJ00155413

5.2 SUMMARY ANALYSIS OF A WINDOW 2K/XP CSV LOG EXPORT 5
5.2.1 Summary 5
5.2.2 Overview 5
5.2.3 Years/months/days 5
5.2.4 Days 5
5.2.5 Day of weeks 5
5.2.6 Hour of days 5
5.2.7 Sources 5
5.2.8 Types 5
5.2.9 Categories 5
5.2.10 Events 5
5.2.11 Users 5
5.2.12 Computers 5
5.2.13 Descriptions 5
5.3 SUMMARY ANALYSIS OF A CISCO FIREWALL/ROUTER/SWITCHES SYSLOG 5
5.3.1 Summary 5
5.3.2 Overview 5
5.3.3 Years/months/days 5
5.3.4 Days 5
5.3.5 Day of weeks 5
5.3.6 Hour of days 5
5.3.7 Logging Devices 5
5.3.8 Operations 5
5.3.9 Messages 5
5.3.10 Message codes 5
5.3.11 Protocols 5
5.3.12 Source IPs 5
5.3.13 Destination IPs 5
5.3.14 Source hostnames 5
5.3.15 Destination hostnames 5
5.3.16 Source ports 5
5.3.17 Destination ports 5
5.3.18 Source sides 5
5.3.19 Destination sides 5
5.3.20 Geographic locations 5
5.3.21 Interfaces 5
5.3.22 Directions 5
5.3.23 Foreign IPs 5
5.3.24 Foreign ports 5
5.3.25 Global IPs 5
5.3.26 Global ports 5
5.3.27 Local IPs 5
5.3.28 Local ports 5
5.3.29 Service names 5
5.3.30 URLs/directories 5
5.3.31 URLs 5
5.3.32 Flags 5
5.3.33 Users 5
5.3.34 Commands 5
5.3.35 Types 5
5.3.36 Lists 5
5.3.37 Sessions overview 5

WITHDRAWN

FUJ00155413

5.3.38 Entry pages 5
5.3.39 Exit pages 5
5.3.40 Session pages 5
5.3.41 Session users 5
5.4 SUMMARY ANALYSIS OF A UNIX SOLARIS 9.0 SYSLOG 5
5.4.1 Overview 5
5.4.2 Years/months/days 5
5.4.3 Days 5
5.4.4 Day of weeks 5
5.4.5 Hour of days 5
5.4.6 Logging devices 5
5.4.7 Syslog messages 5
6.0 APPENDIX B 5
7.0 APPENDIX C 5

WITHDRAWN

FUJ00155413

1.0 Scope of Document

This document defines the process to be followed by the operational security team to meet its obligations under RS/POL/002 Horizon Security Policy and CS/SER/016 the Service Description for the Security Management Service and applies to Horizon only.

This process is concerned with those actions that the operational security team undertake, all other processes, guidelines and work instructions are outside the remit of this document, although a historical background has been included to assist in establishing who and what is required to enable us to establish this process going forward.

1.1 Political Background

Horizon does not currently analyse logs or events from a security compliance perspective and concentrates only on availability incidents. This therefore means that the other two areas of Operational Security Reporting, Confidentiality and Integrity are not picked up. (N.B. this is because PO Ltd has not set any SLT's in this area and apart from a generic ISO 27001 compliance contractual statements no requirement exists or has been paid for).

1.2 Technical Background

1.2.1 Tivoli

Analysis of incidents in Horizon relies mainly on Tivoli Events and not the collection of logs, with the exception of network devices. Events created by applications and databases are only collected if they are written to the Operating System Logs, the one exception being Radius Server Logs.

Those platforms which have a Tivoli Event adapter, e.g. the data centre servers; counters and branches forward events through Tivoli Event Consoles to a master Oracle database.

The Tivoli process concentrates on availability and historically the placement of Event adapters has not been based on risk assessment or an asset register and therefore any future processes would need to take this into account.

It must also be noted that due to the volume and cost of managing events from the Counter estate only events are forwarded from them. For example in the past an assessment of the impact of auditing of more information (files) on the counter, was made and if such data was collected approximately ½ a million events per day occurred, if such events are excluded then there were about 150,000.

All events collected by Tivoli are initially buffered for about 1 hour and are available for view, and these details are then sent to the archive server to ensure that rules of evidence are maintained.

A summarised version of the events is maintained online for approximately 10 days and analysis of availability events is undertaken by SMC. This summary removes all background

WITHDRAWN

FUJ00155413

noise (redundant, repetitive and uninteresting events) and only events identified as interesting are retained.

From a security perspective, only log on and log off data is retained as no requests or analysis has been made for any other requirements and these are therefore seen as background noise.

If an increase in the Event collection of Security events is required as shown in section 4.0 then it must be noted that the volume of data collected and the capacity of the platform holding this information (disk space and memory) and software revision used to manage and analyse it are key. The current Tivoli version in Horizon is Framework 3.71 and this and the Oracle Server storing the data may also need upgrading, both of which are required for HNG-X.

1.2.2 Networks NMS and Syslog Server

The retention of syslogs is used for network devices. The location of this storage is currently being moved to a new DNS and syslog server in the Bootle and Wigan data centres from the old NMS and no analysis is currently undertaken of these logs, although CP 4410 has been approved and is currently going through the release management process for the use of Sawmill to analyse Firewall logs. These logs and events are currently not analysed or included as part of Tivoli.

WITHDRAWN

FUJ00155413

1.2.3 Service Delivery Unit Analyses

In addition to Tivoli, each of the service delivery units has its own toolsets used for monitoring the areas of service it is required to provide. On initial investigation this again mainly covers the area of availability.

The information from these tools is not all currently fed into Tivoli or any other centralised SIEM to manage and monitor security events or incidents neither are regular reports provided to Operational Security from these units.

Examples of these tools are:

- HP Openview is used for monitoring the Network
- Cisco Works and TACACS+ are used for managing access and authentication to network devices
- Athene is used for performance gathering. The Athene data is analysed by the performance monitoring team within the account (the UNIX team can request reports etc. from it but the database is in Bracknell and the UNIX team have no direct access)
- Patrol is used for Unix Operating System monitoring - Patrol events are actually fed into the Tivoli event management system. Some events will be raised as TFS calls by SMC and some events may just be stored in the event archives. As previously stated they are not analysed for Security events and are mainly around availability.
- Insight Manager is used for managing and monitoring Compaq platforms running Windows
- Server View is used for monitoring Fujitsu platforms running Windows
- Sophos is used for managing Anti Virus
- RSA Tokens are used to manage two factor authentication
- KMA is used for manage key management

WITHDRAWN

FUJ00155413
FUJ00155413

2.0 Dependencies

To achieve an effective and efficient Event Management solution Operational Security is dependent on the following

1. Requirements of reports that PO Ltd want to monitor Operational Security, are agreed and documented.
2. Reports required by RMGA to prove operational security compliance are defined and documented.
3. A Fujitsu Services Horizon Security and Control Framework is provided by the Information Governance Team are provided to SI for Designs.
4. The Fujitsu Horizon Security and Control Framework provided by the Information Governance Team must ensure that any non RMGA support and management systems used to support RMGA systems and devices meet the Framework requirements.
5. SI use items 1, 2, 3 and any Operational requirements (see below) to provide Design for Operational Security Incident and Event Monitoring (SIEM) system.
    a. SI designs ensure that details of all platforms that require log analysis is documented and are part of the SIEM system.
    b. SI designs ensure that any adaptors or agents required for SIEM go through the Release Management Process and are included in any Physical Platform Designs
    c. SI designs ensure that details of all users, their rights of access and their roles are documented and easily correlated and are part of the SIEM system.
    d. SI designs ensure system owners are identified and documented as part of the SIEM system.
    e. SI ensures designs include scheduling to push logs to Central Collection Point as part of the SIEM system.
    f. SI designs ensure Firewalls are configured to accept log pushes as part of the SIEM system.
    g. SI designs ensure that Maestro or alternative scheduler is set to schedule the push of logs to Central Repository as part of the SIEM system and audit report of failures is available.
    h. SI designs ensure that Central Collection platform (or platforms assuming resilience is required) has sufficient storage capacity for log storage based on the retention requirements defined in Fujitsu Services Horizon Security and Control Framework.

WITHDRAWN

i. SI designs include a method of log retention so that the rules of Evidence requirement cannot be questioned if used in legal proceeding.

j. SI designs ensure the Central Collection platform have accountability; authentication; and audit of any access.

k. SI designs ensure that the platforms that are used to analyse, and process logs have sufficient processing power, storage and memory to allow summarisation, trending and ad hoc queries when required.

l. SI designs ensure that platforms used to analyse or process reports have accountability, authentication and audit of both the platform and data reports analysed.

m. SI designs ensure that platforms used to analyse, process or report Event information are networked and fire-walled and permitted to undertake all analysis and reporting required

6. Service Delivery Units requirements for Event Capture and event logging are defined in SLA's or OLA's and should include the following Operational Security requirements :

   a. Service Delivery Units configure endpoint devices to meet the requirements defined in the SI Design.

   b. Service Delivery Units ensure logs are pushed to a Central Collection point and are in a standardised log analysis format as defined in the SI designs and ensure that processes are in place to resend any failed log pushes.

   c. Network Teams configure firewalls and Network equipment to permit the pushing of logs to the Central Collection Point.

   d. Service delivery units will ensure that they do not manually analysis of logs will be undertaken by and thus ensure that the segregation of duties between Operations and Audit takes place.

7. An SIEM Tool is available at all required locations Operational Security work and permits the following:

   a. SIEM Tool details any logs that are missing from any reports undertaken.

   b. SIEM Tool converts logs into a standard format

   c. SIEM Tool allows a series of tests to be run against standardised logs to produce results

   d. SIEM Tool permits Operational Security to print and export files to Microsoft Office or alternate tool for summarisation and graphing.

   e. SIEM Tool permits scheduling of both analysis and summary reports against the key headings in the Fujitsu Services Horizon Security and Control Framework.

WITHDRAWN

FUJ00155413

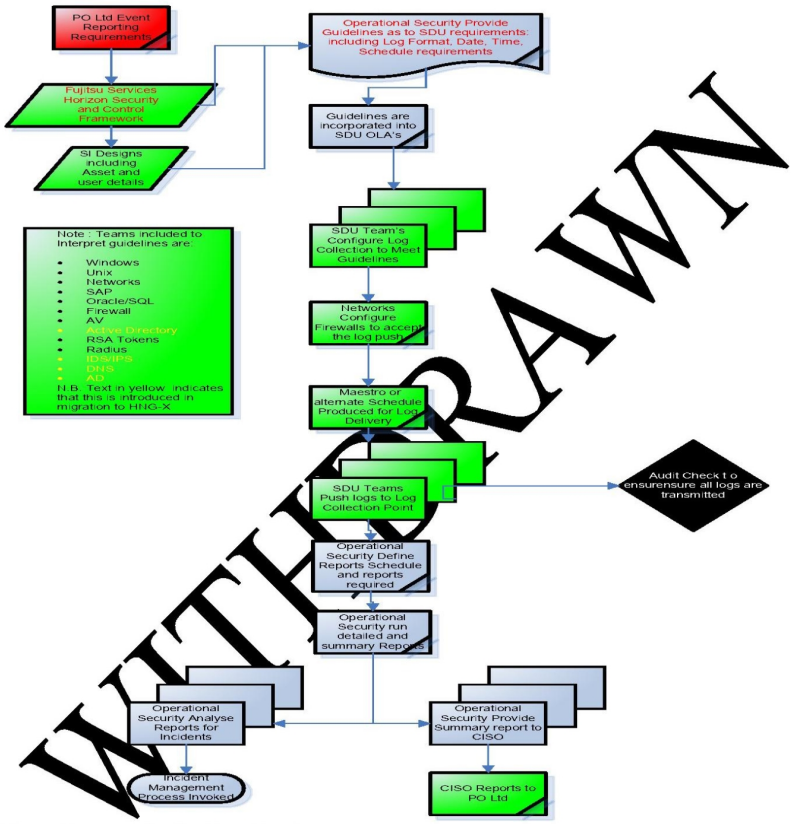
f. SIEM Tool allows trending, summarisation and ad hoc queries when required by authorised users.

g. SIEM Tool permits management of SIEM tool users and their rights.

WITHDRAWN

FUJ00155413

3.0 Process Flow



WITHDRAWN

Figure 1 Process Flow for Event Logging

N.B. Key processes from other areas have been included to illustrate the integration of all areas in producing and analysing event logs

1. Items in Red are PO Ltd Process
2. Items in green are non Operational Security Process
3. Items in grey are Operational Security Processes

FUJ00155413

3.1 Horizon Security and Control Framework

In the absence of a Horizon Security Framework the principles adopted by other Fujitsu Service Account Security Frameworks (e.g. NHS), have been provided by the CISO and will be adopted until one is ready for Horizon and HNG-X and their key points are documented below to provide a background to this process.

The overall frameworks is split into manageable areas that are in line with Security Policy sections,

This comprises five main work strands and twenty separate task areas, or control groups which have been identified as outlined in the table below. These allow the sets of controls to be organised and addressed to the audiences who need to work with them, in a more logical and focused way.

A. PEOPLE	B. INFRASTRUCTURE	C. APPLICATIONS	D. CONTROL	E. OPERATIONAL
A1. Personnel Security A2. Training & Awareness	B1. Operating Systems B2. Backup and Media Management B3. Networks **B4. Event Audit**	C1.Access Management C2a.Solution Design Requirements C2b. Solution Design Processes	D1.Risk Management including Preventive and Corrective Actions D2. Policy; Security Management and Compliance D3. Legal & Contractual Responsibilities D4. Information Classification and Handling D5. Third Party Issues D6. Security Culture & Leadership	E1. Change Control 2. Service Delivery Processes E3.Business Continuity E4. Security Incident Management E5. Physical Security

Figure 2 Security and Control Framework Overview

WITHDRAWN

FUJ00155413

3.2 Event Audit Security Control and Framework Requirements

Event Audit is part of the overall control framework and cannot be considered in isolation in particular it relates to other key controls shown below and these are keys areas that Operational Security needs to report back to both the CISO and PO Ltd on.

- Operating Systems;
- Back-up and Media Management;
- Off-site Issues;
- Networks;
- Access Management;
- Solutions Design;
- Risk Management;
- Legal & Contractual, and;
- Security Incident Management.

The controls in the framework are not intended to be detailed operating procedures or technology-specific security or build standards – these will be drafted by specific operational, delivery or technical teams, hence this operational process. An initial assessment has been undertaken with the Tivoli staff to assess whether the information is currently available or whether development work would be required in Horizon and this is shown in the last column.

The controls in the framework outlined are not therefore exhaustive and do not remove the need to comply with the security requirements in the contract or CS/SER/016 Service Description for the Security Management Service. The controls proposed are not simply technical security countermeasures. They also cover:

- Organisational controls (roles, responsibilities, structures, reporting lines, etc);
- Procedural (prescribed, documented standardised methods and processes for performing functions aimed at ensuring consistency and repeatability of performance, potentially reinforced by training and awareness);
- Technical controls (automated controls, in-built to systems and applications, controlling logical or physical access, or monitoring activity – these help ensure consistent operation of the control by placing less reliance on the human element for their deployment and use);
- People related controls (vetting/clearances, awareness, supervision, review).

WITHDRAWN

FUJ00155413

3.3 Event Audit Framework and current view

Control Group	B. 4 Event Audit				
Key	**7799 Ref**	**27001 Ref**	**Control**	**Countermeasure**	**Responses**
Gathering of Event Information					
868	9.7.2	10.10.2	Monitoring of Activity	Operational activity should be monitored	Tivoli/HP Openview / Athene/Patrol/Network syslogs / Insight Manager and Server view/Sophos AV Logs /RSA Token and KMA logs
869	9.7.2	10.10.2	Monitoring of Activity	Monitor operator interaction via system log reports	Monitoring of Availability is undertaken by Tivoli and the SDU's tools, but Security monitoring is not undertaken
870	9.7.2	10.10.2	Monitoring of Activity	Inform operations staff that their activities are being monitored	Security Awareness program and policy to do this needs to be put in place for Horizon
871	9.7.2	10.10.2	Monitoring of Activity	Regular inspection of console and operations logs	This takes place for availability by SMC and SDU's but no Security Monitoring
794	9.5.5	11.5.4	Use of system utilities	System logging will be enabled to provide audit of all attempts to gain access to system utilities.	This is undertaken via RSA Log's and SSH logs, but analysis of these by security is not undertaken
989	10.4.3	12.4.3	Access control to Program Source	All accesses to the program source libraries to be audited	This is not done by Tivoli, or any of the Management tools above

WITHDRAWN

FUJ00155413

1037	10.5.6	10.10.2	Control of Access to the System Managers Accounts	Generate a continuous record of all commands issued by the System Administrator's account	Each Auditing tools under takes this independently but none of this is centralised and the only logs of commands made is on the Secure Shell.
1205	12.1.7	13.2.3	Collection of Evidence	Sufficient evidence to be collected to support an action against an individual or organisation	This is possible for counters through the ARQ service but not other areas.
1206	12.1.7	13.2.3	Collection of Evidence	For internal disciplinary matters the evidence necessary to be described by internal procedures	Not at present.
1207	12.1.7	13.2.3	Collection of Evidence	Evidence presented at court to comply with the rules of evidence	Fine for ARQ's but not other areas
1208	12.1.7	13.2.3	Collection of Evidence	Evidence presented at court should be admissible	Fine for ARQ's bur not other areas
1209	12.1.7	13.2.3	Collection of Evidence	Information systems to comply with code of practice on the production of admissible evidence	Fine for ARQ's bur not other areas
1210	12.1.7	13.2.3	Collection of Evidence	It should be possible to demonstrate the quality and completeness of evidence	Fine for ARQ's bur not other areas
1211	12.1.7	13.2.3	Collection of Evidence	A strong evidence trail to be provided	Fine for ARQ's bur not other areas
1212	12.1.7	13.2.3	Collection of Evidence	Outside organisations brought in as soon as legal action is contemplated	Policy and processes required here for internal but Fine for ARQ's
1213	12.1.7	13.2.3	Collection of Evidence	Lawyers to be consulted on possible actions to be taken	Policy and processes required here for internal but Fine for ARQ's

WITHDRAWN

FUJ00155413

1214	12.1.7	13.2.3	Collection of Evidence	Police to be informed as soon as possible	Formal processes required here for internal but Fine for ARQ's

WITHDRAWN

FUJ00155413

WITHDRAWN

Logging Events

821	9.7.1	10.10.1	Event Logging	Audit logs recording exceptions and other security relevant events shall be produced and kept for an agreed period, in accordance with policy or guidance, to assist in future investigations and access control monitoring.	Policy and processes required here for internal but Fine for ARQ's.
821a	9.7.1	10.10.1	Event Logging	Audit logs shall be produced for different categories of system access and event, such as: 1. Logs for remote access. 2. Logs for standard user access to management information. 3. Logs for users on support systems, logs for privileged users on support systems. 4. Logs for privileged users on RMGA systems. 5. Logs for PO Ltd users.	1. Remote Access is picked up via the SAS servers. 2. Events on Web Pages are not covered by Tivoli for any Management information accessed. 3. Users outside RMGA network and access and SAS are not covered but these should be picked up by Policies on Core. 4. Privileged users on support systems are not picked up by Tivoli in particular Network Team.
822	9.7.1	10.10.1	Event Logging	Access to Audit Logs shall be strictly controlled and shall be protected from deletion, disablement, modification or fabrication. Wherever possible, there shall be a segregation of duties between overall system security and Audit Logs security. Audit Logs shall be analysed and administered only by appropriately trained staff.	Access to Tivoli Audit logs is controlled by Role. Access to other management systems is also controlled by role. Security analysis of the logs does not take place.

