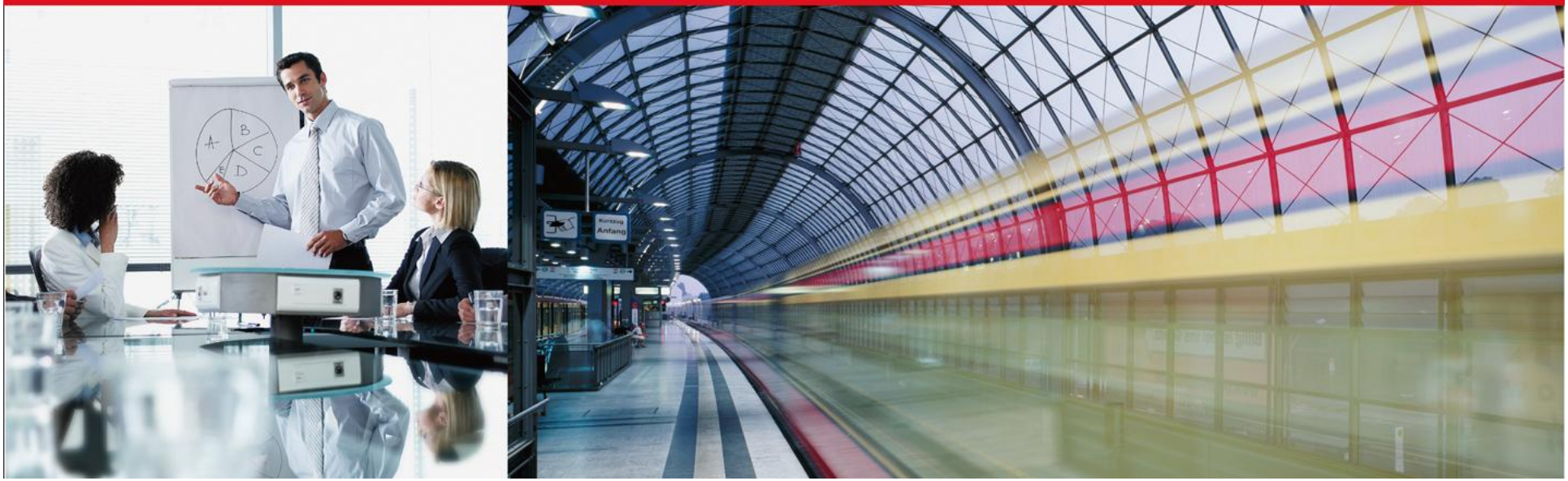
EXPO 2010 SHANGHAI CHINA

IBM

中国2010年上海世博会高级赞助商

IBM服务管理体验之旅

高效管理随需而变 优化服务实践共赢



Title： IBM Tivoli安全軟件銷售經理

姓名 金 天 威 (Eric Chin)
联系方式 echin@tw.ibm.com

演讲主题：

信息安全性是许多企业的首要关注点，因为网络和资源可用性对于保障业务和服务有决定性作用。 为了帮助最大化资源和服务的可用性，同时保护客户信息，信息团队应该具备以下能力：快速识别和处理安全事故；实施安全性策略；支持审计和遵从性计划。

IBM Tivoli Compliance Insight Manager（TCIM)和 IBM Tivoli® Security Operations Manager (TSOM) 可以从资源配置部署及快速识别处理安全事故，保障合规性方面帮助您满足安全运营挑战。

信息安全成为企业CTO/CEO最为头疼的问题

InformationWeek
BUSINESS INNOVATION POWERED BY TECHNOLOGY

Massive Insider Breach at DuPont

February 15, 2007 – A research chemist who worked for DuPont for 10 years before accepting a job with a competitor downloaded 22,000 sensitive documents and viewed 16,706 more …

"The best way to guard against insider breaches is for companies to ***monitor database and network access for unusual activity*** and set thresholds that represent acceptable use for different users."

Source: InformationWeek, Feb. 15, 2007

发生的安全问题:

- 数据被窃取
- 访问关键数据库
- 账号多人共用

Carnegie Mellon CERT Comments:

- "75% of … confidential information thefts studied … were committed by current employees"
- "45% had already accepted a job offer with another company"

如何处理：

- 对于内部访问有更为清晰的了解
- 增加身份控制
- 对特权用户的审计与监控

全面的安全管理必须满足多个方面，包括：风险管理和用户安全管理

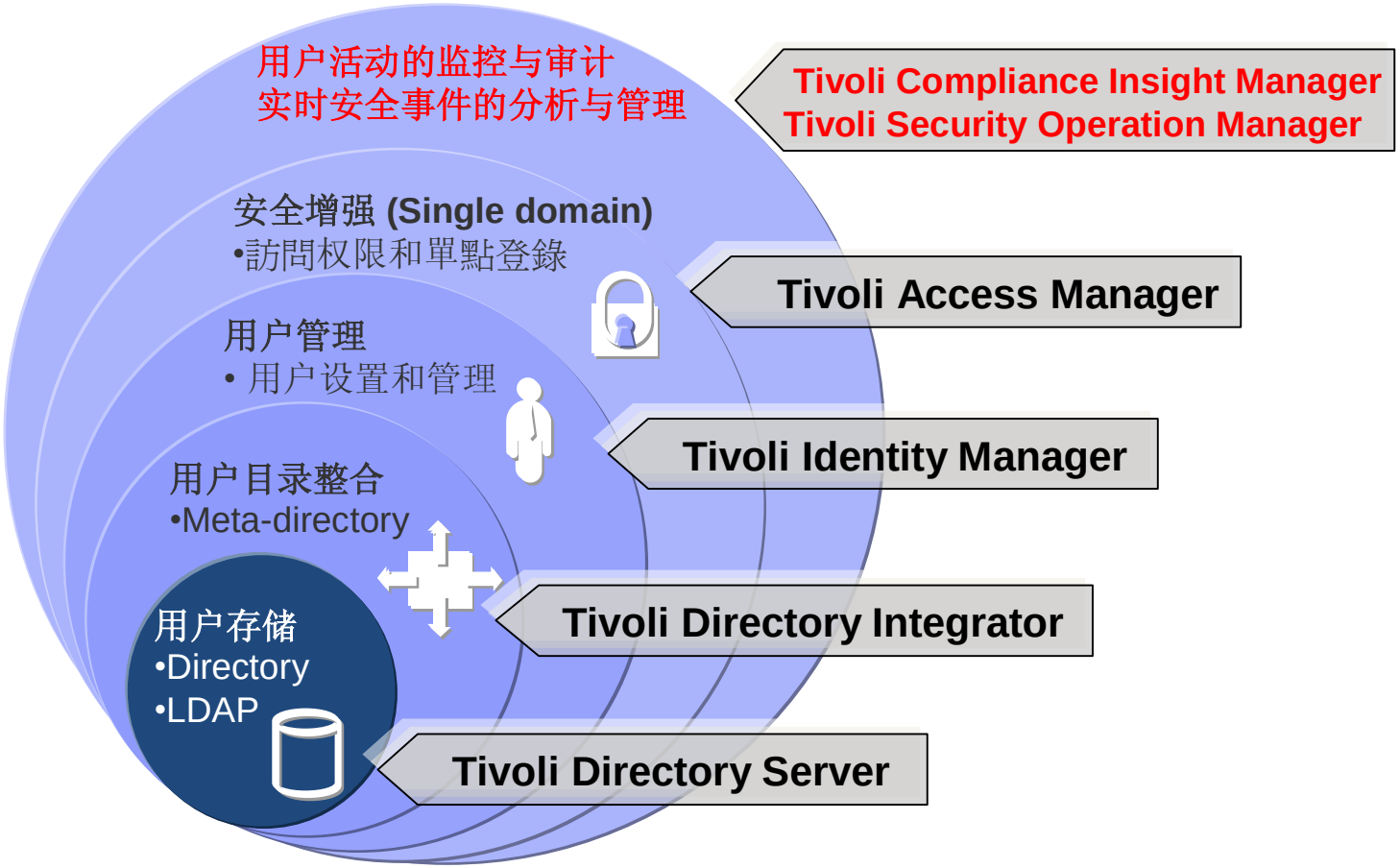
1. “IT 安全管理”

- 主要满足安全风险管理 ***(security threats)***
- 是否遵循制定的安全策略和规范

2. “业务系统安全”

- 主要解决以身份为核心的安全管理 ***(user security)***
  - –谁能进来?
  - –他们能够做什么?
  - –是否能够为审计提供足够的信息

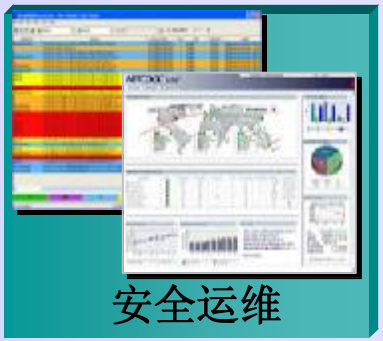
Tivoli 安全管理解决方案构建模块



企业需要集中整合的安全信息管理

实时安全信息

- 以网络、设备为中心的攻击
- 错误配置和误用
- 快速定位攻击行为



安全运维

审计官员

用户行为审计

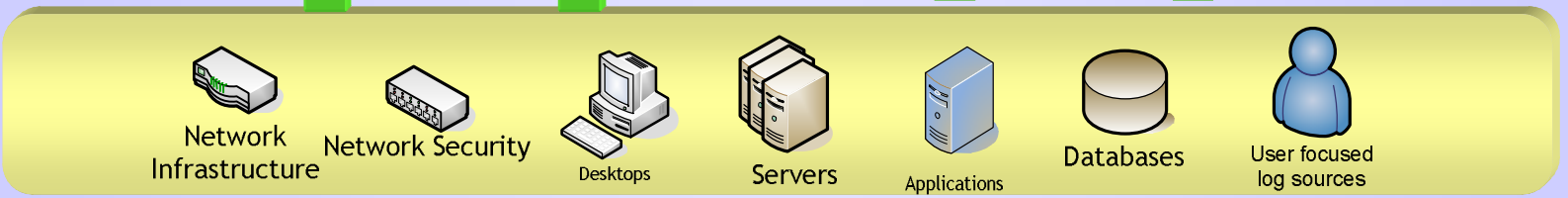
- 发现用户违反规定的非法访问
- 特权用户的审计与监控
- 制度遵从报告

安全事件的分析與管理

安全事件

安全行为

IT安全性的内部审计



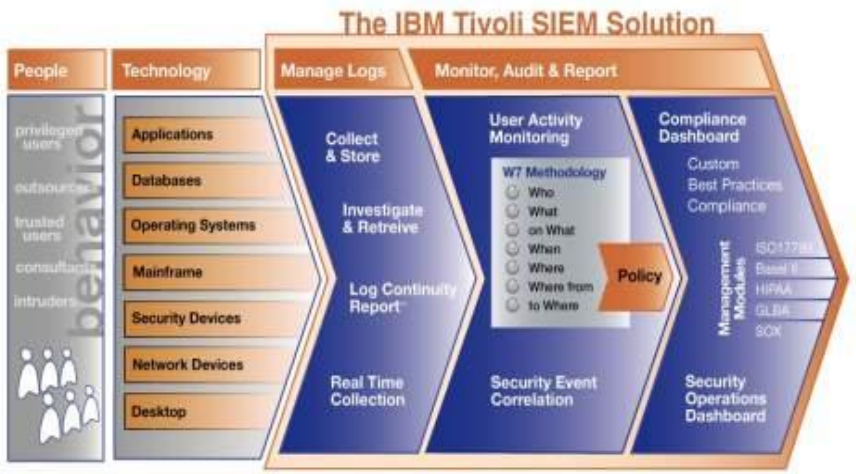
特权用户的监控与审计 – Tivoli Compliance Insight Manager (TCIM)

