IBM Software Group

Tivoli software

SERVICE ORIENTED EVENT ASSESSMENT

CLOSING THE GAP OF COMPLIANCE MANAGEMENT

Dieter Riexinger
IT Architect

ON DEMAND BUSINESS™

09.10.2009

Agenda

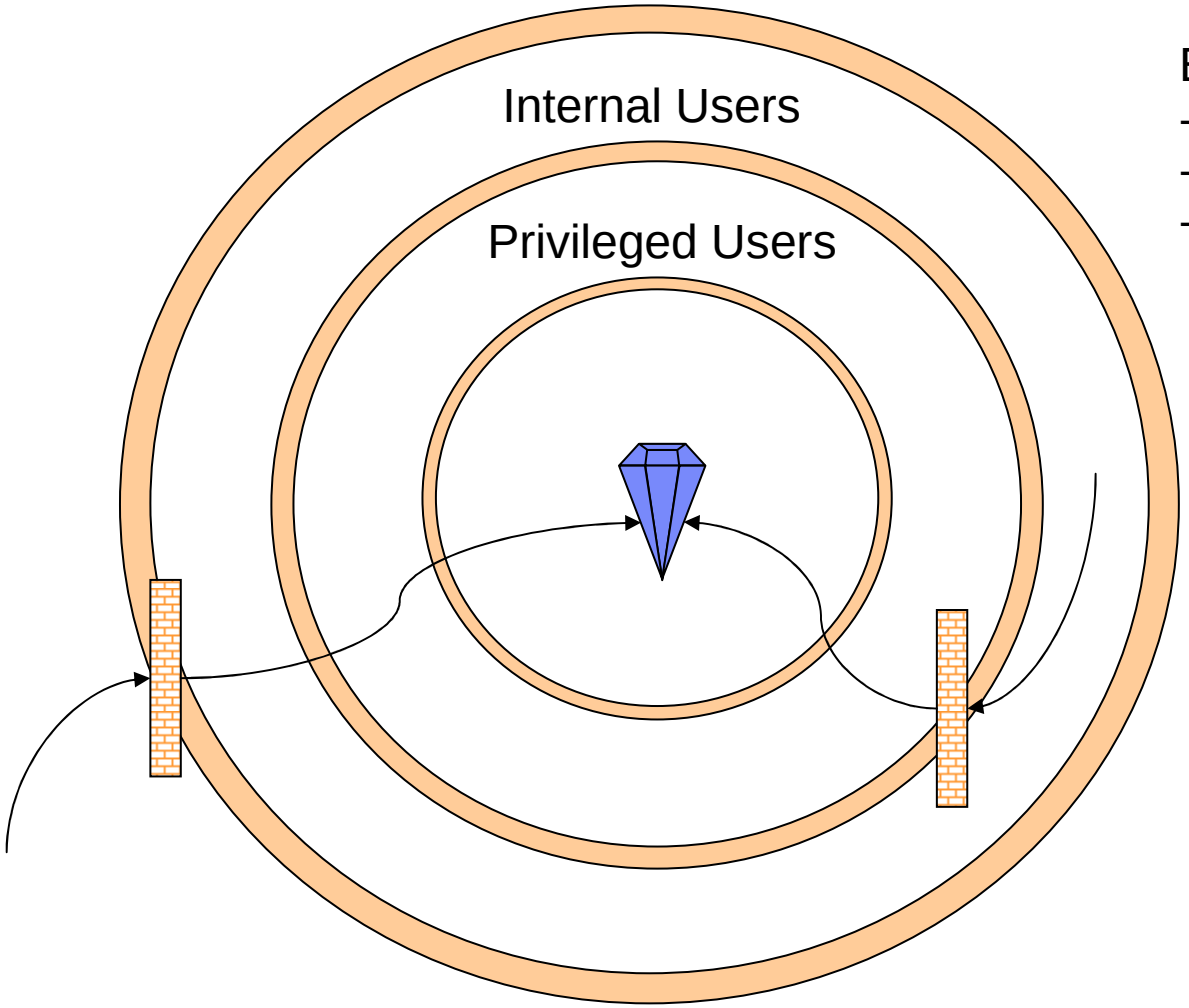
- Introduction
  - Legal obligations and regulations
  - Who causes internal incidents ?
- Security Event Collection
  - Filtering and correlating events
  - The pain of selecting the right events
- Service Oriented Event Assessment
  - Event context creation
  - How to catch the barbarian ?