FUJ00155413

823	9.7.1	10.10.1	Event Logging	The amount of data to be recorded should be configurable	This is done within Tivoli via Filters.
824	9.7.1	10.10.1	Event Logging	Record the User ID	This is done
825	9.7.1	10.10.1	Event Logging	Record the date and time of the event	This is done
826	9.7.1	10.10.1	Event Logging	Record the type of event	This is manipulated in Tivoli
827	9.7.1	10.10.1	Event Logging	Record the files accessed	This is not done due to the volume
828	9.7.1	10.10.1	Event Logging	Record the programs/utilities used	This is not done as no one has requested
829	9.7.1	10.10.1	Event Logging	Record the workstation ID	This is only done when access is through the SAS server
831	9.7.1	10.10.1	Event Logging	The events that need to be accounted for should be configurable and should include recording alerts of when Personal Data is accessed without consent	As the definition has been set in Horizon only recently and currently is obfuscated. This has not been viewed as required by Tivoli.
832	9.7.1	10.10.3	Event Logging	Account for all failed log-on attempts	This is done
833	9.7.1	10.10.3	Event Logging	Account for all privileged operations	This will be picked up by Tivoli if the SDU set the log to capture this information. Logs Managing Tivoli access do
834	9.7.1	10.10.3	Event Logging	Account for all log-ons	This will be picked up by Tivoli if the SDU set the log to capture this information. Believe yes in most cases
835	9.7.1	10.10.3	Event Logging	Account for all log-offs	This will be picked up by Tivoli if the SDU

WITHDRAWN

FUJ00155413

					the log to capture this information. Believe yes in most cases
836	9.7.1	10.10.3	Event Logging	Account for all workstation time outs	This will be picked up by Tivoli if the SDU set the log to capture this information. Only exception is local log on where the local log will store this and it will not be picked up by Tivoli.
837	9.7.1	10.10.3	Event Logging	Account for all updates to access rights	This depends on the Audit Policy set on the platform if the SDU has set this requirement then it will be and will be captured by Tivoli. Tivoli staff is not aware of any standard here.
838	9.7.1	10.10.3	Event Logging	Account for all updates to files	This is not done.
839	9.7.1	10.10.3	Event Logging	Account for every time application software is used	This is not done.
840	9.7.1	10.10.3	Event Logging	Account for every time a file is viewed	This is not done.
841	9.7.1	10.10.3	Event Logging	Account for every print-out	This is not done.
842	9.7.1	10.10.3	Event Logging	Monitor known covert channels	Tivoli staffs do not believe this is done within Tivoli, only where anything is recorded to the SAS server and in the Corporate VPN OOH solution. Further clarification is required from Marc Jarosz in Network Team

WITHDRAWN

FUJ00155413

WITHDRAWN

Event Logging Facilities/Utilities

857	9.7.1	10.10.3	Trusted Facilities Management	Accounting should be carried out by Trusted Facilities	No answer to this yet needs more investigation with SDU's
858	9.7.1	10.10.3	Trusted Facilities Management	Separate accounts for Management Functions	This does not occur within Tivoli unless the SDU has set the log to do so and the Tivoli staff do not think this has happened
859	9.7.1	10.10.3	Trusted Facilities Management	Accounts to be limited to privileged users	This occurs based on roles
860	9.7.1	10.10.3	Trusted Facilities Management	All operations to be accountable	The collection of events is made but accountability is never reviewed within Tivoli as comparisons to roles against actions are not made.
861	9.7.1	10.10.3	Trusted Facilities Management	Audit alarms to be generated	Alarms are raised for failed logons and bad passwords only.
862	9.7.1	10.10.3	Trusted Facilities Management	The raising of an audit alarm to be reported on specific workstations	This does not occur
863	9.7.1	10.10.3	Trusted Facilities Management	All attempts to delete, write or append the Accounting files to be accountable	This does not occur
1245	12.3.1	15.3.1	Auditing Tools	A range of facilities for analysing Accounting Logs should be provided	This does not occur
1246	12.3.1	15.3.1	Auditing Tools	Able to export Accounting Log information into Database and Spreadsheet formats	This does not occur

FUJ00155413

1247	12.3.1	15.3.1	Auditing Tools	Able to export Accounting Log information into Word-Processing formats	This does not occur
1248	12.3.1	15.3.1	Auditing Tools	Able to select particular type of event from the Accounting Log	This does not occur
1249	12.3.1	12.3.1	Auditing Tools	Able to select the actions of an individual including the identification of all Fujitsu Ltd customers whose records have been accessed or modified over a given period of time.	This does not occur
1250	12.3.1	15.3.1	Auditing Tools	Able to select the events that took place within a specific range of dates and times including the identification of all system users who have accessed or modified a given customer records over a given period of time.	This does not occur
1251	12.3.1	15.3.1	Auditing Tools	Able to select combinations of events	This can. be undertaken for availability issues by SMC, but they do not see successful events
1252	12.3.1	15.3.1	Auditing Tools	Able to sort the Accounting Log records	This does not occur
1253	12.3.1	15.3.1	Auditing Tools	Automatic report generation facilities	This does not occur
1254	12.3.1	15.3.1	Auditing Tools	Use of automated monitoring tools that raise alarms on recording suspicious events or suspicious trends in events	This does not occur
1255	12.3.1	[illegible]	Auditing Tools	Able to combine Accounting Log information with information received from other sources	This is only possible from the ARQ area

WITHDRAWN

FUJ00155413

864	9.7.1	10.10.3	Accounting Log Capacity	Accounting should be operational at all times	This does not occur within Tivoli unless the SDU has set the log to do so and the Tivoli staff do not think this has happened
865	9.7.1	10.10.3	Accounting Log Capacity	An alarm to be raised when the Accounting Log reaches **75%** of its maximum permitted size	This does not occur within Tivoli unless the SDU has set the log to do so. SDU's need to confirm if they have
867	9.7.1	10.10.3	Accounting Log Capacity	When the Accounting Log is full, switch to a secondary Accounting Log	This does not occur within Tivoli unless the SDU has set the log to do so. SDU's need to confirm if they have
872	9.7.3	10.10.2	Clock Synchronisation	System clocks should be synchronised	This is done via a network Time Server
873	9.7.3	10.10.2	Clock Synchronisation	Clocks to be synchronised with a common clock	This is done via a network Time Server
874	9.7.3	10.10.2	Clock Synchronisation	Clock synchronisation to be automated	This is done via a network Time Server
1274	12.3.2	15.3.2	Protection of Audit Trails	System audit tools (programs and log files) will only be available to authorised personnel and will be protected to prevent any possible misuse or compromise.	This is Role Based, but analysis of tools against roles needs reviewing in Horizon and definitive storage place for this information kept
1282	12.3.2	15.3.2	Protection of System Audit Tools	Release, use and return of system audit tools to be logged	This is not done.
1236	12.3.1	15.3.1	System Audit Controls	Audit requirements and activities should be planned to minimise the risk of disruption to the business	This is carried out for availability only
1237	12.3.1	15.3.1	System Audit Controls	Audit requirement to be agreed with system	Historically 10/11 years ago but System Owners are not clearly identified in the

WITHDRAWN

				owner	current Horizon solution.
1238	12.3.1	15.3.1	System Audit Controls	The scope of the checks to be agreed and controlled	Historically 10/11 years ago but System Owners are not clearly identified in the current Horizon solution.
1239	12.3.1	15.3.1	System Audit Controls	Checks to be limited to 'read-only' access to software and data	This applies to availability only as other checks are not carried out.
1240	12.3.1	15.3.1	System Audit Controls	Updating of information to be performed only on isolated copies of system files, which should be purged when the audit is complete	This is not done
1241	12.3.1	15.3.1	System Audit Controls	IT resources required to perform the checks to be explicitly identified	This is done through roles and needs to be reviewed.
1242	12.3.1	15.3.1	System Audit Controls	Requirements for special or additional processing to be identified and agreed	This is not done
1243	12.3.1	15.3.1	System Audit Controls	All access to be monitored and logged to provide a reference trail	This is not done within Tivoli, though other SDU tools may do this and not feed the information to Tivoli.
1244	12.3.1	15.3.1	System Audit Controls	All procedures, requirements and responsibilities to be documented	This is dependent where one sits in the RMGA account and it needs a Security Framework and policy to pull together.

WITHDRAWN

FUJ00155413

WITHDRAWN

Log Retention

1256	12.3.1	15.3.1	Retention of Accounting Log	The Accounting Log should be retained to enable investigations to be carried out when necessary	This can be done through Tivoli and SDU tools and backups to the Centera are made and tapes taken.
1257	12.3.1	15.3.1	Retention of Accounting Log	Accounting Logs from technology support systems (e.g. firewalls, IDS) to be kept for 6 months, 6 months off line then discard	This is currently the case for the old NNM and it is expected to be the case with the new syslog server
1258	12.3.1	15.3.1	Retention of Accounting Log	A copy of the Accounting Log to be kept on removable media	This occurs on the Centera
1259	12.3.1	15.3.1	Retention of Accounting Log	Physical access to copy of the Accounts Log to be restricted to people not granted system management privileges	This does occur
1260	12.3.1	15.3.1	Retention of Accounting Log	Accounting Log to be protected against corruption	This is dependent on the SDU unit, in all cases patching and vulnerability management is an issue.
1261	12.3.1	15.3.1	Retention of Accounting Log	Accounting Log to be securely disposed of, by logical erasure/physical destruction, when no longer required	This doe not occur except when platform is decommissioned and networks operations degauss the disk.
1262	12.3.1	15.3.1	Retention of Accounting Log	Use integrity checking countermeasures to ensure that the Log has been archived successfully	This does occur with archives to the Audit Server.
1263	12.3.1	15.3.1	Retention of Accounting Log	Accounting Log for infrastructure on which RMGA systems are run to be kept for 6	This is not done

FUJ00155413

				months on line, 30 months off-line archived	
1264	12.3.1	15.3.1	Retention of Accounting Log	At least once every 12 months check that the Accounting Log tapes can be read.	This is not done
1265	12.3.1	15.3.1	Retention of Accounting Log	Accounting Logs for the application to be kept for the life of the record to which they relate	This is not done
1266	12.3.1	15.3.1	Retention of Accounting Log	Replace Accounting Log tapes when they reach 75% of their normal life expectance	This is not done

WITHDRAWN

WITHDRAWN

Event Auditing/Reviewing Processes

843	9.7.1	10.10.3	Review Event Log	The types of events that need to be logged should be specified	This has not been defined recently but 10/11 years ago
844	9.7.1	10.10.3	Review Event Log	Review number of unsuccessful log-ons	This is not done
845	9.7.1	10.10.3	Review Event Log	Review allocation of accounts with privileged access capability	This is not done
846	9.7.1	10.10.3	Review Event Log	Review access failures	This is not done
847	9.7.1	10.10.3	Review Event Log	Review trends in numbers of successful log-ons	This is not done
848	9.7.1	10.10.3	Review Event Log	Review the number of occasions accounts are being used out of normal hours	This is not done
849	9.7.1	10.10.3	Review Event Log	Review trends in the usage of specific accounts	This is not done
850	9.7.1	10.10.3	Review Event Log	Review trends in the use of the system from remote workstations	This is not done
851	9.7.1	10.10.3	Review Event Log	Track selected transactions	This is not done
852	9.7.1	10.10.3	Review Event Log	Review trends in the reports that are being printed	This is not done
853	9.7.1	10.10.3	Review Event Log	Review trends in the changes in labels	This is not done

FUJ00155413

				associated with IT resources	
854	9.7.1	10.10.3	Review Event Log	The frequency with which the Account Log should be reviewed should be specified	this requires agreement with SDU's and a process
855	9.7.1	10.10.3	Review Event Log	Events Log to be reviewed at least once a week.	With the current toolsets and volume of data this is unachievable.

WITHDRAWN

FUJ00155413

3.4 Operational Security Framework implementation.

The first process that the Operational Security team undertake prior to running any reports is a check that all logs are present and available.

If these logs are unavailable then the Service Delivery Manager responsible for that SDU is informed and a Security incident is raised.

Dependent on the control requirements established in the Security Framework a series of tests are undertaken for each platform and log type to assess whether it passes or fails a particular control requirement on that individual log.

Each test is:

- Given a unique number,
- Given a description,
- Given a test definition,
- Given a successful test criteria
- Validated
- Result of Yes or No for a successful test

Dependent on the type of control for example test 1.1 could be a test for a successful logon and this would apply whether the source of the log was a Windows, UNIX, Application, Database or Network device.

WITHDRAWN

FUJ00155413

The results of each control requirement test are then recorded with the following details:

- The platform concerned including the owner
- The type of log analysed (see below for initial thoughts on types)
  - Windows Operating System (OS),
  - Unix (OS)
  - Router syslog
  - Switch syslog
  - Firewall syslog
  - SAP Log
  - Oracle/SQL database log
  - Anti Virus log
  - Active Directory Log
  - RSA Token Authentication Log
  - Radius Log
  - IDS/IPS log
  - DNS log
  - SSH Log
  - SAS Log
- The day and date of the log
- The number of the test
- Whether it passed or failed
- The day, date and time the log was analysed
- The reason for any failure (including no data available).

If a failure occurs the Service Delivery Manager for that SDU is informed as is the platform owner and a Security Incident is raised under SVM/SDM/PRO/0018 RMGA Customer Service Incident Management Process.

(D.N. The process to do this will need further investigation as some SDU teams do not have access to PEAK which would be the RMGA preferred option)

WITHDRAWN

FUJ00155413

3.5 Tests

Within Horizon currently no event testing is undertaken and therefore an initial baseline of test has been obtained from another Fujitsu account as a starting point for discussion with the relevant Service Delivery Managers, Operation Unit Managers and ISD SDU units and will be expanded once discussion this has taken place.

RMGA collection validation sample.xls

3.6 Reports

3.6.1 Summary Reports

The CISO and Operational Security Team agree regular delivery dates for agreed summary reports required for PO Ltd and those that are required for internal RMGA compliance management.

3.6.2 Compliance Report

Those required for compliance management are to be sent to Information Governance as Audit Records.

Initially the intention is to summarise the compliance test results to the number of pass or fails, collected based on the Horizon Security and Control Framework criterion and the ISO 27001 reference this will need to be agreed with Information Governance.

The Fujitsu Services guideline document shows that the recommended SIEM solution provides COTS off the shelf templates for the reports detailed below. RMGA CISO in conjunction with PO Ltd needs to decide which of these they will require, and Information Governance in conjunction with Operational Security also needs to agree which they want. I have deleted those certain I believe are not applicable to RMGA and have included the full set as an appendix, but this area is open to debate, by all interested parties. In addition I have included those platforms which will be introduced as part of the migration to HNG-X.

WITHDRAWN

WITHDRAWN

1 Compliance Reports - Basel II Yes as is ISO 17799/27001
enVision includes the following standard compliance reports for BASEL II.

1. Computer Account Logon Activity
ISO 17799/27001 Section A.9.5.2Lists all local and remote logon activity for all monitored Windows, HP-UX, AIX Unix, Sun Solaris and Red Hat Linux systems.

2. Computer Account Logon Activity - Windows Detail
ISO 17799/27001 Section A.9.5.2Lists all logon activity for all monitored Windows domains and systems. This report is specific to monitored Windows systems, but provides a greater level of detail than the Computer Account Logon Activity report.

3. Computer Account Status by Account - Windows
ISO 17799/27001 Section A.9.5.3Lists all logon activity for specific user accounts. The user accounts in question should be listed as run-time parameters

4. Control of Collected Evidence
ISO 17799/27001 Section A.12.1.7.1
Lists all changes and object level access events to all collected evidence. This report requires that all evidence be contained within directories included in the Rules for Evidence device group, and that object level auditing be enabled on these directories.

5. Control of Collected Evidence - Windows Detail
ISO 17799/27001 Section A.12.1.7.1
Lists all changes and object level access events to all collected evidence. This report requires that all evidence be contained within directories included in the Rules for Evidence device group, and that object level auditing be enabled on these directories. This report is specific to monitored Windows systems, but provides a greater level of detail than the standard Control of Collected Evidence report.

6. Control of Human Resources Data
ISO 17799/27001 Section A.12.1.

FUJ00155413

WITHDRAWN

Lists all changes and object level access events to the HR device group. This report requires that all software and Human Relation data be contained within directories included in the HR device group, and that object level auditing be enabled on these directories.

7. Control of Human Resources Data - Windows Detail
ISO 17799/27001 Section A.12.1.3

Lists all changes and object level access events to the HR device group. This report requires that all software and Human Relation data be contained within directories included in the HR device group, and that object level auditing be enabled on these directories. This report is specific to monitored Windows systems, but provides a greater level of detail than the standard Control of Human Resources Data report.

8. Control of Operational Software
ISO 17799/27001 Section A.10.4.1
Lists all changes and object level access events to the Operational Software device group. This report requires that all operational software be contained within the Operational Software device group, and that object level auditing be enabled on the directories containing the Operational Software and data.

9. Control of Operational Software - Windows Detail
ISO 17799/27001 Section A.10.4.1

Lists all changes and object level access events to the Operational Software device group. This report requires that all operational software be contained within the Operational Software device group, and that object level auditing be enabled on the directories containing the Operational Software and data. This report is specific to Windows devices but provides more detail than the standard Control of Operational Software report.

10. Control of System Audit Data
ISO 17799/27001 Section A.12.3.2

Lists all changes and object level access events to the software and data used to perform system audits. This report requires that the software, source data and result data be contained within a device group, and object level auditing be enabled on the containing directories.

11. Control of System Audit Data - Windows Detail
ISO 17799/27001 Section A.12.3.2

FUJ00155413

Lists all changes and object level access events to the software and data used to perform system audits. This report requires that the software, source data and result data be contained within a device group, and object level auditing be enabled on the containing directories. This report is specific to Windows devices but provides more detail that the standard Control of System Audit Data report.

12. Control of System Test Data
ISO 17799/27001 Section A.10.4.2

Lists all changes and object level access events to the systems and data used in the testing of Operational Software security. This report requires that all system test data be contained in the Operational Software device group, and object level auditing be enabled on the directories containing the system test software, source data and test results.

13. Control of System Test Data - Windows Detail
ISO 17799/27001 Section A.10.4.2

Lists all changes and object level access events to the systems and data used in the testing of Operational Software security. This report requires that all system test data be contained in the Operational Software device group, and object level auditing be enabled on the directories containing the system test software, source data and test results.

14. External Contractors Report
ISO 17799/27001 Section A.8.1.6

Lists all changes and object level access events to the External Contractor Access device group. This report requires that all computers, software, source data and result findings be contained within a device group, and object level auditing be enabled on the directories containing this data.

15. External Contractors Report - Windows Detail
ISO 17799/27001 Section A.8.1.6

Lists all changes and object level access events to the External Contractor Access device group. This report requires that all computers, software, source data and result findings be contained within a device group, and object level auditing be enabled on the directories containing this data.

16. Financial Data Access
ISO 17799/27001 Section A.12.4

WITHDRAWN

Lists all successful and failed access attempts for all financial data. This report requires that all financial data be contained within a device group, and object level auditing be enabled on the directories containing the financial data.

17. Financial Data Access - Windows Detail
ISO 17799/27001 Section A.12.1.4
Lists all successful and failed access attempts for all financial data. This report requires that all financial data be contained within a device group, and object level auditing be enabled on the directories containing the financial data.

18. Malicious Software Activity Report
ISO 17799/27001 Section A.8.1.2
Lists all malicious software activity for all monitored devices.

19. Operation Change Control Report
ISO 17799/27001 Section A.8.1.2
Lists all configuration and policy changes for the Financial Operational infrastructure.

20. Operation Change Control Report - Windows Detail
ISO 17799/27001 Section A.8.1.2
Lists all configuration and policy changes for the Financial Operational Infrastructure. This report is specific to Windows, but gives a greater level of detail than the standard Operation Change Control Report.

21. Password Changes and Expirations
ISO 17799/27001 Section A.9.2.3
Lists all manual and automatic password change and expiration events. This includes Windows, Sun Solaris, Red Hat Linux, HP-UX and AIX operating systems.

22. Source Code Access
ISO 17799/27001 sec. A.10.4.3

WITHDRAWN

Lists all changes and object level access events to the Source Code device group. This report requires that the source code for all custom software and commercial software customization be contained within a device group, and object level auditing be enabled on the directories containing the source code.

23. Source Code Access - Windows Detail
ISO 17799/27001 sec. A.10.4.3
Lists all changes and object level access events to theSource Code device group. This report requires that the source code for all custom software and commercial software customization be contained within a device group, and object level auditing be enabled on the directories containing the source code.

24. User Activity from External Domains - Windows
ISO 17799/27001 Section A.9.4.3
Lists all activities of non-domain authenticated users. All authenticated domains are identified in run time parameters, and multiple domains can be contained within single quotes and separated by commas.

Reports: 24

8 Compliance Reports - PCI Data Security Standard
enVision includes the following standard compliance reports for the Payment Card Industry (PCI) Data Security Standard.

1. Access to All Audit Trails
PCI Section 10.2.3.
Lists all successful logins to enVision.

2. Administrative Privilege Escalation - Unix & Linux
PCI Section 10.1
Lists all successful administrative privilege escalations on monitored Unix and Linux systems.

WITHDRAWN

FUJ00155413

3. All Actions by Individuals with Root or Administrative Privileges - Unix & Linux
PCI Section 10.2.2
Lists all actions taken by users logged in as root. Modify the report to include any additional user names that have been granted full administrative privileges in your environment.

4. All Actions by Individuals with Root or Administrative Privileges - Windows
PCI Section 10.2.2
Lists all actions taken by users logged in as administrator. Modify the report to include any additional user names that have been granted full administrative privileges in your environment.

5. Anti-Virus Update Procedures
PCI Section 5.2
Lists all update procedures for anti-virus systems.

6. Encrypted Transmission Failures
PCI Section 4.1
Lists all cryptographic operations where use of the cryptography failed or was disabled by the user.

7. Encryption Key Generation and Changes
PCI Section 3.6.1 and 3.6.4
Lists all the generation and period changing of encryption keys used in the secure storage and transfer of card data.

8. Firewall Configuration Changes
PCI Section 1.1.1, 1.1.8
Lists all configuration changes made to firewalls within the PCI device group.

9. Inbound Network Traffic on non-standard ports - Detail
PCI Section 1.3.1, 1.3.2

WITHDRAWN

FUJ00155413

Lists all inbound internet traffic not on ports 80, 22, 443, and 1723.

10. Inbound Network Traffic on non-standard ports - Summary
PCI Section 1.3.1, 1.3.2
Lists all inbound internet traffic not on ports 80, 22, 443, and 1723, summarized by the destination IP address.

11. Individual User Accesses to Cardholder Data - Windows
PCI Section 10.2.1
Lists all successful file access attempts to file objects in the Cardholder Data device group.

12. Initialization of Audit Logs
PCI Section 10.2.6
Lists all access attempts that have been denied due to access control list restrictions.

13. Invalid Logical Access Attempts - ACL Denied Summary
PCI Section 10.2.4
Lists the initialization of audit logs in Windows, Unix, Linux, AIX and HPUX operating systems.

14. Outbound Network Traffic - Detail
PCI Section 1.3.6
Lists all outbound traffic for a specific internal IP address. You must enter the IP address as a run-time parameter.

15. Outbound Network Traffic - Summary
PCI Section 1.3.6
Lists a summary of all outbound traffic by destination.

16. Router Configuration Changes
PCI Section 1.1.9

WITHDRAWN

FUJ00155413

Lists all configuration changes made to routers within the PCI device group.

17. Traffic to Non-Standard Ports - Detail
PCI Section 1.1.6
Lists all firewall traffic on ports other than 80, 22, 443 and 1723 to the IP address specified as a run time parameter. This report can be modified to include the ports not directly justified by PCI.

18. Traffic to Non-Standard Ports - Summary
PCI Section 1.1.6
Summarizes all firewall traffic not on ports 80, 22, 443 and 1723 to the destination computer where the port used is not directly justified by PCI.
Compliance - PCI Data Security Standard

Reports: 18

12 Standard Reports - Alerts
Reports module includes the following standard system reports for alerts.

1. Alert Notes by Date and Time
Lists all alert notes in the database sorted by the time they occurred.

2. Alert Notes by View
Lists all alert notes for a specific view. (The user must modify the report query to specify the view.)

3. Alerts per Hour
Displays the distribution of all alerts over time, in 1 hour intervals.

4. Alerts Status Summary
Lists a count of alerts within a time range, sorted by status: new alert, under investigation, resolved.

WITHDRAWN

FUJ00155413

WITHDRAWN

5. Alerts Under Investigation by Date/Time
Lists all alerts under investigation in the database. Sorted by the time the alerts occurred. Use this report to track alerts under investigation.

6. Alerts Under Investigation by View
Lists all alerts under investigation in the database for a specific view.
You must modify this report prior to running it. (On the Create/Modify Report - Specify Report Selection Criteria window, replace the text type viewname here with the name of the view.)

7. Available Alerts by Date/Time
Lists all alerts and the status of each alert in the database. Sorted by the time the alerts occurred.

8. New Alerts by Date/Time
Lists all new alerts in the database. Sorted by the time the alerts occurred.

9. New Alerts by View
Lists all new alerts in the database for a specific view.
You must modify this report prior to running it. (On the Create/Modify Report - Specify Report Selection Criteria window, replace the text type viewname here with the name of the view.)

10. Percentages of Alerts by NIC Category
Displays the distribution of alerts by NIC category.

11. Percentages of Alerts by Alert Levels
Displays the distribution of alerts by alert levels.

12. Percentages of Alerts by Severity Levels
Displays the distribution of alerts by severity levels.

FUJ00155413

WITHDRAWN

13. Resolved Alerts by Date/Time
Lists all resolved alerts in the database. Sorted by the time the alerts occurred. Use this report to identify the alerts that have been resolved.

