

# IBM Software Day 2007



Hur kan IBM hjälpa dig att förbereda för framtida revisioner?

vad gör dig\*  
unik?

# Agenda

## ***What's the issue?***

- ***What's going on?***
- ***Common issues***

## ***How can we solve this?***

- ***The 3-step solution***
- ***Introducing SIEM***

## ***Why customers turn to IBM***

# What's the issue?



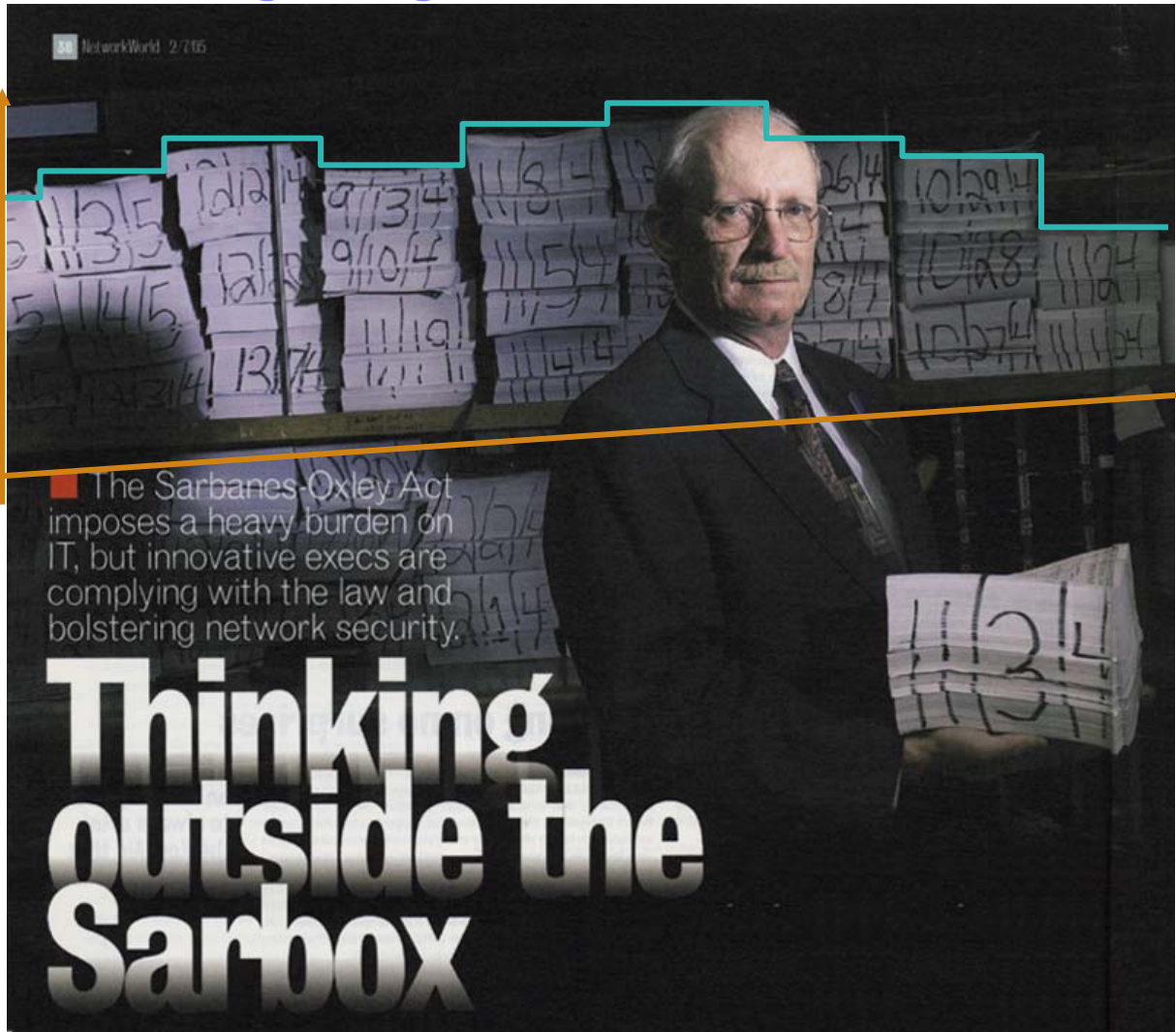
## Increasing Requirements

- PCI
- SOX
- Euro SOX
- BASEL II

## Increasing Cost

- Internal Control
- Fines
- Legal Processes
- Operatioan risk

# What's going on?



How do you know what's happening inside of your IT-environment?

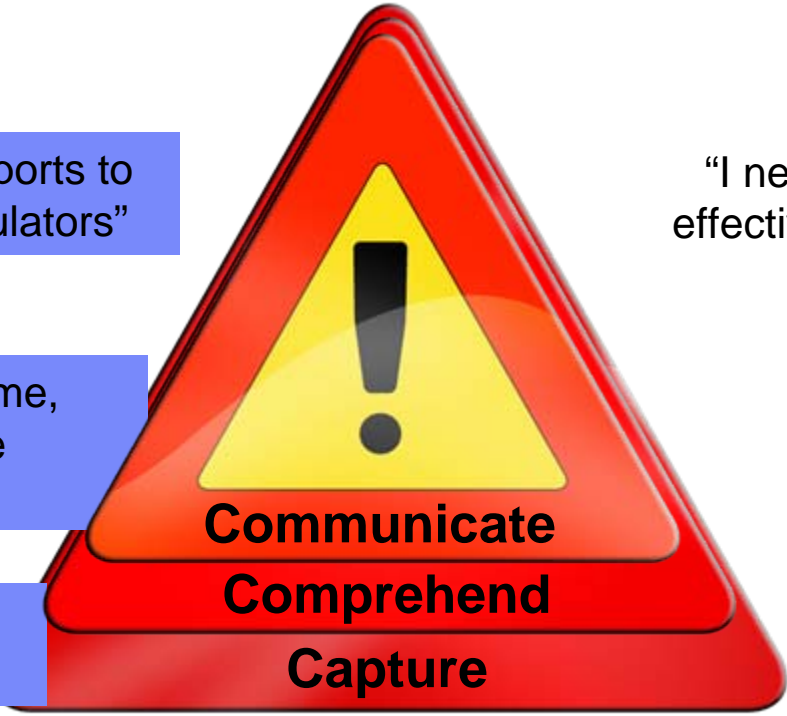
And how can you easily prove that the auditor?