【解决方案】

- 全面的端到端的安全管理，深入的用户活动监控和全面的审计功能。
- 提高信息安全和风险管理工作的效率和可视性
- 评估企业IT资源的总体安全性和制度遵从状态

【实现功能】

- 通過集中的、強大的安全日誌及事件收集和規則分析能力來發現潛在的安全隱患
- 特权用户的监控与审计，监控特权用户活动，解决违规问题并管理数据
- 安全制度遵从显示板和用户行为和安全事件报告以迅速了解安全制度的遵从状况
- 为遵守规章制度提供全面报告



作为安全管理员，你需要如何完成繁重的审计工作？

- 对海量原始日志文件的调查
  - 我需要审计系统本身就可以提供对原始日志文件的调查能力，而不是我自己打开每个文件去查询
- 理解每种系统的日志信息，从而找到安全隐患
  - 我需要审计系统提供对日志的自动翻译到标准格式的能力，而不是我自己来翻译
- 自动完成对违规行为的发现、严重级别定义
  - 我需要可以在审计系统中定义规则，同时审计系统需要根据我定义的规则对每条日志进行自动分析和安全级别定义
- 能否第一时间得到告警
  - 我希望审计系统和企业的IT运维中心进行连接，统一发送告警
- 完成合规报告
  - 我需要审计系统自动生成我企业需要合规报告，而不是我自己来做！

IBM TCIM 提供一专业审计平台，帮助迎接挑战

要求越来越苛刻

环境越来越复杂

成本飚升

1. 安全制度遵从情况的显示板和报告

用户身份识别和行为审计

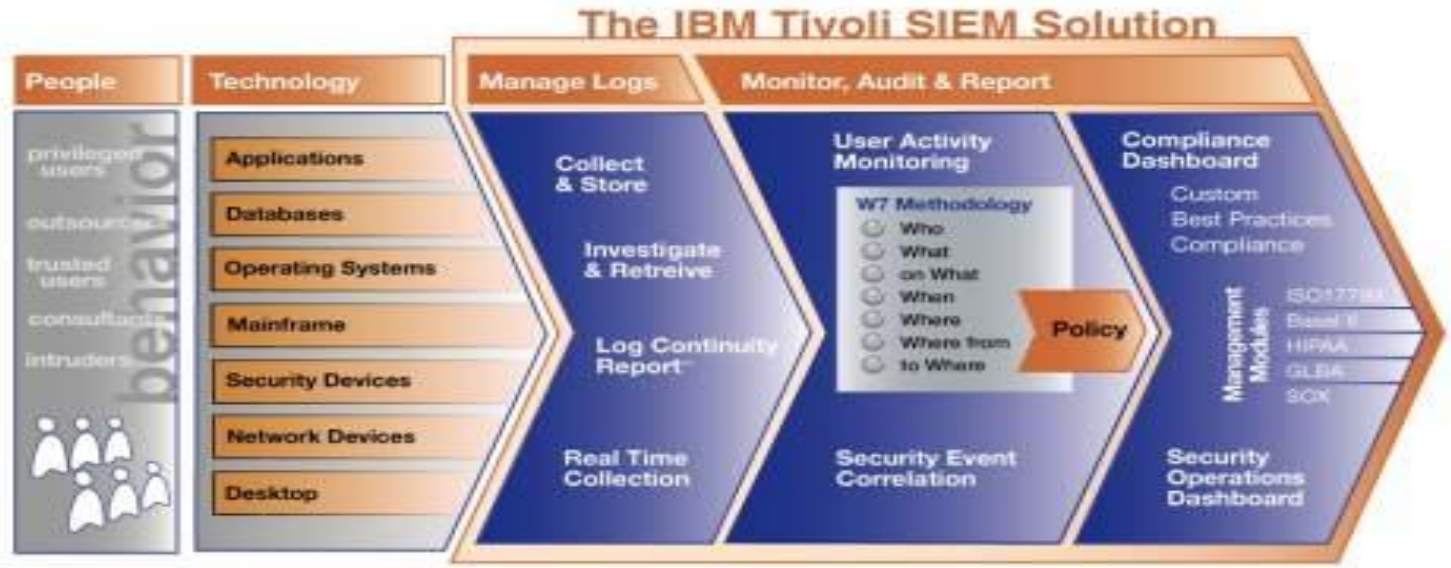
2. 特权用户的监控与审计

3. 数据库的监控和审计

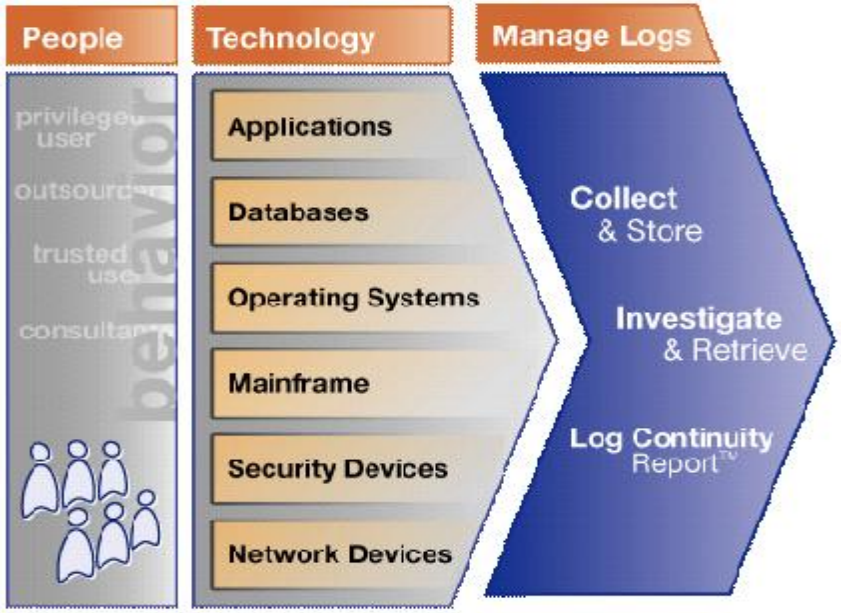
4. 日志和审计跟踪管理

TCIM - 工作原理

- 捕获（Capture）：企业日志收集和管理
- 理解（Comprehend）：精准的日志翻译和解释
- 了解（Communicate）：全面的审计和合规性报告