14. Resolved Alerts by View
Lists all resolved alerts in the database for a specific view.

15. Top 20 Alert Categories
Displays the top alert categories by number of alerts.

Reports: 15

13 Standard Reports - Apache HTTP Server
Reports module includes the following standard reports for the Apache HTTP Server.

1. Top 20 Client IP Addresses by Connection Requests
Displays the top 20 client IP addresses that had the most successful web site connections.

2. Total Bytes by Apache Device Address
Displays total bytes passed by Apache device address.

3. Total Bytes by Client IP Address
Displays total bytes passed by client address.

Reports: 3

16 Standard Reports - Firewall Device Categories
Reports module includes the following standard reports for reporting on firewalls by categories.

1. Firewalls - Top Events by Category
Displays the top events by category from all firewall devices.

2. Top 20 Firewall Categories
Displays the top 20 firewall categories that generate the highest number of events from all firewall devices.

Reports: 2

17 Standard Reports - IDS Device Categories
Reports module includes the following standard reports for reporting on IDS devices by categories.

1. IDS Top Alarms by Category
Displays the top signatures by categories from all IDS devices.

2. Top 20 IDS Categories
Displays the top 20 IDS categories that generate the highest number of events from all IDS devices.

Reports: 2

18 Standard Reports - Statistics
Reports module includes the following standard reports for statistics.
Important! To gather the data for these reports, you must start the Alerter Service.

1. Daily Event Counts
Displays the total event counts by day.

WITHDRAWN

FUJ00155413

WITHDRAWN

2. Hourly Event Counts
Displays the total event counts by hour.

3. Percentage of Events by Device Class
Displays the percentage of the total number of events by device class.

4. Percentage of Events by Device Type
Displays the percentage of total number of events by device type.

5. Percentage of Events by NIC Category
Displays the percentage of the total number of events by NIC Category.

6. Syslog Collection Statistics
Summarizes syslog message quantity and byte count on an hourly basis by logging device. Assesses log host system and disk space requirements. Use this report to identify the periods of highest activity.

7. Top 20 Devices
Displays the top 20 devices generating events during the selected time period.

8. Top 20 Devices Generating Unknown Events
Displays the top 20 devices generating unknown events during the selected time period.

9. Top 20 Device Types Generating Unknown Events
Displays the top 20 device types generating unknown events during the selected time period.

10. Top 20 Event Categories
Displays the top 20 event categories during the selected time period.

FUJ00155413

WITHDRAWN

11. Top 20 Events
Displays the top 20 event IDs collected during the selected time period.

Reports: 11

23 Standard Reports - Cisco Access Control Server
Reports module includes the following standard reports for the Cisco Access Control Server device.

1. ACS Backup And Restore
Displays all backup and restore operations. Sorted by descendingtime.

2. ACS Service Monitoring
Tracks messages and activities internal to Cisco ACS.

3. Administration Audit
Displays an Administrative Report of all activity carried out via the Cisco Secure ACS HTML Management Interface. Sorted by descendingtime.

4. Database Replication
Tracks ACS database replication activity. Sorted by descending time.

5. Failed Authentications
Displays a list of all failed login attempts. Sorted in descending order by descending time.

6. Failed Authentications Count
Displays a count of all failed login attempts. Sorted by descendingtime.

7. Passed Authentications

Displays a list of all users that have successfully logged in. Sorted by descending time.

8. Passed Authentications Count
Displays a count of all users that have successfully logged in. Sorted by descendingtime.

9. TACACS+ Accounting
Tracks all login and log out traffic.

10. TACACS+ Administration - Permanent Configuration Changes
Tracks configuration changes that have been executed using the write memory (write mem), or copy running start (copy run) commands.

11. Top 10 Users
Counts the number of successful logins (successful authentications) and sequentially orders them by username.

12. Top 10 Users by Duration
Calculates the total amount of time that users have spent logged in to network devices and lists them in descending order by time.

Reports: 12
25 Standard Reports - Cisco ASA (Firewall)
Reports module includes the following standard reports for the Cisco ASA (firewall) device.

1. AAA User Authentications
Displays AAA user authentications through Cisco ASA firewalls, sorted by date/time sequence. This report requires AAA user authentication.

2. Bandwidth Usage by Address
Summarizes bandwidth usage by ipal address for all traffic passing through Cisco ASA firewalls. Sorted by total byte usage. Quickly determines "Top Talkers" on your company's network. Only ASA firewalls with debug level logging on are reported.

WITHDRAWN

FUJ00155413

WITHDRAWN

3. Bandwidth Usage by Department

Displays bandwidth usage by department through ASA firewalls. It is used to determine quickly which departments are your bandwidth hogs.

4. Bandwidth Usage by Port

Summarizes bandwidth usage by port for traffic passing through Cisco ASA firewalls. Sorted by total bytes usage count. Quickly determines which applications are consuming the most bandwidth. Other common TCP/IP words used synonymously with applications are port and services. Only ASA firewalls with debug level logging on are reported.

5. Bandwidth Usage per Hour

Displays bandwidth usage per hour through ASA firewalls. It is used to spot quickly bandwidth usage trends occurring during specific time periods. Each tick mark on vertical hourly axes represents accumulated usage for the previous hour.

6. Bandwidth Utilization

This combination of a graph and a report displays the bandwidth utilization on the network.

7. Blocked URL Events

Displays the blocked URL events of internal IP addresses attempting to connect to external web sites that have been restricted by the company sorted by Date/Time. Websense Enterprise software must be installed to activate the URL blocking capability.

8. Configuration Changes

Listing of configuration change messages from Cisco ASA firewalls, sorted by date/time sequence. Monitors when configuration changes were made to Cisco ASA Firewalls. Only ASA firewalls with logging on are reported.

9. Connection Limit Exceeded

Details exceeded connection limits by static addresses.

10. CPU Over-Capacity Events by Date and Time

WITHDRAWN

Listing of all instances of ASA Firewall CPU utilizations rising above 100%. This is generally considered to be a [illegible] condition and if it happens frequently it may be necessary to contact Cisco Systems.

11. Denied Connections per Hour

Displays the number of denied connections per hour through ASA firewalls. It is used to spot quickly security threat trends occurring during specific time periods. Each tick mark on vertical hourly axes represents accumulated denied connections for the previous hour.

12. Denied Inbound IP Spoofing

report tracks when a ASA Firewall receives a external packet with the IP source address equal to the IP destination and the destination port equal to the source port sorted by the destination address. This indicates a spoofed packet designed to attack systems. This attack is referred to as a Land Attack.

13. Denied Inbound Traffic by Address

Summarizes denied inbound traffic filtered through Cisco ASA firewalls by foreign address. Sorted by connection count. Quickly determines which foreign hosts are being denied access to your company's internal network; denied connections could represent an attempted security policy breach, malicious network reconnaissance, or simply point out a host or network device configuration issue. Only ASA firewalls with logging on are reported.

14. Denied Inbound Traffic by Port

Summarizes denied inbound traffic filtered through Cisco ASA firewalls by port. Sorted by connection count. Port is used synonymously with services and/or applications. Quickly determines which applications are being denied access; denied connections could represent an attempted security policy breach, malicious network reconnaissance like a port scan, or simply point out a host or network device configuration issue. Only ASA firewalls with logging on are reported.

15. Denied Outbound Traffic by Address

Summarizes denied outbound traffic filtered through Cisco ASA firewalls by local address. Sorted by connection count. Quickly determines which local addresses are possibly attempting to bypass your company's security policy. Only ASA firewalls with logging on are reported.

16. Denied Outbound Traffic by Port

FUJ00155413

Summarizes denied outbound traffic filtered through Cisco ASA firewalls by port. Sorted by connection count. Port numbers are used to represent services or applications. Quickly determines which outbound applications are being denied; these denied messages could very well represent an attempted security policy breach, malicious network reconnaissance like a port scan, or simply point out a host or network device configuration issue. Only ASA firewalls with logging on are reported.

17. Email Security

Listing of ASA MailGuard messages received from Cisco ASA firewalls. Sorted in date/time sequence. Quickly views possible email security breach attempts that were prevented by ASA firewalls. Only ASA firewalls with logging on are reported.

18. Failover Messages

Displays a list of failover messages from Cisco ASA firewalls by date/time.

19. FTP Requests by Date/ Time

Displays a list of FTP requests through Cisco ASA Firewalls by Date/Time.

20. FTP Requests by Department

Displays FTP requests for each department through Cisco ASA firewalls by number of requests.

21. FTP Requests by Foreign Address

Displays FTP requests to foreign sites by local users through Cisco ASA firewalls by foreign address and the number of requests.

22. FTP Requests by Local Address

Displays FTP requests by each local address through Cisco ASA firewalls by local address and number of requests.

23. Inbound E-mail Recipients

Displays inbound emails and the intended recipients.

24. Inbound E-mail Senders

WITHDRAWN

FUJ00155413

Displays inbound emails and the senders.

25. Inbound Email Traffic

Displays bandwidth usage of inbound email traffic through Cisco ASA firewalls. Sorted by total connection count. Quickly determines 'Top Foreign Email Senders' if your email servers are located on an internal or DMZ interface. Summarizes email traffic from your own email gateways if they are sitting on an external ASA interface. Only ASA firewalls with logging on are reported. The system calculates inbound email traffic by summarizing all the 302002 traffic logged on local port 25.

26. Inbound FTP Traffic

Displays bandwidth usage of inbound FTP traffic through Cisco ASA firewalls. Sorted by total connection count. Quickly determines which external users use FTP most frequently in your company. Only ASA firewalls with logging on are reported. The system calculates inbound FTP traffic by summarizing all the 302002 traffic logged on local ports 20 and 21.

27. Inbound HTTP Traffic

Displays bandwidth usage of inbound HTTP traffic through Cisco ASA firewalls. Sorted by total connection count. Quickly assesses which foreign users are accessing your internal web servers most frequently. Only ASA firewalls with logging on are reported. The system calculates inbound http traffic by summarizing all the 302002 traffic logged on local port 80.

28. Inbound IP Fragmentation Alert

The ASA Firewall limits the number of IP fragments that can be concurrently reassembled. This restriction prevents memory depletion at the firewall under abnormal network conditions. The report is sorted by count by foreign address. If this message persists, a DoS (denial of service) attack might be in progress.

29. Inbound Telnet Traffic

Displays bandwidth usage of inbound Telnet traffic through Cisco ASA firewalls. Sorted by total connection count. Quickly determines top external Telnet users. Only ASA firewalls with logging on are reported. The system calculates inbound Telnet traffic by summarizing all the 302002 traffic logged on local port 23.

WITHDRAWN

FUJ00155413

WITHDRAWN

30. Management Access from External Source
Details all of the device management events on the ASA firewall sorted by Date/Time.

31. Outbound E-mail Recipients
Displays outbound emails and the email's intended recipient(s).

32. Outbound E-mail Senders
Displays outbound emails and the email's sender.

33. Outbound Email Traffic

Summarizes bandwidth usage of outbound email traffic through Cisco ASA firewalls. Sorted by total connection count. Quickly determines 'Top Email Talkers' in your company if your email gateway is located on an external or DMZ interface. Reflects "Top Email Gateways" if your mail gateways are on the ASA's internal interface network. Only ASA firewalls with logging on are reported. The system calculates outbound email traffic by summarizing all the 302002 traffic logged on foreign port 25.

34. Outbound FTP Traffic

Summarizes bandwidth usage of outbound FTP traffic through Cisco ASA firewalls. Sorted by total connection count. Quickly determines which internal users use FTP most frequently in your company. Only ASA firewalls with logging on are reported. The system calculates outbound FTP traffic by summarizing all the 302002 traffic logged on foreign ports 20 and 21.

35. Outbound HTTP Traffic

Summarizes bandwidth usage of outbound HTTP traffic through Cisco ASA firewalls. Sorted by total connection count. Quickly determines 'Top HTTP Talkers' in your company. Only ASA firewalls with logging on are reported. The system calculates outbound http traffic by summarizing all the 302002 traffic logged on foreign port 80.

36. Outbound IP Fragmentation Report

The ASA Firewall limits the number of fragments that can be concurrently reassembled. This restriction prevents memory depletion at the firewall under abnormal network conditions. This report is sorted by count by local address.

WITHDRAWN

37. Outbound Telnet Traffic

Summarizes bandwidth usage of outbound Telnet traffic through Cisco ASA firewalls. Sorted by total connection count. Quickly determines top local Telnet users. Only ASA firewalls with logging on are reported. The system calculates outbound Telnet traffic by summarizing all the 302002 traffic logged on foreign port 23.

38. Permitted Connections per Hour

Displays the number of connections per hour through ASA firewalls. It is used to spot connection trends occurring during specific time periods. Each tick mark on vertical hourly axes represents accumulated permitted connections for the previous hour.

39. RIP External Security Alert

Displays the ASA Firewall events for received internal RIP reply messages with bad authentication sorted by the local address. This could be due to misconfiguration on the router or the ASA Firewall or it could be a unsuccessful attempt to attack the ASA Firewall unit's routing table.

40. RIP Internal Security Alert

Displays he ASA Firewall events for received external RIP reply messages with bad authentication sorted by foreign address. This could be due to misconfiguration on the router or the ASA Firewall or it could be a unsuccessful attempt to attack the ASA Firewall unit's routing table.

41. SiteTrack Detection

Listing of network traffic through Cisco ASA firewalls that contained SiteTrack keywords. Sorted in date/time sequence. Keyword match is identified with parenthesis characters ( ) preceding the message in the Message column. The SiteTrack feature performs a text string comparison of the DNS host name lookup of source and destination IP addresses, as well as accessed URL pages and FTP file names. The DNS Resolver service must be on, and ASA firewall logging must be on.

42. Top 10 Requested URL/FTP Destinations

Displays the top 10 requested URL and FTP destinations by internal users through ASA firewalls. It is used to spot quickly trends of the most popular foreign sites.

FUJ00155413

WITHDRAWN

43. Top 20 Bandwidth Ports
Displays the top 20 ports of bandwidth usage through ASA firewalls. It is used to identify quickly which applications are consuming the most bandwidth.

44. Top 20 Bandwidth Users
Displays the top 20 bandwidth users through ASA firewalls.

45. Top 20 Connections by Address
Displays the top 20 users of connections through ASA firewalls. It is used to determine quickly which users are consuming the most connections.

46. Top 20 Connections by Port
Displays the top 20 ports with the most connections through ASA firewalls. It is used to identify quickly which applications are consuming the most connections.

47. Top 20 Denied Inbound by Address
Displays the top 20 foreign addresses that were denied inbound access by ASA firewalls. It is used to spot quickly foreign hosts that may have been attempting to gain unauthorized access to your network.

48. Top 20 Denied Inbound by Port
Displays the top 20 ports with the most denied inbound connections through ASA firewalls. It is used to identify quickly which applications are the top sources of inbound denied connections.

49. Top 20 Denied Outbound by Address
Displays the top 20 local addresses that were denied outbound access by ASA firewalls. It is used to identify quickly the top internal hosts that may possibly have been attempting to breach your company's outbound internet security policy.

50. Top FTP Destinations
Displays FTP requests to foreign addresses through Cisco ASA firewalls, it is sorted by the number of requests.

FUJ00155413

WITHDRAWN

51. Top URL Destinations
Displays URL requests to foreign addresses through Cisco ASA firewalls, it is sorted by the number of requests.

52. Total Connections by Global / Translated Address
Displays the activity for each global address going through the ASA firewall sorted by Percentage of total connections within a specific time period

53. Translation Activity by Connection ID
Lists build-up and teardown messages for connections through a ASA. These events are sorted using the Connection ID field.

54. URL Requests by Date/Time
Listing of URL and FTP requests through Cisco ASA Firewalls. Sorted in Date/Time sequence. (Only ASA firewalls with logging on are reported.)

55. URL Requests by Department
Summarizes the outbound URL and FTP requests for each department through Cisco ASA firewalls. Sorted by number of requests. Quickly determines which departments are downloading the most URLs and FTP files. Only ASA firewalls with logging on are reported.

56. URL Requests by Foreign Address
Summarizes outbound URL and FTP requests to foreign addresses through Cisco ASA firewalls. Sorted by total connections. It can determine quickly the most common URL and FTP destinations in your company. Only ASA firewalls with logging on are reported.

57. URL Requests by Local Address
Summarizes the outbound URL and FTP requests by each local address through Cisco ASA firewalls. Sorted by local address and number of URL/FTP requests. Quickly determines the most common URL and FTP destinations by local address for your company. Only ASA firewalls with logging on are reported.

58. URL Requests by User Name

FUJ00155413

Summarizes the outbound URL and FTP requests by authenticated user name through Cisco ASA firewalls. Lists the user name and the number of URL/FTP requests. Requires that AAA user authentication be configured on the firewall. Quickly determines the most common URL and FTP destinations on a user name basis for your company. Only ASA firewalls with logging on are reported.

Reports: 58

28 Standard Reports - Cisco Content Services Switch
Reports module includes the following standard reports for the Cisco Content Services Switch device.

1. Down Links
Displays all messages associated with a down link in a given time period.

2. Reboots
Displays all messages associated with device reboots in a given time period.

3. Top 50 Users by Number of Connections
Displays the total number of connections to the Content Switch grouped by the associated username.

4. Total Attacks by Attack Type
Displays the total number of attacks recognized by the device grouped by the attack type.

5. Total Attacks by Destination Address
Displays the total number of attacks recognized by the device grouped by the destination address.

6. Total Attacks by Destination Port
Displays the total number of attacks recognized by the device grouped by the destination port.

7. Total Attacks by Source Address

WITHDRAWN

FUJ00155413

Displays the total number of attacks recognized by the device grouped by the source address.

8. Total Logins by Source Address
Displays the total number of successful logins by source address.

Reports: 8

30 Standard Reports - Cisco PIX - Firewall
Reports module includes the following standard reports for the Cisco PIX (firewall) device.

1. AAA User Authentications
Displays AAA user authentications through Cisco PIX firewalls, sorted by date/time sequence. This report requires AAA user authentication.

2. Bandwidth Usage by Address
Summarizes bandwidth usage by local address for all traffic passing through Cisco PIX firewalls. Sorted by total byte usage. Quickly determines "Top Talkers" on your company's network. Only PIX firewalls with debug level logging on are reported.

3. Bandwidth Usage by Department
Displays bandwidth usage by department through PIX firewalls. It is used to determine quickly which departments are your bandwidth hogs.

4. Bandwidth Usage by Port
Summarizes bandwidth usage by port for traffic passing through Cisco PIX firewalls. Sorted by total byte usage count. Quickly determines which applications are consuming the most bandwidth. Other common TCP/IP words used synonymously with applications are port and services. Only PIX firewalls with debug level logging on are reported.

5. Bandwidth Usage per Hour
Displays bandwidth usage per hour through PIX firewalls. It is used to spot quickly bandwidth usage trends occurring during specific time periods. Each tick mark on vertical hourly axes represents accumulated usage for the previous hour.

WITHDRAWN

FUJ00155413

WITHDRAWN

6. Bandwidth Utilization
This combination of a graph and a report displays the bandwidth utilization on the network.

7. Blocked URL Events
Displays the blocked URL events of internal IP addresses attempting to connect to external web sites that have been restricted by the company sorted by Date/Time. Websense Enterprise software must be installed to activate the URL blocking capability.

8. Configuration Changes
Listing of configuration change messages from Cisco PIX firewalls, sorted by date/time sequence. Monitors when configuration changes were made to Cisco PIX Firewalls. Only PIX firewalls with logging on are reported.

9. Connection Limit Exceeded
Details exceeded connection limits by static addresses.

10. CPU Over-Capacity Events by Date and Time
Listing of all instances of PIX Firewall CPU utilizations rising above 100%. This is generally considered to be an error condition and if it happens frequently it may be necessary to contact Cisco Systems.

11. Denied Connections per Hour
Displays the number of denied connections per hour through PIX firewalls. It is used to spot quickly security threat trends occurring during specific time periods. Each tick mark on vertical hourly axes represents accumulated denied connections for the previous hour.

12. Denied Inbound IP Spoofing
report tracks when a PIX Firewall receives a external packet with the IP source address equal to the IP destination and the destination port equal to the source port sorted by the destination address. This indicates a spoofed packet designed to attack systems. This attack is referred to as a Land Attack.

FUJ00155413

WITHDRAWN

13. Denied Inbound Traffic by Address

Summarizes denied inbound traffic filtered through Cisco PIX firewalls by foreign address. Sorted by connection count. Quickly determines which foreign hosts are being denied access to your company's internal network; denied connections could represent an attempted security policy breach, malicious network reconnaissance, or simply point out a host or network device configuration issue. Only PIX firewalls with logging on are reported.

14. Denied Inbound Traffic by Port

Summarizes denied inbound traffic filtered through Cisco PIX firewalls by port. Sorted by connection count. Port is used synonymously with services and/or applications. Quickly determines which applications are being denied access; denied connections could represent an attempted security policy breach, malicious network reconnaissance like a port scan, or simply point out a host or network device configuration issue. Only PIX firewalls with logging on are reported.

15. Denied Outbound Traffic by Address

Summarizes denied outbound traffic filtered through Cisco PIX firewalls by local address. Sorted by connection count. Quickly determines which local addresses are possibly attempting to bypass your company's security policy. Only PIX firewalls with logging on are reported.

16. Denied Outbound Traffic by Port

Summarizes denied outbound traffic filtered through Cisco PIX firewalls by port. Sorted by connection count. Port numbers are used to represent services or applications. Quickly determines which outbound applications are being denied; these denied messages could very well represent an attempted security policy breach, malicious network reconnaissance like a port scan, or simply point out a host or network device configuration issue. Only PIX firewalls with logging on are reported.

17. Email Security

Listing of PIX MailGuard messages received from Cisco PIX firewalls. Sorted in date/time sequence. Quickly views possible email security breach attempts that were prevented by PIX firewalls. Only PIX firewalls with logging on are reported.

18. Failover Messages

Displays a list of failover messages from Cisco PIX firewalls by date/time.

FUJ00155413

WITHDRAWN

19. FTP Requests by Date/ Time
Displays a list of FTP requests through Cisco PIX Firewalls by Date/Time.

20. FTP Requests by Department
Displays FTP requests for each department through Cisco PIX firewalls by number of requests.

21. FTP Requests by Foreign Address
Displays FTP requests to foreign sites by local users through Cisco PIX firewalls by foreign address and the number of requests.

22. FTP Requests by Local Address
Displays FTP requests by each local address through Cisco PIX firewalls by local address and number of requests.

