What makes you special?

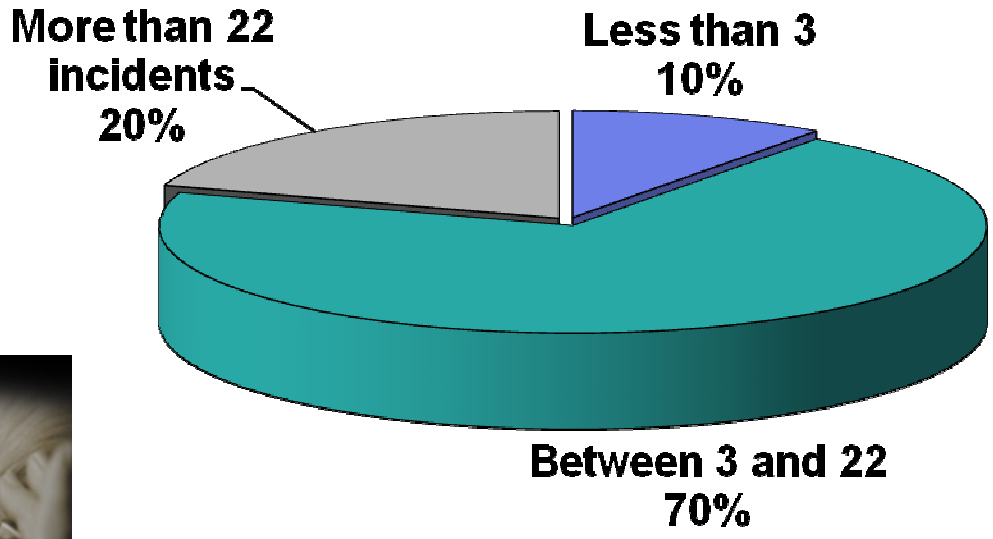
Tivoli Security Information & Event Management

Martin Borrett
Lead Security Architect
Technical Staff Member
NE Europe
IBM SWG

IBM Governance and Risk Management
Business alignment, visibility and control

Security Requirements

Breaches of sensitive business data in past year:



Source: 2006 survey by the IT Policy Compliance Group

Known People (un) Intentionally Do Great Harm

87% of insider incidents are caused by privileged or technical users

Many are inadvertent violations of:

- Change management process
- Acceptable use policy

Others are deliberate, due to:

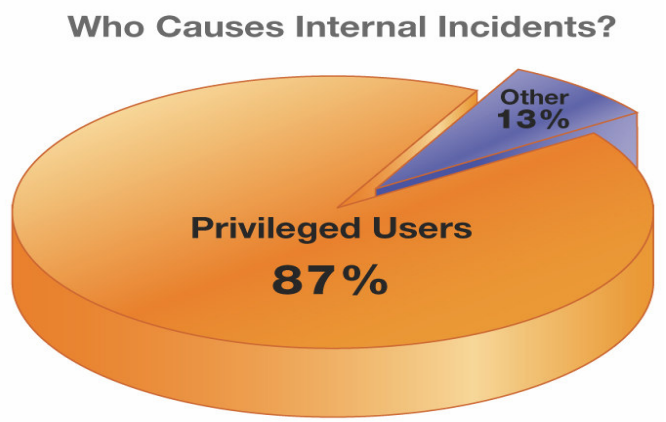
- Revenge (84%)
- "Negative events" (92%)

Regardless, too costly to ignore:

- Internal attacks cost 6% of gross annual revenue
- Costing $400 billion in the US alone

Sources: Forrester research, IdM Trends 2006; USSS/CERT Insider Threat Survey 2005; CSI/FBI Survey

Who Causes Internal Incidents?



Source: USSS/CERT Insider Threat Survey 2005

Who are they?

- Male
- 17-60 Years Old
- 87% technical positions
- About half married
- Variety of racial and ethnic backgrounds

Challenges to address

Increasing Requirements

Increasing Complexity

Increasing Cost

Security Compliance Dashboard and Reporting

Privileged User Monitoring and Audit (PUMA)

Database Monitoring and Audit

Log and Audit Trail Management

Solutions In

Regulators & Auditors Make It Urgent

[ISO17799:2005]
10.10.1 Audit logging

Audit logs recording user activities, exceptions, and information security events should be produced and kept for an agreed period to assist in future investigations and access control monitoring.

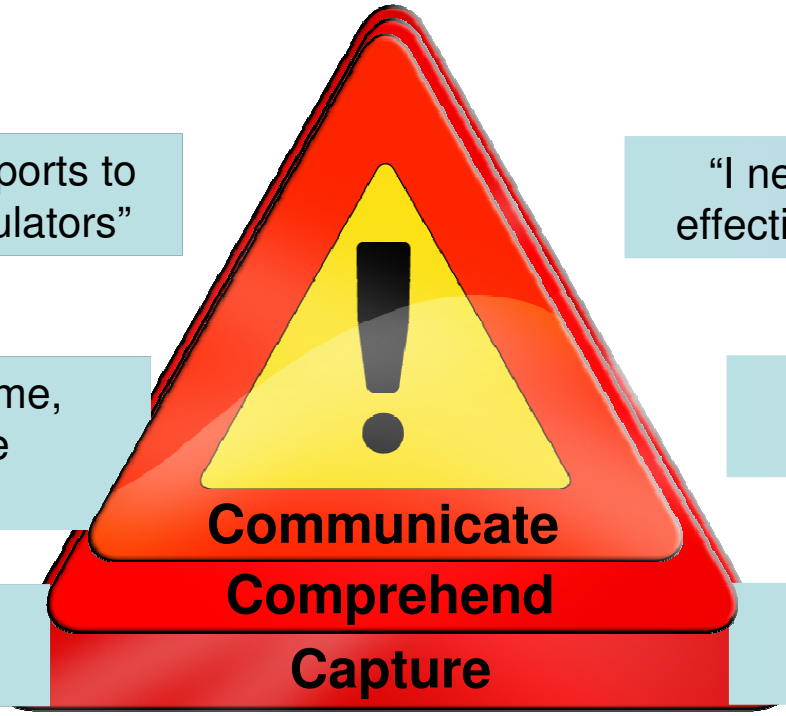
The Problems We Help to Solve

"I need to provide reports to my auditors and regulators"

"I need to prove that I have effective IT security controls"

"My staff lacks the time, expertise, and desire to scan logs"

"I'm concerned about privileged actions"



"I need to store logs for forensics"

"I have no idea which logs to collect or how"

Agenda

Problems

Solution: TSIEM -- The 3 C's

1. Capture – Enterprise Log Management
2. Comprehend – Sophisticated Log Interpretation
3. Communicate – Full Audit and Compliance Reporting

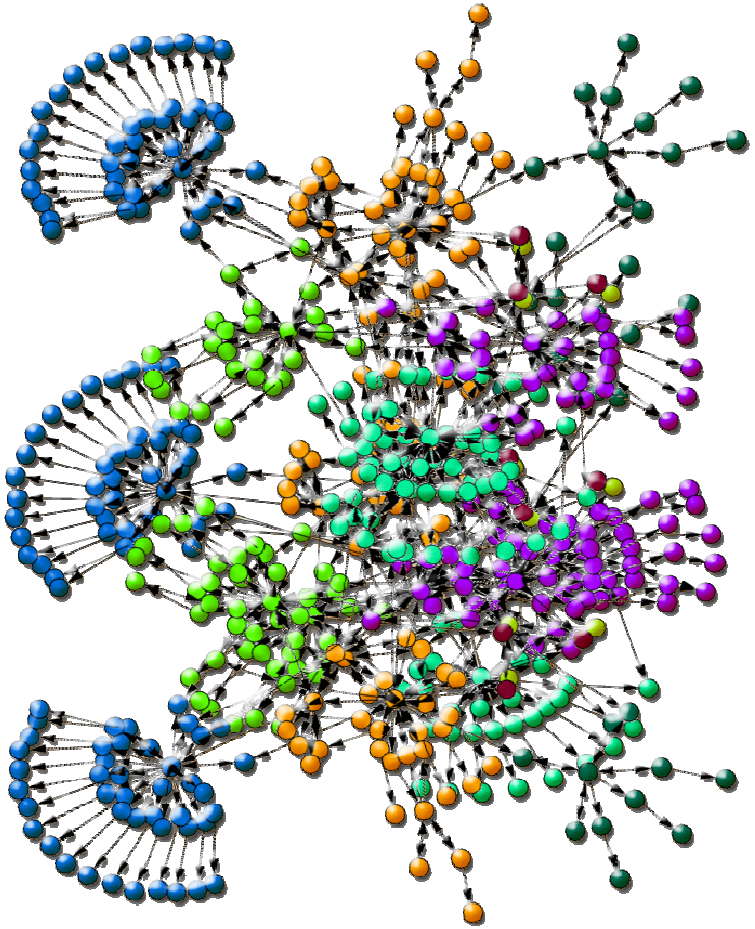
Technology

Proven Results

I Need to Collect Logs but it's Too Hard

Your enterprise

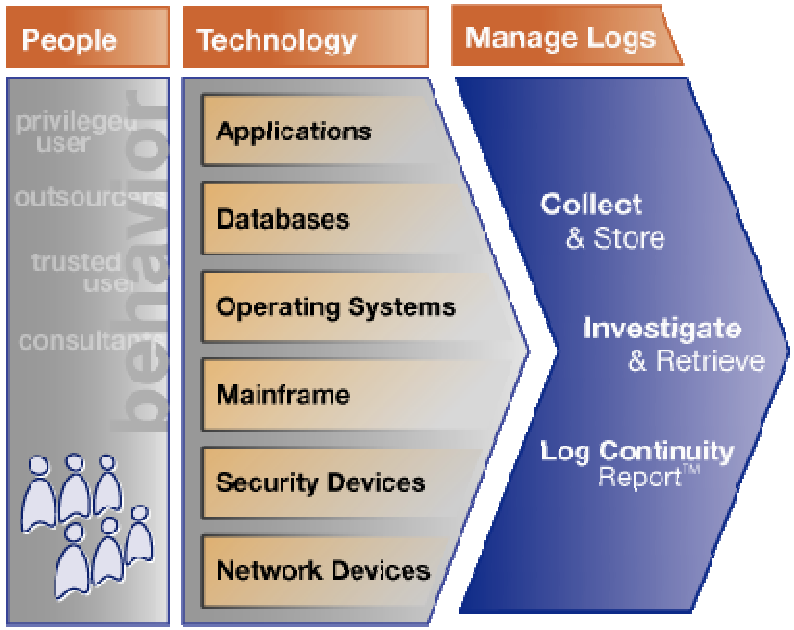
How to collect the logs?