Legal obligations and regulations request protection of assets

The Federal Reserve Board

FEDERAL TRADE COMMISSION
FOR THE CONSUMER

We want to protect our assets from internal and external misuse

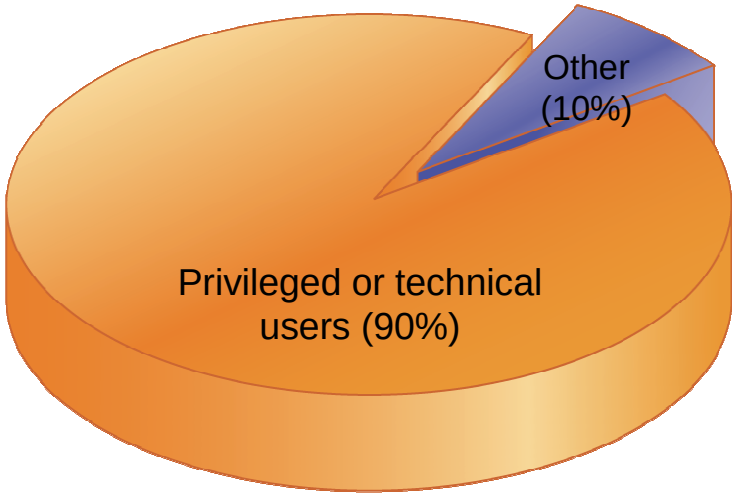


External Users
- Firewall
- Authentication
- Authorization

Who Causes Internal Incidents?

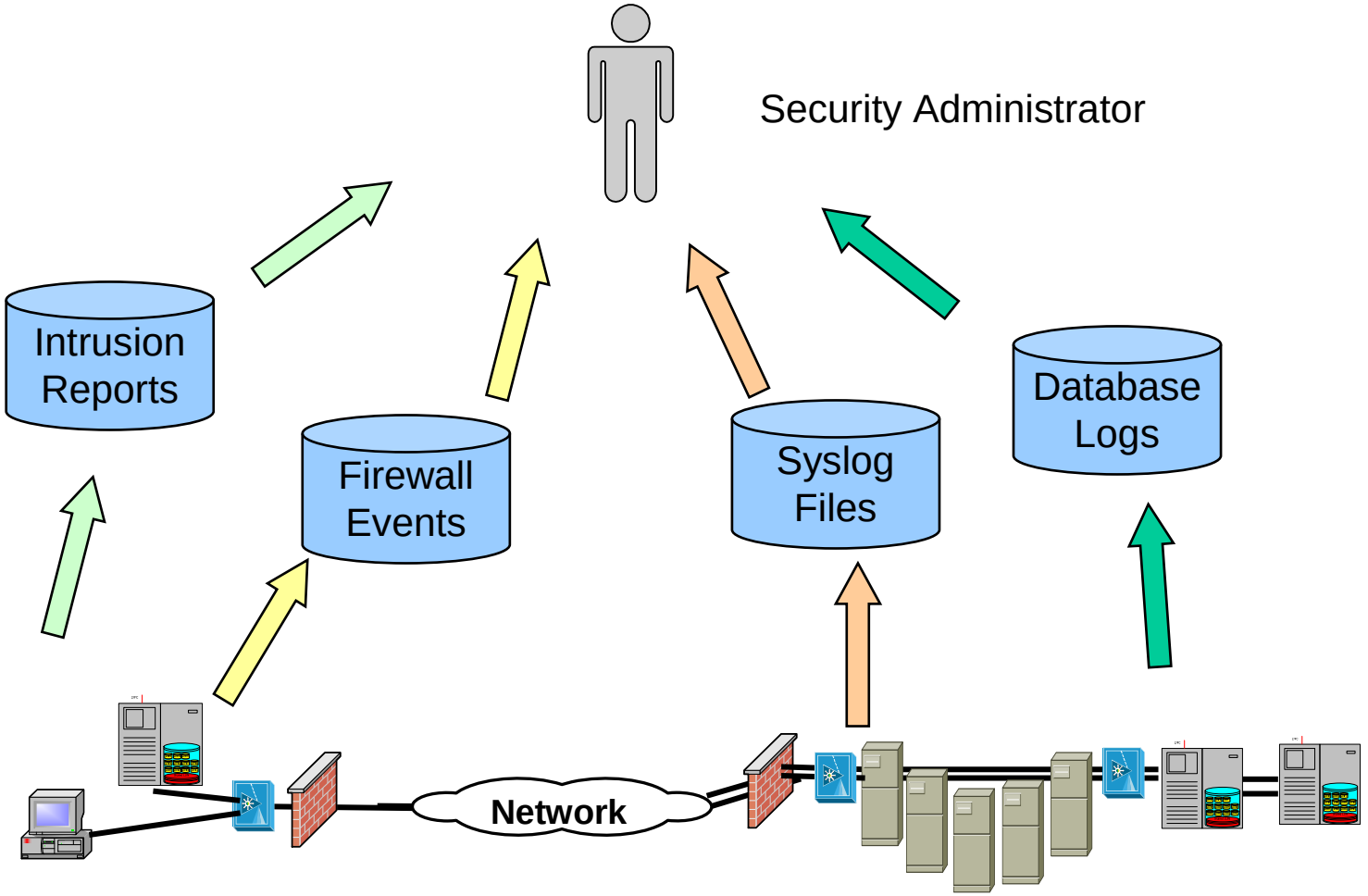
The Barbarian is „Inside the Gate“:

- 90% of insider incidents are caused by privileged or technical users
- Most are inadvertant violations of:
  - Change Management Process
  - Acceptable use policy
  - Account management process
- Others are deliberate, due to:
  - Revenge
  - Negative Events
- Regardless, too costly to ignore:
  - Internal attacks cost 6% of gross annual revenue or 9 dollars per employee per day.

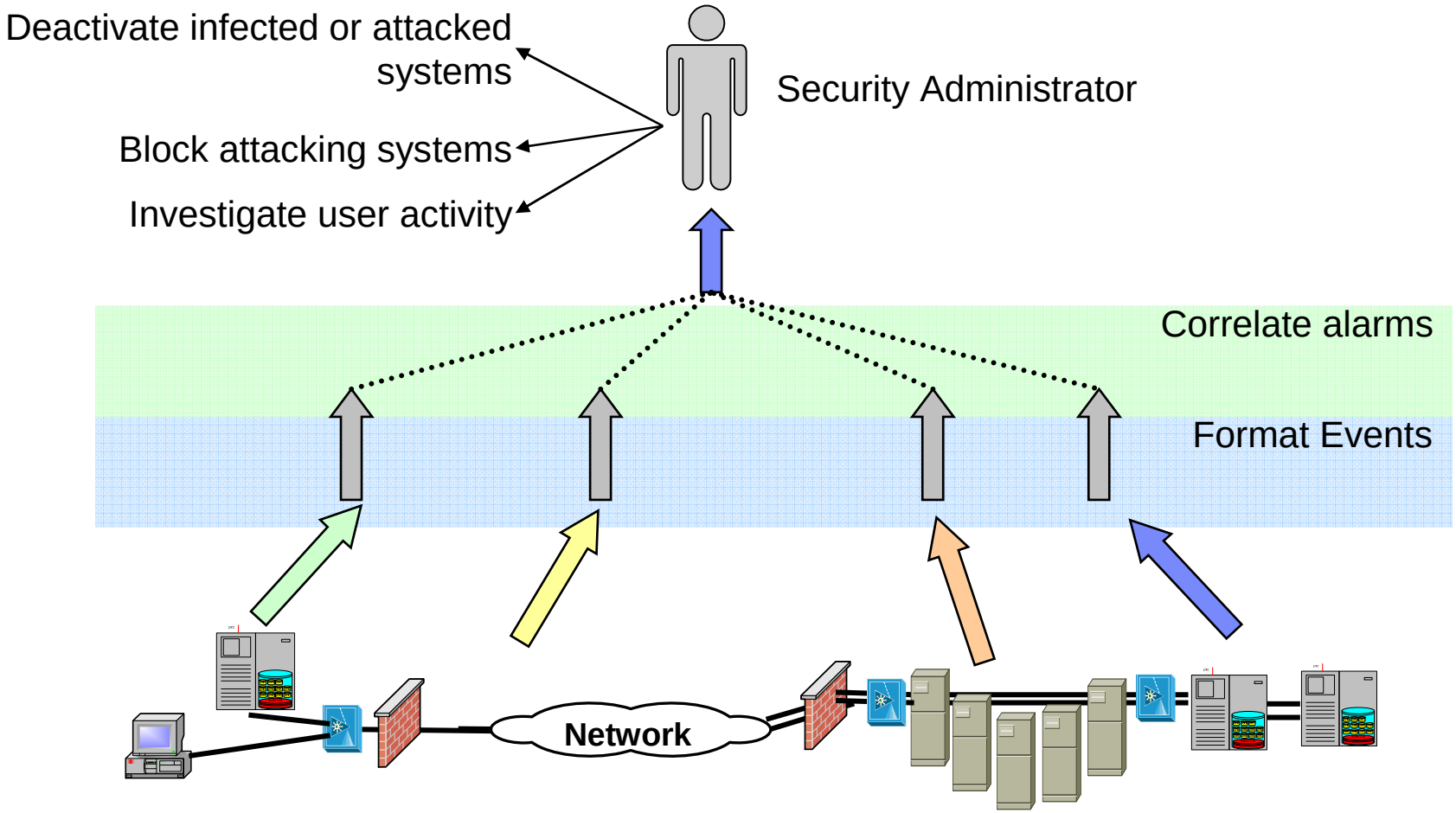


Sources: Forrester research, IdM Trends 2006; USSS/CERT Insider Threat Survey 2005/6/7/8; CSI/FBI Survey, 2005/6/7; National Fraud Survey; CERT, various documents.