23. Inbound E-mail Recipients
Displays inbound emails and the intended recipients.

24. Inbound E-mail Senders
Displays inbound emails and the senders.

25. Inbound Email Traffic

Displays bandwidth usage of inbound email traffic through Cisco PIX firewalls. Sorted by total connection count. Quickly determines 'Top Foreign Email Senders' if your email servers are located on an internal DMZ interface. Summarizes email traffic from your own email gateways if they are sitting on an external PIX interface. Only PIX firewalls with logging on are reported. The system calculates inbound email traffic by summarizing all the 302002 traffic logged on local port 25.

26. Inbound FTP Traffic

Displays bandwidth usage of inbound FTP traffic through Cisco PIX firewalls. Sorted by total connection count. Quickly determines which external users use FTP most frequently in your company. Only PIX firewalls with logging on are reported. The system calculates inbound FTP traffic by summarizing all the 302002 traffic logged on local ports 20 and 21.

FUJ00155413

WITHDRAWN

27. Inbound HTTP Traffic

Displays bandwidth usage of inbound HTTP traffic through Cisco PIX firewalls. Sorted by total connection count. Quickly assesses which foreign users are accessing your internal web servers most frequently. Only PIX firewalls with logging on are reported. The system calculates inbound http traffic by summarizing all the 302002 traffic logged on local port 80.

28. Inbound IP Fragmentation Alert

The PIX Firewall limits the number of IP fragments that can be concurrently reassembled. This restriction prevents memory depletion at the firewall under abnormal network conditions. The report is sorted by count by foreign address. If this message persists, a DoS (denial of service) attack might be in progress.

29. Inbound Telnet Traffic

Displays bandwidth usage of inbound Telnet traffic through Cisco PIX firewalls. Sorted by total connection count. Quickly determines top external Telnet users. Only PIX firewalls with logging on are reported. The system calculates inbound Telnet traffic by summarizing all the 302002 traffic logged on local port 23.

30. Management Access from External Source

Details all of the device management events on the PIX firewall sorted by Date/Time.

31. Outbound E-mail Recipients

Displays outbound emails and the email's intended recipient(s).

32. Outbound E-mail Senders

Displays outbound emails and the email's sender.

33. Outbound Email Traffic

FUJ00155413

Summarizes bandwidth usage of outbound email traffic through Cisco PIX firewalls. Sorted by total connection count. Quickly determines 'Top Email Talkers' in your company if your email gateway is located on an external or DMZ interface. Reflects "Top Email Gateways" if your mail gateways are on the PIXs internal interface network. Only PIX firewalls with logging on are reported. The system calculates outbound email traffic by summarizing all the 302002 traffic logged on foreign port 25.

34. Outbound FTP Traffic

Summarizes bandwidth usage of outbound FTP traffic through Cisco PIX firewalls. Sorted by total connection count. Quickly determines which internal users use FTP most frequently in your company. Only PIX firewalls with logging on are reported. The system calculates outbound FTP traffic by summarizing all the 302002 traffic logged on foreign ports 20 and 21.

35. Outbound HTTP Traffic

Summarizes bandwidth usage of outbound HTTP traffic through Cisco PIX firewalls. Sorted by total connection count. Quickly determines 'Top HTTP Talkers' in your company. Only PIX firewalls with logging on are reported. The system calculates outbound http traffic by summarizing all the 302002 traffic logged on foreign port 80.

36. Outbound IP Fragmentation Alert

The PIX Firewall limits the number of IP fragments that can be concurrently reassembled. This restriction prevents memory depletion at the firewall under abnormal network conditions. This report is sorted by count by local address.

37. Outbound Telnet Traffic

Summarizes bandwidth usage of outbound Telnet traffic through Cisco PIX firewalls. Sorted by total connection count. Quickly determines top local Telnet users. Only PIX firewalls with logging on are reported. The system calculates outbound Telnet traffic by summarizing all the 302002 traffic logged on foreign port 23.

38. Permitted Connections per Hour

Displays the number of connections per hour through PIX firewalls. It is used to spot connection trends occurring during specific time periods. Each tick mark on vertical hourly axis represents accumulated permitted connections for the previous hour.

WITHDRAWN

FUJ00155413

WITHDRAWN

39. RIP External Security Alert

Displays the PIX Firewall events for received internal RIP reply messages with bad authentication sorted by the local address. This could be due to misconfiguration on the router or the PIX Firewall or it could be a unsuccessful attempt to attack the PIX Firewall unit's routing table.

40. RIP Internal Security Alert

Displays he PIX Firewall events for received external RIP reply messages with bad authentication sorted by foreign address. This could be due to misconfiguration on the router or the PIX Firewall or it could be a unsuccessful attempt to attack the PIX Firewall unit's routing table.

41. SiteTrack Detection

Listing of network traffic through Cisco PIX firewalls that contained SiteTrack keywords. Sorted in date/time sequence. Keyword match is identified with parenthesis characters ( ) preceding the message in the Message column. The SiteTrack feature performs a text string comparison of the DNS host name lookup of source and destination IP addresses, as well as accessed URL pages and FTP file names. The DNS Resolver service must be on, and PIX firewall logging must be on.

42. Top 10 Requested URL/FTP Destinations

Displays the top 10 requested URL and FTP destinations by internal users through PIX firewalls. It is used to spot quickly trends of the most popular foreign sites.

43. Top 20 Bandwidth Ports

Displays the top 20 ports of bandwidth usage through PIX firewalls. It is used to identify quickly which applications are consuming the most bandwidth.

44. Top 20 Bandwidth Users

Displays the top 20 bandwidth users through PIX firewalls.

45. Top 20 Connections by Address

Displays the top 20 users of connections through PIX firewalls. It is used to determine quickly which users are consuming the most connections.

46. Top 20 Connections by Port

Displays the top 20 ports with the most connections through PIX firewalls. It is used to identify quickly which applications are consuming the most connections.

47. Top 20 Denied Inbound by Address
Displays the top 20 foreign addresses that were denied inbound access by PIX firewalls. It is used to spot quickly foreign hosts that may have been attempting to gain unauthorized access to your network.

48. Top 20 Denied Inbound by Port
Displays the top 20 ports with the most denied inbound connections through PIX firewalls. It is used to identify quickly which applications are the top sources of inbound denied connections.

49. Top 20 Denied Outbound by Address
Displays the top 20 local addresses that were denied outbound access by PIX firewalls. It is used to identify quickly the top internal hosts that may possibly have been attempting to breach your company's outbound internal security policy.

50. Top FTP Destinations
Displays FTP requests to foreign addresses through Cisco PIX firewalls, it is sorted by the number of requests.

51. Top URL Destinations
Displays URL requests to foreign addresses through Cisco PIX firewalls, it is sorted by the number of requests.

52. Total Connections by Global / Translated Address
Displays the activity for each global address going through the PIX firewall sorted by Percentage of total connections within a specific time period

53. Translation Activity by Connection ID
Lists the build-uUp and teardown messages for connections through a PIX. These events are sorted using the Connection ID field.

54. URL Requests by Date/Time

WITHDRAWN

Listing of URL and FTP requests through Cisco PIX Firewalls. Sorted in Date/Time sequence. This and the URL/FTP query report can be used to view which URLs and FTP files were accessed during a certain date/time range. Only PIX firewalls with logging on are reported.

55. URL Requests by Department

Summarizes the outbound URL and FTP requests for each department through Cisco PIX firewalls. Sorted by number of requests. Quickly determines which departments are downloading the most URLs and FTP files. Only PIX firewalls with logging on are reported.

56. URL Requests by Foreign Address

Summarizes outbound URL and FTP requests to foreign addresses through Cisco PIX firewalls. Sorted by total connections. It can determine quickly the most common URL and FTP destinations in your company. Only PIX firewalls with logging on are reported.

57. URL Requests by Local Address

Summarizes the outbound URL and FTP requests by each local address through Cisco PIX firewalls. Sorted by local address and number of URL/FTP requests. Quickly determines the most common URL and FTP destinations by local address for your company. Only PIX firewalls with logging on are reported.

58. URL Requests by User Name

Summarizes the outbound URL and FTP requests by authenticated username through Cisco PIX firewalls. Sorted by user name and the number of URL/FTP requests. Requires that AAA user authentication be configured on the firewall. Quickly determines the most common URL and FTP destinations on a user name basis for your company. Only PIX firewalls with logging on are reported.

Reports: 58

34 Standard Reports - Cisco Router

Reports module includes the following standard reports for the Cisco Router device.

1. Bandwidth Usage by Address

WITHDRAWN

WITHDRAWN

Summarizes the number of permitted packets per source address for all network traffic through Cisco routers. Sorted by packet count. Only network traffic from Cisco router interfaces with access control lists applied and logging turned on is reported. Source address can be an Internet or intranet address depending on which router interface the access list is applied and in which direction.

2. Bandwidth Usage by Department

Summarizes the number of permitted packets per source address for all network traffic through Cisco routers. Sorted by packet count. Only network traffic from Cisco router interfaces with access control lists applied and logging turned on is reported. Source address can be an Internet or intranet address depending on which router interface the access list is applied and in which direction.

3. Bandwidth Usage by Port

Summarizes the number of permitted packets passing through Cisco routers by port. Sorted by packet count. Only network traffic from Cisco router interfaces with access control lists applied and logging turned on is reported. Source address can be an Internet or intranet address depending on which router interface the access list is applied and in which direction.

4. Denied Packets per Hour

Displays the number of denied packets per hour by Cisco routers. It is used to spot possibly security threat trends over time ranges. Each tick mark on vertical hourly axes represents accumulated denied packets for the previous hour.

5. Denied Traffic by Address

Summarizes the number of denied packets per source address through Cisco routers. Sorted by denied packet count. Only network traffic from Cisco router interfaces with access control lists applied and logging turned on is reported. Source address can be an internal or external address depending on which router interface the access list is applied and in which direction.

6. Denied Traffic by Port

Summarizes denied traffic filtered through Cisco routers by port. Sorted by packet count. Only network traffic from Cisco router interfaces with access control lists applied and logging turned on is reported.

7. Inbound Email Traffic

WITHDRAWN

Summarizes the number of inbound email packets permitted through Cisco routers by destination address. Sorted by router address, access control list, and number of sessions. Only network traffic from Cisco router interfaces with access control lists applied and logging turned on is reported. The system determines inbound or outbound traffic from the network information entered in its IPADDR.TAB file. If this file is not configured, the system assumes traffic is inbound.

8. Inbound FTP Traffic

Summarizes permitted inbound FTP packet usage through Cisco routers. Sorted by router address, access control list, and number of sessions. Only network traffic from Cisco router interfaces with access control lists applied and logging turned on is reported. The system determines whether traffic is inbound or outbound from the information entered in its IPADDR.TAB file located in the Program directory. If this file is not configured, the system assumes traffic is inbound.

9. Inbound HTTP Traffic

Summarizes the number of permitted packets transferred by destination address for inbound HTTP traffic through Cisco routers. Sorted by router address, access control list, and number of sessions. Only network traffic from Cisco router interfaces with access control lists applied and logging turned on is reported. The system determines whether traffic is inbound or outbound from the information entered in its IPADDR.TAB file located in the Program directory. If this file is not configured, the system assumes traffic is inbound.

10. Inbound Telnet Traffic

Summarizes the number of inbound Telnet packets permitted through Cisco routers. Sorted by router address, access control list, and number of sessions. Only network traffic from Cisco router interfaces with access control lists applied and logging turned on is reported. The system determines inbound or outbound traffic from the network information entered in the IPADDR.TAB file. If this file is not configured, the system assumes traffic is inbound.

11. Outbound Email Traffic

Summarizes the number of outbound email packets permitted through Cisco routers by destination address. Sorted by router address, access control list, and number of sessions. Only network traffic from Cisco router interfaces with access control lists applied and logging turned on is reported. The system determines inbound or outbound traffic from the network information entered in the IPADDR.TAB file. If this file is not configured, the system assumes traffic is inbound.

FUJ00155413

WITHDRAWN

12. Outbound FTP Traffic

Summarizes the number of permitted packets transferred per source and destination address pair for outbound FTP sessions through Cisco routers. It is sorted by router address, access control list, and number of sessions. Only network traffic from Cisco router interfaces with access control lists applied and logging turned on is reported. The system determines whether traffic is inbound or outbound from the information entered in its IPADDR.TAB file located in the Program directory. If this file is not configured, the system assumes traffic is inbound.

13. Outbound HTTP Traffic

Summarizes the number of permitted packets transferred by destination address for outbound HTTP traffic through Cisco routers. Sorted by router address, access control list, and number of sessions. Only network traffic from Cisco router interfaces with access control lists applied and logging turned on is reported. The system determines whether traffic is inbound or outbound from the information entered in its IPADDR.TAB file located in the Program directory. If this file is not configured, the system assumes traffic is inbound.

14. Outbound Telnet Traffic

Summarizes the number of outbound Telnet packets permitted through Cisco routers. Sorted by router address, access control list, and number of sessions. Only network traffic from Cisco router interfaces with access control lists applied and logging turned on is reported. The system determines inbound or outbound traffic from the network information entered in the IPADDR.TAB file. If this file is not configured, the system assumes traffic is inbound.

15. Permitted Packets by Address

Displays the number of permitted packets by address through Cisco routers. It is used to spot top packet users through your router.

16. Permitted Packets per Hour

Displays the number of permitted packets per hour by Cisco routers. It is used to spot peak packet usage trends over time ranges. Each tick mark on vertical hourly axes represents accumulated permitted packets for the previous hour.

17. Permitted Packets by Port

Displays the number of permitted packets by port through Cisco routers. It is used to spot top bandwidth applications running across your router.

FUJ00155413

WITHDRAWN

18. SiteTrack Detection

Listing of packets that have been permitted or denied through Cisco routers with host name lookups that match any of the keywords entered in the SiteTrack keyword list. Sorted in date/time sequence. Keyword match is listed in the report with parentheses ( ) preceding the message in the Message field. Keywords need to be entered in the SiteTrack, and its DNS Resolver service must be on for this feature to function. The DNS Resolver service performs a host name lookup of both source and destination IP addresses in every packet it receives from Cisco routers.

19. System Critical Events

Listing of Router system status messages received from Cisco routers. Sorted in date/time sequence. Only Cisco routers with logging turned on are reported.

20. System Interface Events

Listing of system interface status messages from Cisco routers. Sorted in date/time sequence. Only Cisco routers with logging turned on are reported.

21. Top 20 Bandwidth Users

Displays the top 20 bandwidth users by address through Cisco routers. It is used to spot top bandwidth hogs through the router.

22. Top 20 Denied Packets by Address

Displays the top 20 addresses of denied packets through Cisco routers. It is used to spot quickly foreign addresses that are possibly attempting to breach your security policy.

23. Top 20 Denied Packets by Port

Displays the top 20 ports with the most denied packets through Cisco routers. It is used to spot quickly which applications may possibly being used for an attempted security breach.

24. Call Data - Call Information By Call ID

Displays all information associated with specified calls within a time period. Information includes: Setup Time, Username, Number Called/Calling, Origin, Connection Speed, and Traffic Passed.

FUJ00155413

WITHDRAWN

25. Call Data - Top 10 Total Duration By Number Called
Displays the total call time duration associated with the Top 10 Numbers Called. The call time displays in seconds.

26. Call Data - Top 10 Total Duration By Username
Displays the Top 10 Usernames based upon call duration time for the specified time period.

27. Call Data - Total Disconnects by Error for Each Device
Displays the number of events that present an error in the disconnect code for each call.

28. Call Data - Total Usage By Device
Displays the Call Traffic associated with each device. This is an executive level report for Administrators.

29. Call Data - Total Usage By Username
Queries the Call Data Record for all associated Call information. Results display by username associated with calls.

Reports: 29

38 Standard Reports - Cisco VPN 3000 Concentrator
Reports module includes the following standard reports for the Cisco VPN 3000 Concentrator device.

1. Bandwidth Usage per Hour
Displays the VPN bandwidth usage per hour.

2. Connection Statistics by Username
Lists the Date/Time Stamp, Username, and Device Addresses associated with each successful connection attempt.

3. Denied Connections

FUJ00155413

WITHDRAWN

Displays the number of denied connections by VPN gateway.

4. Denied Connections by Date/Time
Displays the VPN denied connections by Date/Time for the entire group of VPN gateways.

5. Denied Connections by Username
Displays the VPN denied connections by Username for the entire group of VPN gateways. Data is sorted by denied connections.

6. Denied Connections per Hour
Displays the VPN denied connections per hour.

7. Successful Authentications by Date/Time
Queries the database for messages that report successful authentication requests, and reports back information such as Date/Time, Device Address, Username, Local PortName, and Groupname.

8. Successful Authentications by GroupName
Queries the database for messages that report successful authentication requests and reports successful connection counts by Groupname.

9. Successful Authentications by UserName
Queries the database for messages that report successful authentication requests and reports successful connection counts by Username.

10. Successful Connections by Device Address
Total of all successful connections to a monitored Cisco VPN 3000 concentrators. It is sorted by Device Address.

11. Systems Events by Device
Lists each system event (configuration changes, hardware errors, etc) for each device. Data is sorted by date/time and VPN device.

12. Top 20 Bandwidth Users By Total Bytes

FUJ00155413

Displays the top 20 users for all VPN gateways by total bytes.

13. Top 20 Users by Durations
Displays the top 20 tunnel connections for all VPN gateways.

14. Top 20 Users by Number of Connections
Displays the top 20 users by connections for all VPN gateways.

15. Total Bytes by UserName
Lists the total bytes by local address for all VPN gateways. Data is sorted by username and total bytes. The total bytes are calculated by adding up the byte entries for each Local Address.

16. Total Duration by Username
Lists the total duration for all users of VPN gateways. Data is sorted by IP address and total duration. The total duration is calculated by adding up the duration entries for each Local Address.

Reports: 16

39 Standard Reports - Correlated Alerts
Reports module includes the following standard reports for correlated alerts.

1. Correlated Alerts Details
Lists all the alerts that caused a correlated alert.

2. Correlated Alerts List
Lists all correlated alerts in a given time period.

3. Correlated Alerts Summary

WITHDRAWN

FUJ00155413

Displays the top 20 correlated alerts in descending order.

Reports: 3

40 Standard Reports - Correlated Multi-Device Reports
Reports module includes the following standard reports for the multi-device reports.

1. IDS devices - Top 10 Source Addresses of Alarms
Displays the top 10 source addresses of intrusion detection alarms.

2. IDS devices - Top 10 Alarms
Displays the top 10 alarms (by signature id) that have been generated.

3. IDS devices - Top 10 Destinations of Alarms
Displays the top 10 destination IP addresses that have been targeted for attack.

4. Top 10 Requested URL/FTP Destinations
Displays the top 10 URL/FTP destinations by internal users.

5. Top 20 Bandwidth Ports
Displays the top 20 ports of bandwidth usage.

6. Top 20 Bandwidth Users
Displays the top 20 bandwidth users.

7. Top 20 Connections by Address
Displays the top 20 users of connection.

WITHDRAWN

FUJ00155413

8. Top 20 Connections by Port
Displays the top 20 ports with the most connections.

9. Top 20 Denied Inbound by Address
Displays the top 20 foreign addresses that were denied inbound access.

10. Top 20 Denied Inbound by Port
Displays the top 20 ports with the most denied connections.

11. Top 20 Denied Outbound by Address
Displays the top 20 local addresses that were denied outbound access.

Reports: 11

42 Standard Reports - DHCP
Reports module includes the following standard system reports for DHCP processing.

1. DHCP Lease Change
Lists the lease time of DHCP IP addresses.
Database Tables
DHCP Support

Reports: 1

WITHDRAWN

FUJ00155413

WITHDRAWN

66 Standard Reports - Linux
Reports module includes the following standard reports for the Novell Linux and Red Hat Linux devices.

1. Linux - Failed Authentications by Device
Displays the failed Authentication attempts for each monitored device by Date/Time.

2. Linux - Failed SuperUser Attempts
Displays the failed attempts to use the Switch User command and the username associated with the attempt.

3. Linux - Successful Connections
Displays the successful connection information.

4. Linux - Successful SuperUser Attempts
Displays the successful attempts to utilize the Switch User command to root and the username associated with the attempt.

5. Linux - Total Connections by Address
Displays the total connections by foreign address.

6. Linux - Total Connections by Username
Displays the total connections for each user within the specified time range.

Reports: 6

FUJ00155413

WITHDRAWN

68 Standard Reports - McAfee IntruShield
Reports module includes the following standard reports for the McAfee IntruShielddevice.

1. Alarm Destination Report
Displays alarms sorted by the Destination IP Address that generated the alarm.

2. Alarm Levels
Displays the number of alarms for each alarm level.

3. Alarm Report
Lists alarms based on signature names, sorted by alarms and signature names.

4. Alarms by Hour
Displays the number of alarms by hour for a given time period.

5. Alarms by Sensor
Lists the alarm count for each sensor.

6. Alarms by Sensor Device
Displays the total number of alarms generated by each sensor device. The report is sorted by total number of alarms.

7. Top 10 Sources of Alarms
Lists the top 10 source IP addresses that have generated the most events/alarms.

8. Top 20 Alarms
Displays the top 20 alarms by signature IDs that have been generated.

FUJ00155413

9. Top 20 Alarms by Port
Displays the Top 20 alarms based on the destination port.

10. Top 20 Destinations of Alarms
Displays the top 20 destination IP addresses that have been targeted for attack.

11. Top 20 Source-Destination Pairs of Alarms
Displays the top 20 source/destination pair that have generated the most alarms.

12. Top 20 Sources of Alarms
Lists the top 20 source IP addresses that have generated the most events/alarms.

Reports: 12

69 Standard Reports - McAfee VirusScan Enterprise
The Reports module includes the following standard reports for McAfee VirusScan Enterprise.

1. Top 20 infected systems
Displays top 20 infected systems found on the network

2. Top 20 Viruses Detected
Displays top 20 viruses found on the network

3. Virus Detection Details
Lists all the detected viruses, sorted by date/time.

Reports: 3

WITHDRAWN

WITHDRAWN

71 Standard Reports - Microsoft Exchange Server
Reports module includes the following standard reports for Microsoft Exchange Server.

1. MS Exchange - Exchange Error Condition
Displays all Exchange error events.

2. MS Exchange - Failed Logons Attempts to Mailboxes
Displays failed logons to mailboxes in Microsoft Exchange environment.

3. MS Exchange - Failed Mailbox Creation/Deletion
Displays failed mailbox creation and deletion.

4. MS Exchange - Internet Traffic by Email Accounts
Displays the inbound and outbound Internet traffic to email accounts.