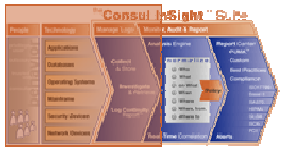
Capture

- Thousands of points across the enterprise generating event logs
- Regulators and auditors require you to capture and retain these log files
- Internal and external threats mean you need to investigate activities
- Time and cost constraints means it must be fast and affordable

Enterprise Log Management



Capture



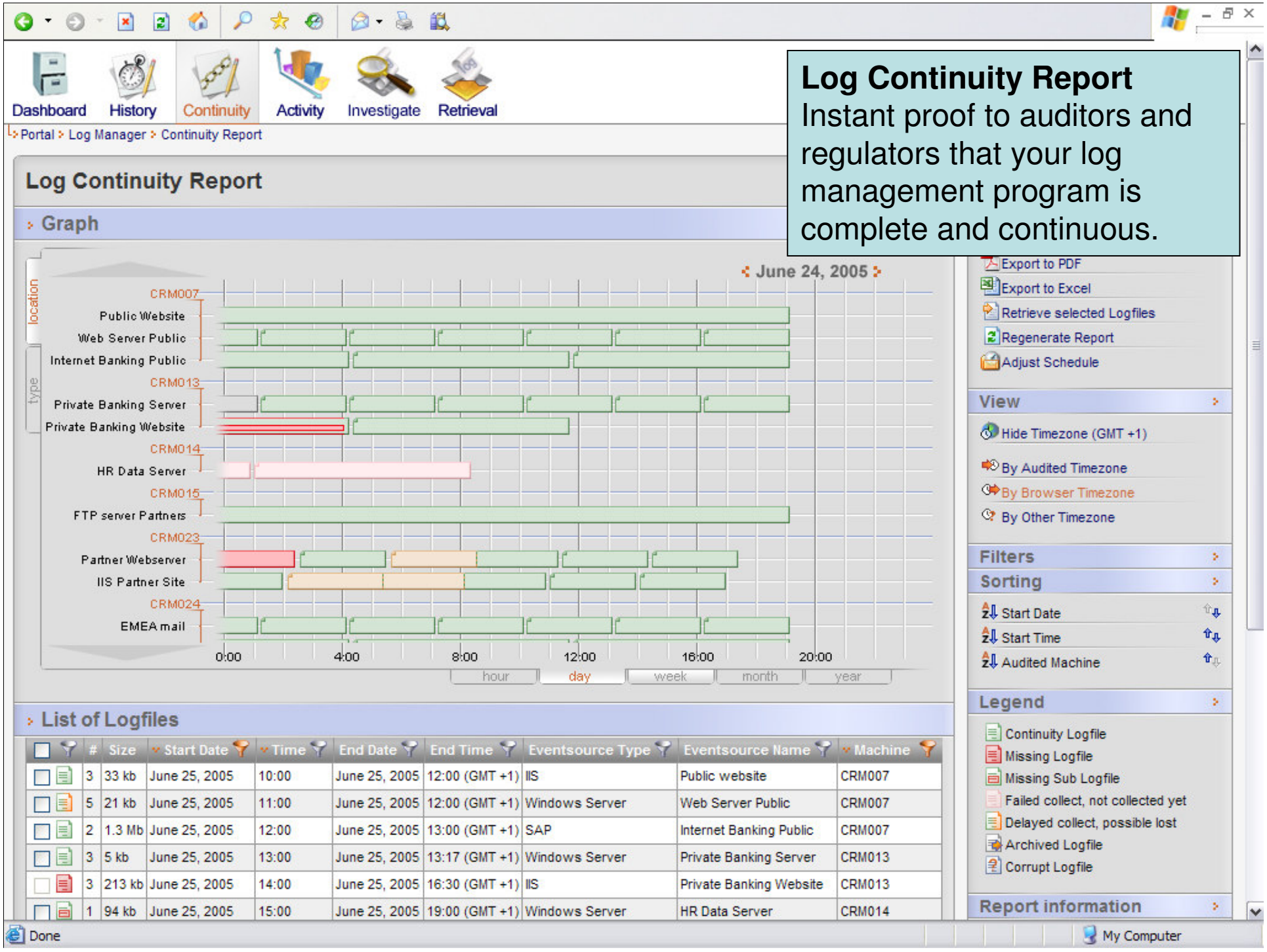
Capabilities:

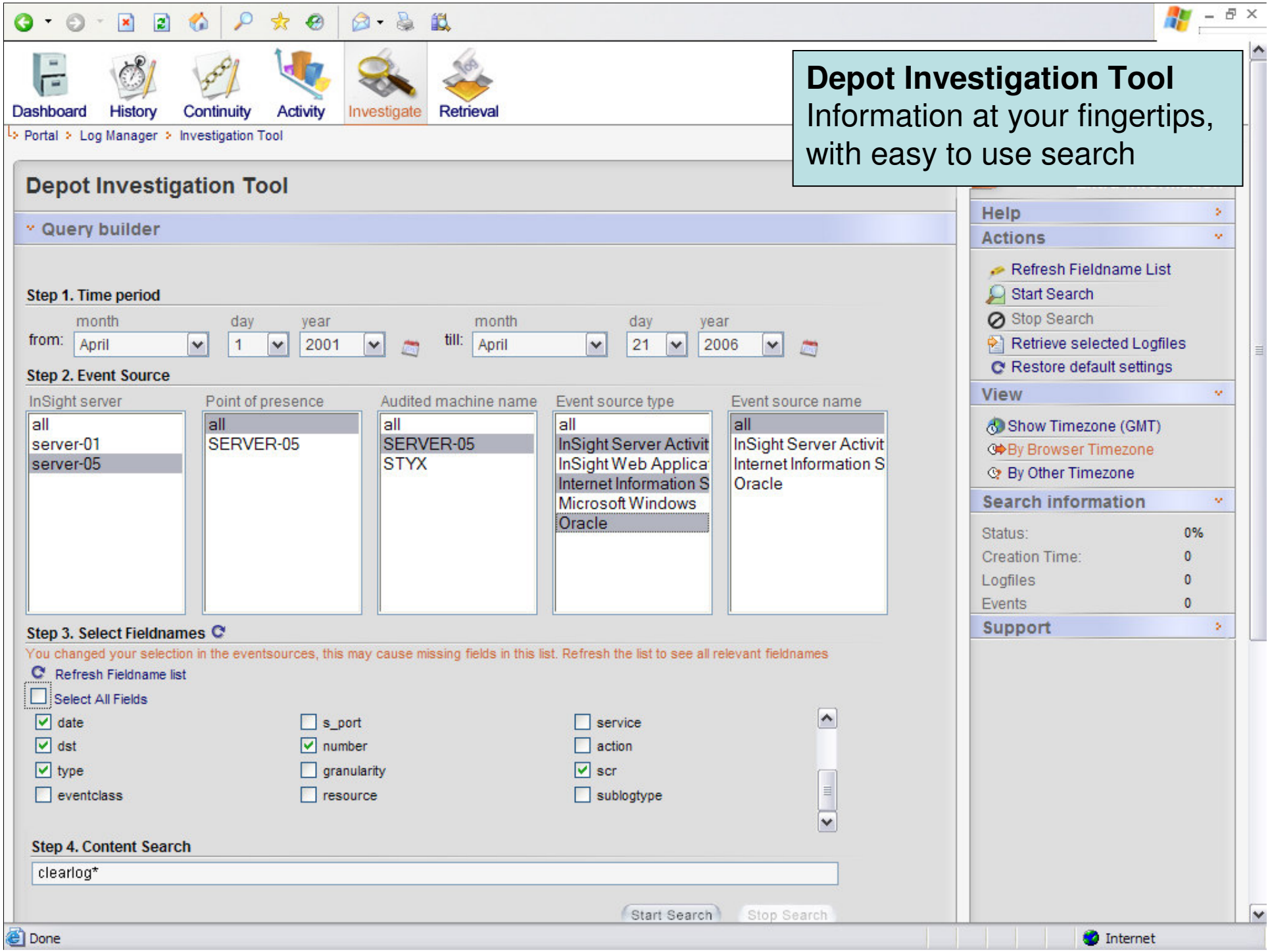
- Secure, reliable log capture from any platform
- Auto collection of syslogs
- Full support for native log collection
- Store in an efficient, compressed depot
- Access data when needed
- Search across all logs
- Reports to prove complete collection

Benefits:

- Reduce costs by automating and centralizing collection
- Be “audit ready” at any time!

Implementation time: plug and play.


Dashboard
History
Continuity
Activity
Investigate
Retrieval
Portal › Log Manager › Continuity Report
Log Continuity Report
Instant proof to auditors and regulators that your log management program is complete and continuous.
Log Continuity Report
Graph
June 24, 2005
location
type
CRM007
Public Website
Web Server Public
Internet Banking Public
CRM013
Private Banking Server
Private Banking Website
CRM014
HR Data Server
CRM015
FTP server Partners
CRM023
Partner Webserver
IIS Partner Site
CRM024
EMEA mail
0:00
4:00
8:00
12:00
16:00
20:00
hour
day
week
month
year
Export to PDF
Export to Excel
Retrieve selected Logfiles
Regenerate Report
Adjust Schedule
View
Hide Timezone (GMT +1)
By Audited Timezone
By Browser Timezone
By Other Timezone
Filters
Sorting
Start Date
Start Time
Audited Machine
Legend
Continuity Logfile
Missing Logfile
Missing Sub Logfile
Failed collect, not collected yet
Delayed collect, possible lost
Archived Logfile
Corrupt Logfile
Report information
List of Logfiles
Size Start Date Time End Date End Time Eventsource Type Eventsource Name Machine
3 33 kb June 25, 2005 10:00 June 25, 2005 12:00 (GMT +1) IIS Public website CRM007
5 21 kb June 25, 2005 11:00 June 25, 2005 12:00 (GMT +1) Windows Server Web Server Public CRM007
2 1.3 Mb June 25, 2005 12:00 June 25, 2005 13:00 (GMT +1) SAP Internet Banking Public CRM007
3 5 kb June 25, 2005 13:00 June 25, 2005 13:17 (GMT +1) Windows Server Private Banking Server CRM013
3 213 kb June 25, 2005 14:00 June 25, 2005 16:30 (GMT +1) IIS Private Banking Website CRM013
1 94 kb June 25, 2005 15:00 June 25, 2005 19:00 (GMT +1) Windows Server HR Data Server CRM014
Done
My Computer


Dashboard
History
Continuity
Activity
Investigate
Retrieval
Portal › Log Manager › Investigation Tool
Depot Investigation Tool
Information at your fingertips, with easy to use search
Depot Investigation Tool
Query builder
Step 1. Time period
from: month April day 1 year 2001
till: month April day 21 year 2006
Step 2. Event Source
InSight server: all, server-01, server-05
Point of presence: all, SERVER-05
Audited machine name: all, SERVER-05, STYX
Event source type: all, InSight Server Activit, InSight Web Applica, Internet Information S, Microsoft Windows, Oracle
Event source name: all, InSight Server Activit, Internet Information S, Oracle
Step 3. Select Fieldnames
You changed your selection in the eventsources, this may cause missing fields in this list. Refresh the list to see all relevant fieldnames
Refresh Fieldname list
Select All Fields
date, dst, type, eventclass
s_port, number, granularity, resource
service, action, scr, sublogtype
Step 4. Content Search
clearlog*
Start Search
Stop Search
Help
Actions
Refresh Fieldname List
Start Search
Stop Search
Retrieve selected Logfiles
Restore default settings
View
Show Timezone (GMT)
By Browser Timezone
By Other Timezone
Search information
Status: 0%
Creation Time: 0
Logfiles 0
Events 0
Support
Done
Internet