# Common issues

“I need to provide reports to my auditors and regulators”

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

“I need to store logs for forensics”



“I need to prove that I have effective IT security controls”

“I’m concerned about privileged actions”

“I have no idea which logs to collect or how”

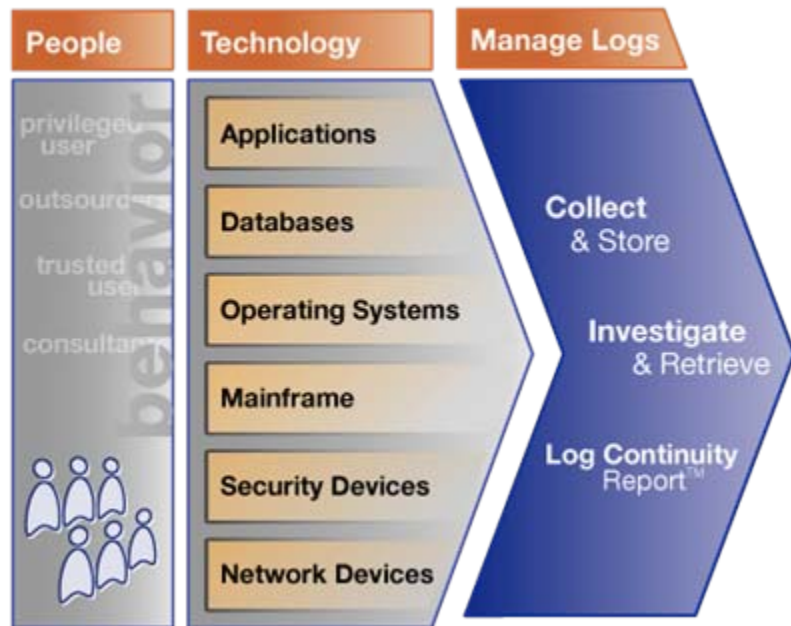
# How can we solve this - The 3-step-solution

*Capture*

*Comprehend*

*Communicate*

# Step one - Enterprise Log Management



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**



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 | Point of presence | Audited machine name | Event source type      | Event source name      |
|----------------|-------------------|----------------------|------------------------|------------------------|
| all            | all               | all                  | all                    | all                    |
| server-01      | SERVER-05         | SERVER-05            | InSight Server Activit | InSight Server Activit |
| server-05      |                   | STYX                 | InSight Web Applica    | Internet Information S |
|                |                   |                      | Microsoft Windows      | Oracle                 |
|                |                   |                      | 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

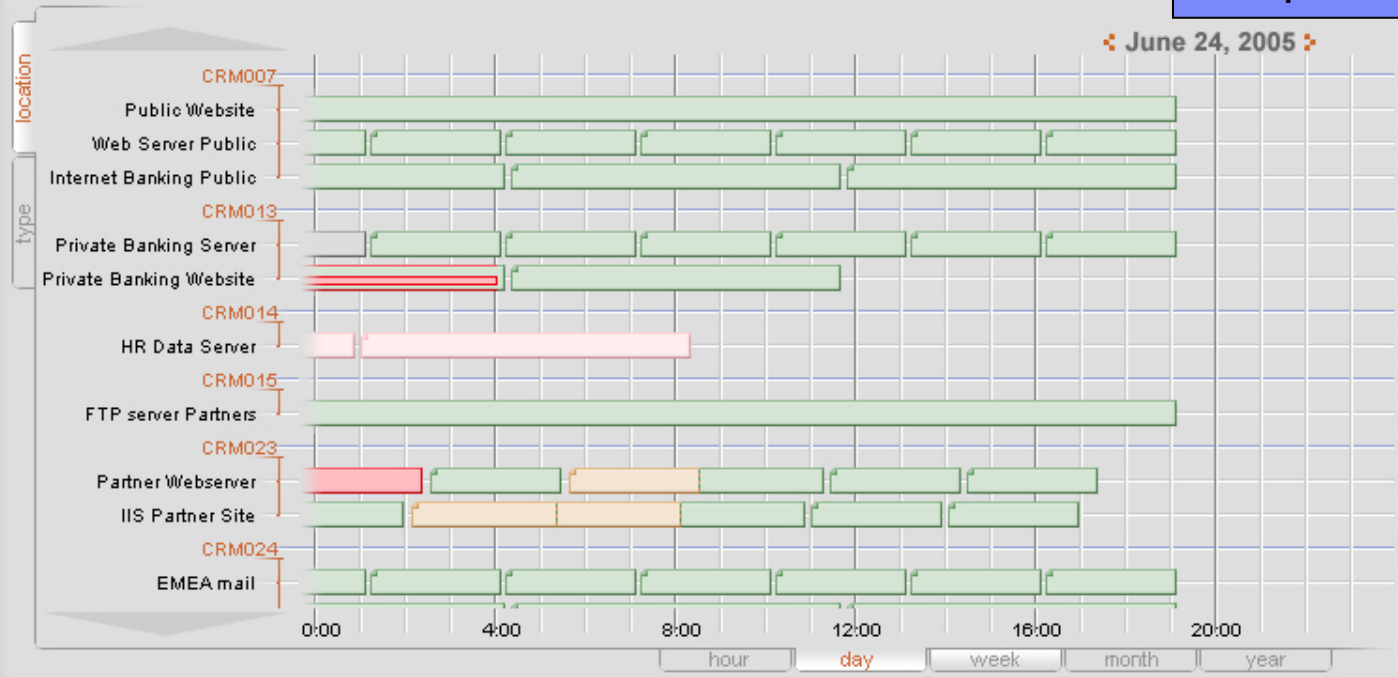
**Support**



**Log Continuity Report**  
 Instant proof to auditors and regulators that your log management program is complete and continuous.