5. MS Exchange - Logons to Mailbox with Administrator Privileges
Displays successful logons to mailboxes in Microsoft Exchange environment by users who have administrator privileges on the mailboxes.

6. MS Exchange - Mailboxes with the most logon failures
Displays users responsible for the greatest number of failed logons.

7. MS Exchange - Non-owner Mailbox Access
Displays users who connect to Exchange mailboxes apart from their primary user accounts.

8. MS Exchange - Successful Logons to Mailboxes
Displays successful logons to mailboxes in Microsoft Exchange environment.

9. MS Exchange - Top 10 Email Accounts Receiving Messages

FUJ00155413

Displays the top 10 email accounts receiving the most messages.

10. MS Exchange - 10 Email Accounts Receiving Messages Volume
Displays the top 10 email accounts receiving the most message volume.

11. MS Exchange - Top 10 Email Accounts Sending Messages
Displays the top 10 email accounts sending the most messages.

12. MS Exchange - Top 10 Email Account Sending Messages Volume
Displays the top 10 email accounts sending the most message volume.

13. MS Exchange - Top 10 Sender-Receiver Pairs
Displays top 10 pairs of email accounts sending messages to, and receiving messages from, each other.

14. MS Exchange - Top 10 Sender-Receiver Pairs within the organization
Displays the top 10 email accounts receiving the most messages.

15. MS Exchange - Top 10 Email Accounts mailing most with an Internet
Displays the top 10 email accounts responsible for the most Internet traffic.

16. MS Exchange - Use of Send Privileges
Displays users who grant users permissions to Send As privileges.

Reports: 16

72 Standard Reports - Microsoft IIS
Reports module includes the following standard reports for Microsoft IIS.

WITHDRAWN

FUJ00155413

WITHDRAWN

1. Access Denied Attempts (500)

Displays page access attempts that were denied over time. If multiple sites were chosen, an additional run time option is to select if the access denied attempts were displayed cumulatively, or comparatively.

2. Browser Versions

Displays the percentage of browser types to the sites selected.

3. Hits per Day

Displays the number of requested pages for the sites chosen during run time. An additional run time option allows you to select if you want the information for multiple sites summed together or compared against each other.

4. Top 20 Page not Found (404)

Displays the top 20 requested files that were not found. If multiple sites were chosen at run time, the site where the file was requested from is also included in the report.

5. Top 20 Referring Domains

Displays the top 20 referring domains. If multiple sites are chosen at run time, the name the site is referred to is also in the report.

6. Top 20 Referring Pages

Displays the top 20 referring URLs, as well as the number of refers each URL provided. If multiple sites are chosen at run time, the name the site is referred to is also in the report.

7. Top 20 Requested Content

Displays a summary of the top 20 requests by the root level directory in which the file is contained. This provides a summary of the most active areas of the web site. If there are multiple sites chosen at run time, the name of the site where the directory resides will also be included in the report.

8. Top 20 Requested Pages

Displays a summary of the top 20 most requested pages for the sites chosen during run time. If multiple sites are chosen at run time for this report, the name of the site the requested page is served from is also included in the report.

9. Top 20 Script Errors (501)
Displays the top 20 requested page, script error combinations. A page may appear on this report multiple times if the page has different multiple script errors. If multiple sites are chosen at run time for inclusion in the report, the site the page resides on is included in the report.

10. Visitors per Day
Displays of the number of unique IP addresses of visitors for the sites chosen during run time. An IP address is only counted the first time is appears during the chosen time period.

Reports: 10

73 Standard Reports - Microsoft ISA
Reports module includes the following standard reports for Microsoft ISA.

1. Attacks
Displays all of the attacks that were identified by the ISA Firewall Service.

2. Firewall Errors
Displays the Firewall Error messages as recorded by the ISA Firewall Service.

3. Total Bytes by Client IP
Displays the total bytes of all connections associated to specific Client IPs.

4. Total Duration by Client IP
Displays the total duration of all connections associated to specific Client IPs.

WITHDRAWN

FUJ00155413

5. Total Number of Connections by Domain Name
Displays the number of connections associated to each Domain Name during a given time period.

6. Total Number of Connections by Server IP
Displays number of connections associated to each Server IP during a given time period.

Reports: 6

74 Standard Reports - Microsoft SQL Server

1. Configuration changes
Displays configuration changes made to MS SQL Server systems.

2. Database backups
Displays backup events from MS SQL Server systems.

3. Errors that can be corrected by a user
Displays all error conditions from MS SQL Server systems that can be corrected by a user.

4. Failed Logons
Displays all failed logons events to MS SQL Server systems.

5. Fatal Errors
Displays fatal errors from MS SQL Server systems.

6. Insufficient Resources
Displays insufficient resource events from MS SQL Server systems.

WITHDRAWN

FUJ00155413

7. Logon/Logoff Events
Displays all logons and logoff events to MS SQL Server systems.

8. Nonfatal Internal Errors
Displays nonfatal internal errors from MS SQL Server systems.

9. Object events
Displays object trace events from MS SQL Server systems.

Reports: 9

75 Standard Reports - Account Management
Reports module includes the following standard reports for Windows.

1. Account Changes Details
List of all account changes.

2. Account Changes Summary
Shows the number of account changes by event ID in descending order.

3. Computer Account Changes
List of all computer account changes.

4. Global Group Account Changes
List of all global group account changes.

5. Local Group Account Changes
List of all local group account changes.

WITHDRAWN

FUJ00155413

WITHDRAWN

6. Universal Group Account Changes
List of all universal group account changes.

7. User Group Account Changes
List of all user account changes.

Reports: 7

76 Standard Reports - Application Errors
Reports module includes the following standard reports for Windows.

1. Errors Reported by Dr. Watson
List of errors reported by Dr. Watson.

2. Top 20 Application Errors
Displays the top 20 application errors collected from all Microsoft Windows servers.

3. Top 20 Errors-Logging Applications
Displays the top 20 applications logging application errors from all Microsoft Windows servers.

Reports: 3

77 Standard Reports - Disk and Memory
Reports module includes the following standard reports for Windows.

1. Bad Blocks
List of system events reporting bad blocks.

FUJ00155413

2. Disk at Near Capacity
List of system events reporting disk at near capacity.

3. Out of Virtual Memory
List of system events reporting out of virtual memory.

Reports: 3

78 Standard Reports - Files/Objects Access
Reports module includes the following standard reports for Windows.

1. Access to Files
List of all files accessed in folders monitored for access auditing.

2. Registry Access
List of all accesses to registry files and keys.

3. Write Access to System Files
List of all files opened with write access rights in the system32 folder.

Reports: 3

79 Standard Reports - Logon/Logoff
Reports module includes the following standard reports for Windows.

1. Failed Logons
List of all failed logon events including failure reason, user name, domain name and workstation.

WITHDRAWN

FUJ00155413

WITHDRAWN

2. Local Logons/logoffs by User
List of all local logon and logoff activities sorted by user name.

3. Logons/logoffs by User
List of all logon and logoff activities sorted by user name.

Reports: 3

80 Standard Reports - Policy Changes and Audit Logs
Reports module includes the following standard reports for Windows.

1. Audit Log Cleared
List of audit log cleared events.

2. Audit Log Full
List of audit log is full events.

3. Audit Policy Changes
List of all audit policy changes.

4. Policy Changes Details
List of all policy changes events.

5. Policy Changes Summary
Shows the number of policy changes by event ID in descending order.

6. Trusted Domain Changes

FUJ00155413

List of all trusted domain changes.

7. User Rights Changes
List of all user rights changes.

Reports: 7

81 Standard Reports - Restart/Shutdown
Reports module includes the following standard reports for Windows.

1. System Restarts/Shutdowns
List of all system restarts and shutdowns.

Reports: 1

82 Standard Reports - Summary Reports
Reports module includes the following standard reports for Windows.

1. Application Log Activity per Computer
Total count of application events per computer in descending order.

2. Application Log Activity per User
Total count of application events per user in descending order.

3. Security Log Activity per Computer
Total count of security events per computer in descending order.

4. Security Log Activity per User

WITHDRAWN

FUJ00155413

Total count of security events per user in descending order.

5. System Log Activity per Computer
Total count of system events per computer in descending order.

Reports: 5

83 Standard Reports - Trend Reports
Reports module includes the following standard reports for the Windows devices.

1. Application Log Activity
Displays the number of application events over time.

2. Security Account Logon Activity
Displays the number of security account logon events over time.

3. Security Account Management Activity
Displays the number of security account management events over time.

4. Security Detailed Tracking Activity
Displays a number of security detailed tracking events over time.

5. Security Log Activity
Displays the number of security events over time.

6. Security Logon/Logoff Activity
Displays the number of security logon/logoff events over time.

WITHDRAWN

FUJ00155413

7. Security Object Access Activity
Displays the number of security object access events over time.

8. Security Policy Change Activity
Displays the number of security policy change events over time.

9. Security Privilege Use Activity
Displays the number of security privilege use events over time.

10. Security System Event Activity
Displays the number of security system event events over time.

11. System Log Activity
Displays the number of system events over time.

Reports: 11

84 Standard Reports - User Activity
Reports module includes the following standard reports for Windows.

1. Applications by Users
List of applications running on computers over the network, sorted by user name.

2. Print Jobs by Users Summary
Summary of print jobs by users, showing user name, number of print jobs and total pages and total bytes.

3. Privileged Activities by User
List of activities invoking right or privileges, sorted by user name.

WITHDRAWN

FUJ00155413

Reports: 3

88 Standard Reports - Audit
Reports module includes the following standard system reports for the system auditing function.

1. Configuration Changes by Action
Lists all the configuration changes with the specified Action.
Runtime parameters - Action.

2. Configuration Changes by Date/Time
Lists all configuration changes made to enVision.

3. Configuration Changes by Object Type
Lists all configuration changes made against the specified object.
Runtime parameters - Object Type.

4. Configuration Changes by User
Lists all configuration changes made by the specified user.
Runtime parameters - User ID.

5. Report Access Activity by Date/Time
Lists all reports that have been either e-mailed or viewed and by whom (usernames).

6. Report Access Activity by User
List all reports that the specified user has e-mailed or viewed.
Runtime parameters - User ID.

WITHDRAWN

FUJ00155413

7. Report Emailing Activity by Date/Time
Lists all reports that have been e-mailed and by whom (usernames).

8. Report Emailing Activity by User
List all reports that the specified user has e-mailed.
Runtime parameters - User ID.

9. Report Viewing Activity by Date/Time
Lists all reports that have been viewed and by whom (usernames).

10. Report Viewing Activity by User
List all reports that the specified user has viewed.
Runtime parameters - User ID.

11. User Session Activity by Date/Time
Lists all the successful and failed enVision log in/log out attempts.

12. User Session Activity by User
Lists all the successful and failed enVision log in/log out attempts by the specified user.
Runtime parameters - User ID.

Reports: 12

89 Standard Reports - System
Reports module includes the following standard HIC System reports.

1. Appliance Disk Errors
Lists all the application disk errors.

WITHDRAWN

FUJ00155413

2. Appliance Operating Environment Errors
Lists all the appliance operating environment errors.

3. Failed Terminal Server Logins to the Appliance
Lists all failed terminal server login attempts to the appliance.

4. Failed enVision Logins
Lists all failed attempts to log in to enVision.

5. Monitored Device Collection Errors
Lists all errors in collection of data from monitored devices.
NIC System Device

Reports: 5

94 Standard Reports - Oracle
Reports module includes the following standard reports for the Oracle device.

1. Audit Details by Action
Displays detailed audit actions by action.

2. Audit Details by Database Process ID
Displays detailed audit actions by database process ID.

3. Audit Details by System
Displays detailed audit actions by system name.

WITHDRAWN

FUJ00155413

4. Audit Details by User
Displays detailed audit actions by user name.
Standard Reports

Reports: 4

95 Standard Reports - RSA Security SecurID
Reports module includes the following standard reports for the RSA Security SecurID

1. Deleted Agent Hosts
Displays any new agent hosts added to the existing users in the RSA database in the specified time period.

2. Failed Authentication Attempts
Displays all of the failed authentication attempts by Username.

3. Group Modifications
Displays any modifications to the existing groups in the RSA database in the specified time period.

4. New Agent Hosts
Displays any new agent hosts added to the existing users in the RSA database in the specified time period.

5. New Groups Added
Displays all of the new groups added to the RSA database in the specified time period.

6. New Users Added
Displays all of the new users added to the RSA database in the specified time period.

7. Successful Authentication Attempts

WITHDRAWN

FUJ00155413

Displays all of the successful authentication attempts by Username.

8. User Modifications
Displays any modifications to the existing users in the RSA database in the specified time period.

Reports: 8

97 Standard Reports - SNORT
Reports module includes the following standard reports for the SNORT device.

1. Alarm Destination Report
Lists alarms sorted by the Destination IP Address that generated the alarm.

2. Alarm Levels
Displays the number of alarms for each alarm level.

3. Alarm Report
Lists alarms based on signature names, sorted by alarms and signature names.

4. Alarms by Hour
Displays the number of alarms by hour for a given time period.

5. Alarms by Sensor
Lists the alarm count for each sensor.

6. Alarms by Sensor Device
Displays the alarm count for each sensor device.

WITHDRAWN

FUJ00155413

7. Top 10 Alarm Signatures
Lists the top 10 alarms (by signature name) that have been generated.

8. Top 10 Destinations of Alarms
Lists the top 10 destination IP addresses that have been targeted for attack.

9. Top 10 Source-Destination Pairs of Alarms
Lists the top 10 source/destination pair that have generated the most alarms.

10. Top 10 Sources of Alarms
Displays the top 10 sources of alarms by source IP address.

Reports: 10

99 Standard Reports - Sun Solaris
Reports module includes the following standard reports for the Sun Solaris BSM device.

1. Kernel-Level Events
Lists kernel-level events generated by system calls.

2. Login and Logout Events
Lists login and logout audit events.

3. Nonattributable Events
Lists the events that occur at the kernel-interrupt level or before user is identified and authenticated.

4. Permission Changes
Lists permission changes by a process or user.

WITHDRAWN

FUJ00155413

5. Privileged Operations
Lists the use of privelege capabilities or role-based access control.

6. User-Level Events
Lists the user-level events generated by application software.

Reports: 6

100 Standard Reports - Sun Solaris
Reports module includes the following standard reports for the Sun Solaris BSM device.

1. Failed Super User Attempts
Displays users who attempted to Switch User to "root" and was denied.

2. Percentage of Connections by Service
Queries for messages with a message ID of 317013 and counts them reported by agent (service). This message is created by the inetd daemon and logs all connections by service (for example: login, ftp, telnet, etc).

3. Super User Access
Queries for messages with message ID of 36[illegible]01, and displays which users Switched User to "root" and at what time.

4. Total Connections by Foreign Address
Displays the total connections by source address.

5. Total Connections by Port
Displays the Total number of connections grouped by port number.

WITHDRAWN

FUJ00155413

Reports: 5

110 Standard Reports - Tripwire Enterprise
Reports module includes the following standard reports for the Tripwire Enterprise device.

1. Changes
Lists the nodes with detected changes sorted by time of change occurrence.

2. Changes by Severity
Lists the nodes with detected changes sorted by detected severity.

3. Change Rates
Lists changes detected sorted by frequency of occurrence.

4. Nodes
Lists all Tripwire unique nodes.

5. System Access
Lists user logon and logoffs.

Reports: 5

WITHDRAWN

FUJ00155413

WITHDRAWN

FUJ00155413

3.6.3 Operational Security Management and ad hoc Reports

Currently the only Security Event analysis reports that Operational Security can produce are ad hoc reports when provided with a correctly formatted log.

Managed and scheduled Event and Incident Summary Reports need to be agreed with Operational Security Manager and initially these reports need to highlight breaches in Confidentiality, Integrity or availability by Service Delivery Unit with drill down facilities if required.

Key areas that these and ad hoc reports need to consider for summarisation dependent on the type of log analysed are:

- Date and time Summaries
- Log Source summaries
- Types of Event Summaries
- Event Categorisation Summaries
- Event Number Summaries
- Event User Summaries
- Computer or device summaries
- Event Description Summaries
- Trended Summary
- Overall Summary of each of above category

The use of Sawmill a tool which Operational Security already has would give much of the required output on an ad hoc basis if original logs were available and an audit plan of platforms based on risk provided.

Sawmill Proof of Concept

A proof of concept into its use has been undertaken with

- CSV output logs for Windows NT Events
- CSV output logs for Windows 2000 Events
- Syslogs from Solaris
- Syslogs from Cisco Routers
- Syslogs from Cisco Firewalls

To assess whether this is feasible and summary results are documented as an appendix to this document.

WITHDRAWN

FUJ00155413

An attempt has taken place to analyse a limited set of Tivoli logs using a specialised configuration file developed, by Sawmill's proprietor and this is also shown in Appendix A shows details.

3.7 Sawmill Process

- To initially access Sawmill you need to log on with the user name and password given by the administrator:

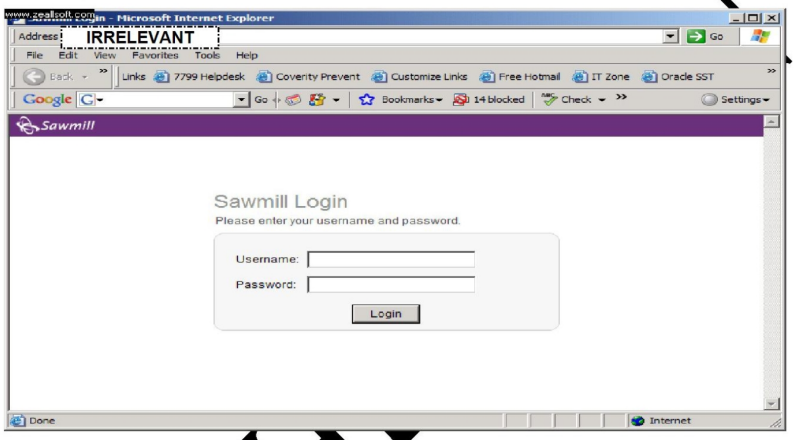


Figure 3 Sawmill Logon Screen

- Once you have logged in then you need to set a profile up this is done by clicking the Create new profile text.

WITH

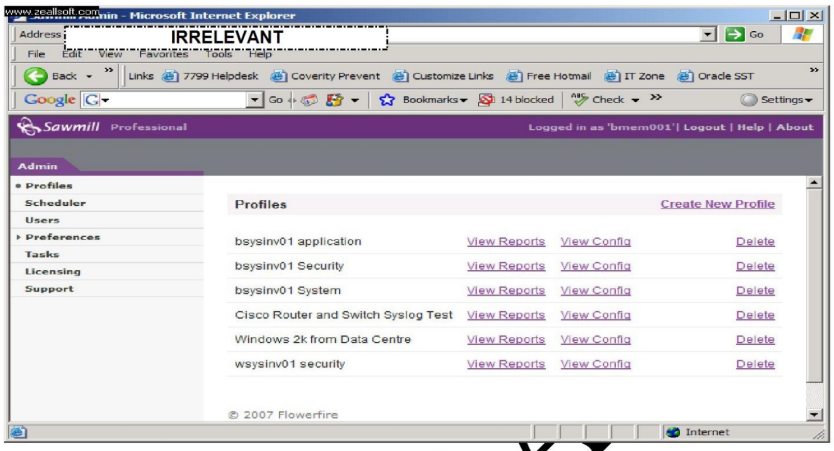


Figure 4 Profile Creation Screen

- You then need to select the location of the source of your log, note that log patterns and subdirectories can be selected by using wildcards and by ticking the process sub folders .

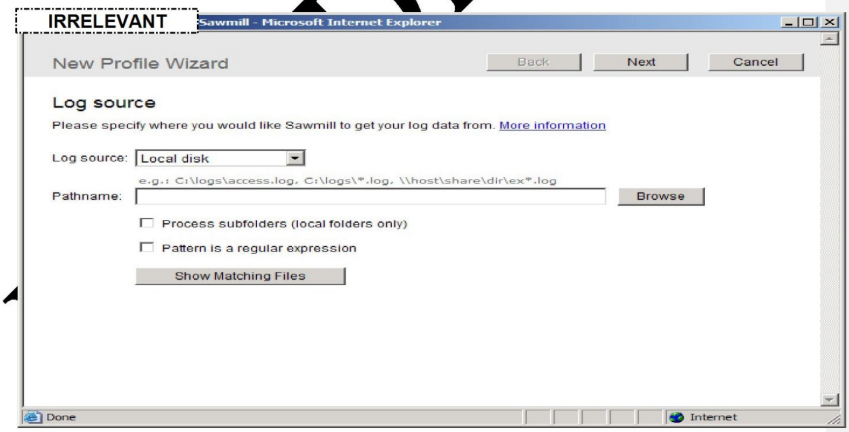


Figure 5 File or Directory Path Selection

- If you chose to use the browse button to select the log you are presented with a screen as shown below.

FUJ00155413

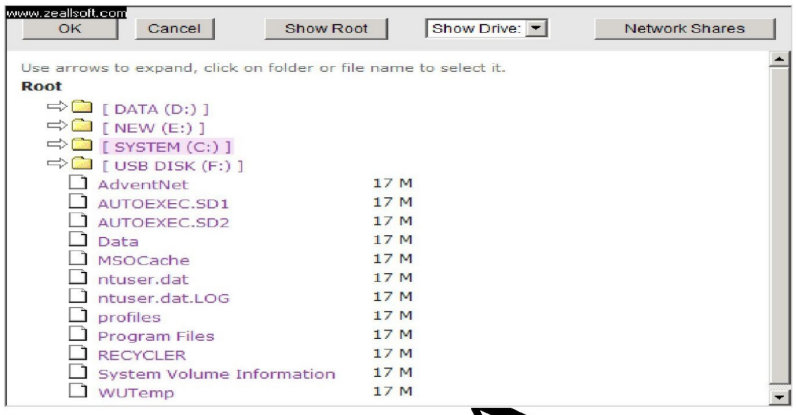


Figure 5 Browse the Selection Menu

- Once you have clicked and selected the file or directory the following screen appears to show the log is being processed.