Agenda

Problems

Solution: TSIEM -- The 3 C's

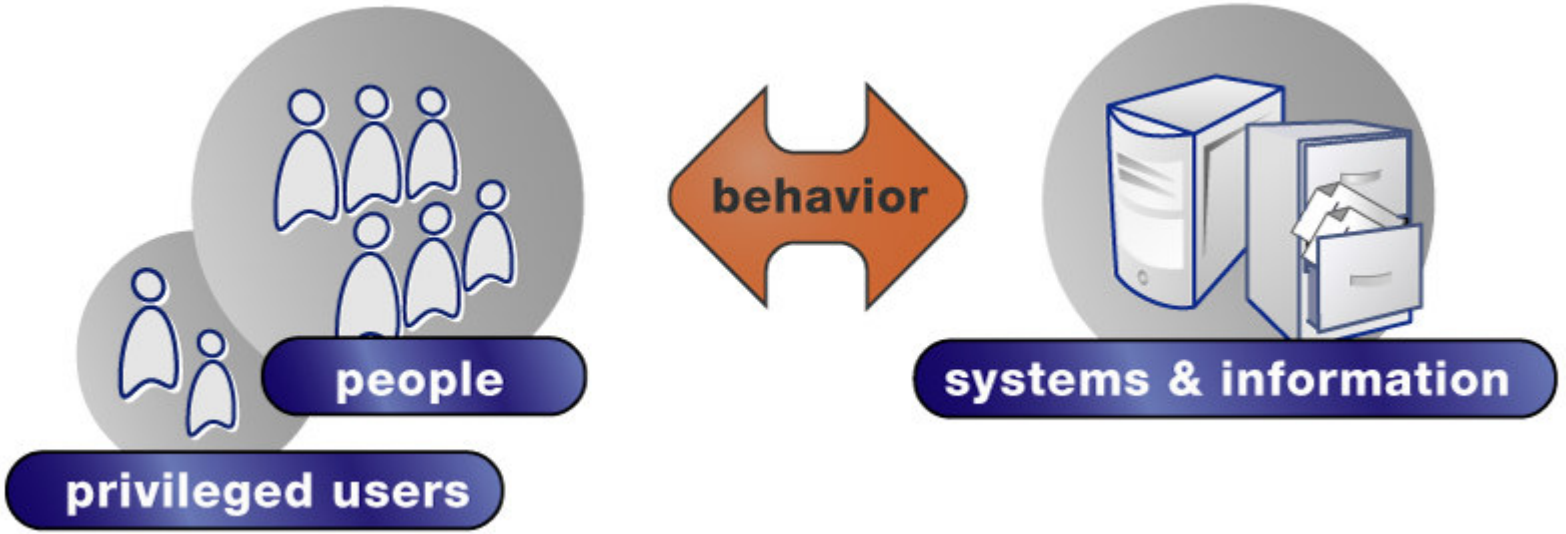
1. Capture – Enterprise Log Management
2. Comprehend – Sophisticated Log Interpretation
3. Communicate – Full Audit and Compliance Reporting

Technology

Proven Results

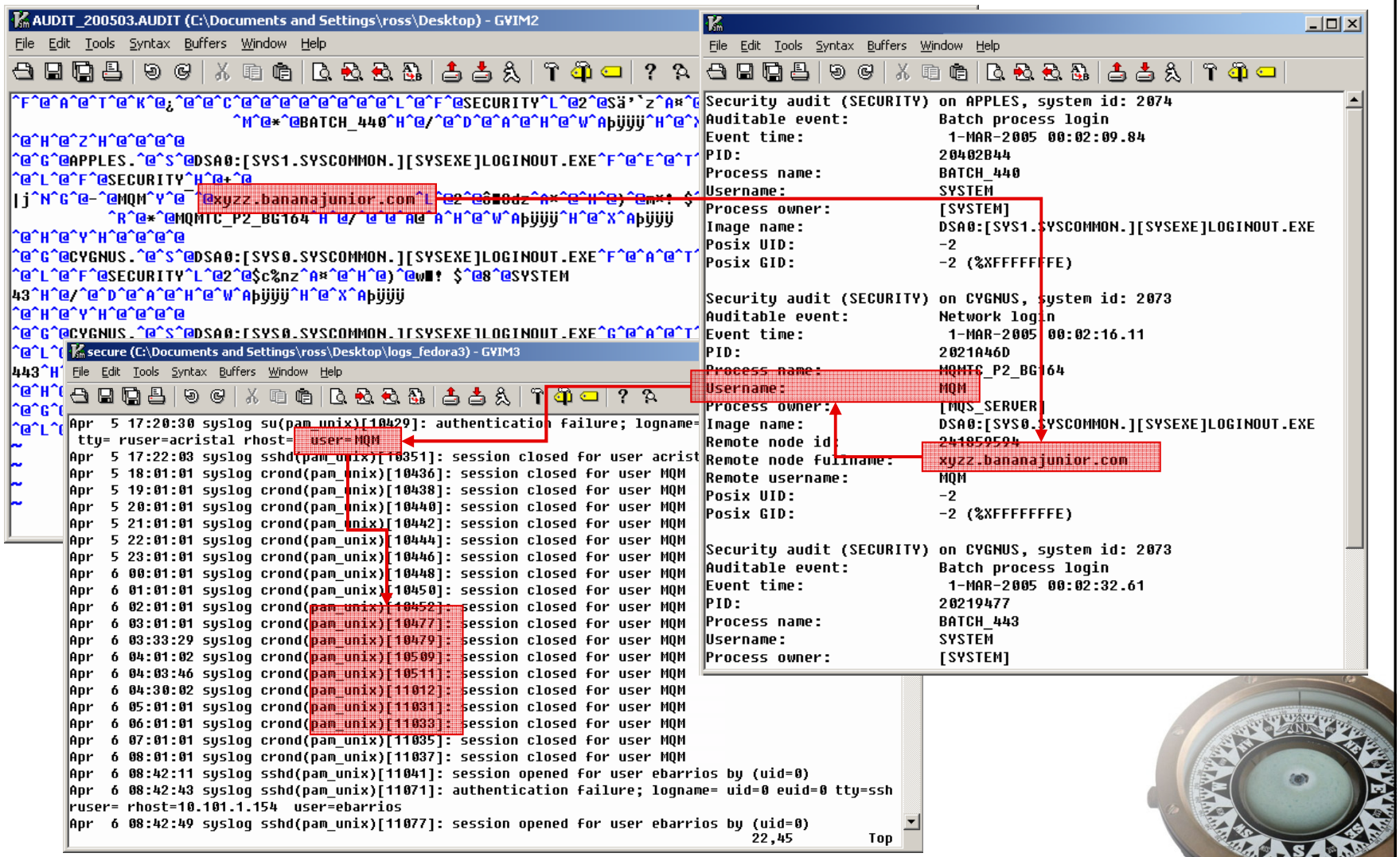
What are People Doing on My Network?

Comprehend



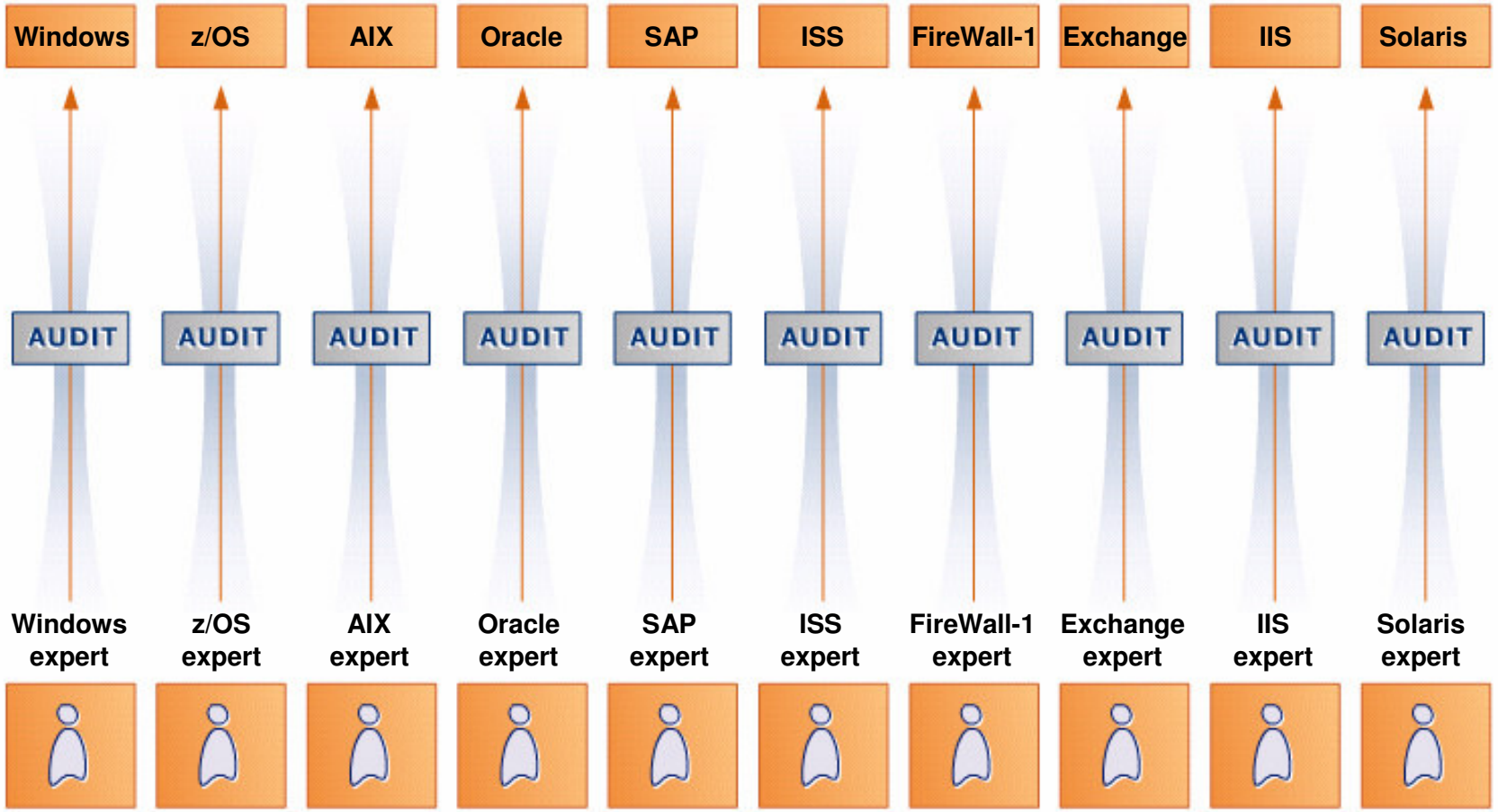
87% of insider incidents are caused by privileged and technical users.

How do I make sense of all this?