捕获 (Capture)：企业日志收集和管理



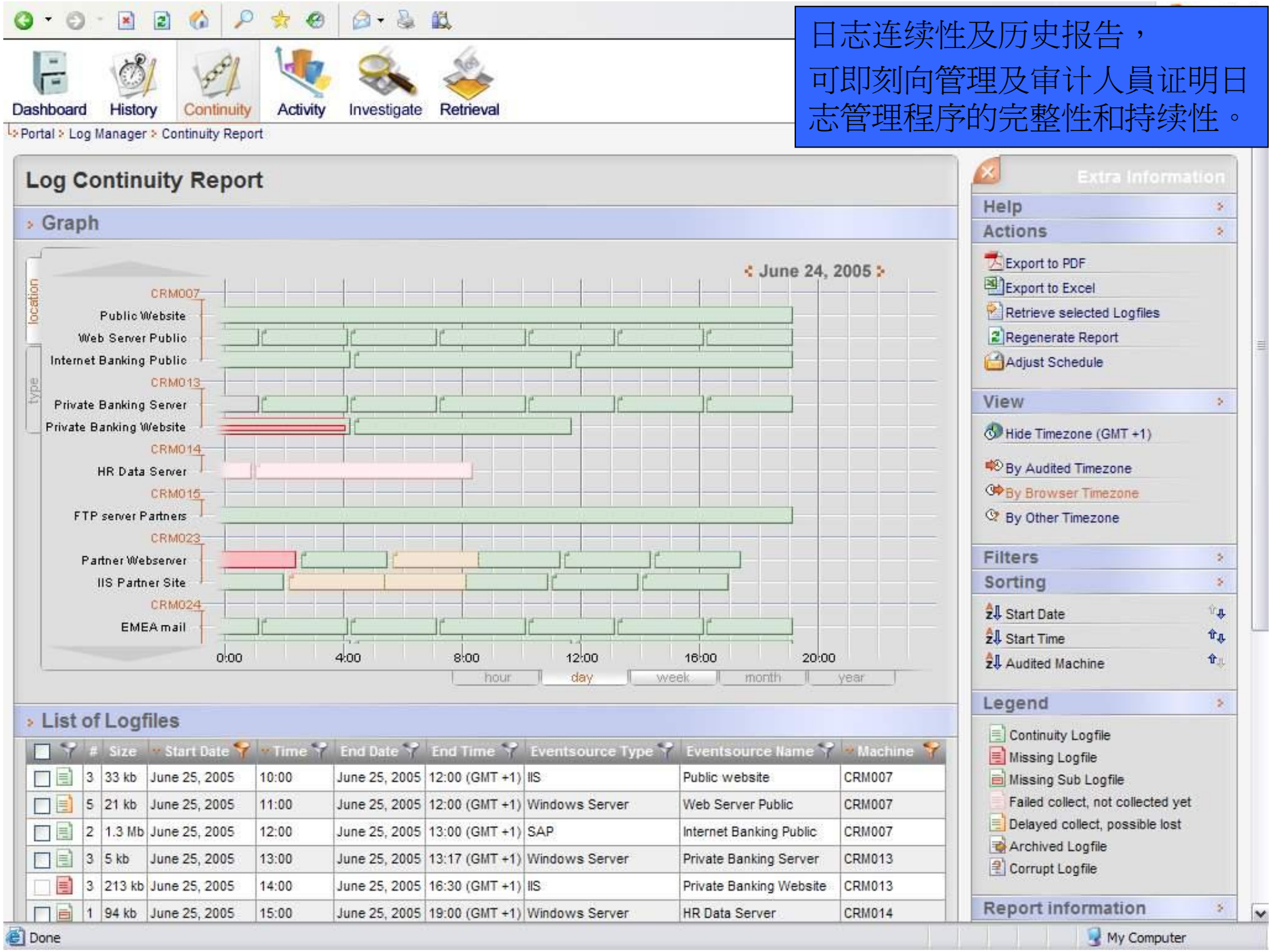
功能：

- 从任何平台安全可靠地捕获日志
- 自动收集系统日志
- 将日志保存在经过压缩的高效存储库中
- 在所有日志中查找数据
- 通过报告证明对日志进行了全面收集

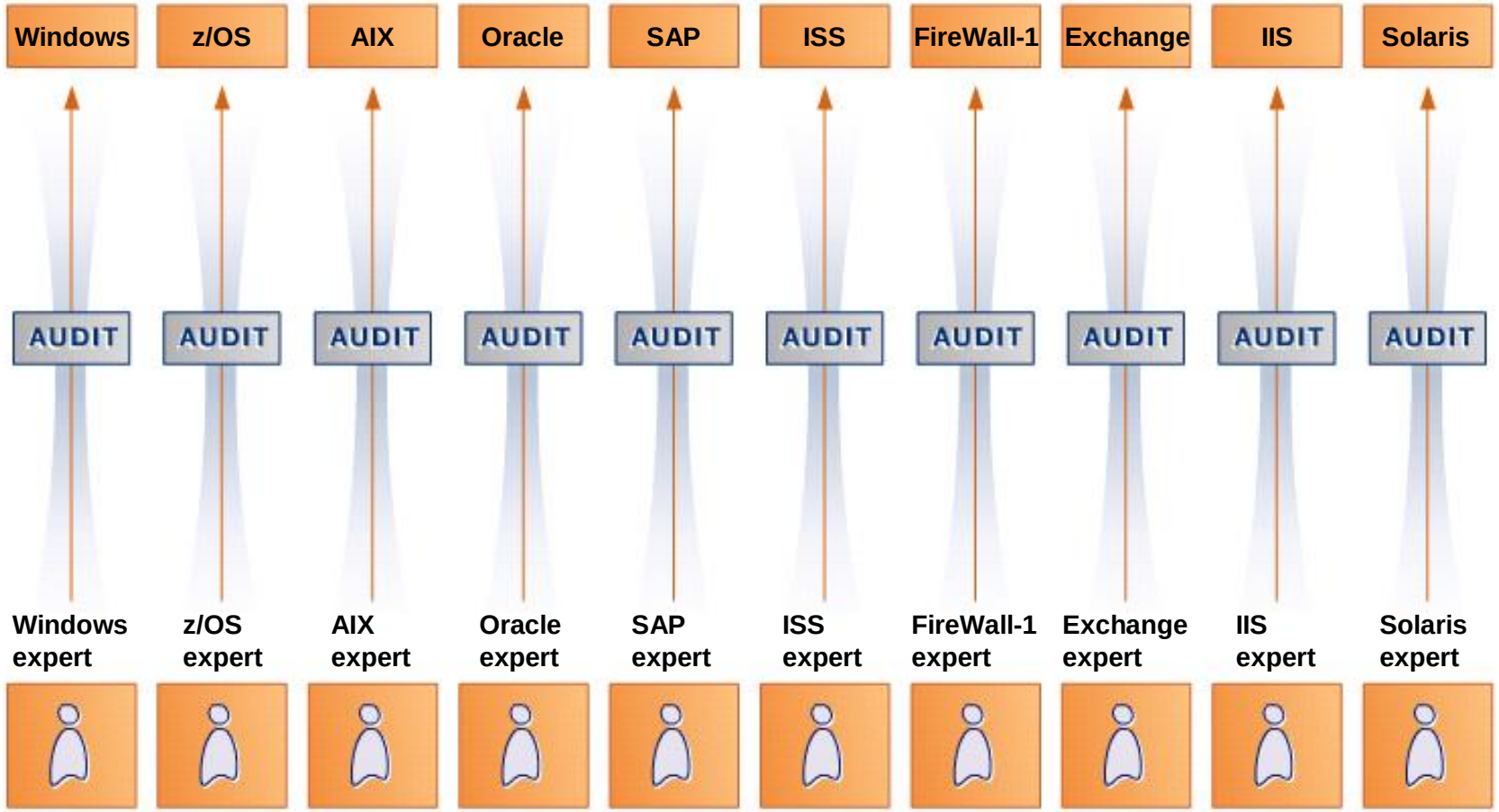
成效：

- 集中的自动收集日志可降低成本
- 随时应对“审计”！

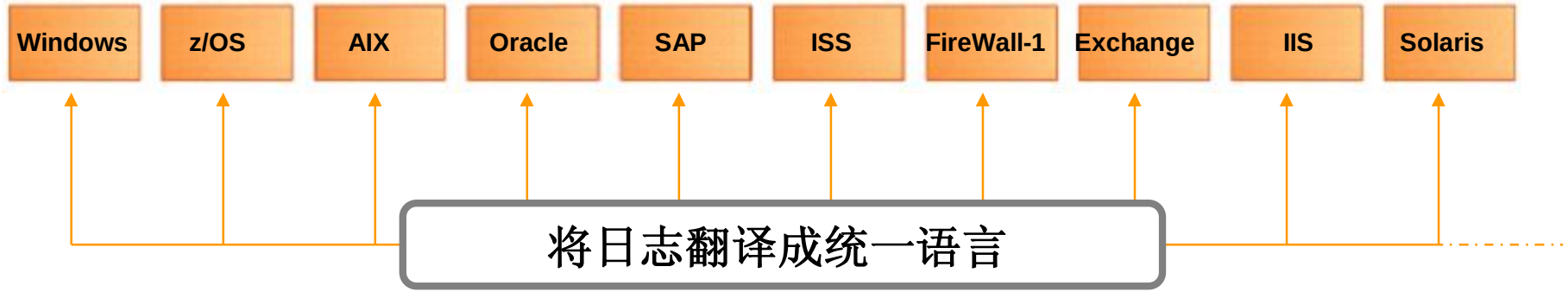
日志连续性及历史报告，
可即刻向管理及审计人員证明日志管理程序的完整性和持续性。