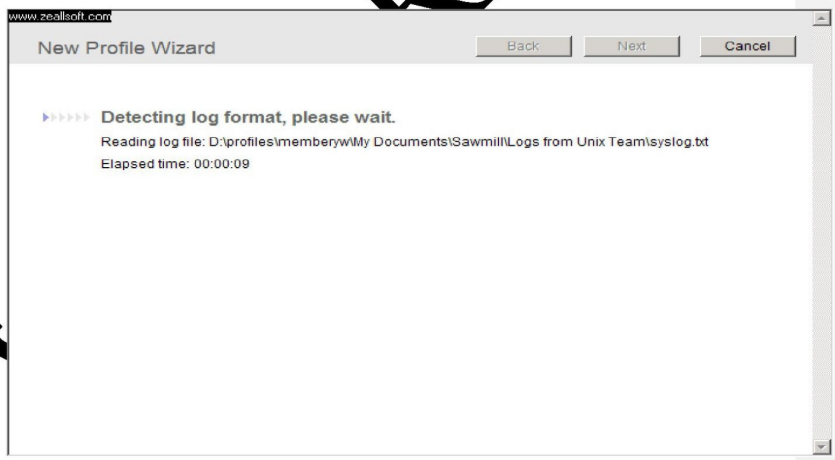


Figure 6 Log Detection Screen

- If the log format is not recognised then the following screen appears, if you know the format of the log click next otherwise cancel and check with the SDU you have received the correct log format.

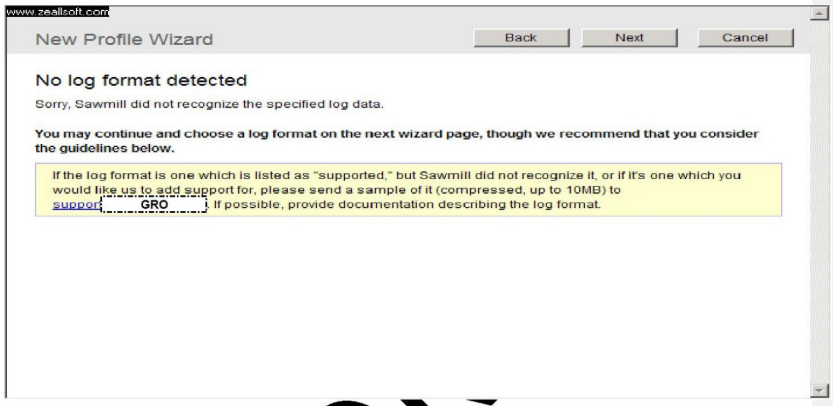


Figure 7 Log Format not recognised

- The next window allows you to select the log format you wish to analyse and press next

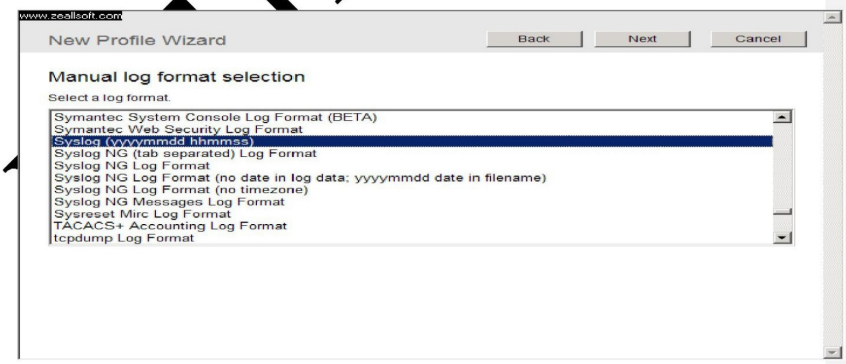


Figure 8 Manual log format Selection

FUJ00155413

- Some formats will give you a secondary screen choice such as syslog, as there are not agreed common standards between manufacturers for the format of a syslog log, once satisfied press next.

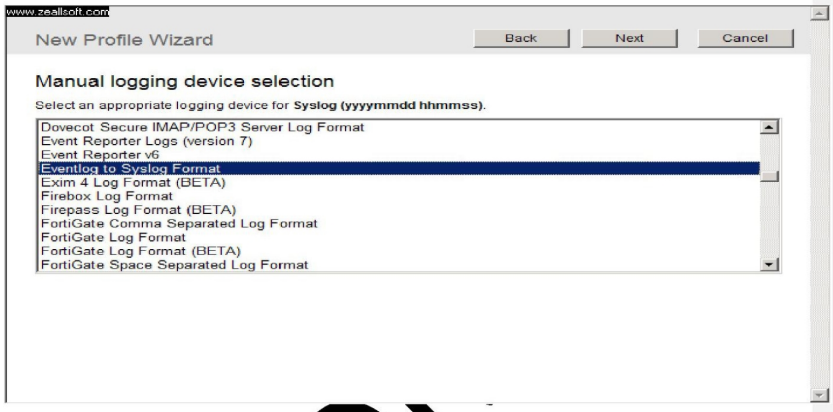


Figure 9 Log type of Device Selected

- Each log type selected requires a name for the profile it sets up and this screen does this, enter the name you have chosen, I recommend platform and latest date of the log e.g. mboinv0112 107 and click the finish button.

Figure 10 Name of new Profile

FUJ00155413

- Once the Finish button is pressed then the log is analyzed and a report and can be drilled through by using date ranges and selection criteria for the data from the task bar on the left hand side. Samples of some summary reports for which suitable logs have been available are included in the appendix A.

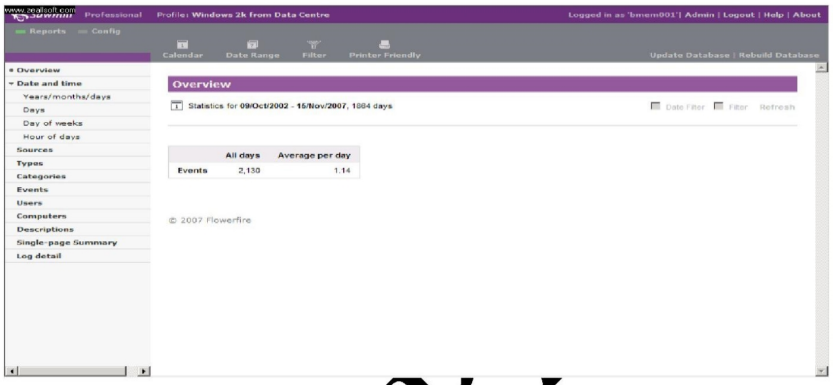


Figure 11 Log Report with Analysis options on Left

WITHDR

4.0 Audit

This process is subject to PCI and ISO 27001 Audit which is arranged by the Security and Governance Team.

However, in order to provide some guidelines as to the key areas that Operational Security needs to analyse to assess whether a Security Incident has occurred the following areas are considered key, the item also shows other sources of base data that needs to be used to confirm the validity of the output:

1. Identify that only authorised users are accessing the platforms their roles permit them to do so – Event log Analysis and PVCS documentation
2. Identify that only authorised platforms (i.e. Names and IP's) access the network – PVCS documentation, Networks IP List and Event logs
3. Identify any unauthorised use of ports and protocols – Analysis of Event logs and PVCS documentation
4. Identify any changes that take place without a Change Control – e.g. CP or OCP both to Operating Systems and Applications – Audits and check against CP and OCP data for any actions taken and Nessus passive scans to see what is still outstanding
5. Identify any vulnerabilities on platforms particularly those identified by the supplier as Critical or High – MBSA and OVAL runs on targeted at risk platforms

FUJ00155413

6. Identify any unauthorised changes to users rights based on their roles – PVCS documentation and access to Event logs and CP, OCPS and Audit
7. Identify any unauthorised changes to permissions on files dependent on the role and rights allocated to that role – Alerts, Audits ,Event logs, CP, OCP's and alerts
8. Identify any unauthorised File or Data Transfers particularly to CD, DVD or USB or unauthorised networks – Audits, Alerts and CP, OCP's and Event logs
9. Identify any AV alerts – Alerts, Event logs,
10. Identify any unauthorised changes to Router, Switch, Firewall and Contents Switches in particular Configuration, Access Lists and Rulebases – Audit, Alerts, Event logs, CP,OCP,
11. Identify any unauthorised changes to Audit Logs and other log files – Alerts, Audit, OCP, CP
12. Identify any unauthorised changes to passwords or password brute force attacks – Alerts, Audits, RSA, OCP, CP and PVCS documentation
13. Identify any buffer overflow attacks – Alerts, Audits
14. Identify any unauthorised shares or trusts that permit escalation of privilege or network hopping – Audit, Event logs, PVCS documentation, OCP, CP's
15. Identify any unauthorised use of audits or other tools to hide attacks – Alerts, Event logs, Audit, OCP, CP's
16. Identify any unauthorised scheduling of batch jobs – Alerts , Audit, Event logs, PVCS Documentation
17. Identify any unauthorised services – Alerts, Audit, PVCS Documentation, Event Logs
18. Identify any unauthorised remote control services – Alerts, Audit, PVCS Documentation, Event Logs
19. Identify any unauthorised installed monitoring mechanisms – Alerts, Audits, Event logs, PVCS Documentation
20. Identify any infected startup files or Trojans– Alerts, Audit, PVCS documentation, Event logs
21. Check for any default users or manufacturers default settings used – Alerts, Audit, Event Logs, PVCS documentation
22. Check for the use of available exploit code for a DOS or DDOS – Event Log
23. Alert on any traffic patterns that indicate that a potential hack is being prepared for (not so much Horizon but will be required as migrate to HNG-X and RMG Network is more open)

WITHDRAWN

FUJ00155413

5.0 Appendix A

5.1 Tivoli Event Log Summary by Sawmill

5.1.1 Summary

Statistics for **09/Oct/2007 - 14/Dec/2007**, 67 days

Date Filter Filter **Refresh**

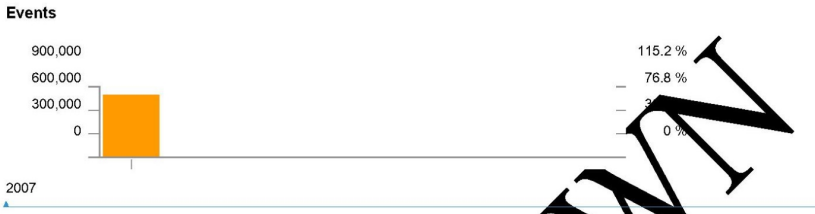
5.1.2 Overview

	All days	Average per day
Events	781,488	11,664.00

WITHDRAWN

FUJ00155413

5.1.3 Years/months/days



Formatted: Font color: Auto

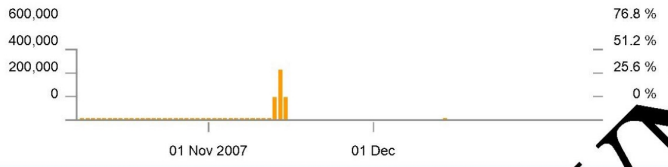
	Date/time	Events
1	2007	781,488
	Total	781,488

WITHDRAWN

FUJ00155413

5.1.4 Days

Events



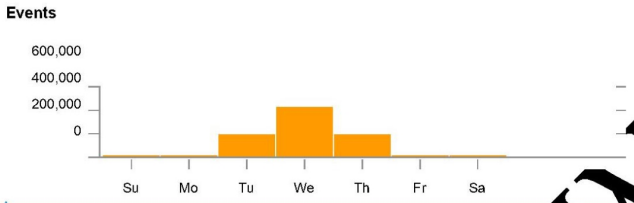
Formatted: Font color: Auto

	Date/time	Events
1	09/Oct/2007	2
2	10/Oct/2007	2
3	11/Oct/2007	[illegible]
4	12/Oct/2007	2
5	13/Oct/2007	2
6	14/Oct/2007	2
7	15/Oct/2007	2
8	16/Oct/2007	2
9	17/Oct/2007	2
10	18/Oct/2007	2
	29 other items	781,468
	Total	781,488

WITHDRAWN

FUJ00155413

5.1.5 Day of weeks



Formatted: Font color: Auto

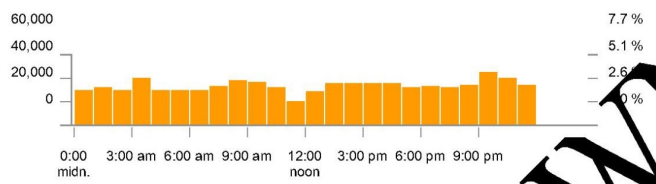
	Day of week	Events
1	Sunday	9,898
2	Monday	311
3	Tuesday	179,[illegible]
4	Wednesday	413,302
5	Thursday	178,759
6	Friday	96
7	Saturday	94
	Total	781,488

WITHDRAWN

FUJ00155413

5.1.6 Hour of days

Events



Formatted: Font color: Auto

WITHDRAWN

	Hour of day	Events
1	midnight - 1:00 AM	29,408
2	1:00 AM - 2:00 AM	30,670
3	2:00 AM - 3:00 AM	28,547
4	3:00 AM - 4:00 AM	39,781
5	4:00 AM - 5:00 AM	28,783
6	5:00 AM - 6:00 AM	28,608
7	6:00 AM - 7:00 AM	29,139
8	7:00 AM - 8:00 AM	31,939
9	8:00 AM - 9:00 AM	37,383
10	9:00 AM - 10:00 AM	36,130
11	10:00 AM - 11:00 AM	31,501
12	11:00 AM - noon	19,275
13	noon - 1:00 PM	28,076
14	1:00 PM - 2:00 PM	34,119
15	2:00 PM - 3:00 PM	34,316
16	3:00 PM - 4:00 PM	34,728
17	4:00 PM - 5:00 PM	34,343
18	5:00 PM - 6:00 PM	31,433
19	6:00 PM - 7:00 PM	31,982
20	7:00 PM - 8:00 PM	30,932

FUJ00155413

21	8:00 PM - 9:00 PM	33,689
22	9:00 PM - 10:00 PM	43,928
23	10:00 PM - 11:00 PM	39,580
24	11:00 PM - midnight	33,198
Total		781,488

5.1.7 Console hostnames

Default report view on zoom when clicking on a table item

Overview

Formatted: Font color: Auto, Not Hidden
Formatted: Font color: Auto, Not Hidden
Formatted: Font color: Auto, Not Hidden

Console_hostname	Events	0 – 100 %
IRRELEVANT	120,698	15.4 %
	109,383	14.0 %
	91,431	11.7
	86,109	11.0 %
	79,280	10.1 %
	77,468	9.9 %
IRRELEVANT	54,535	7.0 %
	37,983	4.9 %
	34,435	4.4 %
	32,720	4.2 %
9 other items	57,446	7.4 %
Total	781,488	100 %

DRAFT

5.1.8 Log sources

Default report view on zoom when clicking on a table item: Overview

Formatted: Font color: Auto, Not Hidden
Formatted: Font color: Auto, Not Hidden
Formatted: Font color: Auto, Not Hidden

Log_source	Events		0 - 100 %
1NT	670,964	85.9 %	
2EACRR	66,287	8.5 %	
3VPN	19,872	2.5 %	
4TIVOLI	14,644	1.9 %	
5SSCMonitor	8,837	1.1 %	
6PATROL	478	0.1 %	
7AntiVirus	2	0.1 %	
8SNMP	4	0.0 %	
Total	**781,488**	**100 %**	

WITHDRAWN

FUJ00155413

5.1.9 Log source types

Formatted: Font color: Auto, Not Hidden

- Default report view on zoom when clicking on a table item: Overview

Formatted: Font color: Auto, Not Hidden

Formatted: Font color: Auto, Not Hidden

Log_source_types	Events		0 - 100 %
1Security	335,554	42.9 %	
2VPN_LOOPBACK	197,504	25.3 %	
3EACRR	66,287	8.5 %	
4VPN Keymg	35,657	4.6 %	
5NT	19,872	[illegible] %	
6CNIM	17,569	2.2 %	
7H ROLLOUTSYNC	[illegible]961	1.5 %	
8TIVADMIN	9,723	1.2 %	
9SSCMonitor	8,837	1.1 %	
10ServiceMonitor	5,836	0.7 %	
2604 other items	72,688	9.3 %	

WITHDRAWN

FUJ00155413

Total	781,488	100 %

WITHDRAWN

FUJ00155413

5.1.10 Event origins

Formatted: Font color: Auto, Not Hidden

- Default report view on zoom when clicking on a table item: Overview

Formatted: Font color: Auto, Not Hidden

Formatted: Font color: Auto, Not Hidden

Event_origin	Events		0 - 100 %
IRRELEVANT	105,416	13.5 %	
	105,267	13.5 %	
	15,117	1.9 %	
	14,274	1.8 %	
	14,203	1.[illegible] %	
	10,753	1.4 %	
	8,335	1.[illegible]	
	7,997	1.0 %	
	7,995	1.0 %	
	7,115	0.9 %	
8451 other items	485,016	62.1 %	

WITHDRAWN

FUJ00155413

Total	781,488	100 %

WITHDRAWN

FUJ00155413

5.1.11 Hostnames

Formatted: Font color: Auto, Not Hidden

- Default report view on zoom when clicking on a table item: Overview

Formatted: Font color: Auto, Not Hidden

Formatted: Font color: Auto, Not Hidden

Hostname	Events		0 - 100 %
IRRELEVANT	105,416	13.5 %	
	105,267	13.5 %	
	15,117	1.9 %	
	14,274	1.8 %	
	14,203	1.[illegible] %	
	10,753	1.4 %	
	8,335	1.[illegible]	
	7,997	1.0 %	
	7,995	1.0 %	
	7,115	0.9 %	
9140 other items	485,016	62.1 %	

WITHDRAWN

FUJ00155413

Total	781,488	100 %

WITHDRAWN

FUJ00155413

5.1.12 Severities

Default report view on zoom when clicking on a table item: Overview

Formatted: Font color: Auto, Not Hidden
Formatted: Font color: Auto, Not Hidden
Formatted: Font color: Auto, Not Hidden

Severity	Events		0 - 100 %
120	653,644	83.6 %	
230	86,571	11.1 %	
350	40,730	5.2 %	
440	543	0.1 %	
Total	**781,488**	**100 %**	

WITHDRAWN

FUJ00155413

5.1.13 Event codes

Formatted: Font color: Auto, Not Hidden

- Default report view on zoom when clicking on a table item: Overview

Formatted: Font color: Auto, Not Hidden

Formatted: Font color: Auto, Not Hidden

Event code	Events		0 - 100 %
1538	231,157	30.1 %	
21	210,241	27.4 %	
332	66,288	8.6 %	
4528	30,747	4.0 %	
54308	21,095	2.8 %	
6576	20,897	2.7 %	
76969	19,872	2.6 %	
8540	18,361	2.4 %	
9577	16,661	2.2 %	
10490	14,085	1.8 %	
372 other items	117,440	15.3 %	

WITHDRAWN

FUJ00155413

Total	766,844	100 %

WITHDRAWN

FUJ00155413

5.1.14 Actions

Formatted: Font color: Auto, Not Hidden

Default report view on zoom when clicking on a table item: Overview

Formatted: Font color: Auto, Not Hidden

Formatted: Font color: Auto, Not Hidden

Action	Events		0 - 100 %
1User Logoff	188,471	76.6 %	
2Successful Logon	27,695	11.2 %	
3Successful Network Logon	18,361	7.5 %	
4File Open	11,663	4.7 %	
Total	**246,190**	**100 %**	

5.1.15 Username

Default report view on zoom when clicking on a table item: Overview

Formatted: Font color: Auto, Not Hidden

Formatted: Font color: Auto, Not Hidden

Formatted: Font color: Auto, Not Hidden

Username	Events		0 - 100 %
1Administrator	174,867	71.0 %	
IRRELEVANT	19,035	7.7 %	
	15,646	6.4 %	
	7,421	3.0 %	

WITHDRAWN

FUJ00155413

IRRELEVANT	4,490	1.8 %	
	4,207	1.7 %	
	2,385	1.0 %	
	1,988	0.8 %	

IRRELEVANT	1,877	0.8 %	
	1,874	0.8 %	
185 other items	12,400	5.0 %	
Total	246,[illegible]	[illegible]	

WITHDRAWN

FUJ00155413

5.1.16 Domains

Formatted: Font color: Auto, Not Hidden

- Default report view on zoom when clicking on a table item: Overview

Formatted: Font color: Auto, Not Hidden

Formatted: Font color: Auto, Not Hidden

Domain	Events	0 - 100 %
IRRELEVANT	17,536	7.5 %
	10,341	4.4 %
	8,742	3.7 %
	6,940	3.0 %
	4,094	1.7 %
	3,968	1.7 %
	3,902	1.7 %
	3,421	1.5 %
	3,421	1.5 %
	3,409	1.5 %
110 other items	168,753	72.0 %

WITHDRAWN

FUJ00155413

Total	234,527	100 %

WITHDRAWN

FUJ00155413

5.1.17 Login ids

Formatted: Font color: Auto, Not Hidden

- Default report view on zoom when clicking on a table item: Overview

Formatted: Font color: Auto, Not Hidden

Formatted: Font color: Auto, Not Hidden

Login_id	Events		0 - 100 %
IRRELEVANT	2	0.0 %	
	1	0.0 %	
	1	0.0 %	
	1	0.0 %	
	1	0.0 %	
	1	0.0 %	
	1	0.0 %	
	1	0.0 %	
	1	0.0 %	
	1	0.0 %	
46045 other items	46,045	100.0 %	

WITHDRAWN

FUJ00155413

Total	46,056	100 %

WITHDRAWN

FUJ00155413

5.1.18 Login types

Formatted: Font color: Auto, Not Hidden

- Default report view on zoom when clicking on a table item: Overview

Formatted: Font color: Auto, Not Hidden

Formatted: Font color: Auto, Not Hidden

Login_type	Events		0 - 100 %
12	198,160	84.5 %	
23	31,776	13.5 %	
34	3,986	1.7 %	
47	396	0.2 %	
55	209	0.1 %	
Total	234,527	100 %	

WITHDRAWN

FUJ00155413

5.1.19 Auth pkgs

Formatted: Font color: Auto, Not Hidden

- Default report view on zoom when clicking on a table item: Overview

Formatted: Font color: Auto, Not Hidden

Formatted: Font color: Auto, Not Hidden

Auth_pkg	Events	0 - 100 %
1MICROSOFT_AUTHENTICATION_PACKAGE_V1_0	18,922	41.1 %
2NTLM	18,361	39.9 %
3TivoliAP	8,[illegible]	1[illegible] %
4Negotiate	367	0.8 %
Total	[illegible]56	**100 %**

WITHDRAWN

FUJ00155413

5.1.20 File names

Formatted: Font color: Auto, Not Hidden

- Default report view on zoom when clicking on a table item: Overview

Formatted: Font color: Auto, Not Hidden

Formatted: Font color: Auto, Not Hidden

File name	Events		0 - 100 %
1C:\WINNT\system32\RedPike.dll	4,525	38.8 %	
C:\Cryptography\bin\KMAgent.IN 2I	3,342	28.7 %	
C:\Cryptography\bin\CryptoAPI.i 3ni	2,648	22.[illegible] %	
4C:\Cryptography\keys	404	3.5 %	
5C:\Cryptography\bin	[illegible]	1.[illegible]	
6C:\sshadmin	97	0.8 %	
7C:\Support\Tools\SMCSUP	50	0.4 %	
8C:\Support\Tools\SSCSUP	50	0.4 %	
9C:\Support\Tools\SYSMANSUP	50	0.4 %	
C:\Support\Tools\Generic\NTRes 10kit	50	0.4 %	
56 other items	285	2.4 %	