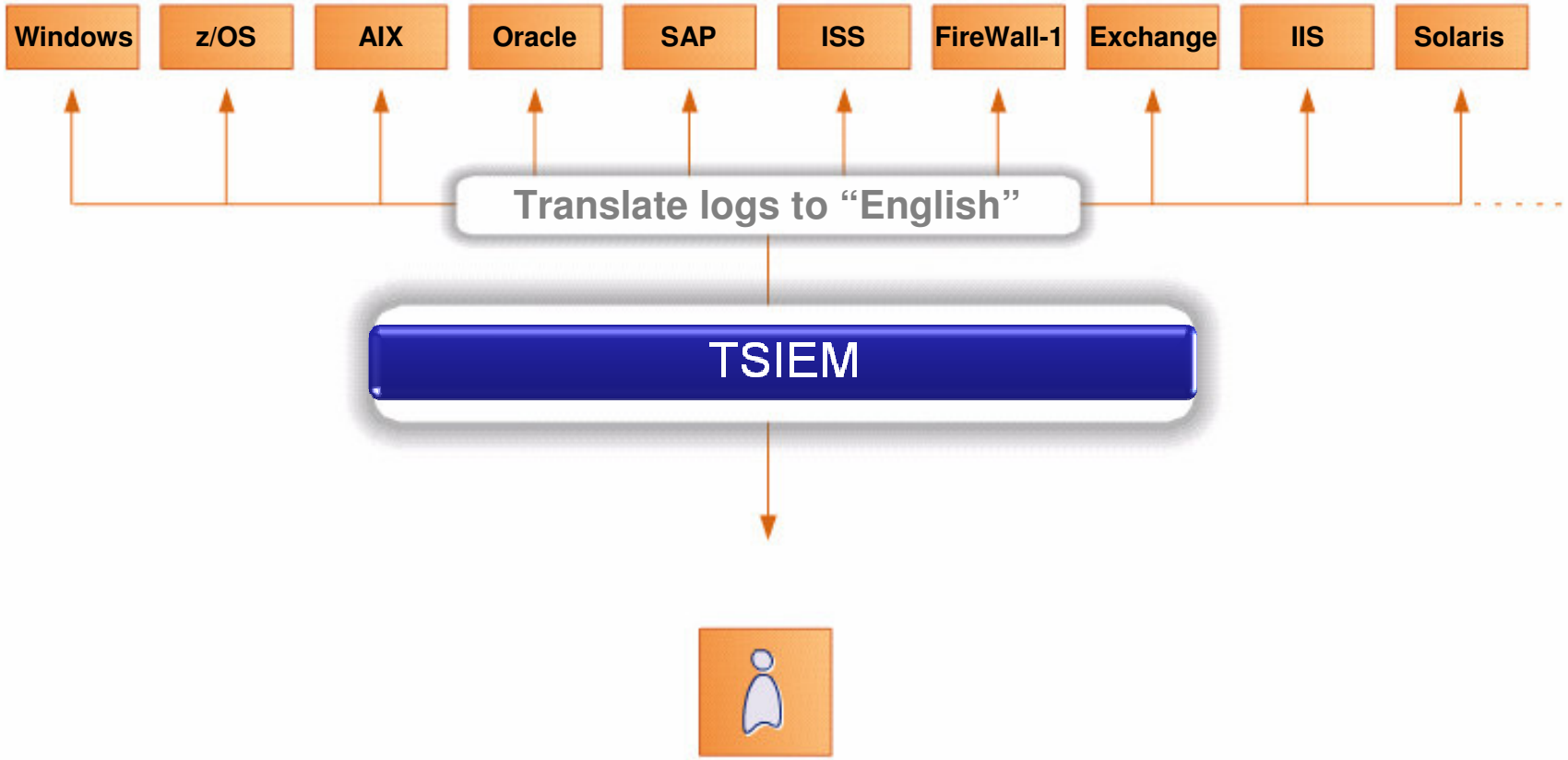
Comprehend

After Log Capture, Translation is Next



Comprehend

Now all Logs in Your Enterprise in a Single Language



Comprehend

TSIEM saves your information security and compliance staff time and money by automating monitoring across the enterprise.

Translate Logs into English
IBM Tivoli's W7 Methodology

Comprehend

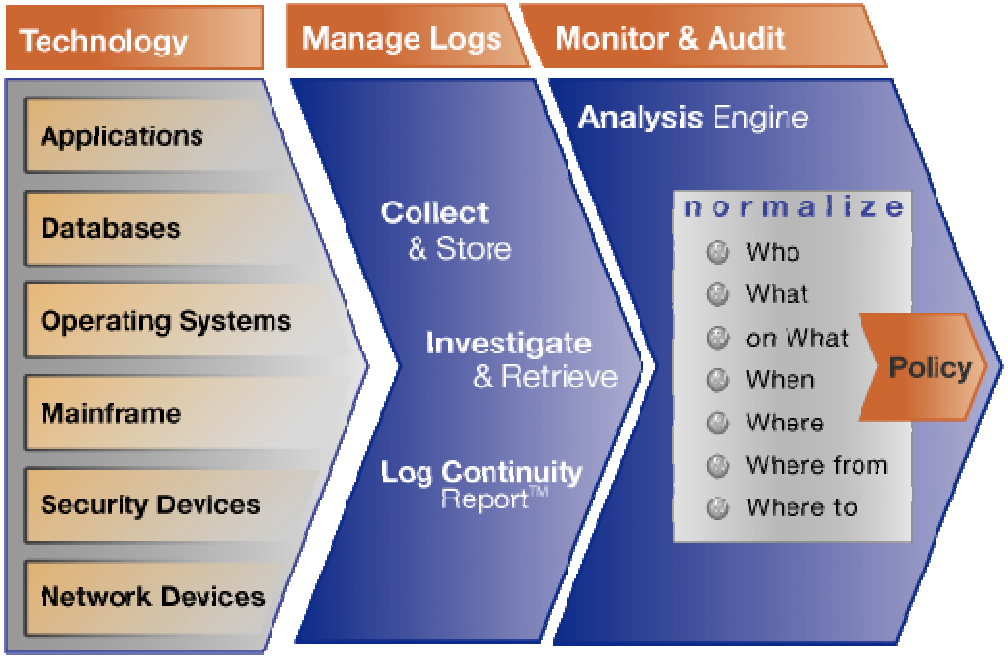
Who did **What** type of action **on What**?

When did he do it and **Where**, **From Where** and **Where To**?

We do the hard work, so you don't have to!!

Sophisticated Log Interpretation and Correlation

Comprehend

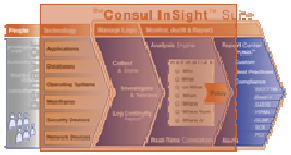


Capabilities:

- W7 normalization
- Interpret EVERY log (Syslog and native logs) into English
- Compare billions of log entries to baseline policy

Benefits:

- Interpret and monitor all logs with fewer and less expensive resources
- More quickly detect and solve security problems



Out of the box log normalization!

Compliance Dashboard
Logs after W7 – Billions of log files summarized on one overview graphic!

Dashboard | Trends | Reports | Policies | Groups | Settings | Regulations | Log off

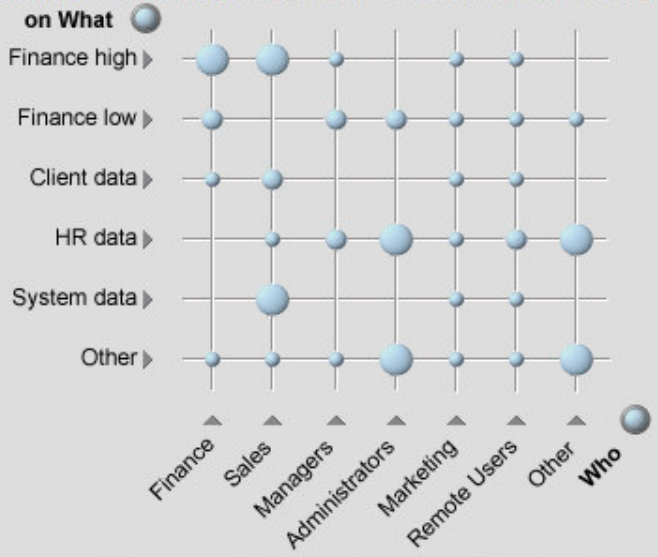
Dashboard

Compliance Dashboard

Enterprise Overview

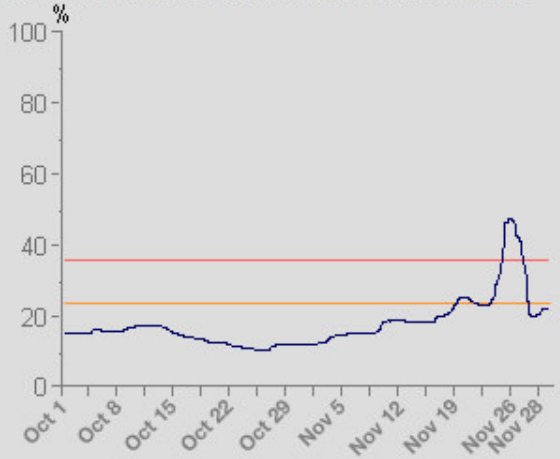
Settings

Events by top event count by "on What" and "Who" for Oct 1, 2005 till Nov. 28, 2005.