## Log Continuity Report

### Graph



### 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  |

- 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

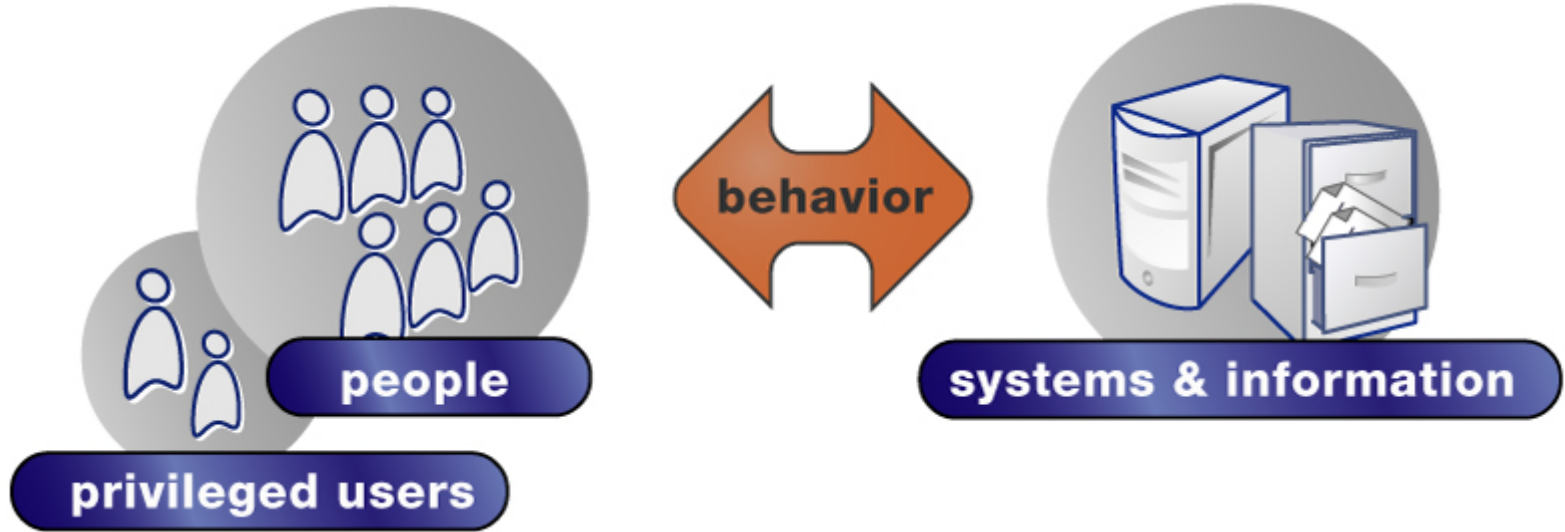
- #### Filters
- #### Sorting
- Start Date
  - Start Time
  - Audited Machine

- #### Legend
- Continuity Logfile
  - Missing Logfile
  - Missing Sub Logfile
  - Failed collect, not collected yet
  - Delayed collect, possible lost
  - Archived Logfile
  - Corrupt Logfile

#### Report information

# Step two – understanding the logs

Comprehend



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

# How do you make sense of all this?

Comprehend

The image displays two terminal windows side-by-side, illustrating the process of parsing security audit logs. The left window shows a raw log entry with a red box highlighting the remote node ID 'xyzz.bananajunior.com'. The right window shows a formatted view of the same log entry, with red boxes and arrows highlighting specific fields: 'Process name: MQMTC\_P2\_BG164', 'Process owner: [MQM\_SERVER]', and 'Remote node id: 241859594'. The bottom window shows a list of system logs with a red box highlighting 'user=MQM'.

```

AUDIT_200503.AUDIT (C:\Documents and Settings\ross\Desktop) - GVIM2
...
^@^H^@^Y^H^@^L^@^F^@SECURITY^L^@2^@S^@z^@A^@*^@
^M^@*^@BATCH_440^H^@/^@D^@A^@H^@W^@Apjyjj^H^@^
^@^H^@^Z^@H^@^@^@^@
^@^G^@APPLES.^@S^@DSA0:[SYS1.SYSCOMMON.][SYSEXE]LOGINOUT.EXE^F^@E^@T
^@L^@F^@SECURITY^H^@^@
|j^N^G^@-^@MQM^Y^@ ^xyzz.bananajunior.com^L^@2^@00^@0d^@x^@E^@H^@E^@m^@*^@
^R^@*^@MQMTC_P2_BG164^H^@/^@A^@A^@H^@W^@Apjyjj^H^@^X^@Apjyjj
^@^H^@^Y^H^@^@^@^@
^@^G^@CYGNUS.^@S^@DSA0:[SYS0.SYSCOMMON.][SYSEXE]LOGINOUT.EXE^F^@A^@T
^@L^@F^@SECURITY^L^@2^@Q^@c^@n^@z^@A^@*^@H^@E^@w^@!^@ $^@8^@SYSTEM
43^H^@/^@D^@A^@H^@W^@Apjyjj^H^@^X^@Apjyjj
^@^H^@^Y^H^@^@^@^@
^@^G^@CYGNUS.^@S^@DSA0:[SYS0.SYSCOMMON.][SYSEXE]LOGINOUT.EXE^G^@A^@T
^@L^@F^@SECURITY^L^@2^@Q^@c^@n^@z^@A^@*^@H^@E^@w^@!^@ $^@8^@SYSTEM
secure (C:\Documents and Settings\ross\Desktop\logs_fedora3) - GVIM3
443^H^@/^@D^@A^@H^@W^@Apjyjj^H^@^X^@Apjyjj
^@^H^@^Y^H^@^@^@^@
^@^G^@CYGNUS.^@S^@DSA0:[SYS0.SYSCOMMON.][SYSEXE]LOGINOUT.EXE^G^@A^@T
^@L^@F^@SECURITY^L^@2^@Q^@c^@n^@z^@A^@*^@H^@E^@w^@!^@ $^@8^@SYSTEM
Apr 5 17:20:30 syslog su(pam_unix)[10429]: authentication failure; logname=
tty=ruser=acristal rhost= user=MQM
Apr 5 17:22:03 syslog sshd(pam_unix)[10351]: session closed for user acrist
Apr 5 18:01:01 syslog crond(pam_unix)[10436]: session closed for user MQM
Apr 5 19:01:01 syslog crond(pam_unix)[10438]: session closed for user MQM
Apr 5 20:01:01 syslog crond(pam_unix)[10440]: session closed for user MQM
Apr 5 21:01:01 syslog crond(pam_unix)[10442]: session closed for user MQM
Apr 5 22:01:01 syslog crond(pam_unix)[10444]: session closed for user MQM
Apr 5 23:01:01 syslog crond(pam_unix)[10446]: session closed for user MQM
Apr 6 00:01:01 syslog crond(pam_unix)[10448]: session closed for user MQM
Apr 6 01:01:01 syslog crond(pam_unix)[10450]: session closed for user MQM
Apr 6 02:01:01 syslog crond(pam_unix)[10452]: session closed for user MQM
Apr 6 03:01:01 syslog crond(pam_unix)[10477]: session closed for user MQM
Apr 6 03:33:29 syslog crond(pam_unix)[10479]: session closed for user MQM
Apr 6 04:01:02 syslog crond(pam_unix)[10509]: session closed for user MQM
Apr 6 04:03:46 syslog crond(pam_unix)[10511]: session closed for user MQM
Apr 6 04:30:02 syslog crond(pam_unix)[11012]: session closed for user MQM
Apr 6 05:01:01 syslog crond(pam_unix)[11031]: session closed for user MQM
Apr 6 06:01:01 syslog crond(pam_unix)[11033]: session closed for user MQM
Apr 6 07:01:01 syslog crond(pam_unix)[11035]: session closed for user MQM
Apr 6 08:01:01 syslog crond(pam_unix)[11037]: session closed for user MQM
Apr 6 08:42:11 syslog sshd(pam_unix)[11041]: session opened for user ebarrios by (uid=0)
Apr 6 08:42:43 syslog sshd(pam_unix)[11071]: authentication failure; logname= uid=0 euid=0 tty=ssh
ruser= rhost=10.101.1.154 user=ebarrios
Apr 6 08:42:49 syslog sshd(pam_unix)[11077]: session opened for user ebarrios by (uid=0)
22,45 Top
  