WITHDRAWN

FUJ00155413

Total	11,663	100 %

5.1.21 Messages

Formatted: Font color: Auto, Not Hidden

Overview

Default report view on zoom when clicking on a table item

Formatted: Font color: Auto, Not Hidden

Formatted: Font color: Auto, Not Hidden

Message	Events		0 - 100 %
1EACRR spostemsg	66,283	12.4 %	
2VPN Server Ping Success monid:vpn_route monsev:G	16,560	3.1 %	
Riposte function 'RiposteConnect' failed. The RPC server is unavailable. 3(0x6BA).	11,821	2.2 %	
The authentication string '/L=P /O=3221' for IP address IRRELEVANT does 4not match '/C=44 /CN=E /STA=65535 /L=P /PN=1000...	3,014	0.6 %	
5MONID:APOP.BO01.SVR MONSEV:G	2,463	0.5 %	
6MONID:APOP.BO.SVR MONSEV:G	2,463	0.5 %	
7MONID:APOP.BO02.SVR MONSEV:G	2,462	0.5 %	
8MONID:BBND.BO.SVR MONSEV:G	2,462	0.5 %	
9MONID:MGRM.BO02.SVR MONSEV:G	2,460	0.5 %	

FUJ00155413

10MONID:BBND.BO01.SVR MONSEV:G	2,459	0.5 %	
116113 other items	422,669	79.0 %	
Total	535,116	100 %	

© 2008 Flowerfire

WITHDRAWN

5.2 Summary Analysis of a Window 2k/XP CSV log export

5.2.1 Summary

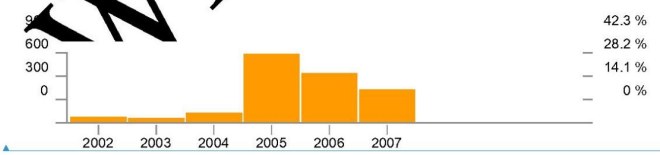
Statistics for **09/Oct/2002 - 15/Nov/2007**, 1864 days

5.2.2 Overview

	All days	Average per day
Events	2,130	

5.2.3 Years/months/days

Events



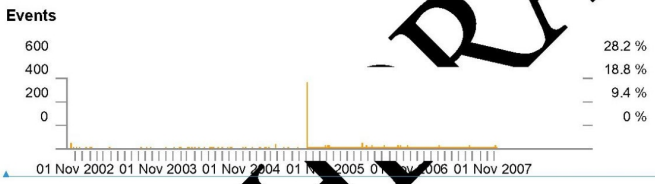
Formatted: Font color: Auto

Date/time	Events

FUJ00155413

1	2002	59
2	2003	41
3	2004	118
4	2005	879
5	2006	618
6	2007	415
	Total	**2,130**

5.2.4 Days



	Date/time	Events
1	09/Oct/2002	9
2	14/Oct/2002	38
3	21/Oct/2002	6
4	05/Nov/2002	1
5	14/Nov/2002	4
6	16/Dec/2002	1

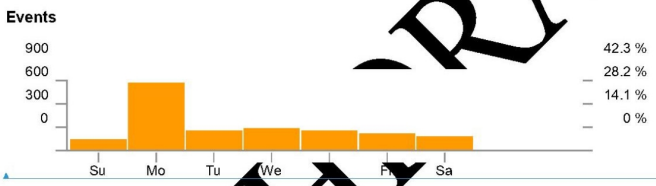
WITHDRAWN

Formatted: Font color: Auto

FUJ00155413

7	05/Jan/2003	2
8	09/Jan/2003	5
9	29/Mar/2003	1
10	14/Aug/2003	5
	531 other items	2,058
	Total	2,130

5.2.5 Day of weeks



	Day of week	Events
1	Sunday	[illegible]
2	Monday	854
3	Tuesday	237
4	Wednesday	281
5	Thursday	246
6	Friday	211

WITHDRAWN

Formatted: Font color: Auto

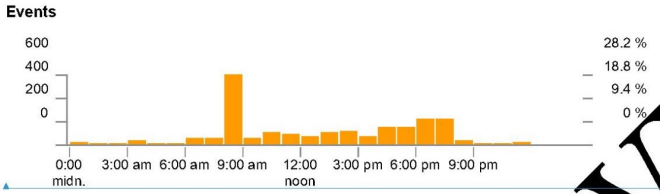
FUJ00155413

7	Saturday	167
	Total	2,130

WITHDRAWN

FUJ00155413

5.2.6 Hour of days



Formatted: Font color: Auto

	Hour of day	Events
1	midnight - 1:00 AM	19
2	1:00 AM - 2:00 AM	3
3	2:00 AM - 3:00 AM	9
4	3:00 AM - 4:00 AM	25
5	4:00 AM - 5:00 AM	7
6	5:00 AM - 6:00 AM	11
7	6:00 AM - 7:00 AM	48
8	7:00 AM - 8:00 AM	58
9	8:00 AM - 9:00 AM	592
10	9:00 AM - 10:00 AM	58
11	10:00 AM - 11:00 AM	97
12	11:00 AM - noon	85
13	noon - 1:00 PM	68
14	1:00 PM - 2:00 PM	95
15	2:00 PM - 3:00 PM	110
16	3:00 PM - 4:00 PM	66
17	4:00 PM - 5:00 PM	143
18	5:00 PM - 6:00 PM	144
19	6:00 PM - 7:00 PM	212
20	7:00 PM - 8:00 PM	215
21	8:00 PM - 9:00 PM	25
22	9:00 PM - 10:00 PM	14
23	10:00 PM - 11:00 PM	6
24	11:00 PM - midnight	20
	Total	**2,130**

WITHDRAWN

FUJ00155413

5.2.7 Sources

Formatted: Font color: Auto, Not Hidden

Default report view on zoom when clicking on a table item: Single-page Summary Hierarchy

Formatted: Font color: Auto, Not Hidden

Formatted: Font color: Auto, Not Hidden

Source	Events		0 - 100 %
1Application Popup	581	27.3 %	
2Automatic Updates	394	18.5 %	
3Removable Storage Service	392	18.4 %	
4RCONSVC	156	7.3 %	
5WMDM PMSP Service	85	4.0 %	
6EvntAgnt	84	3.9 %	
7EventLog	77	3.[illegible] %	
8Active Server Pages	64	3.0 %	
9MsiInstaller	34	1.6 %	
10FTPCtrs	34	1.6 %	
27 other items	229	10.8 %	
Total	2,130	100 %	

WITHDRAWN

FUJ00155413

5.2.8 Types

Default report view on zoom when clicking on a table item: Overview

Formatted: Font color: Auto, Not Hidden
Formatted: Font color: Auto, Not Hidden
Formatted: Font color: Auto, Not Hidden

Type	Events		0 - 100 %
1Information	1,491	70.0 %	
2Warning	563	26.4 %	
3Error	76	3.6 %	
Total	2,130	100 %	

5.2.9 Categories

Formatted: Font color: Auto, Not Hidden

Default report view on zoom when clicking on a table item: Overview

Formatted: Font color: Auto, Not Hidden
Formatted: Font color: Auto, Not Hidden

Category	Events		0 - 100 %
1None	1,[illegible]23	80.[illegible]	
2Download	394	18.5 %	
3CRM	[illegible]5	0.2 %	
4SVC	4	0.2 %	
5Devices	3	0.1 %	
6Firing Agent	1	0.0 %	

WITHDRAWN

FUJ00155413

Total	2,130	100 %

WITHDRAWN

FUJ00155413

5.2.10 Events

Formatted: Font color: Auto, Not Hidden

- Default report view on zoom when clicking on a table item: Overview

Formatted: Font color: Auto, Not Hidden

Formatted: Font color: Auto, Not Hidden

Event	Events		0 - 100 %
126	581	27.3 %	
216	394	18.5 %	
3135	173	8.1 %	
4134	173	8.1 %	
5105	88	4.1 %	
62018	80	3.8 %	
72004	78	3.7 %	
82006	78	3.7 %	
93	64	[illegible] %	
101000	50	2.3 %	
42 other items	371	[illegible] %	
Total	[illegible]	100 %	

WITHDRAWN

FUJ00155413

5.2.11 Users

Formatted: Font color: Auto, Not Hidden

Default report view on zoom when clicking on a table item: Overview

Formatted: Font color: Auto, Not Hidden

Formatted: Font color: Auto, Not Hidden

User	Events		0 - 100 %
IRRELEVANT	2,124	99.7 %	
	6	0.3 %	
Total	2,130	100 %	

5.2.12 Computers

Formatted: Font color: Auto, Not Hidden

Default report view on zoom when clicking on a table item: Overview

Formatted: Font color: Auto, Not Hidden

Formatted: Font color: Auto, Not Hidden

Computer	Events		0 - 100 %
IRRELEVANT	[illegible]	89.5 %	
	164	7.7 %	
	[illegible]	2.3 %	
	6	0.3 %	
	4	0.2 %	
Total	2,130	100 %	

DRAWN

FUJ00155413

5.2.13 Descriptions

Formatted: Font color: Auto, Not Hidden

- Default report view on zoom when clicking on a table item: Overview

Formatted: Font color: Auto, Not Hidden

Formatted: Font color: Auto, Not Hidden

Description	Events	0 - 100 %
1Application popup: ping.exe - DLL Initialization Failed : The application failed to initialize because the window statio...	547	25.7 %
2Unable to connect: Windows is unable to connect to the Automatic Updates service and therefore cannot download and insta...	394	18.5 %
3Received a device interface ARRIVAL notification for device:	173	8.1 %
4Received a device interface REMOVAL notification for device:	173	8.1 %
5The service was started.	85	4.0 %
6SNMP Event Log Extension Agent is starting.	80	3.8 %
7The description for Event ID (2000) in Source (RCONSVC) cannot be found. The local computer may not have the necessa...	78	3.7 %
8Service started.	64	3.0 %
9The description for Event ID (2000) in Source (RCONSVC) cannot be found. The local computer may not have the necessa...	45	2.1 %
10Received Handle Query Remove notification.	43	2.0 %
135 other items	448	21.0 %
Total	2,130	100 %

WITHDRAWN

FUJ00155413

5.3 Summary Analysis of a Cisco Firewall/Router/Switches syslog

5.3.1 Summary

Statistics for **16/Jan/2008**, 1 day

5.3.2 Overview

	All days	Average per day
Events	5,530	-
Page views	5,529	-
Unique source IPs	96	-
Bytes	0 b	-
Destination bytes	0 b	-
Duration	08:53:42	-

WITHDRAWN

FUJ00155413

5.3.3 Years/months/days

Events

Years/months/days

	Date/time	Events	Page views	Unique source IPs	Bytes	Destination bytes	Duration
1	2008	5,530	5,529	96	0 b	0 b	08:53:42
	Total	5,530	5,529	96	0 b	0 b	08:53:42

WITHDRAWN

FUJ00155413

5.3.4 Days

Events

Days

	Date/time	Events	Page views	Unique source IPs	Bytes	Destination bytes	Duration
1	16/Jan/2008	5,530	5,529	96	0 b	0 b	08:53:42
	Total	5,530	5,529	96	0 b	0 b	08:53:42

WITHDRAWN

FUJ00155413

5.3.5 Day of weeks

Day of weeks

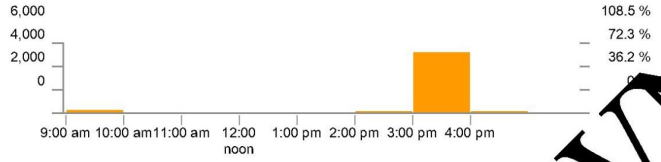
	▲ Day of week	Events	Page views	Unique source IPs	Bytes	Destination bytes	Duration
1	Wednesday	5,530	5,529	96	0 b	0 b	08:53:42
	Total	5,530	5,529	96	0 b	0 b	08:53:42

WITHDRAWN

FUJ00155413

5.3.6 Hour of days

Events



Hour of days

	Hour of day	Events	Page views	Unique source IPs	Bytes	Destination bytes	Duration
1	9:00 AM - 10:00 AM	233	233	17	0 b	0 b	08:44:48
2	2:00 PM - 3:00 PM	71	71	4	0 b	0 b	00:00:00
3	3:00 PM - 4:00 PM	5,116	5,115	80	0 b	0 b	00:08:54
4	4:00 PM - 5:00 PM	110	110	7	0 b	0 b	00:00:00
	Total	5,530	5,529	96	0 b	0 b	08:53:42

WITHDRAWN

FUJ00155413

5.3.7 Logging Devices

Logging devices

- Default report view on zoom when clicking on a table item: Overview

Logging device	Events		0 - 100 %	Page views	Unique source IPs	Bytes	Destination bytes	Duration
IRRELEVANT	504	9.1 %		504	[illegible]	[illegible]	0 b	00:00:00
	430	7.8 %		430	1	0 b	0 b	00:00:00
	428	7.7 %		[illegible]	1	0 b	0 b	00:00:00
	409	7.4 %		409	27	0 b	0 b	00:00:00
	363	[illegible] %		362	3	0 b	0 b	00:00:00
	315	5.7 %		315	1	0 b	0 b	00:00:00
	[illegible]	5.3 %		295	1	0 b	0 b	00:00:00
	289	5.2 %		289	1	0 b	0 b	00:00:00
	270	4.9 %		270	32	0 b	0 b	00:00:00
[illegible]	233	4.2 %		233	17	0 b	0 b	08:44:48
36	1,994	36.1 %		1,994	-	0 b	0 b	00:08:54

FUJ00155413

other items								
Total	5,530	100 %		5,529	96	0 b	0 b	08:53:42

5.3.8 Operations

Operations

- Default report view on zoom when clicking on a table item: Overview

Operation	Events		0 - 100 %	Page views	Unique source IPs	Bytes	Destination bytes	Duration
1Teardown	2,230	54.7 %		2,230	90	0 b	0 b	08:53:42
2Built	1,794	44.0 %		1,794	1	0 b	0 b	00:00:00
3Deny	46	1.1 %		46	5	0 b	0 b	00:00:00
Accessed 4URL	5	0.1 %		4	3	0 b	0 b	00:00:00
Total	**4,075**	**100 %**		**4,074**	**94**	**0 b**	**0 b**	**08:53:42**

5.3.9 Messages

Messages

- Default report view on zoom when clicking on a table item: Overview

WITHDRAWN

FUJ00155413

Message	Events	0 - 100 %	Page views	Unique source IPs	Bytes	Destination bytes	Duration
Total	0	100 %	0	0	0 b	0 b	00:00:00

WITHDRAWN

FUJ00155413

5.3.10 Message codes

Message codes

Default report view on zoom when clicking on a table item: Overview

Message code	Events	0 - 100 %	Page views	Destination	Events	Bytes								
IRRELEVANT	854	15.4 %	854	IRRELEVANT	327	0 b	5.9 %	0 b	00:00:00	327	1	0 b	0 b	00:00:00
					326	0 b	5.9 %	0 b	00:00:00	326	1	0 b	0 b	00:00:00
	849	15.4 %	849		244	0 b	4.4 %			244	63	0 b	0 b	00:00:00
	485	8.8 %	485		236	0 b	4.3 %	0 b	00:00:00	236	1	0 b	0 b	00:00:00
	469	8.5 %	469	36 other items	976	0 b	17.6 %	0 b	00:00:00	975	-	0 b	0 b	08:53:42
	424	7.7 %	424	Total	5,530	0 b	100 %	0 b	00:00:00	5,529	96	0 b	0 b	08:53:42
	340	6.1 %	340	1	1	0 b		0 b	00:00:00					

FUJ00155413

5.3.11 Protocols

Protocols

Default report view on zoom when clicking on a table item: Overview

Protocol	Events		0 - 100 %	Page views	Unique source IPs	Bytes	Destination bytes	Duration
1TCP	2,726	67.0 %		2,726	19	0 b	0 b	00:00:00
2UDP	978	24.0 %		978	65	0 b	0 b	00:00:00
3ICMP	339	8.3 %		339	3	0 b	0 b	00:00:00
local-4host	21	0.5 %		21	19	0 b	0 b	08:53:42
5static	5	0.1 %		5	1	0 b	0 b	00:00:00
6dynamic	1	0.0 %		1	1	0 b	0 b	00:00:00
Total	**4,070**	**100 %**		**4,070**	**92**	**0 b**	**0 b**	**08:53:42**

WITHDRAWN

FUJ00155413

5.3.12 Source IPs

Source IPs

Default report view on zoom when clicking on a table item: Single-page Summary Hierarchy

Source IP	Events		0 - 100 %	Page views	Unique source IPs	Bytes	Destination bytes	Duration
IRRELEVANT	140	22.9 %		140	[illegible]	0 b	0 b	00:00:00
	38	6.2 %		38	1	0 b	0 b	00:00:00
	37	6.0 %		37	1	0 b	0 b	00:00:00
	37	6.0 %		37	1	0 b	0 b	00:00:00
	37	6.0 %		37	1	0 b	0 b	00:00:00
	34	5.6 %		34	1	0 b	0 b	00:00:00
	34	5.6 %		34	1	0 b	0 b	00:00:00
	20	3.3 %		20	1	0 b	0 b	00:00:00
	[illegible]	3.1 %		19	1	0 b	0 b	00:00:00
	16	2.6 %		16	1	0 b	0 b	00:00:00
85 other items	200	32.7 %		199	-	0 b	0 b	08:53:42
Total	612	100 %		611	95	0 b	0 b	08:53:42

FUJ00155413

5.3.13 Destination IPs

Destination IPs

Default report view on zoom when clicking on a table item: Overview

Destination IP	Events		0 - 100 %	Page views	Unique source IPs	Bytes	Destination bytes	Duration
IRRELEVANT	6	27.3 %		6	1	0 b	0 b	00:00:00
	3	13.6 %		2	2	0 b	0 b	00:00:00
	2	9.1 %		1	1	0 b	0 b	00:00:00
	1	4.5 %		1	1	0 b	0 b	00:00:00
	1	4.5 %		1	1	0 b	0 b	00:00:00
	1	4.5 %		1	1	0 b	0 b	00:00:00
	1	4.5 %		1	1	0 b	0 b	00:00:00
	1	4.5 %		1	1	0 b	0 b	00:00:00
		4.5 %		1	1	0 b	0 b	00:00:00
	1	4.5 %		1	1	0 b	0 b	00:00:00
4 other items	4	18.2 %		4	-	0 b	0 b	00:00:00
Total	22	100 %		21	9	0 b	0 b	00:00:00

FUJ00155413

5.3.14 Source hostnames

Source hostnames

Default report view on zoom when clicking on a table item: Overview

Source hostname	Events	0 - 100 %	Page views	Unique source IPs	Bytes	Destination bytes	Duration
Total	0	100 %	0	0	0 b	0 b	00:00:00

5.3.15 Destination hostnames

Destination hostnames

Default report view on zoom when clicking on a table item: Overview

Destination hostname	Events	0 - 100 %	Page views	Unique source IPs	Bytes	Destination bytes	Duration
Total	0	100 %	0	0	0 b	0 b	00:00:00

WITHDRAWN

FUJ00155413

5.3.16 Source ports

Source ports

Default report view on zoom when clicking on a table item: Overview

Source port	Events		0 - 100 %	Page views	Unique source IPs	Bytes	Destination bytes	Duration
17561	140	24.3 %		140	1	0 b	0 b	00:00:00
2161	129	22.4 %		129	55	0 b	0 b	00:00:00
3123	16	2.8 %		16	12	0 b	0 b	00:00:00
41786	4	0.7 %		4	2	0 b	0 b	00:00:00
51783	4	0.7 %		4	2	0 b	0 b	00:00:00
61789	4	0.7 %		4	2	0 b	0 b	00:00:00
71774	4	0.7 %		4	2	0 b	0 b	00:00:00
81780	4	0.7 %		4	2	0 b	0 b	00:00:00
91[illegible]	4	0.7 %		4	2	0 b	0 b	00:00:00
1034195	4	0.7 %		4	1	0 b	0 b	00:00:00
151 other items	263	45.7 %		263	-	0 b	0 b	00:00:00
Total	576	100 %		576	70	0 b	0 b	00:00:00

FUJ00155413

5.3.17 Destination ports

Destination ports

Default report view on zoom when clicking on a table item: Overview

Destination port	Events		0 - 100 %	Page views	Unique source IPs	Bytes	Destination bytes	Duration
1138	6	85.7 %		6	1	0 b	0 b	00:00:00
2949	1	14.3 %		1	1	0 b	0 b	00:00:00
Total	7	100 %		7	1	0 b	0 b	00:00:00

WITHDRAWN

FUJ00155413

5.3.18 Source sides

Source sides

Default report view on zoom when clicking on a table item: Overview

Source side	Events		0 - 100 %	Page views	Unique source IPs	Bytes	Destination bytes	Duration
IRRELEVANT	528	88.4 %		528	56	0 b	0 b	00:00:00
	39	6.5 %		39	9	0 b	0 b	00:00:00
	15	2.5 %		[illegible]	13	0 b	0 b	00:25:02
	5	0.8 %		5	3	0 b	0 b	00:00:00
	4	0.7 %		4	2	0 b	0 b	00:00:00
	3	0.5 %		3	3	0 b	0 b	00:08:54
	3	0.5 %		3	3	0 b	0 b	08:19:46
Total	597	100 %		597	89	0 b	0 b	08:53:42

WITHDRAWN

FUJ00155413

5.3.19 Destination sides

Destination sides

Default report view on zoom when clicking on a table item: Overview

Destination side	Events	0 - 100 %	Page views	Unique source IPs	Bytes	Destination bytes	Duration
IRRELEVANT	7	100.0 %	7	1	0 b	0 b	00:00:00
Total	7	100 %	7	1	0 b	0 b	00:00:00

5.3.20 Geographic locations

Geographic locations

Default report view on zoom when clicking on a table item: Single-page Summary Hierarchy

Geographic location	Events	0 - 100 %	Page views	Unique source IPs	Bytes	Destination bytes	Duration
Total	0	100 %	0	0	0 b	0 b	00:00:00

5.3.21 Interfaces

Interfaces

WITHDRAWN

FUJ00155413

- Default report view on zoom when clicking on a table item: Overview

Interface	Events	0 - 100 %	Page views	Unique source IPs	Bytes	Destination bytes	Duration
1dmz	1 100.0 %		1	1	0 b	0 b	00:00:00
Total	1 100 %		1	1	0 b	0 b	00:00:00