Trend graphic

Percentage of Exceptions for Oct 1, 2005 till Nov 28, 2005



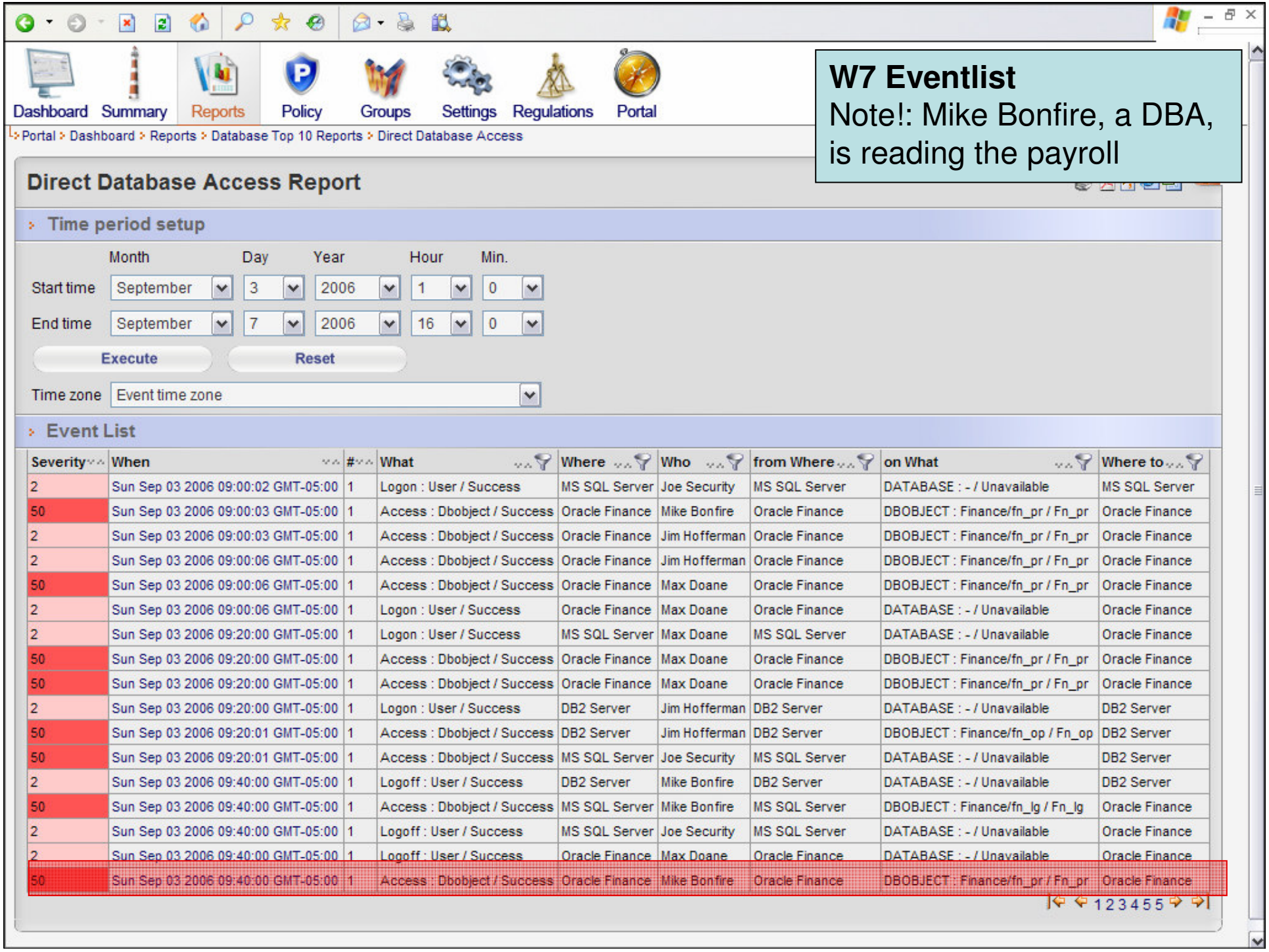
Contact us

In the US:
contactsales@consul.com
Direct Line: +1 703 675 2022
Toll Free (US only): 800 258 5077

EMEA and Asia Pac:
contactsales@consul.com
Direct Line: +31 15 251 3333

Database Overview

Name: AggrDb
Status: Loaded & Selected
Loading Date: Nov 29, 2005
Content: Aggregation of all collected material for the last 90 days.


Dashboard
Summary
Reports
Policy
Groups
Settings
Regulations
Portal
Portal › Dashboard › Reports › Database Top 10 Reports › Direct Database Access
Direct Database Access Report
Time period setup
Month
Day
Year
Hour
Min.
Start time
September
3
2006
1
0
End time
September
7
2006
16
0
Execute
Reset
Time zone
Event time zone
Event List
Severity
When
#
What
Where
Who
from Where
on What
Where to
2 Sun Sep 03 2006 09:00:02 GMT-05:00 1 Logon : User / Success MS SQL Server Joe Security MS SQL Server DATABASE : - / Unavailable MS SQL Server
50 Sun Sep 03 2006 09:00:03 GMT-05:00 1 Access : Dbobject / Success Oracle Finance Mike Bonfire Oracle Finance DBOBJECT : Finance/fn_pr / Fn_pr Oracle Finance
2 Sun Sep 03 2006 09:00:03 GMT-05:00 1 Access : Dbobject / Success Oracle Finance Jim Hofferman Oracle Finance DBOBJECT : Finance/fn_pr / Fn_pr Oracle Finance
2 Sun Sep 03 2006 09:00:06 GMT-05:00 1 Access : Dbobject / Success Oracle Finance Jim Hofferman Oracle Finance DBOBJECT : Finance/fn_pr / Fn_pr Oracle Finance
50 Sun Sep 03 2006 09:00:06 GMT-05:00 1 Access : Dbobject / Success Oracle Finance Max Doane Oracle Finance DBOBJECT : Finance/fn_pr / Fn_pr Oracle Finance
2 Sun Sep 03 2006 09:00:06 GMT-05:00 1 Logon : User / Success Oracle Finance Max Doane Oracle Finance DATABASE : - / Unavailable Oracle Finance
2 Sun Sep 03 2006 09:20:00 GMT-05:00 1 Logon : User / Success MS SQL Server Max Doane MS SQL Server DATABASE : - / Unavailable Oracle Finance
50 Sun Sep 03 2006 09:20:00 GMT-05:00 1 Access : Dbobject / Success Oracle Finance Max Doane Oracle Finance DBOBJECT : Finance/fn_pr / Fn_pr Oracle Finance
50 Sun Sep 03 2006 09:20:00 GMT-05:00 1 Access : Dbobject / Success Oracle Finance Max Doane Oracle Finance DBOBJECT : Finance/fn_pr / Fn_pr Oracle Finance
2 Sun Sep 03 2006 09:20:00 GMT-05:00 1 Logon : User / Success DB2 Server Jim Hofferman DB2 Server DATABASE : - / Unavailable DB2 Server
50 Sun Sep 03 2006 09:20:01 GMT-05:00 1 Access : Dbobject / Success DB2 Server Jim Hofferman DB2 Server DBOBJECT : Finance/fn_op / Fn_op DB2 Server
50 Sun Sep 03 2006 09:20:01 GMT-05:00 1 Access : Dbobject / Success MS SQL Server Joe Security MS SQL Server DATABASE : - / Unavailable DB2 Server
2 Sun Sep 03 2006 09:40:00 GMT-05:00 1 Logoff : User / Success DB2 Server Mike Bonfire DB2 Server DATABASE : - / Unavailable DB2 Server
50 Sun Sep 03 2006 09:40:00 GMT-05:00 1 Access : Dbobject / Success MS SQL Server Mike Bonfire MS SQL Server DBOBJECT : Finance/fn_lg / Fn_lg Oracle Finance
2 Sun Sep 03 2006 09:40:00 GMT-05:00 1 Logoff : User / Success MS SQL Server Joe Security MS SQL Server DATABASE : - / Unavailable Oracle Finance
2 Sun Sep 03 2006 09:40:00 GMT-05:00 1 Logoff : User / Success Oracle Finance Max Doane Oracle Finance DATABASE : - / Unavailable Oracle Finance
50 Sun Sep 03 2006 09:40:00 GMT-05:00 1 Access : Dbobject / Success Oracle Finance Mike Bonfire Oracle Finance DBOBJECT : Finance/fn_pr / Fn_pr Oracle Finance
1 2 3 4 5 5
W7 Eventlist
Note!: Mike Bonfire, a DBA, is reading the payroll

Agenda

Problems

Solution: TSIEM -- The 3 C's

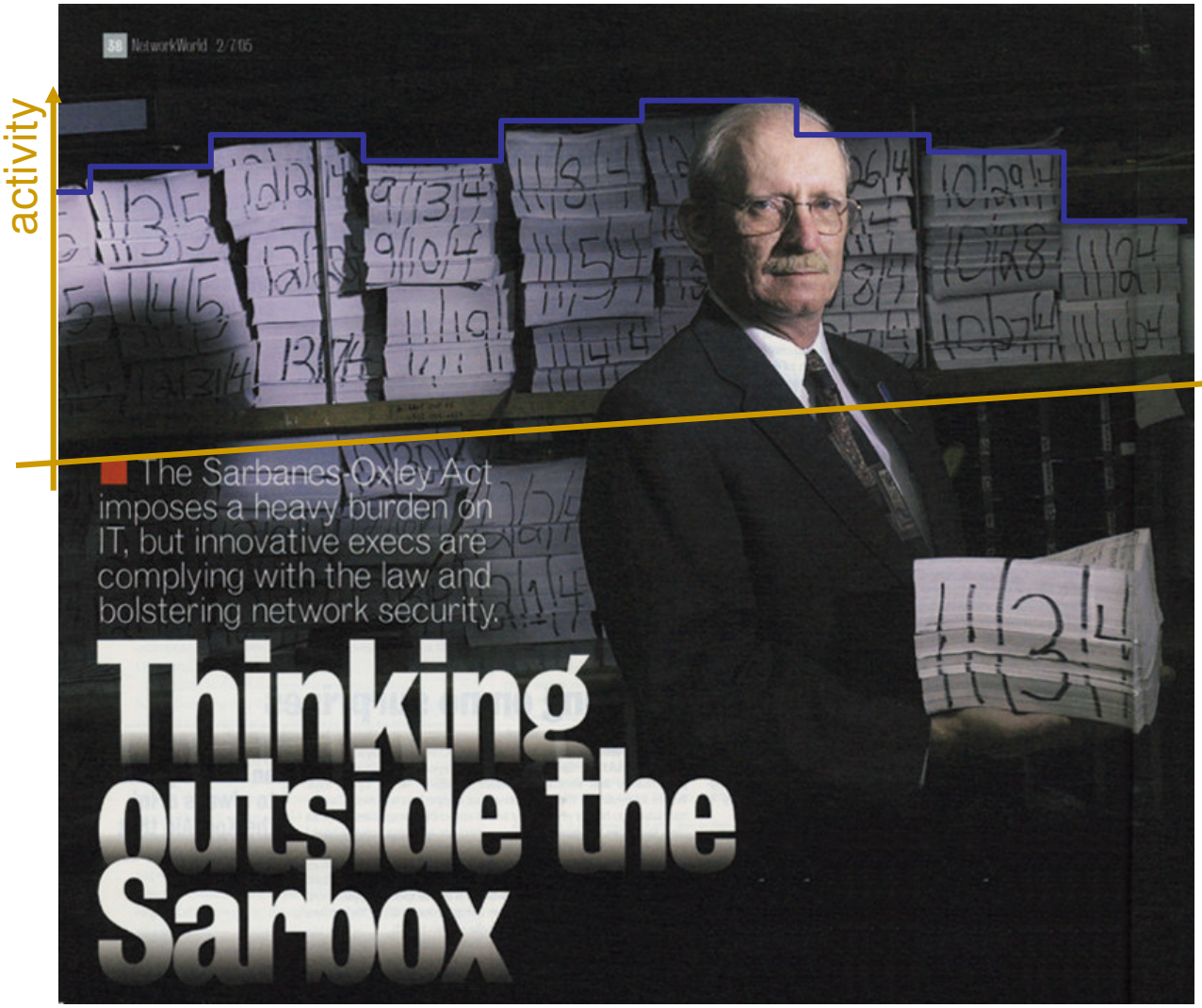
1. Capture – Enterprise Log Management
2. Comprehend – Sophisticated Log Interpretation
3. Communicate – Full Audit and Compliance Reporting