```

```

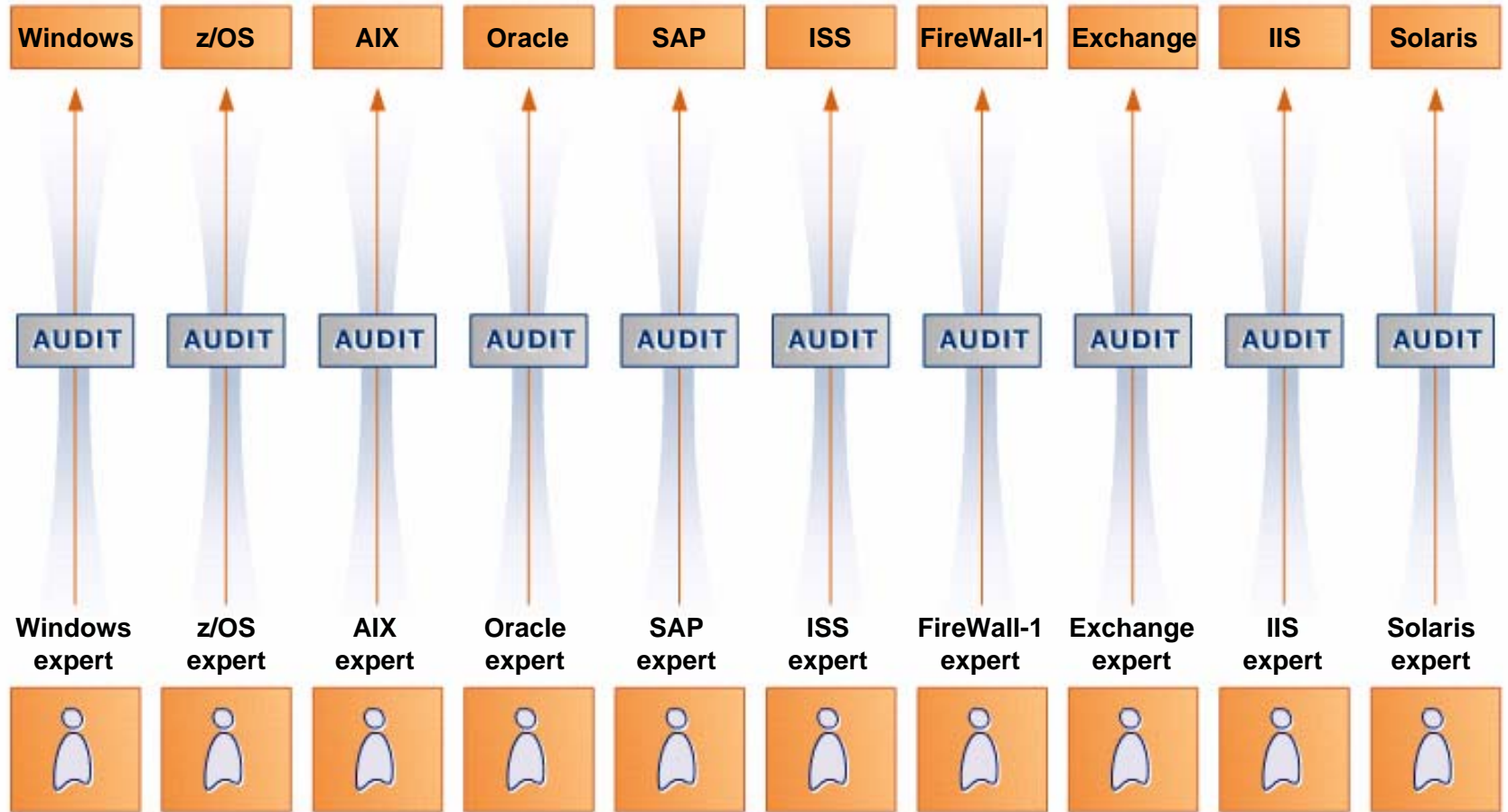
Security audit (SECURITY) on APPLES, system id: 2074
Auditable event: Batch process login
Event time: 1-MAR-2005 00:02:09.84
PID: 20402B44
Process name: BATCH_440
Username: SYSTEM
Process owner: [SYSTEM]
Image name: DSA0:[SYS1.SYSCOMMON.][SYSEXE]LOGINOUT.EXE
Posix UID: -2
Posix GID: -2 (%XFFFFFFFFE)

Security audit (SECURITY) on CYGNUS, system id: 2073
Auditable event: Network login
Event time: 1-MAR-2005 00:02:16.11
PID: 2021A46D
Process name: MQMTC_P2_BG164
Username: MQM
Process owner: [MQM_SERVER]
Image name: DSA0:[SYS0.SYSCOMMON.][SYSEXE]LOGINOUT.EXE
Remote node id: 241859594
Remote node fullname: xyzz.bananajunior.com
Remote username: MQM
Posix UID: -2
Posix GID: -2 (%XFFFFFFFFE)

Security audit (SECURITY) on CYGNUS, system id: 2073
Auditable event: Batch process login
Event time: 1-MAR-2005 00:02:32.61
PID: 20219477
Process name: BATCH_443
Username: SYSTEM
Process owner: [SYSTEM]
  