日志捕获后的工作是翻译和解释



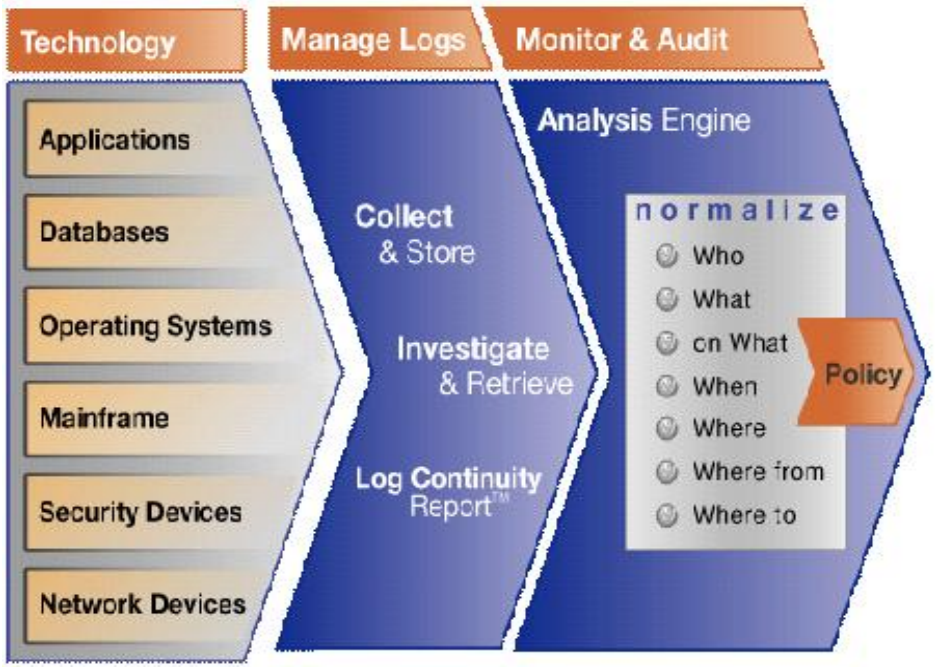
IBM TCIM 统一所有企业日志的语言



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

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

理解 (Comprehend)：精准的日志翻译和解释



功能：

- W7 标准化
- 将每个日志 (系统日志和本机日志) 翻译
- 将几十亿个日志项目与基准制度进行比较

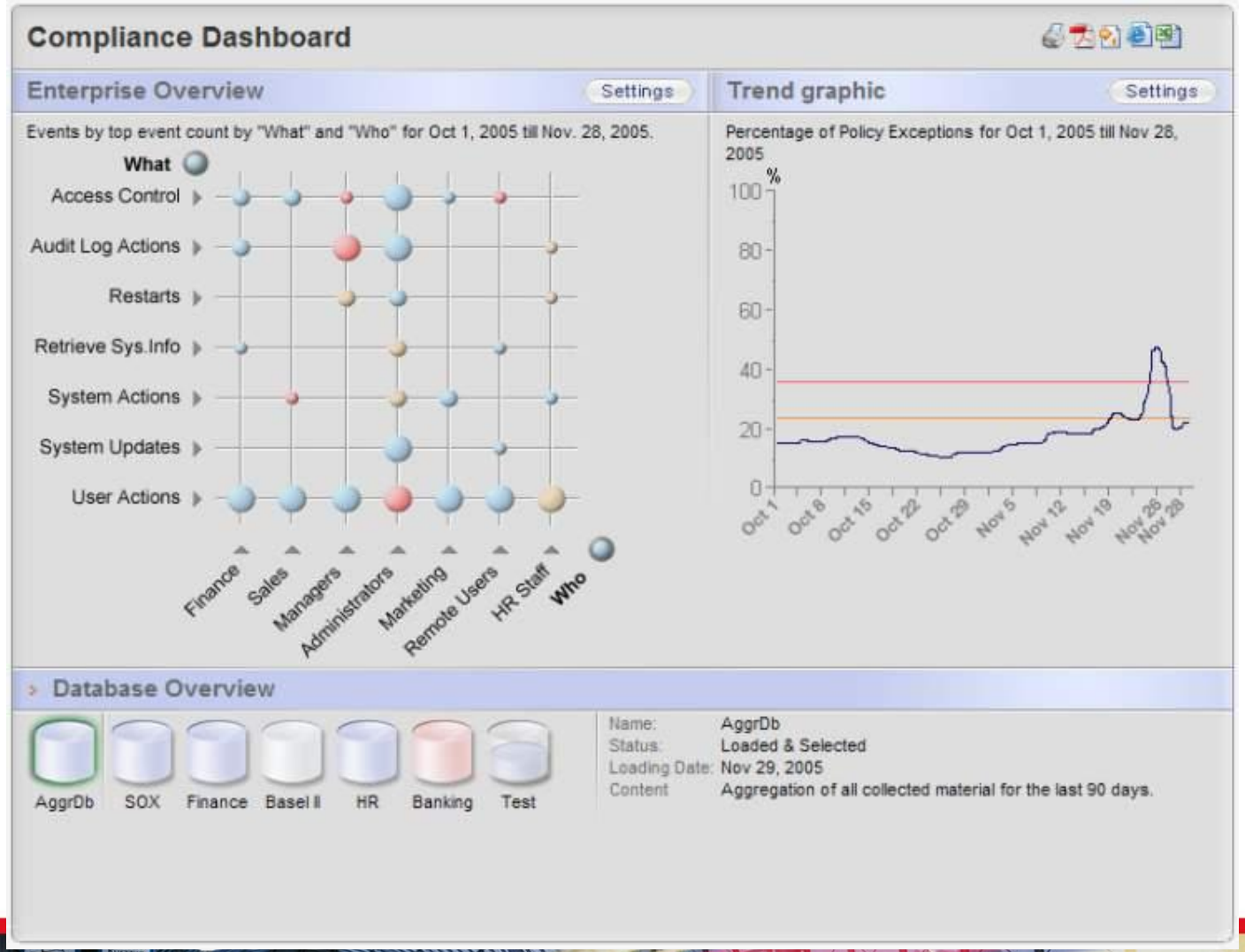
成效：

- 通过更少的资源和更低的成本来翻译并监控所有的日志
- 快速检测并解决安全问题

TCIM – 合规性显示板

制度遵从显示板

W7 处理器后的日志– 通过一个简单的图形汇总几亿个日志文件！



快速深入察看细节

违规

特别提示

故障

趋势

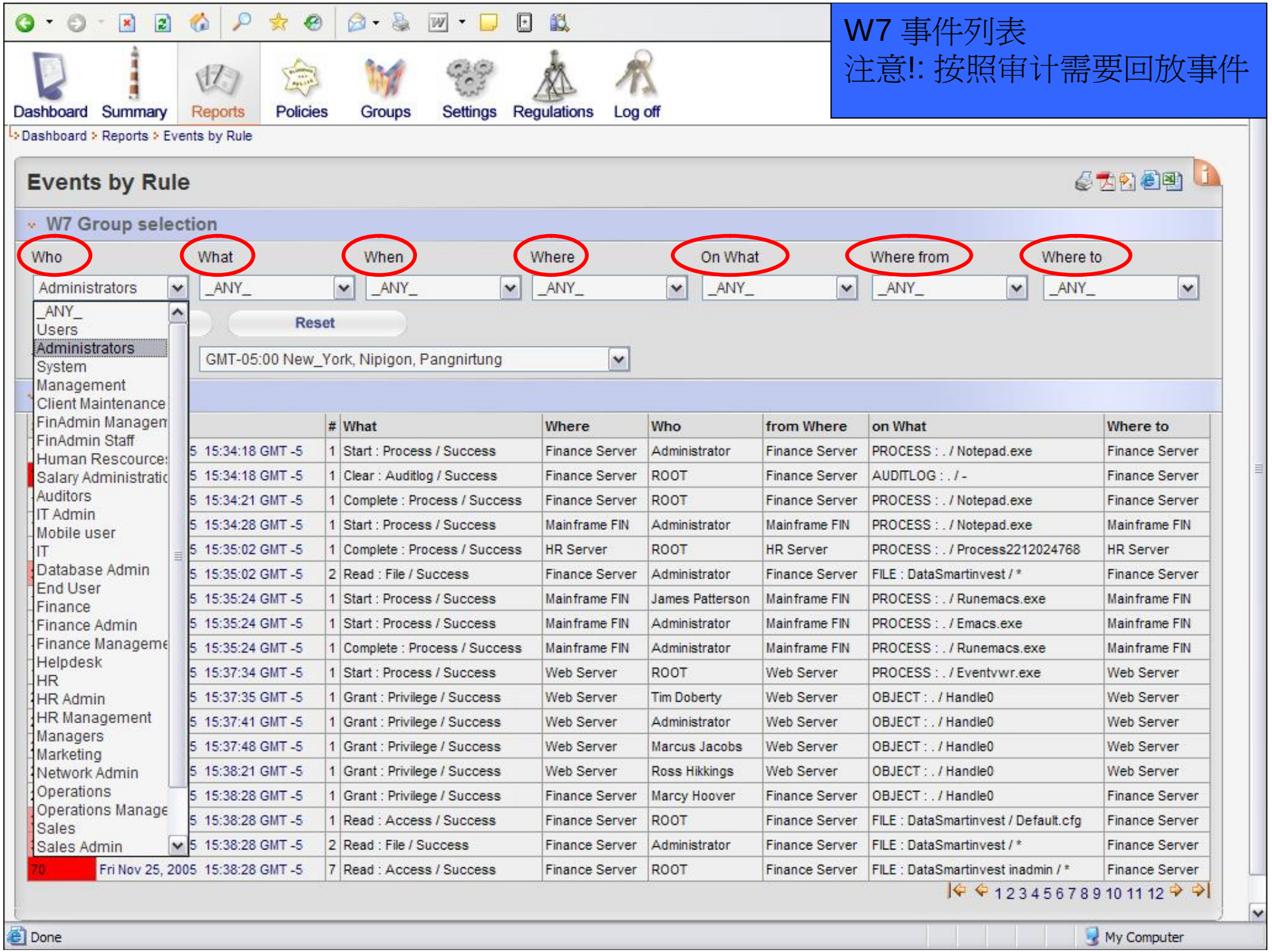
报告数据库

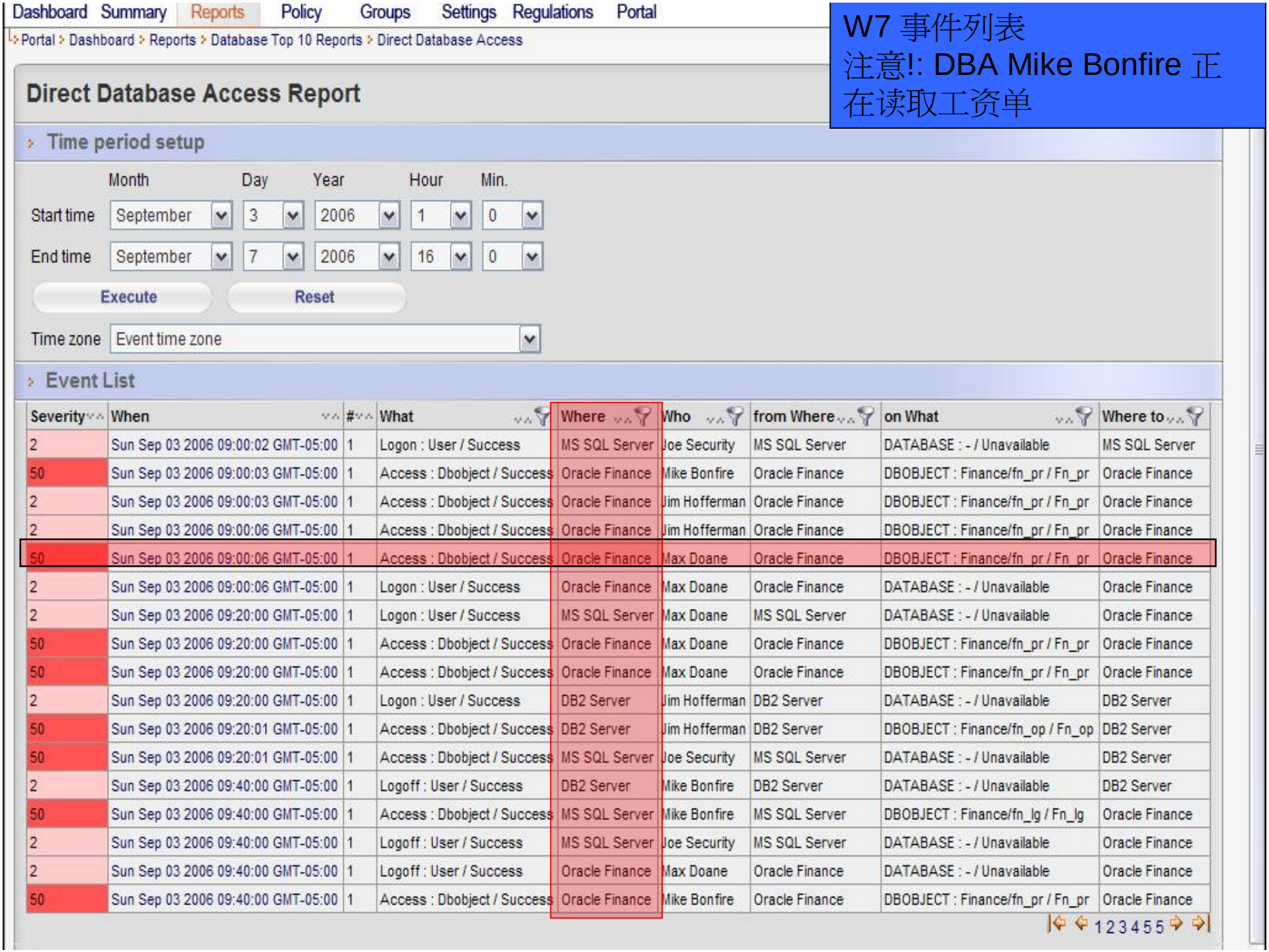
汇聚数据库

企业概述

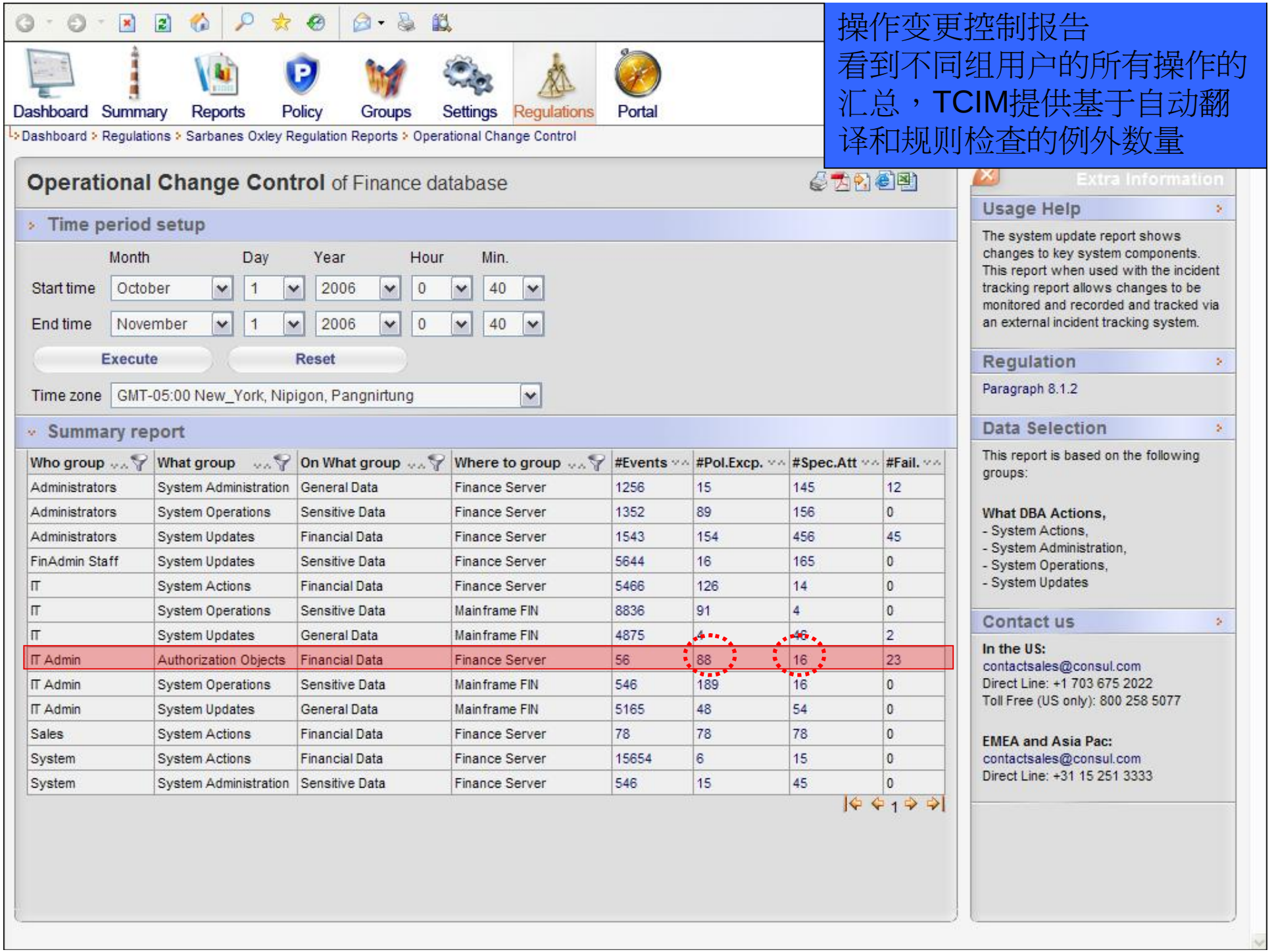
报告分发

自助审计


W7 事件列表
注意!: 按照审计需要回放事件
Dashboard
Summary
Reports
Policies
Groups
Settings
Regulations
Log off
Dashboard > Reports > Events by Rule
Events by Rule
W7 Group selection
Who
What
When
Where
On What
Where from
Where to
Administrators
ANY
Reset
GMT-05:00 New_York, Nipigon, Pangnirtung
ANY
Users
Administrators
System
Management
Client Maintenance
FinAdmin Managen
FinAdmin Staff
Human Rescource:
Salary Administratic
Auditors
IT Admin
Mobile user
IT
Database Admin
End User
Finance
Finance Admin
Finance Manageme
Helpdesk
HR
HR Admin
HR Management
Managers
Marketing
Network Admin
Operations
Operations Manage
Sales
Sales Admin
| What | Where | Who | from Where | on What | Where to
5 15:34:18 GMT -5 | 1 | Start : Process / Success | Finance Server | Administrator | Finance Server | PROCESS : . / Notepad.exe | Finance Server
5 15:34:18 GMT -5 | 1 | Clear : Auditlog / Success | Finance Server | ROOT | Finance Server | AUDITLOG : . / - | Finance Server
5 15:34:21 GMT -5 | 1 | Complete : Process / Success | Finance Server | ROOT | Finance Server | PROCESS : . / Notepad.exe | Finance Server
5 15:34:28 GMT -5 | 1 | Start : Process / Success | Mainframe FIN | Administrator | Mainframe FIN | PROCESS : . / Notepad.exe | Mainframe FIN
5 15:35:02 GMT -5 | 1 | Complete : Process / Success | HR Server | ROOT | HR Server | PROCESS : . / Process2212024768 | HR Server
5 15:35:02 GMT -5 | 2 | Read : File / Success | Finance Server | Administrator | Finance Server | FILE : DataSmartinvest / * | Finance Server
5 15:35:24 GMT -5 | 1 | Start : Process / Success | Mainframe FIN | James Patterson | Mainframe FIN | PROCESS : . / Runemacs.exe | Mainframe FIN
5 15:35:24 GMT -5 | 1 | Start : Process / Success | Mainframe FIN | Administrator | Mainframe FIN | PROCESS : . / Emacs.exe | Mainframe FIN
5 15:35:24 GMT -5 | 1 | Complete : Process / Success | Mainframe FIN | Administrator | Mainframe FIN | PROCESS : . / Runemacs.exe | Mainframe FIN
5 15:37:34 GMT -5 | 1 | Start : Process / Success | Web Server | ROOT | Web Server | PROCESS : . / Eventvwr.exe | Web Server
5 15:37:35 GMT -5 | 1 | Grant : Privilege / Success | Web Server | Tim Doberty | Web Server | OBJECT : . / Handle0 | Web Server
5 15:37:41 GMT -5 | 1 | Grant : Privilege / Success | Web Server | Administrator | Web Server | OBJECT : . / Handle0 | Web Server
5 15:37:48 GMT -5 | 1 | Grant : Privilege / Success | Web Server | Marcus Jacobs | Web Server | OBJECT : . / Handle0 | Web Server
5 15:38:21 GMT -5 | 1 | Grant : Privilege / Success | Web Server | Ross Hikkings | Web Server | OBJECT : . / Handle0 | Web Server