Technology

Proven Results

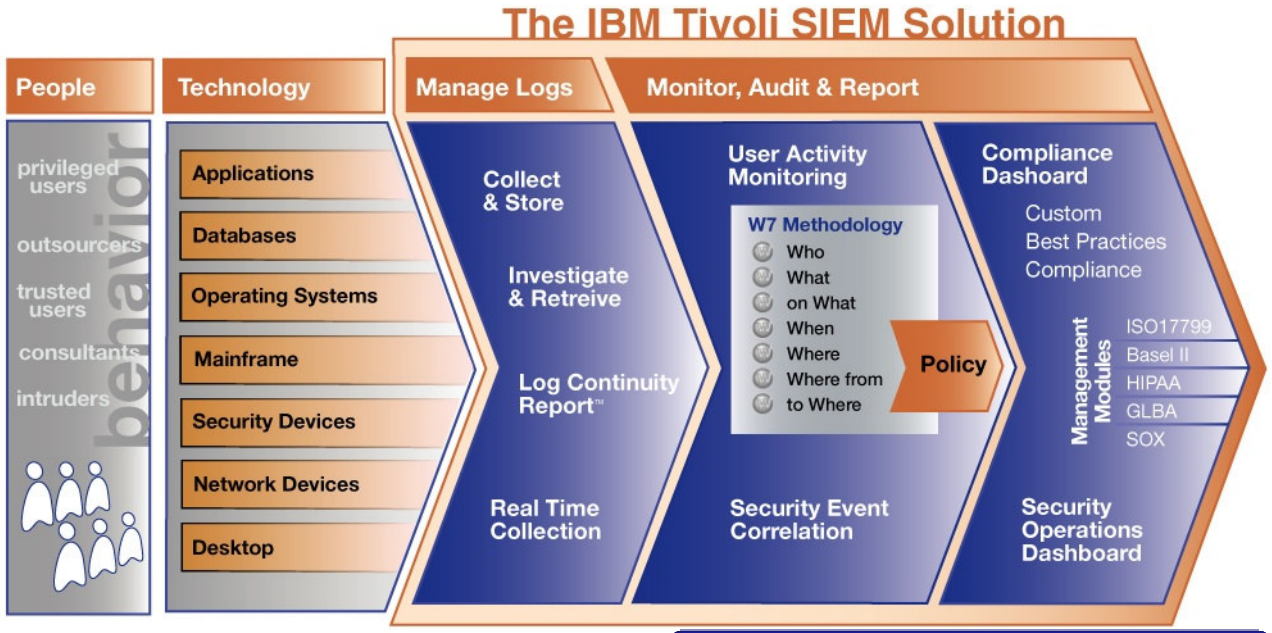
You Need Reports to Communicate

Communicate



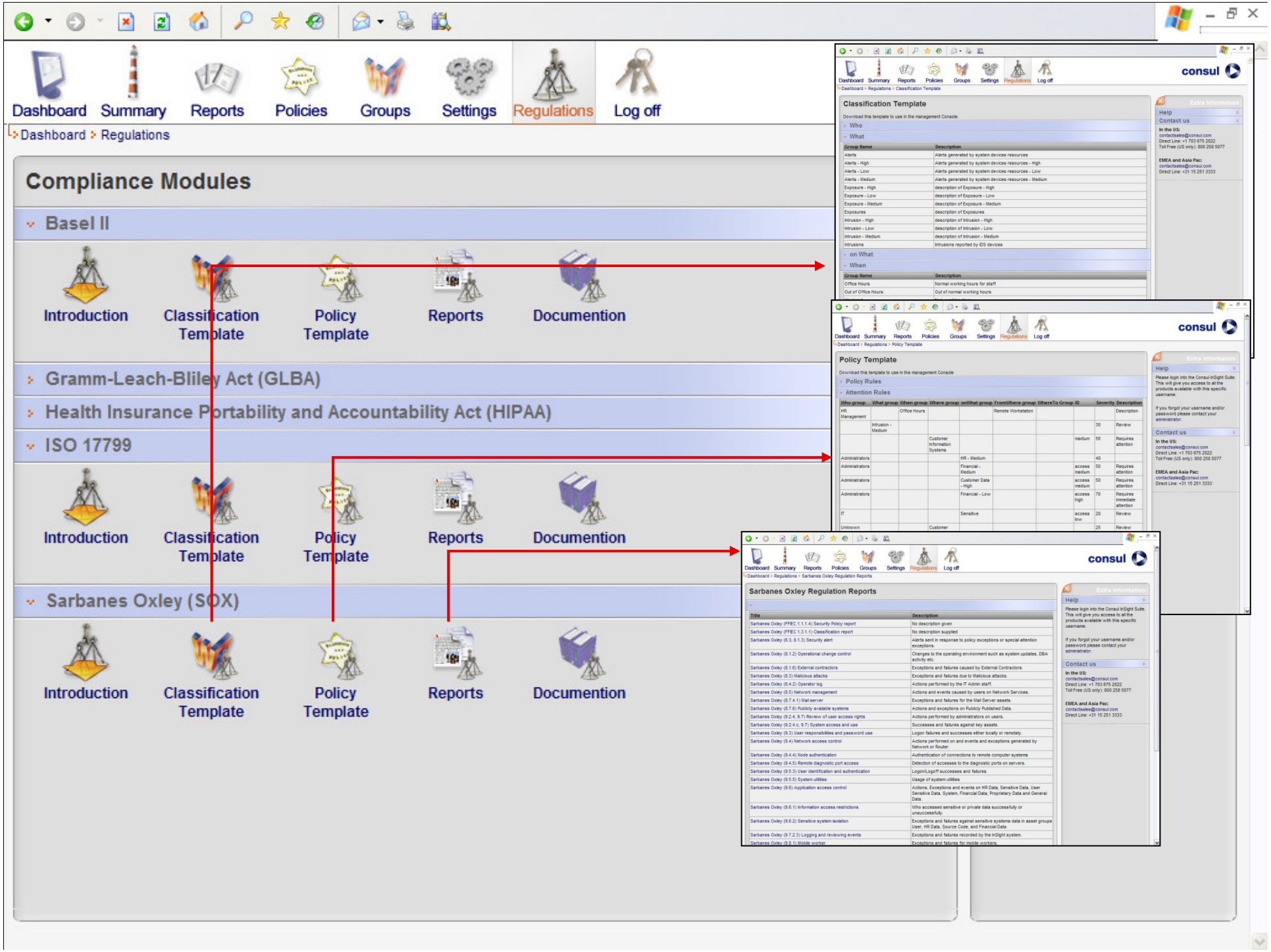
Full Audit and Compliance Reporting

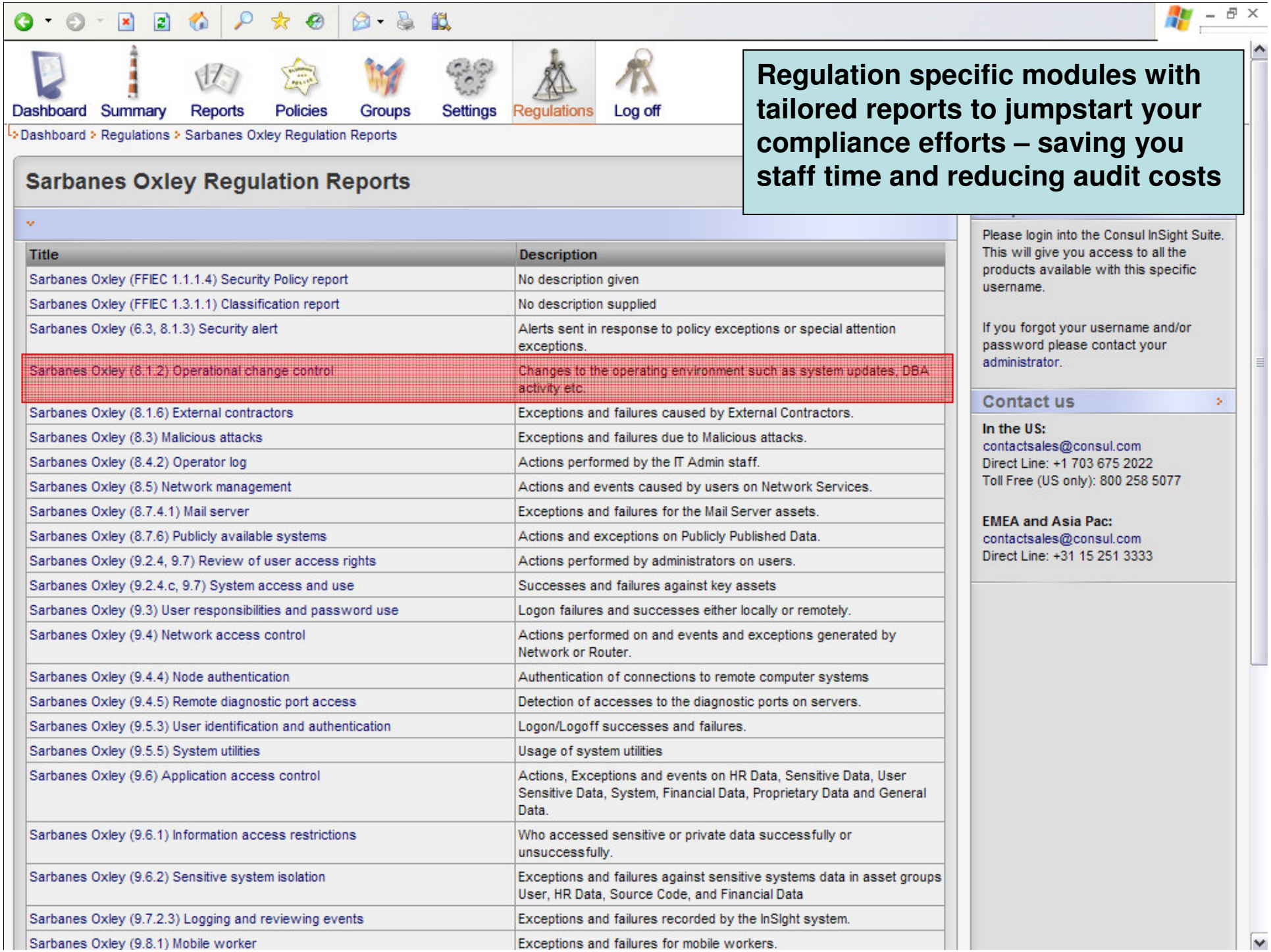
Communicate

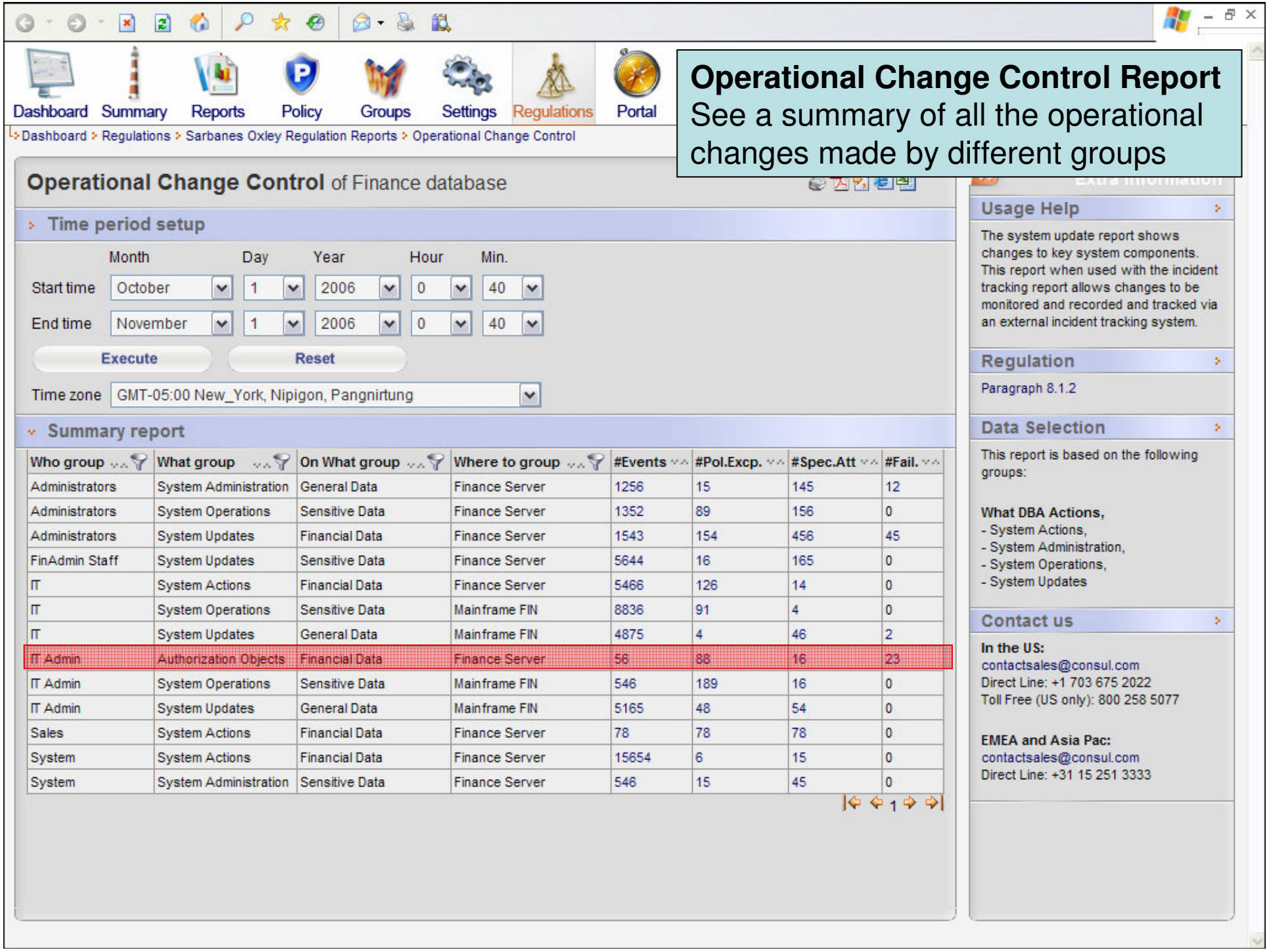


- Hundreds of reports
- Compliance modules
- Special attention alerts
- Custom reports

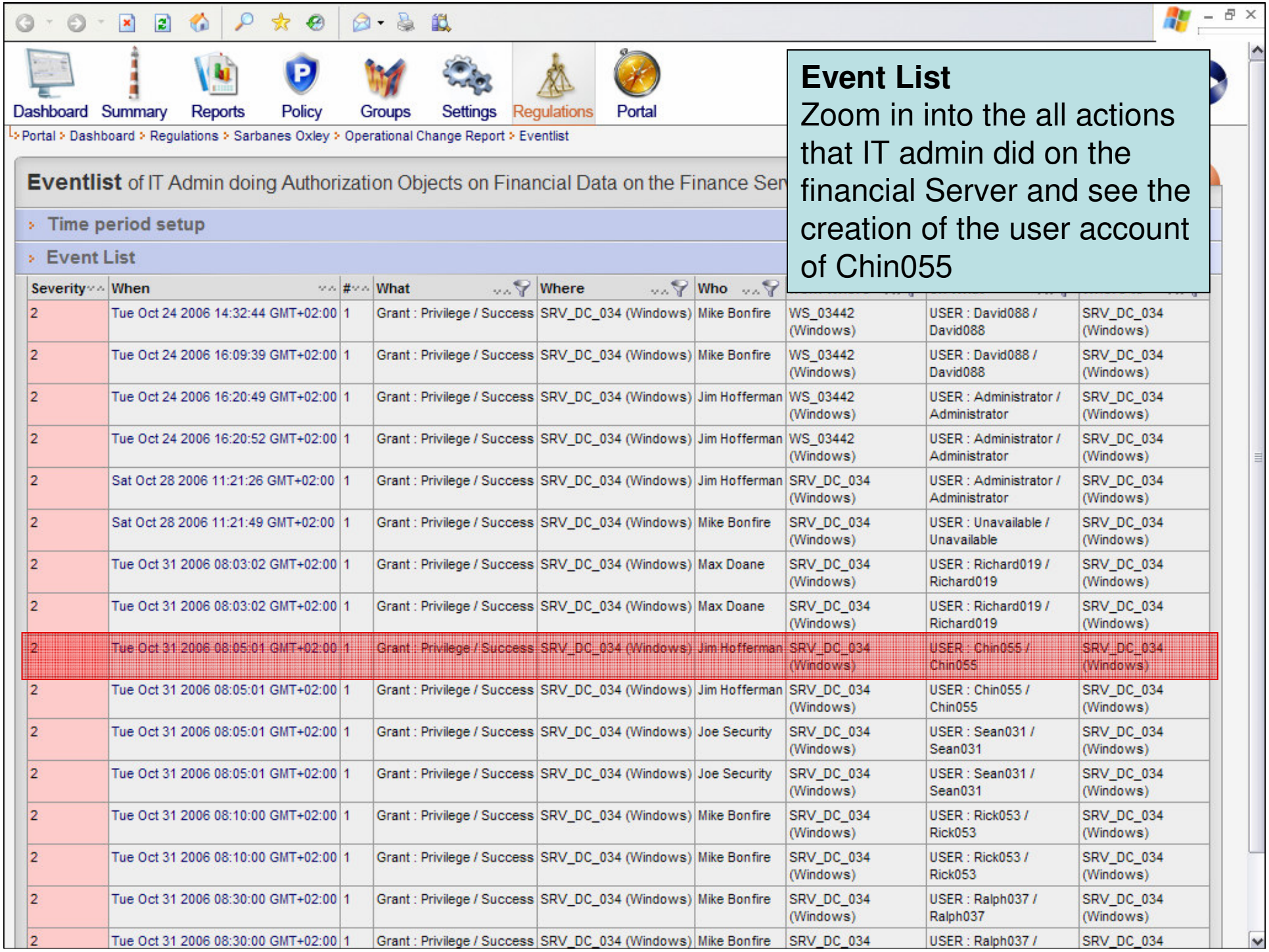
- Reduce length and effort required for audits
- Reports in an instant, saving time
- Reduce risk of insider threat:
  - Info protection
  - Change control
  - User management


Dashboard
Summary
Reports
Policies
Groups
Settings
Regulations
Log off
Dashboard > Regulations
Compliance Modules
Basel II
Introduction
Classification Template
Policy Template
Reports
Documention
Gramm-Leach-Bliley Act (GLBA)
Health Insurance Portability and Accountability Act (HIPAA)
ISO 17799
Introduction
Classification Template
Policy Template
Reports
Documention
Sarbanes Oxley (SOX)
Introduction
Classification Template
Policy Template
Reports
Documention
consul
Classification Template
Policy Template
Sarbanes Oxley Regulation Reports


Dashboard
Summary
Reports
Policies
Groups
Settings
Regulations
Log off
Dashboard › Regulations › Sarbanes Oxley Regulation Reports
Sarbanes Oxley Regulation Reports
Regulation specific modules with tailored reports to jumpstart your compliance efforts – saving you staff time and reducing audit costs
Title
Description
Sarbanes Oxley (FFIEC 1.1.1.4) Security Policy report
No description given
Sarbanes Oxley (FFIEC 1.3.1.1) Classification report
No description supplied
Sarbanes Oxley (6.3, 8.1.3) Security alert
Alerts sent in response to policy exceptions or special attention exceptions.
Sarbanes Oxley (8.1.2) Operational change control
Changes to the operating environment such as system updates, DBA activity etc.
Sarbanes Oxley (8.1.6) External contractors
Exceptions and failures caused by External Contractors.
Sarbanes Oxley (8.3) Malicious attacks
Exceptions and failures due to Malicious attacks.
Sarbanes Oxley (8.4.2) Operator log
Actions performed by the IT Admin staff.