```

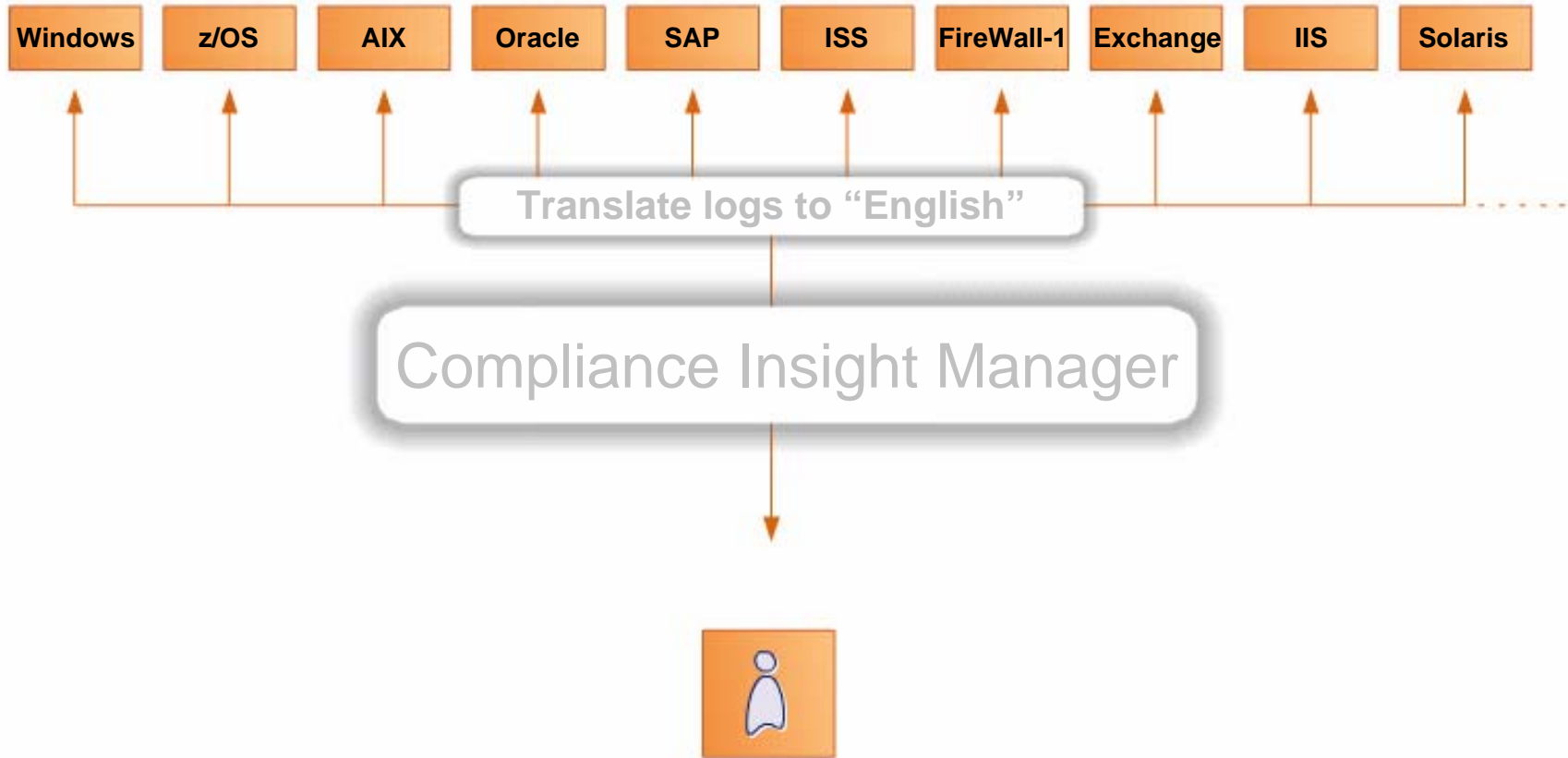
# *Today -skill is needed on all platforms*

Comprehend



*With TCIM – all logs are translated into a normalized form*

Comprehend



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

# Normalization - the W7 Methodology

Comprehend

Who did What type of action on What?