5 15:38:28 GMT -5 | 1 | Grant : Privilege / Success | Finance Server | Marcy Hoover | Finance Server | OBJECT : . / Handle0 | Finance Server
5 15:38:28 GMT -5 | 1 | Read : Access / Success | Finance Server | ROOT | Finance Server | FILE : DataSmartinvest / Default.cfg | Finance Server
5 15:38:28 GMT -5 | 2 | Read : File / Success | Finance Server | Administrator | Finance Server | FILE : DataSmartinvest / * | Finance Server
70 Fri Nov 25, 2005 15:38:28 GMT -5 | 7 | Read : Access / Success | Finance Server | ROOT | Finance Server | FILE : DataSmartinvest inadmin / * | Finance Server
1 2 3 4 5 6 7 8 9 10 11 12
Done
My Computer



W7 事件列表
注意!: DBA Mike Bonfire 正在读取工资单


操作变更控制报告
看到不同组用户的所有操作的汇总，TCIM提供基于自动翻译和规则检查的例外数量
Dashboard
Summary
Reports
Policy
Groups
Settings
Regulations
Portal
Dashboard > Regulations > Sarbanes Oxley Regulation Reports > Operational Change Control
Operational Change Control of Finance database
Time period setup
Month Day Year Hour Min.
Start time October 1 2006 0 40
End time November 1 2006 0 40
Execute
Reset
Time zone GMT-05:00 New_York, Nipigon, Pangnirtung
Summary report
Who group | What group | On What group | Where to group | #Events | #Pol.Excp. | #Spec.Att | #Fail.
Administrators | System Administration | General Data | Finance Server | 1256 | 15 | 145 | 12
Administrators | System Operations | Sensitive Data | Finance Server | 1352 | 89 | 156 | 0
Administrators | System Updates | Financial Data | Finance Server | 1543 | 154 | 456 | 45
FinAdmin Staff | System Updates | Sensitive Data | Finance Server | 5644 | 16 | 165 | 0
IT | System Actions | Financial Data | Finance Server | 5466 | 126 | 14 | 0
IT | System Operations | Sensitive Data | Mainframe FIN | 8836 | 91 | 4 | 0
IT | System Updates | General Data | Mainframe FIN | 4875 | 4 | 46 | 2
IT Admin | Authorization Objects | Financial Data | Finance Server | 56 | 88 | 16 | 23
IT Admin | System Operations | Sensitive Data | Mainframe FIN | 546 | 189 | 16 | 0
IT Admin | System Updates | General Data | Mainframe FIN | 5165 | 48 | 54 | 0
Sales | System Actions | Financial Data | Finance Server | 78 | 78 | 78 | 0
System | System Actions | Financial Data | Finance Server | 15654 | 6 | 15 | 0
System | System Administration | Sensitive Data | Finance Server | 546 | 15 | 45 | 0
1
Extra Information
Usage Help
The system update report shows changes to key system components. This report when used with the incident tracking report allows changes to be monitored and recorded and tracked via an external incident tracking system.
Regulation
Paragraph 8.1.2
Data Selection
This report is based on the following groups:
What DBA Actions,
- System Actions,
- System Administration,
- System Operations,
- System Updates
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

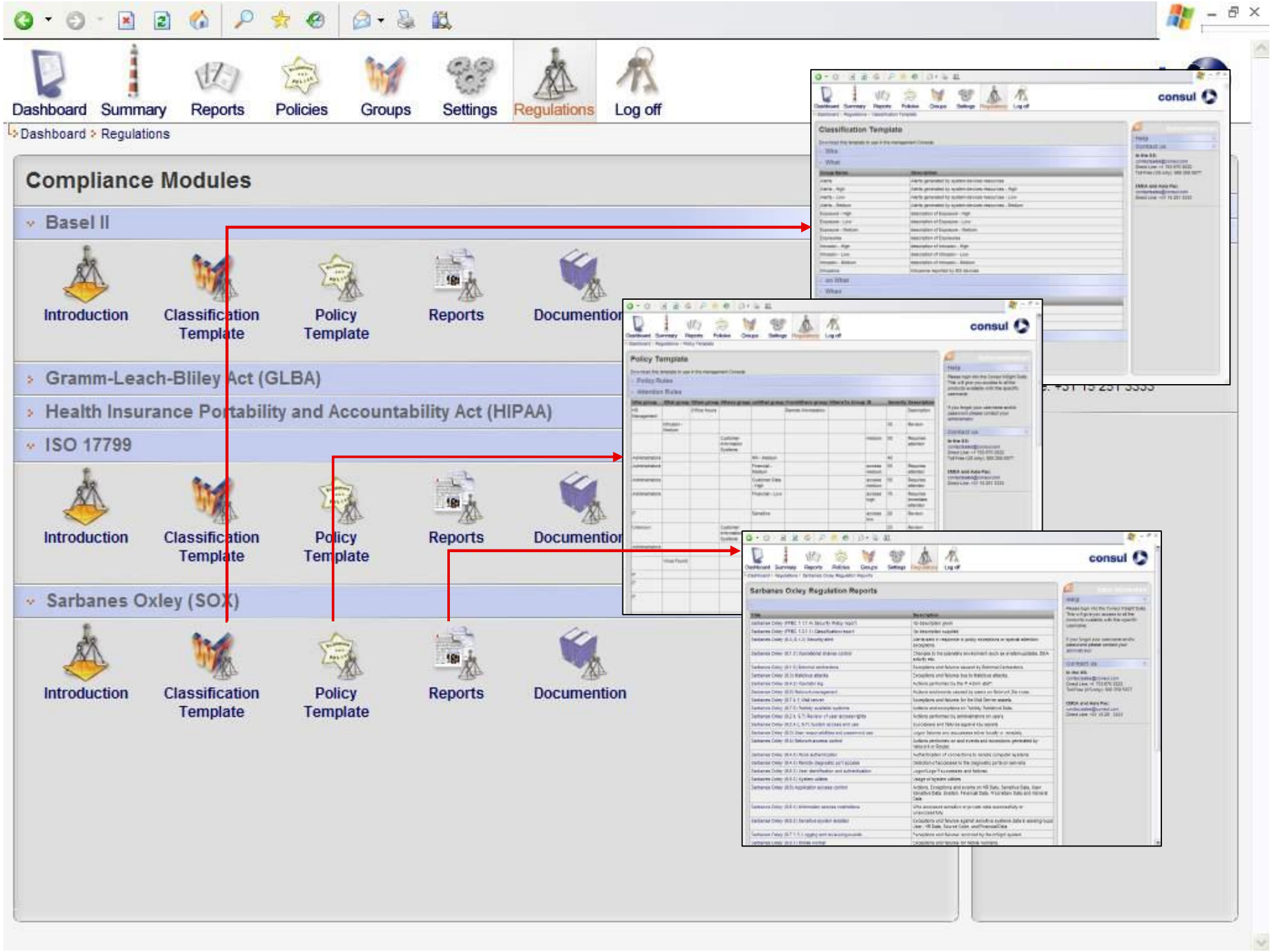
了解 (Communicate)：全面的审计和合规性报告

功能：

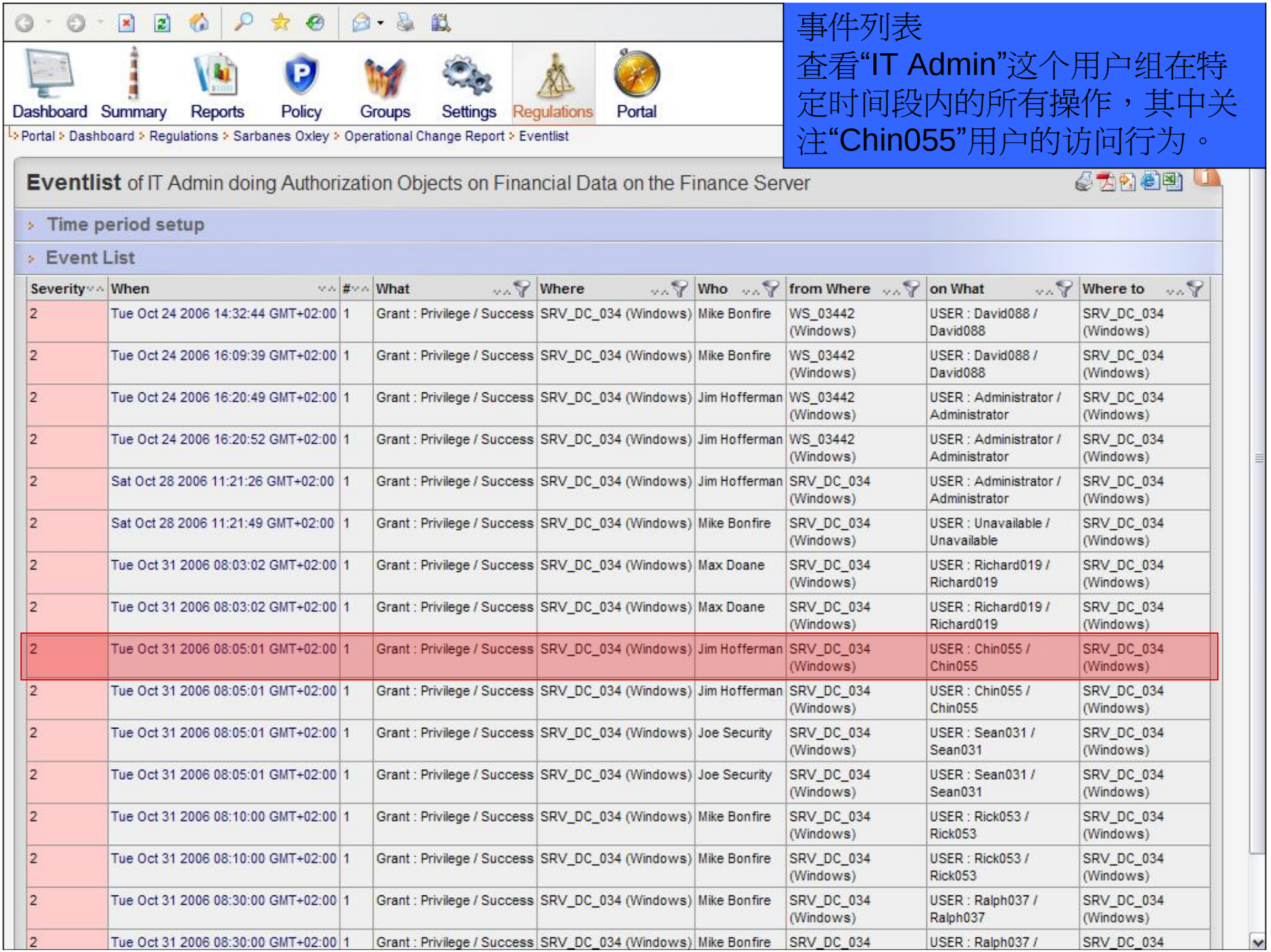
- 企业制度遵从显示板
- 几百个报告
- 制度遵从模块
- 特别注意警报

成效：

- 帮助审计公司省时省力
- 即时报告，节省时间
- 降低内部威胁风险：
  - 信息保护
  - 变化控制
  - 用户管理


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
consul
Policy Template
consul
Sarbanes Oxley Regulation Reports