Sarbanes Oxley (8.5) Network management
Actions and events caused by users on Network Services.
Sarbanes Oxley (8.7.4.1) Mail server
Exceptions and failures for the Mail Server assets.
Sarbanes Oxley (8.7.6) Publicly available systems
Actions and exceptions on Publicly Published Data.
Sarbanes Oxley (9.2.4, 9.7) Review of user access rights
Actions performed by administrators on users.
Sarbanes Oxley (9.2.4.c, 9.7) System access and use
Successes and failures against key assets
Sarbanes Oxley (9.3) User responsibilities and password use
Logon failures and successes either locally or remotely.
Sarbanes Oxley (9.4) Network access control
Actions performed on and events and exceptions generated by Network or Router.
Sarbanes Oxley (9.4.4) Node authentication
Authentication of connections to remote computer systems
Sarbanes Oxley (9.4.5) Remote diagnostic port access
Detection of accesses to the diagnostic ports on servers.
Sarbanes Oxley (9.5.3) User identification and authentication
Logon/Logoff successes and failures.
Sarbanes Oxley (9.5.5) System utilities
Usage of system utilities
Sarbanes Oxley (9.6) Application access control
Actions, Exceptions and events on HR Data, Sensitive Data, User Sensitive Data, System, Financial Data, Proprietary Data and General Data.
Sarbanes Oxley (9.6.1) Information access restrictions
Who accessed sensitive or private data successfully or unsuccessfully.
Sarbanes Oxley (9.6.2) Sensitive system isolation
Exceptions and failures against sensitive systems data in asset groups User, HR Data, Source Code, and Financial Data
Sarbanes Oxley (9.7.2.3) Logging and reviewing events
Exceptions and failures recorded by the InSIght system.
Sarbanes Oxley (9.8.1) Mobile worker
Exceptions and failures for mobile workers.
Please login into the Consul InSight Suite. This will give you access to all the products available with this specific username.
If you forgot your username and/or password please contact your administrator.
Contact us
In the US:
contactsales@consul.com
Direct Line: +1 703 675 2022
Toll Free (US only): 800 258 5077
EMEA and Asia Pac:
contactsales@consul.com
Direct Line: +31 15 251 3333