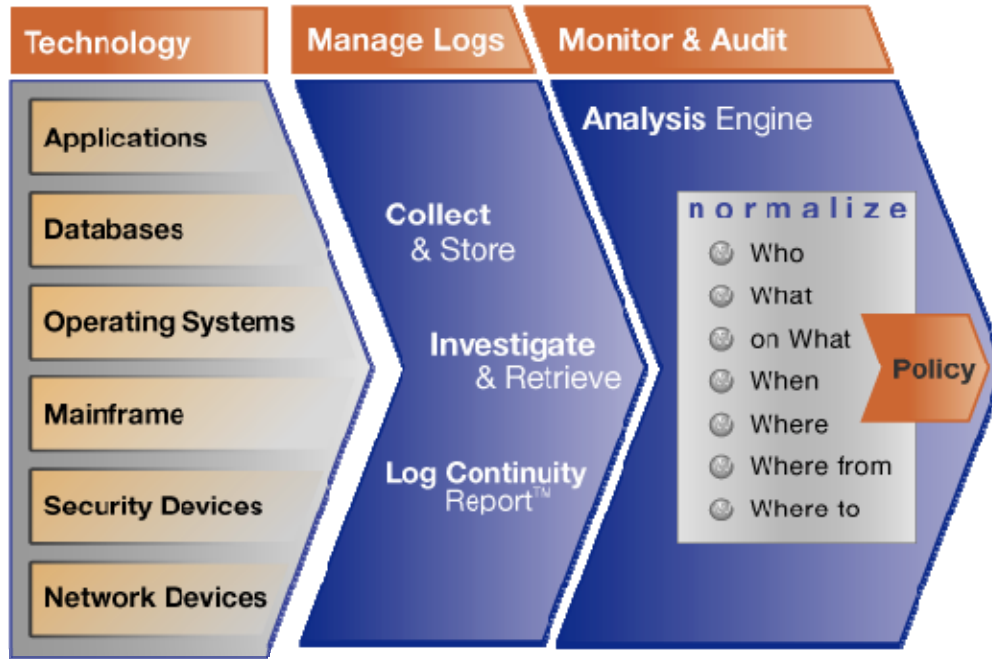
When did he do it and Where, From Where and Where To?

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



# Sophisticated Log Interpretation and Correlation

Comprehend



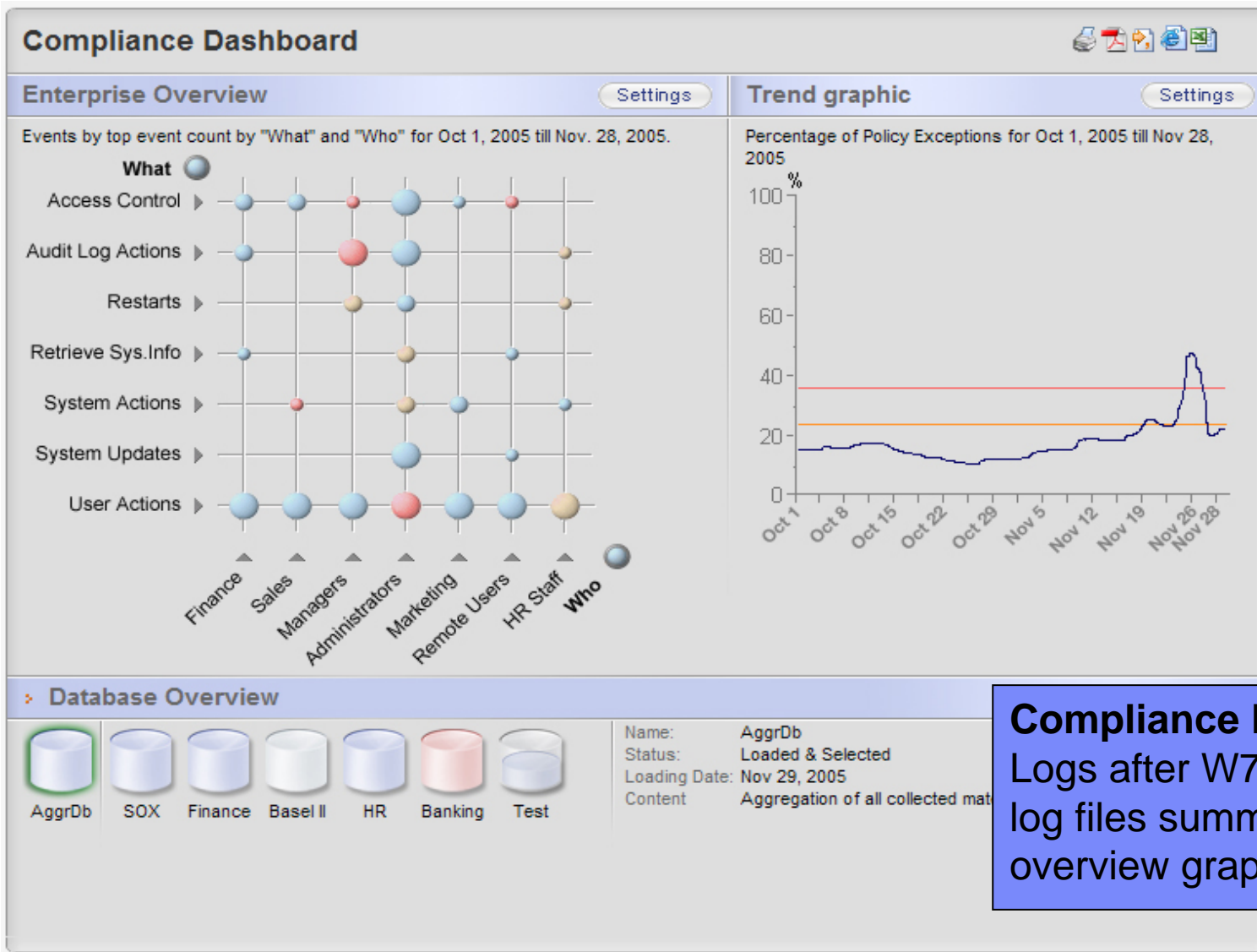
Capabilities:

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



**Out of the box log normalization!**

# Compliance Dashboard



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



# W7 Eventlist

Note!: Mike Bonfire, a DBA, is reading the payroll

## 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

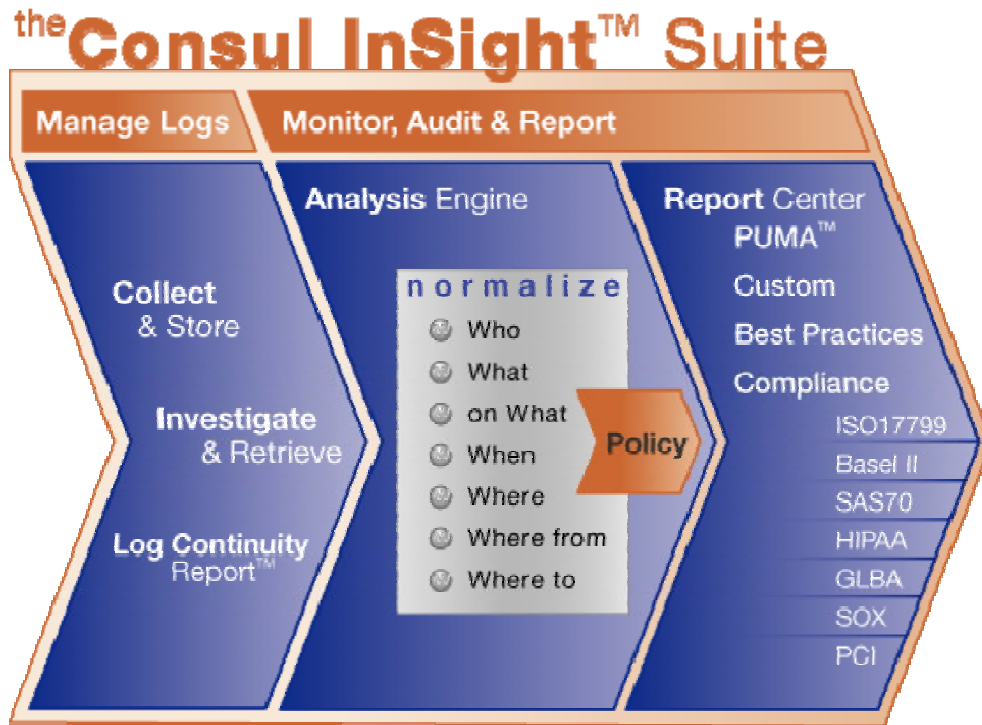
Time zone Event time zone

### 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 Hofferan | 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 Hofferan | 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 Hofferan | DB2 Server     | DATABASE : - / Unavailable       | DB2 Server     |
| 50       | Sun Sep 03 2006 09:20:01 GMT-05:00 | 1 | Access : Dbobject / Success | DB2 Server     | Jim Hofferan | 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 |

# Step three – Communicating

Communicate



Capabilities:

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

**Regulation specific modules with tailored reports to jumpstart your compliance efforts – saving you staff time and reducing audit costs**

## Sarbanes Oxley Regulation Reports

| 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**

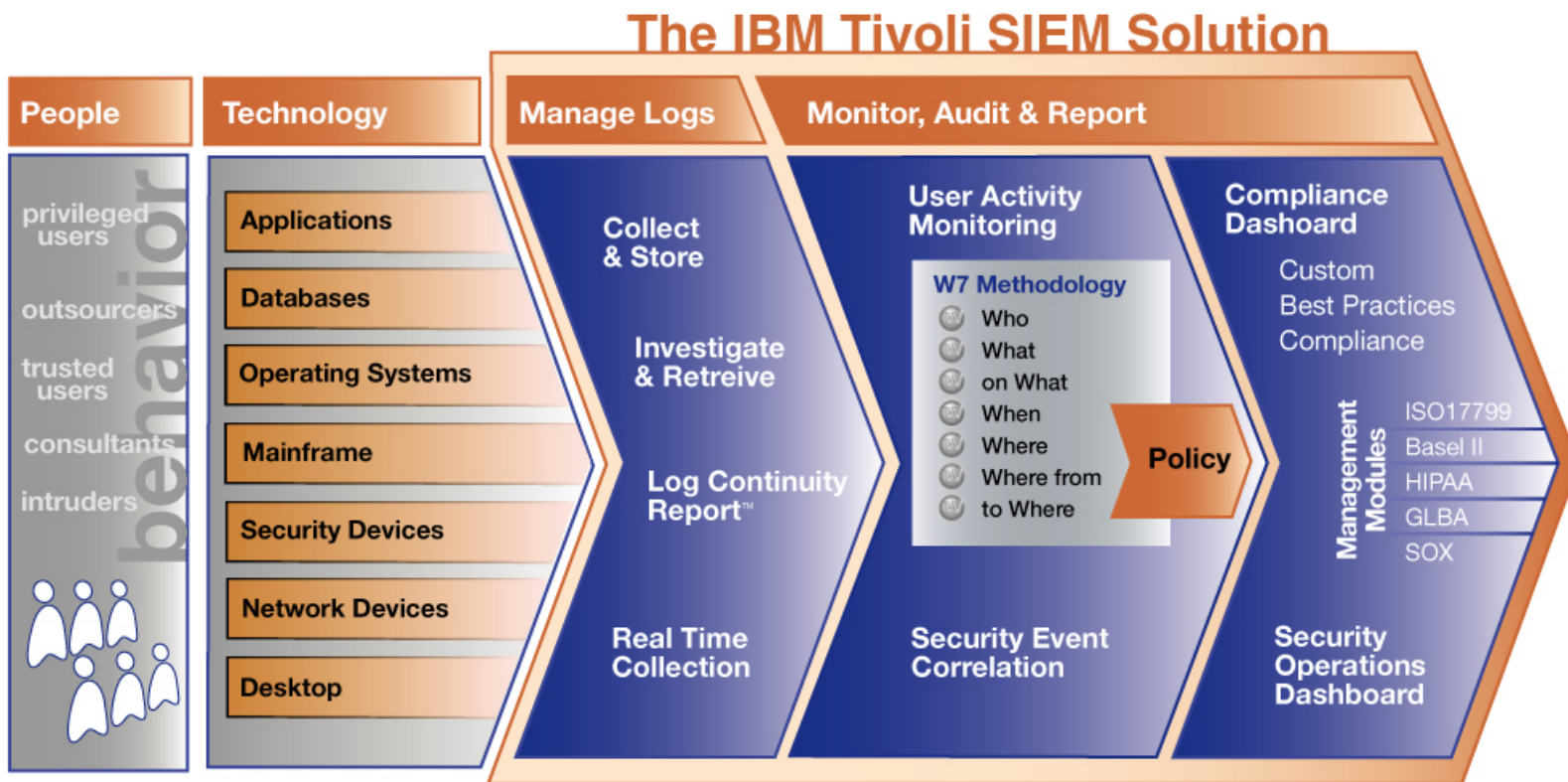
**In the US:**  
[contactsales@consul.com](mailto:contactsales@consul.com)  
 Direct Line: +1 703 675 2022  
 Toll Free (US only): 800 258 5077