事件列表
查看“IT Admin”这个用户组在特定时间段内的所有操作，其中关注“Chin055”用户的访问行为。



Eventlist of IT Admin doing Authorization Objects on Financial Data on the Finance Server

› Time period setup

› Event List

Severity	When	#	What	Where	Who	from Where	on What	Where to
2	Tue Oct 24 2006 14:32:44 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Mike Bonfire	WS_03442 (Windows)	USER : David088 / David088	SRV_DC_034 (Windows)
2	Tue Oct 24 2006 16:09:39 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Mike Bonfire	WS_03442 (Windows)	USER : David088 / David088	SRV_DC_034 (Windows)
2	Tue Oct 24 2006 16:20:49 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Jim Hofferman	WS_03442 (Windows)	USER : Administrator / Administrator	SRV_DC_034 (Windows)
2	Tue Oct 24 2006 16:20:52 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Jim Hofferman	WS_03442 (Windows)	USER : Administrator / Administrator	SRV_DC_034 (Windows)
2	Sat Oct 28 2006 11:21:26 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Jim Hofferman	SRV_DC_034 (Windows)	USER : Administrator / Administrator	SRV_DC_034 (Windows)
2	Sat Oct 28 2006 11:21:49 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Mike Bonfire	SRV_DC_034 (Windows)	USER : Unavailable / Unavailable	SRV_DC_034 (Windows)
2	Tue Oct 31 2006 08:03:02 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Max Doane	SRV_DC_034 (Windows)	USER : Richard019 / Richard019	SRV_DC_034 (Windows)
2	Tue Oct 31 2006 08:03:02 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Max Doane	SRV_DC_034 (Windows)	USER : Richard019 / Richard019	SRV_DC_034 (Windows)
2	Tue Oct 31 2006 08:05:01 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Jim Hofferman	SRV_DC_034 (Windows)	USER : Chin055 / Chin055	SRV_DC_034 (Windows)
2	Tue Oct 31 2006 08:05:01 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Jim Hofferman	SRV_DC_034 (Windows)	USER : Chin055 / Chin055	SRV_DC_034 (Windows)
2	Tue Oct 31 2006 08:05:01 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Joe Security	SRV_DC_034 (Windows)	USER : Sean031 / Sean031	SRV_DC_034 (Windows)
2	Tue Oct 31 2006 08:05:01 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Joe Security	SRV_DC_034 (Windows)	USER : Sean031 / Sean031	SRV_DC_034 (Windows)
2	Tue Oct 31 2006 08:10:00 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Mike Bonfire	SRV_DC_034 (Windows)	USER : Rick053 / Rick053	SRV_DC_034 (Windows)
2	Tue Oct 31 2006 08:10:00 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Mike Bonfire	SRV_DC_034 (Windows)	USER : Rick053 / Rick053	SRV_DC_034 (Windows)
2	Tue Oct 31 2006 08:30:00 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Mike Bonfire	SRV_DC_034 (Windows)	USER : Ralph037 / Ralph037	SRV_DC_034 (Windows)
2	Tue Oct 31 2006 08:30:00 GMT+02:00	1	Grant : Privilege / Success	SRV_DC_034 (Windows)	Mike Bonfire	SRV_DC_034	USER : Ralph037 /	SRV_DC_034

事件具体报告
可深入到具体事件并察看所有事件的具体情况，甚至能够深入察看原始的日志文件

Dashboard | Summary | Reports | Policy | Groups | Settings | Regulations | Portal

Portal > Dashboard > Regulations > Sarbanes Oxley > Operational Change Report > Eventlist > Event-detail

Event Detail

Event information

	Field	Group	
Severity	2 (1x)	-	
When	Fri Oct 31, 2006 08:05:01 GMT +02:00	Office Hours (10)	10
What	Grant : Privilege / Success	Security Changes Administration	50 40
Where	SRV_DC_034 (Windows)	Finance Server	50
Who	Jim Hofferman	Administrators Database Admin Finance Admin	30 30 20
From Where	XPWKST03 (Windows)	Workstation	10
On What	USER : Chin055 / Chin055	Authorization Objects	30 20
Where To	SRV_DC_034 (Windows)	Finance Server	50

Incident Tracking

Additional information

Investigate

Time: Fri Oct 31, 2006 08:05:01 GMT +02:00 (+/-) 1 minute

Selected time zone: GMT+01:00 Rome, San_Marino, Sarajevo

Filter by Platform: SRV_DC_034 (Windows)

Filter by User: Jim Hofferman

Investigate

Logrecords...

Extra Information

Help

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

AUDIT_280503.AUDIT (C:\Documents and Settings\voss\Desktop) - GVIM2

File Edit Tools Syntax Buffers Window Help

My Computer

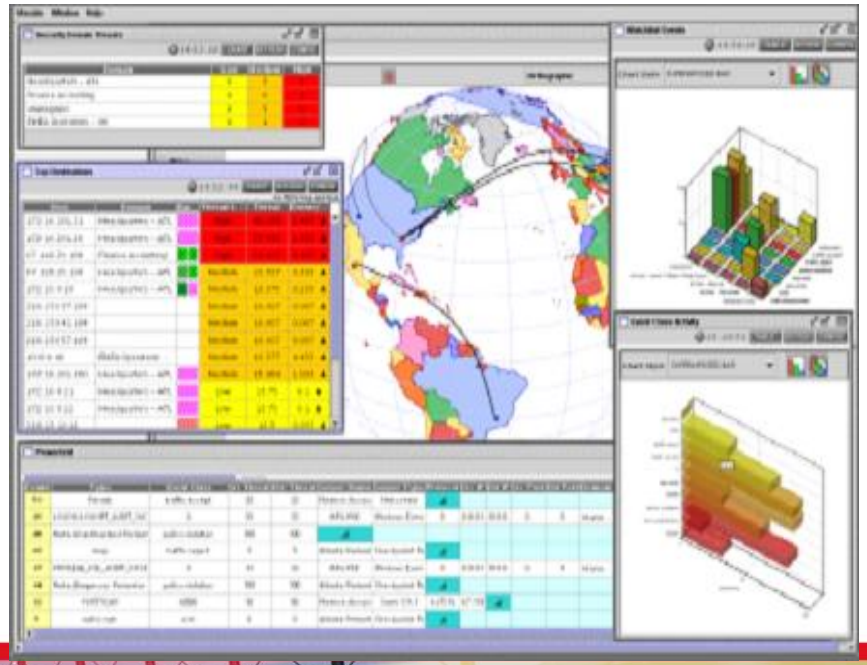
安全信息管理解决方案 – Tivoli Security Operation Manager (TSOM)

【价值定位】

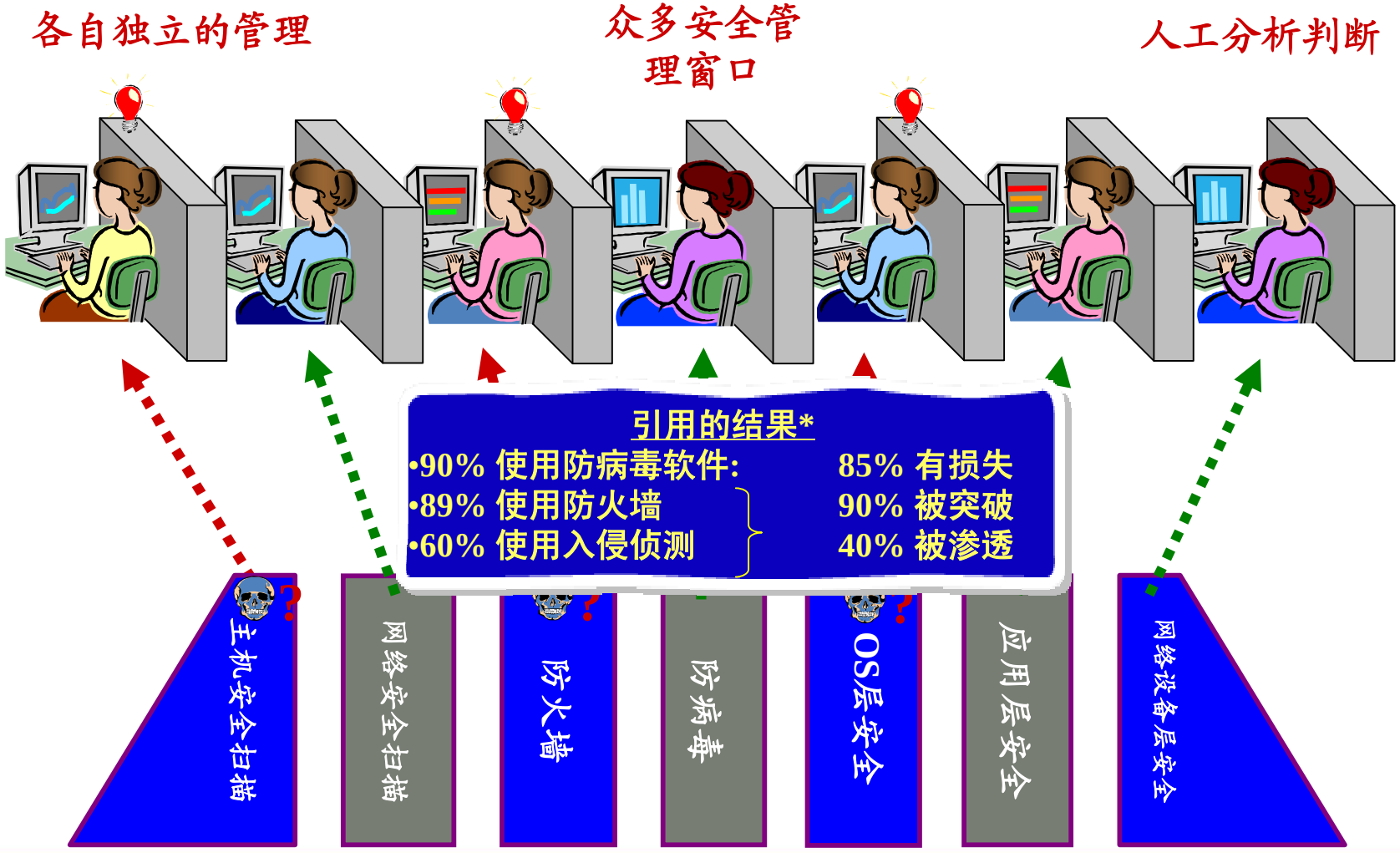
- 24×7全天候实时监控，快速识别并解决安全问题
- 提高信息安全的效率和可视性，降低整体企业资安维运成本
- IT 流程优化：讯息共享 (NOC, SOC, HelpDesk, 安全审计, ...)