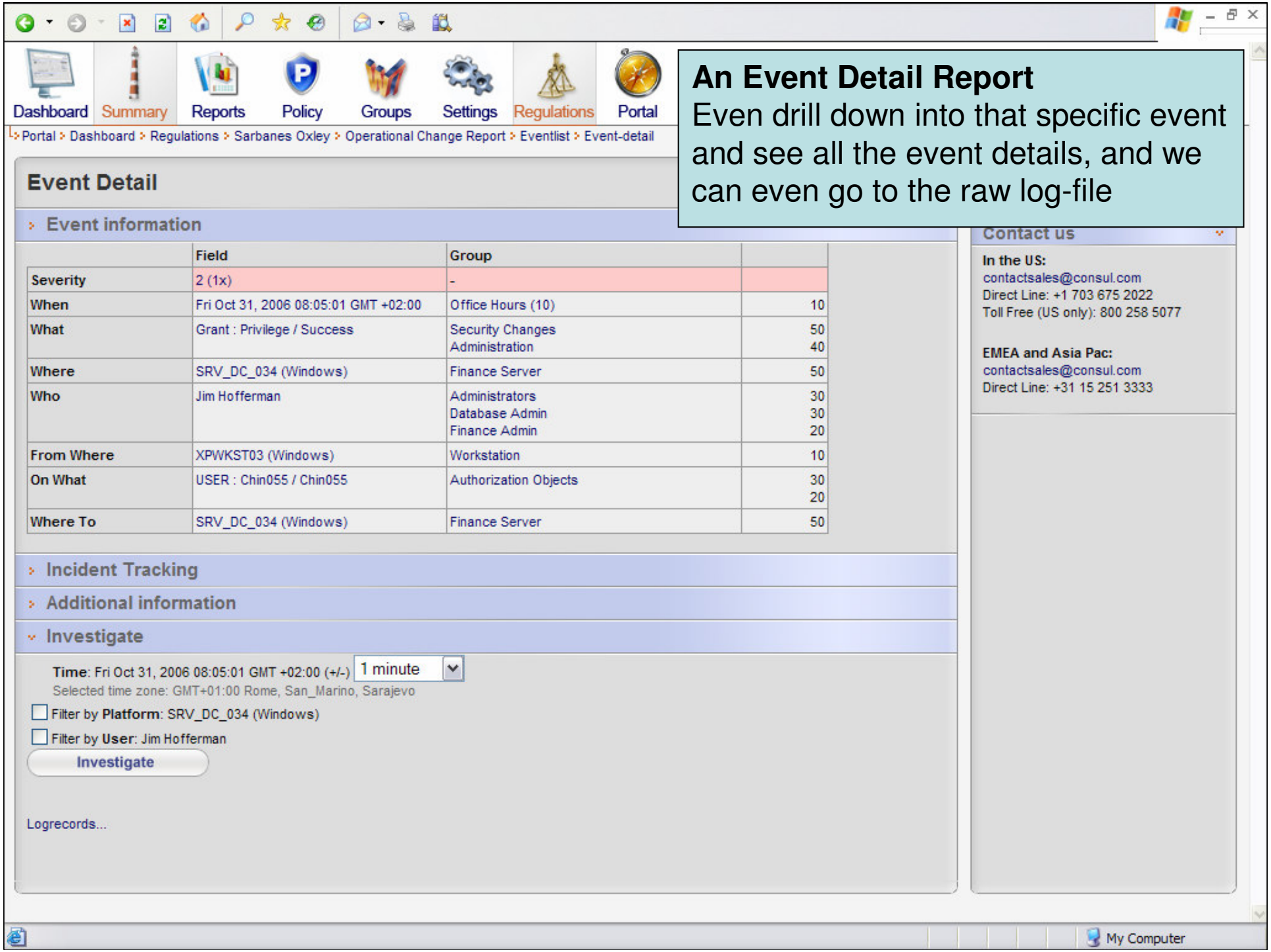


Operational Change Control Report
See a summary of all the operational changes made by different groups



Event List

Zoom in into the all actions that IT admin did on the financial Server and see the creation of the user account of Chin055

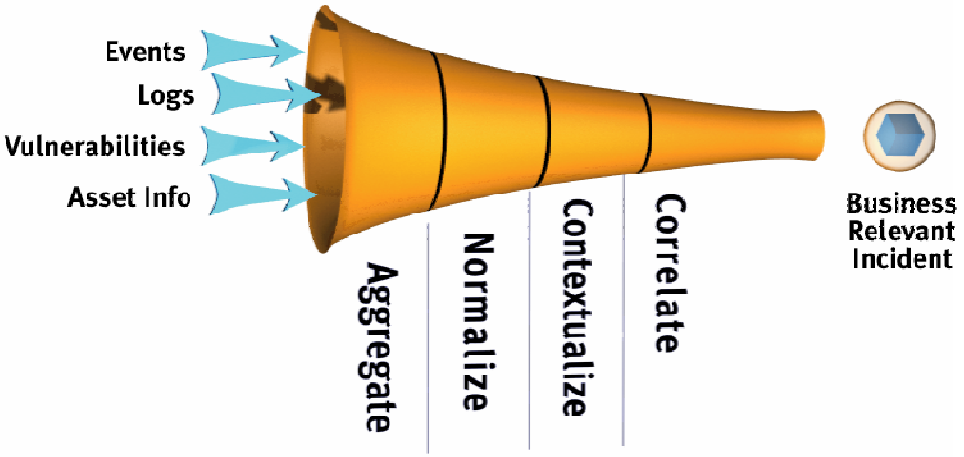


An Event Detail Report

Even drill down into that specific event and see all the event details, and we can even go to the raw log-file

IBM TSOM – Real-Time Correlation and Monitoring

IBM Tivoli Security Operations Manager (TSOM) is a real-time security information and event management (SIEM) platform designed to improve the effectiveness and efficiency of security operations and information risk management. TSOM centralizes and stores security data from throughout the heterogeneous technology infrastructure so that security analysts can:

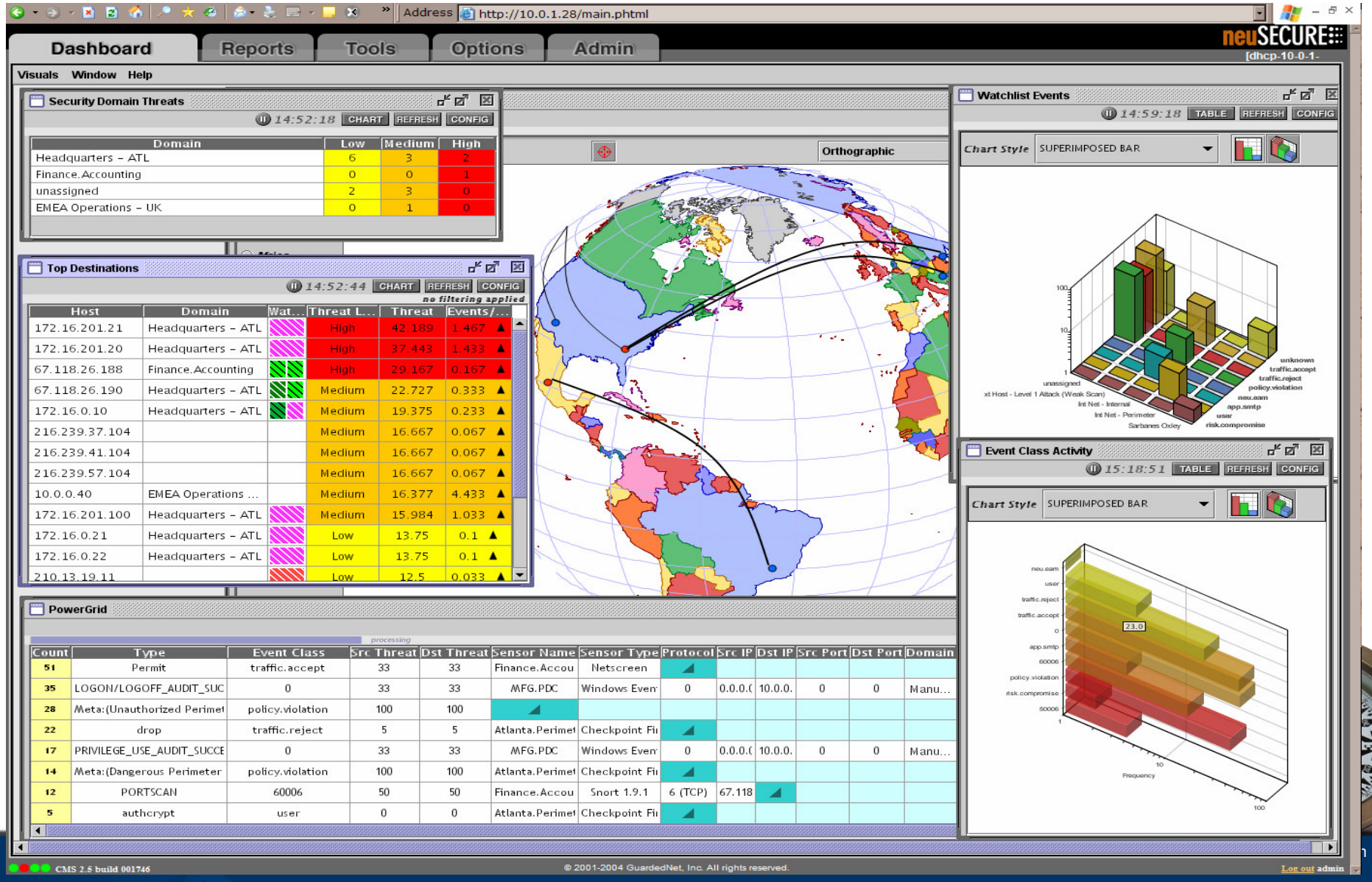


Key Features

- **Log Management** - automated aggregation of security events and audit logs
- **Correlation -** Real-time, cross-device event correlation for incident management and investigation
- **Regulatory Compliance** – reporting and policy monitoring to support regulatory compliance initiatives
- Maximize and amplify security operations resources through automation
- Integrates Security Operations with other IT Operations groups via Netcool and TEC

"TSOM automates the aggregation and correlation process. It mitigates false positives and alerts my team to real threats in a timely manner. The product is more or less what I would have designed and built myself, given four years and a pool of developers." ~ Communications User of TSOM

Consolidated View via TSOM Customizable Dashboard



Agenda

Problems

Solution: TSIEM-- The 3 C's

1. Capture – Enterprise Log Management
2. Comprehend – Sophisticated Log Interpretation
3. Communicate – Full Audit and Compliance Reporting

Technology

Proven Results

Architecture

Agenda

Problems

Solution: TSIEM

1. Capture – Enterprise Log Management
2. Comprehend – Sophisticated Log Interpretation
3. Communicate – Full Audit and Compliance Reporting

Technology

Proven Results

Customers Turn to TSIEM

Multinational Insurance Company	To close compliance gaps for SOX; centralize collection, monitoring, and reporting of millions of log files; and provide transparency into the activities of privileged users across a heterogeneous network.
Major US Payment Processor	To prepare for federal regulations and to meet the requirements of the VISA CISP, this large payment processor brought Consul onboard to help audit enterprise IT.
Major Office Supplies Store	The Manager of Data Security began looking for a solution to audit their entire enterprise IT environment.
Large US Grocery Chain	Needed IT audit solution they could roll-out across the corporate network to audit AIX, mainframe, UNIX, Windows and OS/400, and then to 2,500 stores.
Industrial Cleaning Firm	In order to meet SOX requirements and IT Security best practices, the Director of IT Security began looking for a product that could help them manage their log data.
Major Office Equipment Manufacturer	Company received a mandate from their CEO to comply with federal regulatory requirements, specifically Sarbanes-Oxley
Global Food Manufacturer	IT Security team driven by requirements given to them by Internal Auditors to meet Sarbanes-Oxley requirements

The TSIEM Difference

Increasing Requirements

Increasing Complexity

Increasing Cost

- Unique ability to monitor user behavior
- Enterprise compliance dashboard
- Compliance management modules and regulation-specific reports
- Broadest, most complete log and audit trail capture capability
- W7 log normalization translates your logs into English
- Easy ability to compare behavior to regulatory and company policies

What makes you special?

Tivoli Security Information & Event Management

IBM Governance and Risk Management

Business alignment, visibility and control