**EMEA and Asia Pac:**  
[contactsales@consul.com](mailto:contactsales@consul.com)  
 Direct Line: +31 15 251 3333

# PCI Compliance Reporting

| ▼ PCI  |  |   |   |
|--|--|---|---|
| Type   | Title  | Description   | Action  |
|  | PCI (10.1) Access to System Components   | Accessing System components                                     |     |
|  | PCI (10.2.1) All Access to Credit Card Data                                    | Display all access to credit card database tables               |     |
|  | PCI (10.2.2) All Actions by Individuals with Root or Administrative Privileges | This report displays all actions by root on UNIX/LINUX systems. |     |
|  | PCI (10.2.3) Access to all audit trails  | Access to all audit trails                                      |     |
|  | PCI (10.2.4) Invalid logical access attempts                                   | Invalid logical access attempts                                 |     |
|  | PCI (10.2.6) Initialization of the audit logs                                  | Initialization of the audit logs                                |     |
|  | PCI (10.2.7) System-level object access  | Accessing system level objects                                  |     |
|  | PCI (10.3) Audit trail entries for all system components                       | List of audit trail entries for all system components           |     |
|  | PCI Failed Access attempts to Credit Card Data                                 | Display all Failed access to credit card database tables        |     |

# Introducing ... The IBM Tivoli SIEM Solution



# Adding real time security event correlation

Address <http://10.0.1.28/main.phtml> [dhcp-10-0-1-]

Dashboard Reports Tools Options Admin

### Security Domain Threats

14:52:18 CHART REFRESH CONFIG

| Domain               | Low | Medium | High |
|----------------------|-----|--------|------|
| Headquarters - ATL   | 6   | 3      | 2    |
| Finance.Accounting   | 0   | 0      | 1    |
| unassigned           | 2   | 3      | 0    |
| EMEA Operations - UK | 0   | 1      | 0    |

### Top Destinations

14:52:44 CHART REFRESH CONFIG

no filtering applied

| Host           | Domain              | Wat... | Threat L... | Threat | Events/... |
|----------------|---------------------|--------|-------------|--------|------------|
| 172.16.201.21  | Headquarters - ATL  | High   | High        | 42.189 | 1.467 ▲    |
| 172.16.201.20  | Headquarters - ATL  | High   | High        | 37.443 | 1.433 ▲    |
| 67.118.26.188  | Finance.Accounting  | High   | High        | 29.167 | 0.167 ▲    |
| 67.118.26.190  | Headquarters - ATL  | Medium | Medium      | 22.727 | 0.333 ▲    |
| 172.16.0.10    | Headquarters - ATL  | Medium | Medium      | 19.375 | 0.233 ▲    |
| 216.239.37.104 |                     | Medium | Medium      | 16.667 | 0.067 ▲    |
| 216.239.41.104 |                     | Medium | Medium      | 16.667 | 0.067 ▲    |
| 216.239.57.104 |                     | Medium | Medium      | 16.667 | 0.067 ▲    |
| 10.0.0.40      | EMEA Operations ... | Medium | Medium      | 16.377 | 4.433 ▲    |
| 172.16.201.100 | Headquarters - ATL  | Medium | Medium      | 15.984 | 1.033 ▲    |
| 172.16.0.21    | Headquarters - ATL  | Low    | Low         | 13.75  | 0.1 ▲      |
| 172.16.0.22    | Headquarters - ATL  | Low    | Low         | 13.75  | 0.1 ▲      |
| 210.13.19.11   |                     | Low    | Low         | 12.5   | 0.033 ▲    |

Orthographic

### Watchlist Events

14:59:18 TABLE REFRESH CONFIG

Chart Style SUPERIMPOSED BAR

unknown traffic.accept  
traffic.reject  
policy.violation  
risk.comprise  
app.smtip  
user

### Event Class Activity

15:18:51 TABLE REFRESH CONFIG

Chart Style SUPERIMPOSED BAR

Frequency

### PowerGrid

processing

| Count | Type                       | Event Class      | Src Threat | Dst Threat | Sensor Name     | Sensor Type   | Protocol | Src IP  | Dst IP   | Src Port | Dst Port | Domain  |
|-------|----------------------------|------------------|------------|------------|-----------------|---------------|----------|---------|----------|----------|----------|---------|
| 51    | Permit                     | traffic.accept   | 33         | 33         | Finance.Accou   | Netscreen     |          |         |          |          |          |         |
| 35    | LOGON/LOGOFF_AUDIT_SUC     | 0                | 33         | 33         | MFG.PDC         | Windows Even  | 0        | 0.0.0.0 | 10.0.0.0 | 0        | 0        | Manu... |
| 28    | Meta:(Unauthorized Perimet | policy.violation | 100        | 100        |                 |               |          |         |          |          |          |         |
| 22    | drop                       | traffic.reject   | 5          | 5          | Atlanta.Perimet | Checkpoint Fi |          |         |          |          |          |         |
| 17    | PRIVILEGE_USE_AUDIT_SUCCE  | 0                | 33         | 33         | MFG.PDC         | Windows Even  | 0        | 0.0.0.0 | 10.0.0.0 | 0        | 0        | Manu... |
| 14    | Meta:(Dangerous Perimeter  | policy.violation | 100        | 100        | Atlanta.Perimet | Checkpoint Fi |          |         |          |          |          |         |
| 12    | PORTSCAN                   | 60006            | 50         | 50         | Finance.Accou   | Snort 1.9.1   | 6 (TCP)  | 67.118  |          |          |          |         |
| 5     | authcrypt                  | user             | 0          | 0          | Atlanta.Perimet | Checkpoint Fi |          |         |          |          |          |         |

# *Why customers turn to IBM*

- World leading Enterprise Compliance Dashboard
- World leading Compliance Management Modules and regulation-specific reports
- Unique ability to monitor user behavior
- Possibility to get the best of two worlds (SIM & SEM)
- Proven technology (21 years) combined with the worldwide IBM implementation and support team

# Customers who have chosen IBM

## **Codan / Royal & Sun Alliance**

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



## *Next step*

- Call me for a meeting: 070-793 30 55  
[ronny.linnerheim@se.ibm.com](mailto:ronny.linnerheim@se.ibm.com)



# Questions?

## Customers Worldwide



## Recognized by the press and analysts