【实现功能】

- 集中汇整、关联、分析、研判所有来自各方的安全事件
- 提供广泛的设备支持，包括安全性、网络、主机和应用
- 安全事件的關聯分析和優先順序處理及检测能力
- 整合的安全视图来管理复杂的安全环境
- 自动响应和报警处理
- 即時安全事件顯示，報告和預測分析



对于安全威胁，我们已经建立了众多安全堡垒，但 ....



作为安全管理员，你又如何面对这些难题：

- 企业部署了多个安全产品，你如何及时了解发生了什么问题？
  - 我需要一个可以整合企业所有安全信息的平台
- 你能否第一时间得到告警通知？
  - 我希望实时安全信息系统和企业的IT运维中心进行连接，统一发送告警
- 当多个安全设备都发生了报警，你需要多长时间来判断危险根源？
  - 我希望借助于实时安全信息系统的自动分析能力，而不仅仅是我的经验
- 你是否了解整个安全系统的运行状况和安全威胁的统计
  - 我需要实时安全信息系统自动生成统计报告，而不是我的手工统计
- 你如何应付领导随时的查询
  - 我希望所有的数据都存在实时安全信息系统的历史数据库中，我可以随时查询

TSOM - 实时安全信息管理平台

- 实时安全信息管理平台的5大环节
  - 安全事件集中收集和标准化
  - 安全事件的关联分析和优先级处理
  - 实时安全事件显示
  - 自动响应和故障报警处理
  - 报表和预测分析

- 通过实时安全信息管理平台，可以---
  - 实时、高效的事件处理性能及关联分析技术来提高安全事件的认识度
  - 了解企业发生了哪些安全相关事件，最快时间找到安全隐患
  - 从数据收集和关联分析到事件的响应动作与报告，实现安全运行的自动化
  - 提高信息安全的可视性，降低企业信息安全运维成本

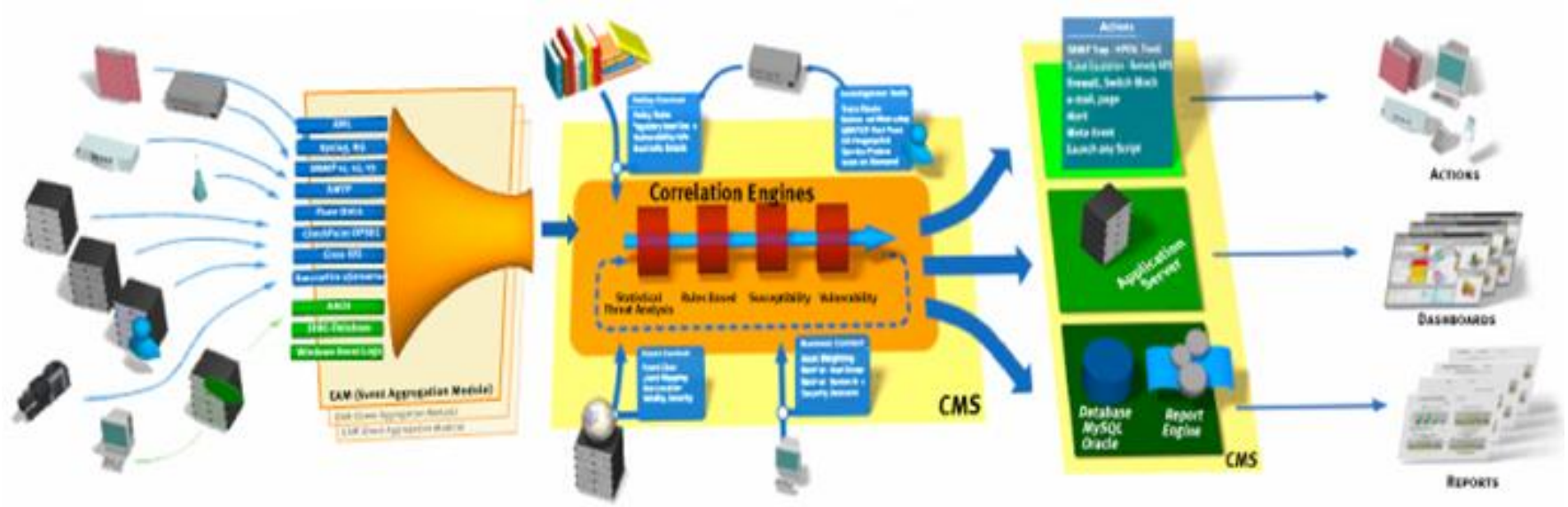
TSOM – 工作原理

事件聚合模块 (EAM)

- Ø 采集大范围的事件、日志信息、安全漏洞信息、被管理资产信息、....
- Ø 事件信息的标准化

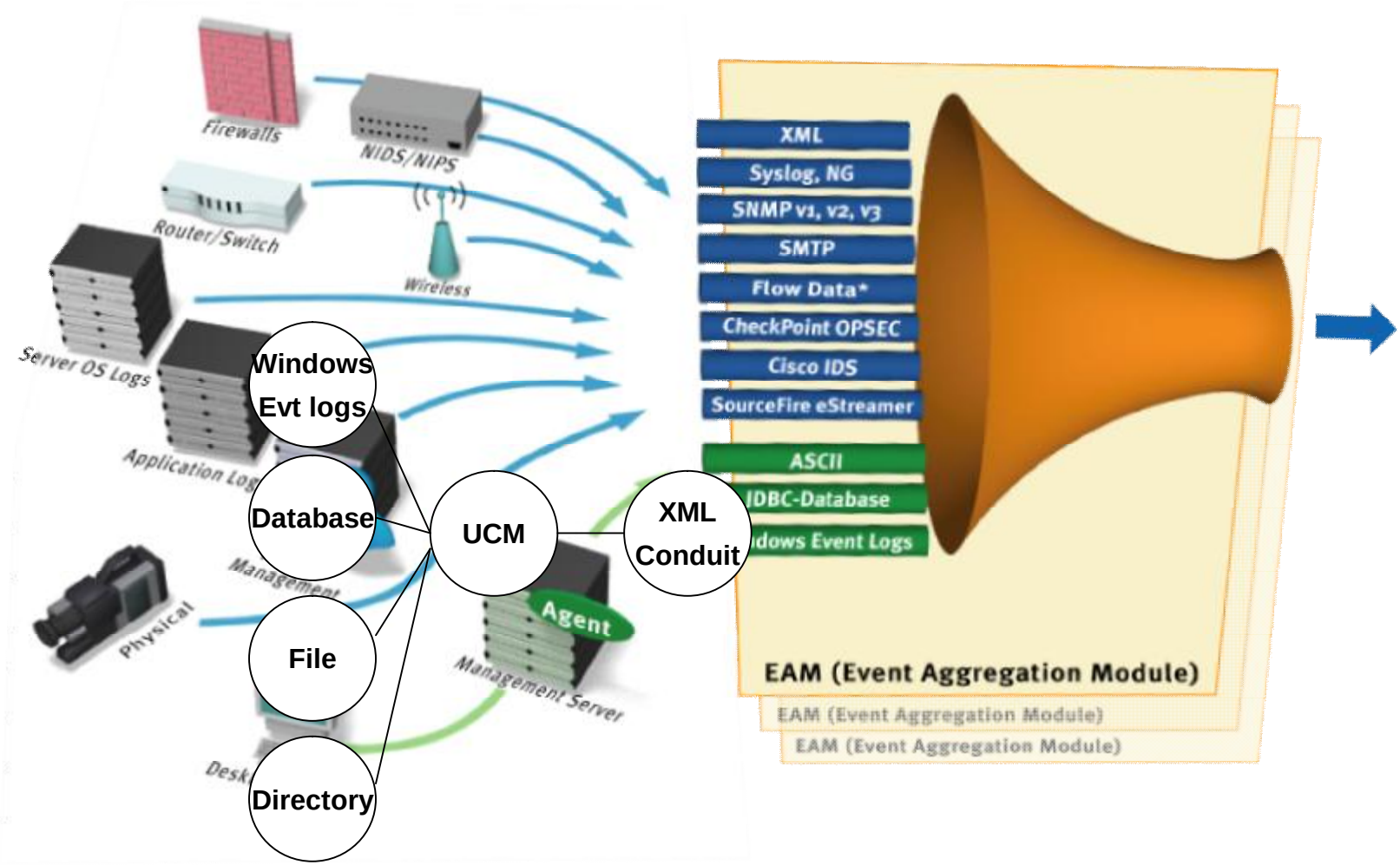
管理服务器 (CMS)

- Ø 事件信息的汇整、关联分析、研判所有来自各方的安全事件。
- Ø 安全事件的展现、对安全事件的响应动作与报告

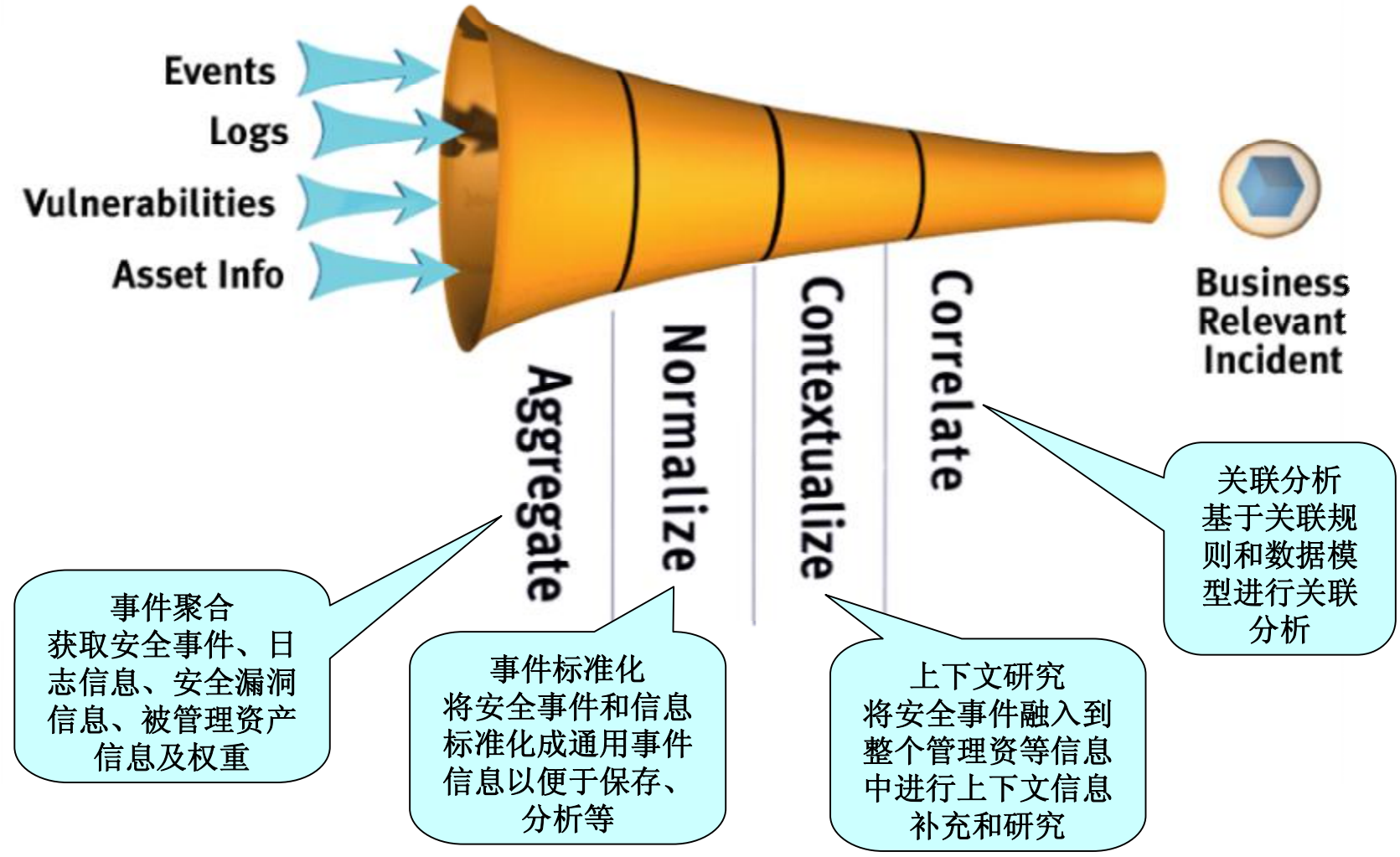


使用多种技术实现事件关联

TSOM 架构 – 信息采集


Firewalls
NIDS/NIPS
Router/Switch
Wireless
Server OS Logs
Application Logs
Physical
Windows Evt logs
Database
File
Directory
UCM
XML Conduit
Agent
Management Server
XML
Syslog, NG
SNMP v1, v2, v3
SMTP
Flow Data*
CheckPoint OPSEC
Cisco IDS
SourceFire eStreamer
ASCII
EAM (Event Aggregation Module)
EAM (Event Aggregation Module)
EAM (Event Aggregation Module)