5.3.22 Directions

Directions

Default report view on zoom when clicking on a table item: Overview

Direction	Events	0 - 100 %	Page views	Unique source IPs	Bytes	Destination bytes	Duration
1outbound	891 56.3 %		891	1	0 b	0 b	00:00:00
2inbound	691 43.7 %		691	1	0 b	0 b	00:00:00
Total	1,582 100 %		1,582	1	0 b	0 b	00:00:00

WITHDRAWN

FUJ00155413

5.3.23 Foreign IPs

Foreign IPs

Default report view on zoom when clicking on a table item: Overview

Foreign IP	Events		0 - 100 %	Page views	Unique source IPs	Bytes	Destination bytes	Duration
IRRELEVANT	152	10.9 %		152	[illegible]	0 b	0 b	00:00:00
	96	6.9 %		96	1	0 b	0 b	00:00:00
	59	4.2 %		[illegible]	1	0 b	0 b	00:00:00
	52	3.7 %		52	1	0 b	0 b	00:00:00
	38	2.7 %		38	1	0 b	0 b	00:00:00
	37	2.7 %		37	1	0 b	0 b	00:00:00
	[illegible]	2.7 %		37	1	0 b	0 b	00:00:00
	37	2.7 %		37	1	0 b	0 b	00:00:00
	[illegible]	2.4 %		34	1	0 b	0 b	00:00:00
	34	2.4 %		34	1	0 b	0 b	00:00:00
157 other items	818	58.7 %		818	-	0 b	0 b	00:00:00
Total	1,394	100 %		1,394	1	0 b	0 b	00:00:00

FUJ00155413

5.3.24 Foreign ports

Foreign ports

Default report view on zoom when clicking on a table item: Overview

Foreign port	Events		0 - 100 %	Page views	Unique source IPs	Bytes	Destination bytes	Duration
1161	233	16.7 %		233	1	0 b	0 b	00:00:00
20	222	15.9 %		222	1	0 b	0 b	00:00:00
37328	156	11.2 %		156	1	0 b	0 b	00:00:00
427324	98	7.0 %		98	1	0 b	0 b	00:00:00
580	67	4.8 %		67	1	0 b	0 b	00:00:00
618191	49	3.5 %		49	1	0 b	0 b	00:00:00
7123	35	2.5 %		35	1	0 b	0 b	00:00:00
81772	34	2.4 %		34	1	0 b	0 b	00:00:00
92[illegible]95	[illegible]	[illegible].7 %		10	1	0 b	0 b	00:00:00
101315	6	0.4 %		6	1	0 b	0 b	00:00:00
215 other items	484	34.7 %		484	-	0 b	0 b	00:00:00
Total	1,394	100 %		1,394	1	0 b	0 b	00:00:00

FUJ00155413

5.3.25 Global IPs

Global IPs

Default report view on zoom when clicking on a table item: Overview

Global IP	Events	0 - 100 %	Page views	Unique source IPs	Bytes	Destination bytes	Duration
Total	0	100 %	0	0	0 b	0 b	00:00:00

5.3.26 Global ports

Global ports

Default report view on zoom when clicking on a table item: Overview

Global port	Events	0 - 100 %	Page views	Unique source IPs	Bytes	Destination bytes	Duration
Total	0	100 %	0	0	0 b	0 b	00:00:00

5.3.27 Local IPs

Local IPs

Default report view on zoom when clicking on a table item: Overview

WITHDRAWN

FUJ00155413

Local IP	Events	0 - 100 %	Page views	Unique source IPs	Bytes	Destination bytes	Duration
Total	0	100 %	0	0	0 b	0 b	00:00:00

WITHDRAWN

FUJ00155413

5.3.28 Local ports

Local ports

Default report view on zoom when clicking on a table item: Overview

Local port	Events	0 - 100 %	Page views	Unique source IPs	Bytes	Destination bytes	Duration
Total	0	100 %	0	0	0 b	0 b	00:00:00

5.3.29 Service names

Service names

Default report view on zoom when clicking on a table item: Overview

Service name	Events	0 - 100 %	Page views	Unique source IPs	Bytes	Destination bytes	Duration
113[illegible]_(empty)	[illegible]	85.7 %	6	1	0 b	0 b	00:00:00
2949_(empty)	1	14.3 %	1	1	0 b	0 b	00:00:00
Total	7	100 %	7	92	0 b	0 b	00:00:00

WITHDRAWN

FUJ00155413

5.3.30 URLs/directories

URLs/directories

Default report view on zoom when clicking on a table item: Single-page Summary Hierarchy

URL	Events	0 - 100 %	Page views	Unique source IPs	Bytes	Destination bytes	Duration
IRRELEVANT	1 20.0 %		1	1	0 b	0 b	00:00:00
	1 20.0 %		1	1	0 b	0 b	00:00:00
	1 20.0 %		1	1	0 b	0 b	00:00:00
	1 20.0 %		0	1	0 b	0 b	00:00:00
	1 20.0 %		1	1	0 b	0 b	00:00:00
Total	5 100 %		4	3	0 b	0 b	00:00:00

WITHDRAWN

FUJ00155413

5.3.31 URLs

URLs

Default report view on zoom when clicking on a table item: Overview

URL	Events	0 - 100 %	Page views	Unique source IPs	Bytes	Destination bytes	Duration
IRRELEVANT	20.0 %		1	1	0 b	0 b	00:00:00
	20.0 %		1	1	0 b	0 b	00:00:00
	[illegible]		1	1	0 b	0 b	00:00:00
	20.0 %		0	1	0 b	0 b	00:00:00
	20.0 %		1	1	0 b	0 b	00:00:00
Total	5 100 %		4	3	0 b	0 b	00:00:00

WITHDRAWN

FUJ00155413

5.3.32 Flags

Flags

Default report view on zoom when clicking on a table item: Overview

Flags	Events	0 - 100 %	Page views	Unique source IPs	Bytes	Destination bytes	Duration
Total	0	100 %	0	0	0 b	0 b	00:00:00

5.3.33 Users

Users

Default report view on zoom when clicking on a table item: Overview

User	Events	0 - 100 %	Page views	Unique source IPs	Bytes	Destination bytes	Duration
Total	0	100 %	0	0	0 b	0 b	00:00:00

WITHDRAWN

FUJ00155413

5.3.34 Commands

Commands

Default report view on zoom when clicking on a table item: Overview

Command	Events	0 - 100 %	Page views	Unique source IPs	Bytes	Destination bytes	Duration
Total	0	100 %	0	0	0 b	0 b	00:00:00

5.3.35 Types

Types

Default report view on zoom when clicking on a table item: Overview

Type	Events	0 - 100 %	Page views	Unique source IPs	Bytes	Destination bytes	Duration
1from	28	75.7 %	28	3	0 b	0 b	00:00:00
2src	9	24.3 %	9	1	0 b	0 b	00:00:00
Total	37	100 %	37	3	0 b	0 b	00:00:00

WITHDRAWN

FUJ00155413

5.3.36 Lists

Lists

Default report view on zoom when clicking on a table item: Overview

List	Events	0 - 100 %	Page views	Unique source IPs	Bytes	Destination bytes	Duration
Total	0	100 %	0	0	0 b	0 b	00:00:00

WITHDRAWN

FUJ00155413

5.3.37 Sessions overview

	All days	Average per d
Total accesses	113	-
Total sessions	109	
Sessions by one-time users	83	
Sessions by repeat users	26	
Total session users	96	
One-time users	83	
Repeat users	[illegible]	
Two-time users	13	
Three-time users	0	-

Four-time users	0	-
Five-time users	0	-
Six+-time users	0	-
Total duration of all sessions	00:43:44	-
Average accesses per session	1.04	-
Average sessions per user	1.14	-
Median sessions per user	1.00	-
Maximum concurrent sessions	2	-
Average session duration	00:00:24	-

WITHDRAWN

FUJ00155413

5.3.38 Entry pages

Entry pages

Page	Sessions	0 - 100 %
IRRELEVANT	107	98.2 %
IRRELEVANT	1	0.9 %
IRRELEVANT	[illegible]	[illegible]
Total	109	100 %

5.3.39 Exit pages

Exit pages

Page	Sessions	0 - 100 %
IRRELEVANT	107	98.2 %
IRRELEVANT	1	0.9 %
IRRELEVANT	1	0.9 %
Total	109	100 %

WITHDRAWN

WITHDRAWN

5.3.40 Session pages

Session pages

Page	Sessions		0 - 100 %	Events		0 - 100 %	Time spent		0 - 100 %
	107	96.4 %		109	96.5 %		00:43:44	100.0 %	
	1	0.9 %		1	0.9 %		00:00:00	0.0 %	
	1	0.9 %		1	0.9 %		00:00:00	0.0 %	
	1	0.9 %		1	0.9 %		00:00:00	0.0 %	
	1	0.9 %		1	0.9 %		00:00:00	0.0 %	
Total	111	100 %		113	100 %		00:43:44	100 %	

IRRELEVANT

FUJ00155413

5.3.41 Session users

Session users

Default report view on zoom when clicking on a table item: Overview

User	Sessions		0 - 100 %	Events		0 - 100 %	Time spent		0 - 100 %
IRRELEVANT	2	1.8 %		2	1.8 %		00:00:00	0.0 %	
	2	1.8 %		2	1.8 %		00:00:00	0.0 %	
	2	1.8 %		[illegible]	[illegible]		00:00:00	0.0 %	
	2	1.8 %		2	1.8 %		00:00:00	0.0 %	
	2	1.8 %		2	1.8 %		00:00:00	0.0 %	
	2	1.8 %		2	1.8 %		00:00:00	0.0 %	
	2	1.8 %		2	1.8 %		00:00:00	0.0 %	
	2	1.8 %		2	1.8 %		00:00:00	0.0 %	
	2	1.8 %		2	1.8 %		00:00:00	0.0 %	
10(empty)	2	1.8 %		6	5.3 %		00:43:44	100.0 %	
86 other items	89	81.7 %		89	78.8 %		00:00:00	0.0 %	
Total	109	100 %		113	100 %		00:43:44	100 %	

© 2008 Flowerfire

5.3.41.1 Loading document, please wait.

5.4 Summary Analysis of a UNIX Solaris 9.0 syslog

5.4.1 Overview

	All days	Average per day
Messages	1,711	213.88

5.4.2 Years/months/days

Messages

Years/months/days

	Date/time	Messages
1	2008	1,711
	Total	1,711

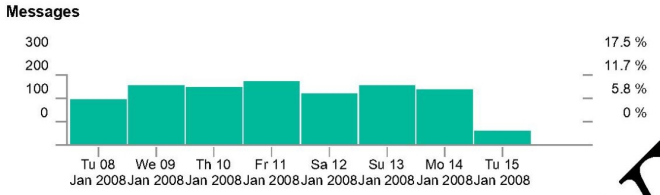
WITHDRAWN

FUJ00155413

WITHDRAWN

FUJ00155413

5.4.3 Days



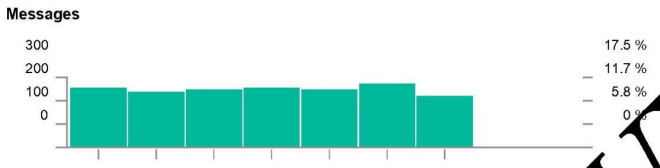
Days

	Date/time	Messages
1	08/Jan/2008	189
2	09/Jan/2008	251
3	10/Jan/2008	247
4	11/Jan/2008	265
5	12/Jan/2008	216
6	13/Jan/2008	251
7	14/Jan/2008	234
8	15/Jan/2008	58
	Total	1,711

WITHDRAWN

FUJ00155413

5.4.4 Day of weeks



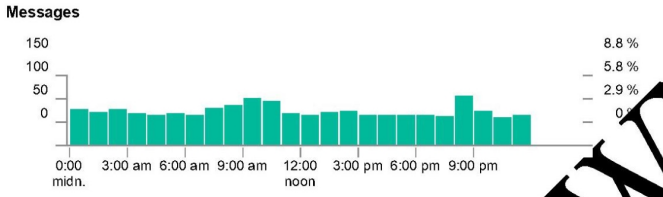
Day of weeks

	Day of week	Messages
1	Sunday	251
2	Monday	234
3	Tuesday	247
4	Wednesday	251
5	Thursday	247
6	Friday	265
7	Saturday	216
	Total	1,711

WITHDRAWN

FUJ00155413

5.4.5 Hour of days



WITHDRAWN

FUJ00155413

Hour of days

Hour of day	Messages
1 midnight - 1:00 AM	74
2 1:00 AM - 2:00 AM	68
3 2:00 AM - 3:00 AM	75
4 3:00 AM - 4:00 AM	67
5 4:00 AM - 5:00 AM	63
6 5:00 AM - 6:00 AM	67
7 6:00 AM - 7:00 AM	63
8 7:00 AM - 8:00 AM	79
9 8:00 AM - 9:00 AM	83
10 9:00 AM - 10:00 AM	98
11 10:00 AM - 11:00 AM	93
12 11:00 AM - noon	66
13 noon - 1:00 PM	[illegible]
14 1:00 PM - 2:00 PM	70
15 2:00 PM - 3:00 PM	73
16 3:00 PM - 4:00 PM	64
17 4:00 PM - 5:00 PM	63
18 5:00 PM - 6:00 PM	63
19 6:00 PM - 7:00 PM	63
20 7:00 PM - 8:00 PM	60
21 8:00 PM - 9:00 PM	105
22 9:00 PM - 10:00 PM	72
23 10:00 PM - 11:00 PM	56
24 11:00 PM - midnight	63
Total	1,711

WITHDRAWN

FUJ00155413

5.4.6 Logging devices

Logging devices

Logging device	Messages		0 - 100 %
IRRELEVANT	1,711	100.0 %	
Total	1,711	100 %	

WITHDRAWN

5.4.7 Syslog messages

Syslog messages

Syslog message	Messages		0 - 100 %
	754	[illegible]	
	523	30.6 %	
	192	11.2 %	
	12	0.7 %	
	10	0.6 %	
	9	0.5 %	
	7	0.4 %	
	7	0.4 %	
	7	0.4 %	
	7	0.4 %	
126 other items	183	10.7 %	
Total	1,711	100 %	

IRRELEVANT

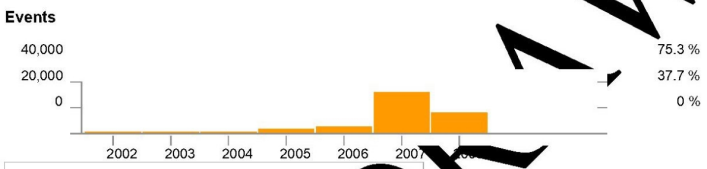
FUJ00155413

5.5 Summary Analysis of Windows NT Event Logs

5.5.1 Overview

	All days	Average per day
Events	53,096	21.03

5.5.2 Years/months/days



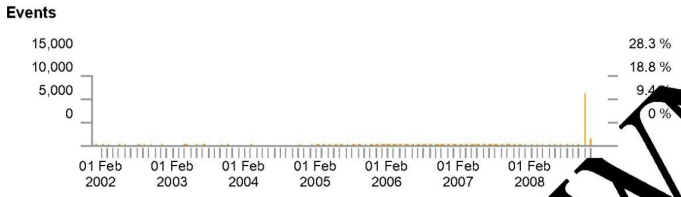
Years/months/days

	Date/time	Events
1	2002	522
2	2003	112
3	2004	17
4	2005	2,381
5	2006	4,667
6	2007	30,601
7	2008	14,796

WITHDRAWN

Total	53,096

5.5.3 Days



Days

	Date/time	Events
1	03/Jan/2002	20
2	08/Jan/2002	2
3	08/Feb/2002	10
4	08/Mar/2002	1
5	03/May/2002	3
6	04/Jun/2002	333
7	08/Aug/2002	4
8	10/Sep/2002	1
9	12/Oct/2002	26
10	08/Dec/2002	122

WITHDRAWN

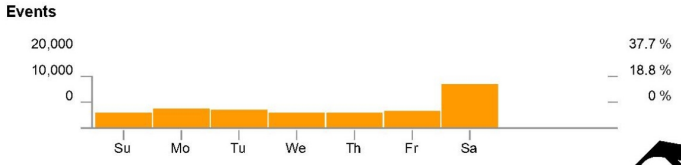
FUJ00155413

381 other items	52,574
Total	53,096

WITHDRAWN

FUJ00155413

5.5.4 Day of weeks



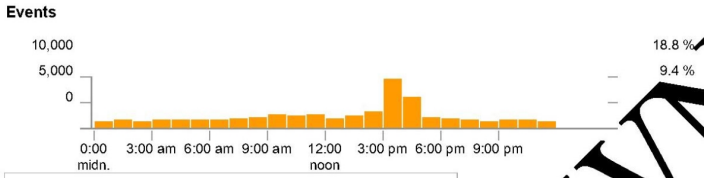
Day of weeks

	Day of week	Events
1	Sunday	5,681
2	Monday	7,214
3	Tuesday	6,499
4	Wednesday	5,544
5	Thursday	5,53[illegible]
6	Friday	5,965
7	Saturday	16,6[illegible]5
	Total	53,096

WITHDRAWN

FUJ00155413

5.5.5 Hour of days



Hour of days

Hour of day	Events
1 midnight - 1:00 AM	1,301
2 1:00 AM - 2:00 AM	1,382
3 2:00 AM - 3:00 AM	1,23[illegible]
4 3:00 AM - 4:00 AM	1,338
5 4:00 AM - [illegible]00 AM	1,34[illegible]
6 5:00 AM - 6:00 AM	1,326
7 6:00 AM - [illegible]00 AM	1,348
8 7:00 AM - 8:00 AM	1,629
9 8:00 AM - 9:00 AM	1,888
10 9:00 AM - 10:00 AM	2,567
11 10:00 AM - 11:00 AM	2,366
12 11:00 AM - noon	2,439
13 [illegible]oon - 1:00 PM	1,810
14 1:00 PM - 2:00 PM	2,267
15 2:00 PM - 3:00 PM	2,944
16 3:00 PM - 4:00 PM	9,458
17 4:00 PM - 5:00 PM	6,050
18 5:00 PM - 6:00 PM	2,041
19 6:00 PM - 7:00 PM	1,763
20 7:00 PM - 8:00 PM	1,383
21 8:00 PM - 9:00 PM	1,239
22 9:00 PM - 10:00 PM	1,340
23 10:00 PM - 11:00 PM	1,347

WITHDRAWN

24	11:00 PM - midnight	1,285
	Total	53,096

5.5.6 Sources

Sources

Source	Events		0 - 100 %
1TimeServ	27,602	52.0 %	
2NETLOGON	12,496	23.5 %	
3Security	10,930	20.6 %	
4SweepNT	1,008	1.9 %	
5BROWSER	199	0.4 %	
6N100	122	0.2 %	
7PMC	10[illegible]	0.2 %	
8EventLog	96	0.2 %	
9Se[illegible]ce Con[illegible]ger	94	0.2 %	
10RCONSVC	54	0.1 %	
19 other items	394	0.7 %	
Total	53,096	100 %	

WITHDRAWN

FUJ00155413

5.5.7 Types

Types

Type	Events		0 - 100 %
1Information	40,172	75.7 %	
2Success Audit	10,961	20.6 %	
3Warning	1,043	2.0 %	
4Error	914	1.7 %	
5Failure Audit	6	0.0 %	
Total	53,096	100 %	

5.5.8 Categories

Categories

Category	Events		0 - 100 %
1None	40,838	76.9 %	
2Object Access	10,493	19.8 %	
3SweepInfo	1,008	1.9 %	
4Logon/Logoff	383	0.7 %	
5Service	214	0.4 %	
6Debug	36	0.1 %	
7System Event	29	0.1 %	

WITHDRAWN

Account 8Management	25	0.0 %
9VPN	23	0.0 %
10Events	15	0.0 %

4 other items	32	0.1 %
Total	53,096	100 %

5.5.9 Events

Events

Event	Events		0 - 100 %
10	26,858	50.6 %	
25711	11,807	22.2 %	
3560	5,247	9.9 %	
4562	5,246	9.9 %	
55810	90[illegible]	[illegible].7 %	
65722	609	1.1 %	
711	394	[illegible] %	
864	393	0.7 %	
9538	189	0.4 %	
10528	189	0.4 %	
84 other items	1,260	2.4 %	
Total	53,096	100 %	

WITHDRAWN

FUJ00155413

WITHDRAWN

FUJ00155413

5.5.10 Users

Users

User	Events		0 - 100 %
IRRELEVANT	41,888	78.9 %	
	5,417	10.2 %	
	5,402	10.2 %	
	124	0.2 %	
	91	0.2 %	
	39	0.1 %	
	16	0.0 %	
	12	0.0 %	
	[illegible]	0.0 %	
	10	0.0 %	
19 other items	86	0.2 %	
Total	53,096	100 %	

WITHDRAWN

FUJ00155413

5.5.11 Computers

Computers

Computer	Events		0 - 100 %
IRRELEVANT	37,210	70.1 %	
IRRELEVANT	15,886	29.9 %	
Total	53,096	100 %	

WITHDRAWN

FUJ00155413

5.5.12 Details

Details

Detail	Events		0 - 100 %
1Time set (offset < .5 second)	26,8[illegible]	[illegible].5 %	
2Object Open:	5,247	9.9 %	
3Handle Closed:	5,246	9.9 %	
The partial synchronization request from the server IRRELEVANT completed 4successfully. 1 changes(s) has(have) been retu...	3,609	6.8 %	
The partial synchronization request from the server IRRELEVANT 5completed successfully. 1 changes(s) has(have) been retu...	3,602	6.8 %	
The partial synchronization request from the server IRRELEVANT 6completed successfully. 1 changes(s) has(have) been retu...	3,595	6.8 %	
7t respond	394	0.7 %	
8The specified NTPServer supports RFC-868(Time)	393	0.7 %	
The partial synchronization request from the server IRRELEVANT 9completed successfully. 2 changes(s) has(have) been retu...	219	0.4 %	
The partial synchronization request from the server IRRELEVANT 10completed successfully. 2 changes(s) has(have) been retu...	216	0.4 %	
582 other items	3,762	7.1 %	
Total	53,089	100 %	

FUJ00155413

6.0 Appendix B

This appendix includes details of the prioritisation that platforms are given based on their Security Tier and Domain for HNG-X and is to be used as a guideline for Horizon. The Analysis of logs and Events will be prioritised based on this.

devgenspe0007-01.xls

7.0 Appendix C

Appendix C summarizes the Security events that Windows platforms generate and will need to be included as a basis for analysis. Linux and Solaris events will follow in a later version of this document.

Windows Events

8.0 Appendix D

Appendix D gives full details of the reports created by Fujitsu Services recommended SIEM.

TRIOLE_Security-Information-Event-Mana

WITHDRAWN