TSOM的事件关联服务体系

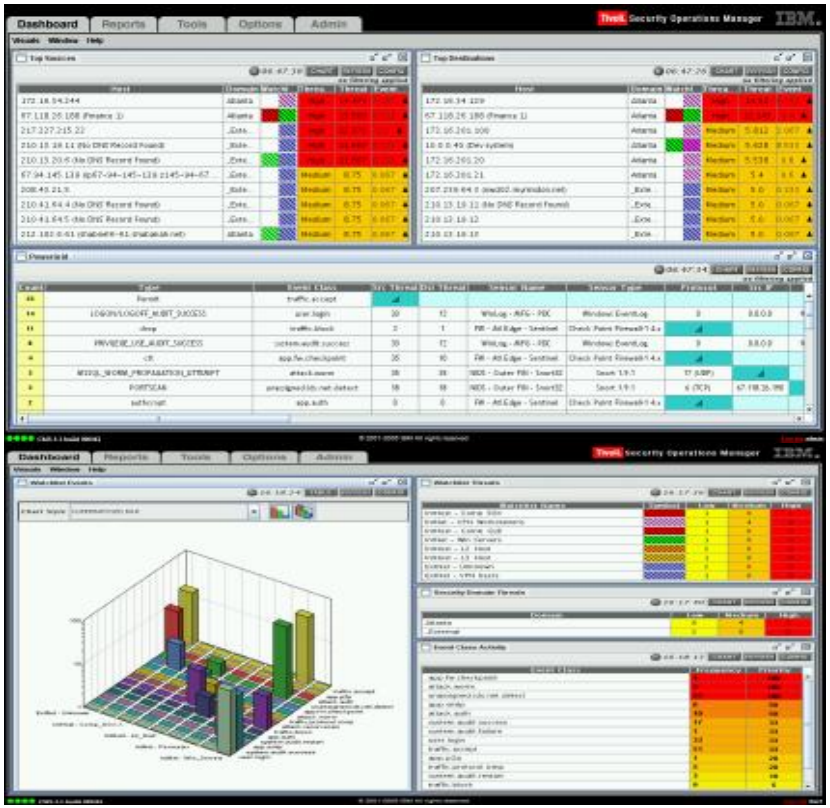


TSOM - 四个阶段关联分析进程

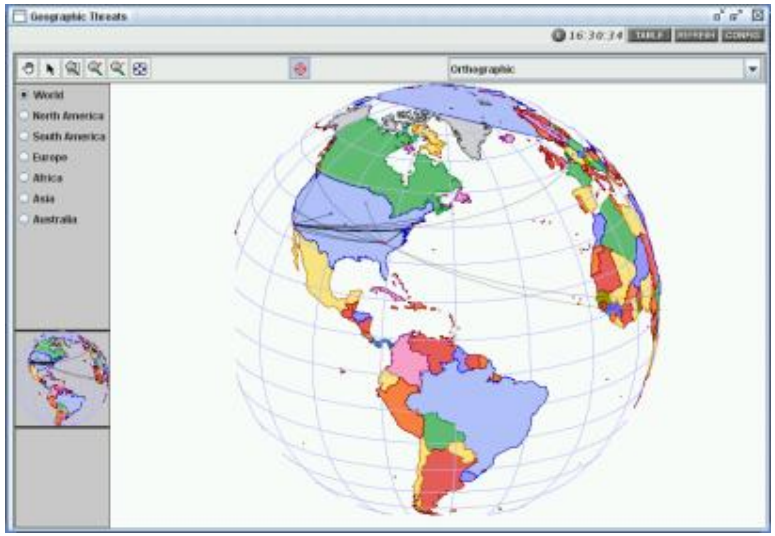
- 基于统计的关联 (Statistical Correlation)
  - 适用于发现未知攻击、异常行为
  - 根据事件优先级，事件频率，源和目标资源严重程度，对所有事件信息进行统计分析
- 基于规则的关联 (Rule Correlation)
  - 基于规则的引擎，用于描述和发现对业务影响重要的已知的事件
  - 灵活的规则结构; 适用于清晰的安全情况
- 基于安全漏洞的关联(Vulnerability Correlation)
  - 将特定的事件与已知安全漏洞进行对应
  - 适用于特定，明确的情况
  - 需要较多的维护，但是可以对特殊的攻击进行有针对性的管理
- 基于敏感性的关联(Susceptibility Correlation)
  - 用于确认问题，风险控制的优先级
  - 提高对易感服务器的威胁的可视性，降低对非易感服务器的噪音

提供企业安全系统运行的全部视图

- Open Executive Dashboard in IE

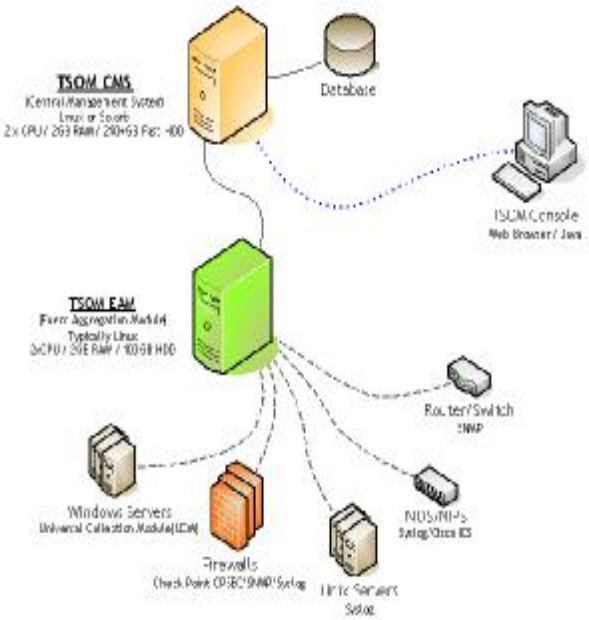


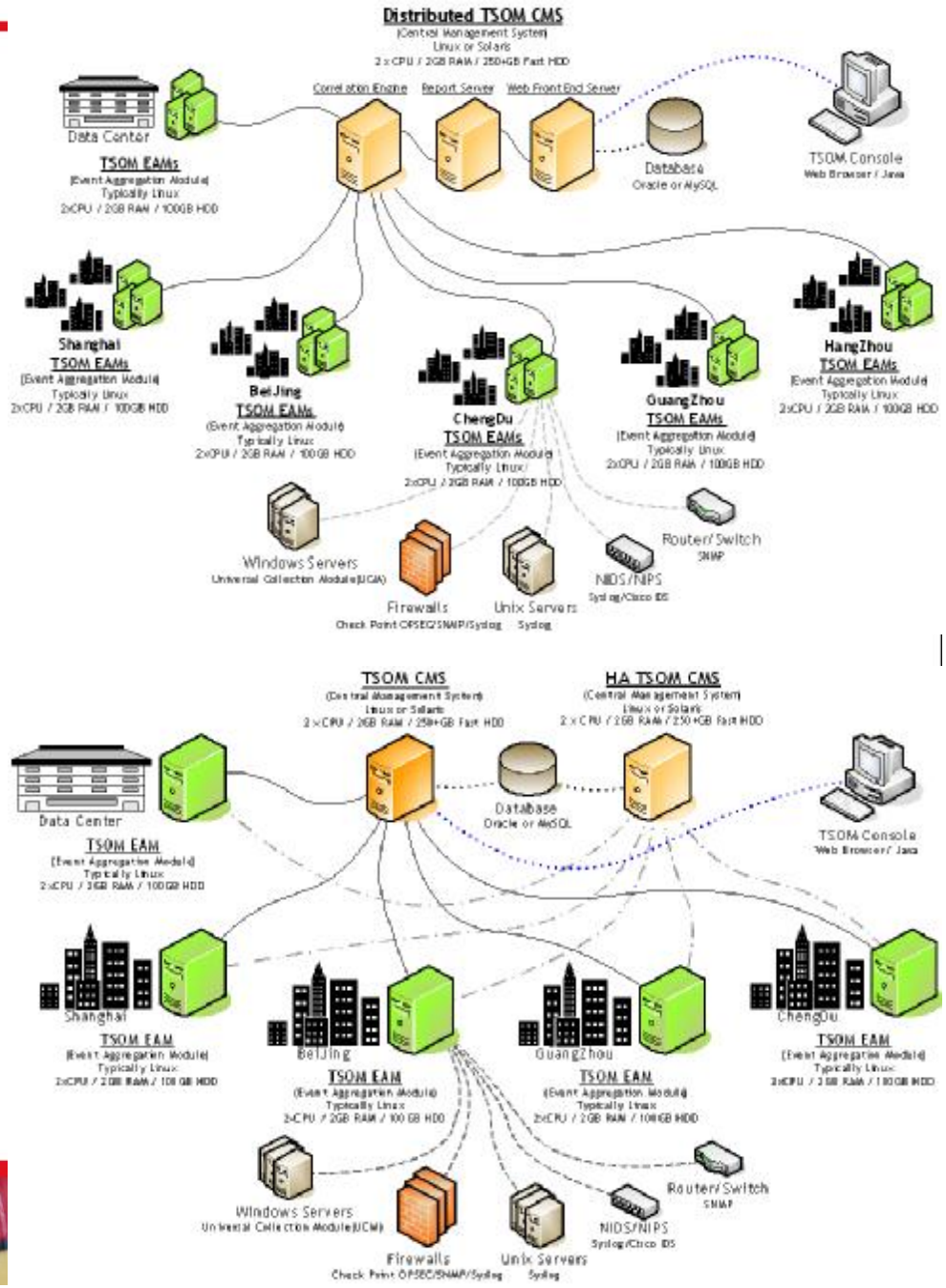
- Geographical Threat View



TSOM - 实施结构

- Ø 多种灵活的部署
- Ø 高扩展性
- Ø 高可用性





IBM安全信息管理解决方案的特性

- 实时安全威胁分析+事后审计分析
- 安全日志信息的深度管理，成熟的翻译能力
- 专业的审计服务，面向审计提供的大量特性，包括原始文件保存、原始信息搜索
- 易于部署，高度扩展性
- 面向不同类型角色用户的访问界面，易于使用


Thank
You


Kurzzug
Anfang