Security Administrators are faced with a huge number of security events in different formats

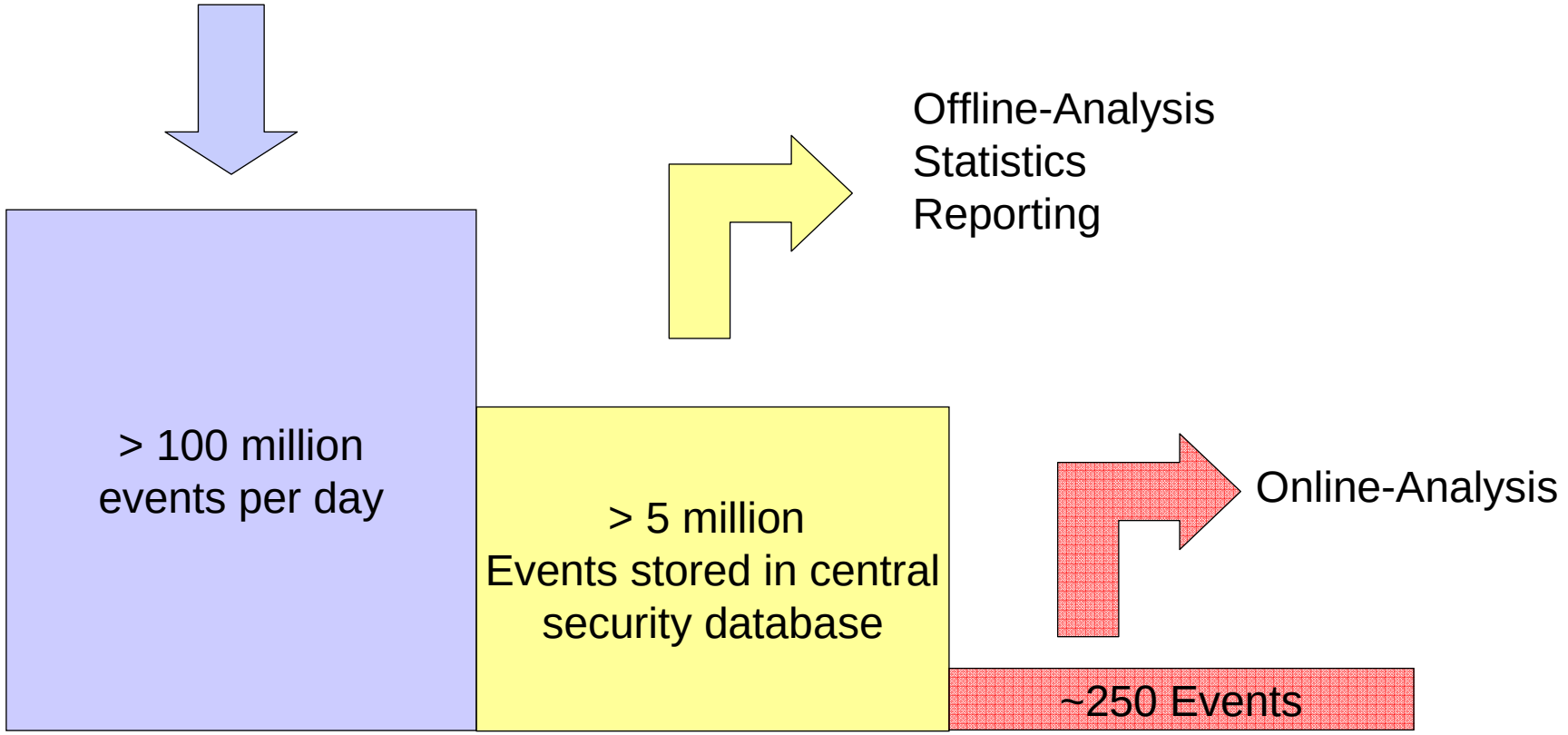


Event Management Systems collect, format and correlate security events

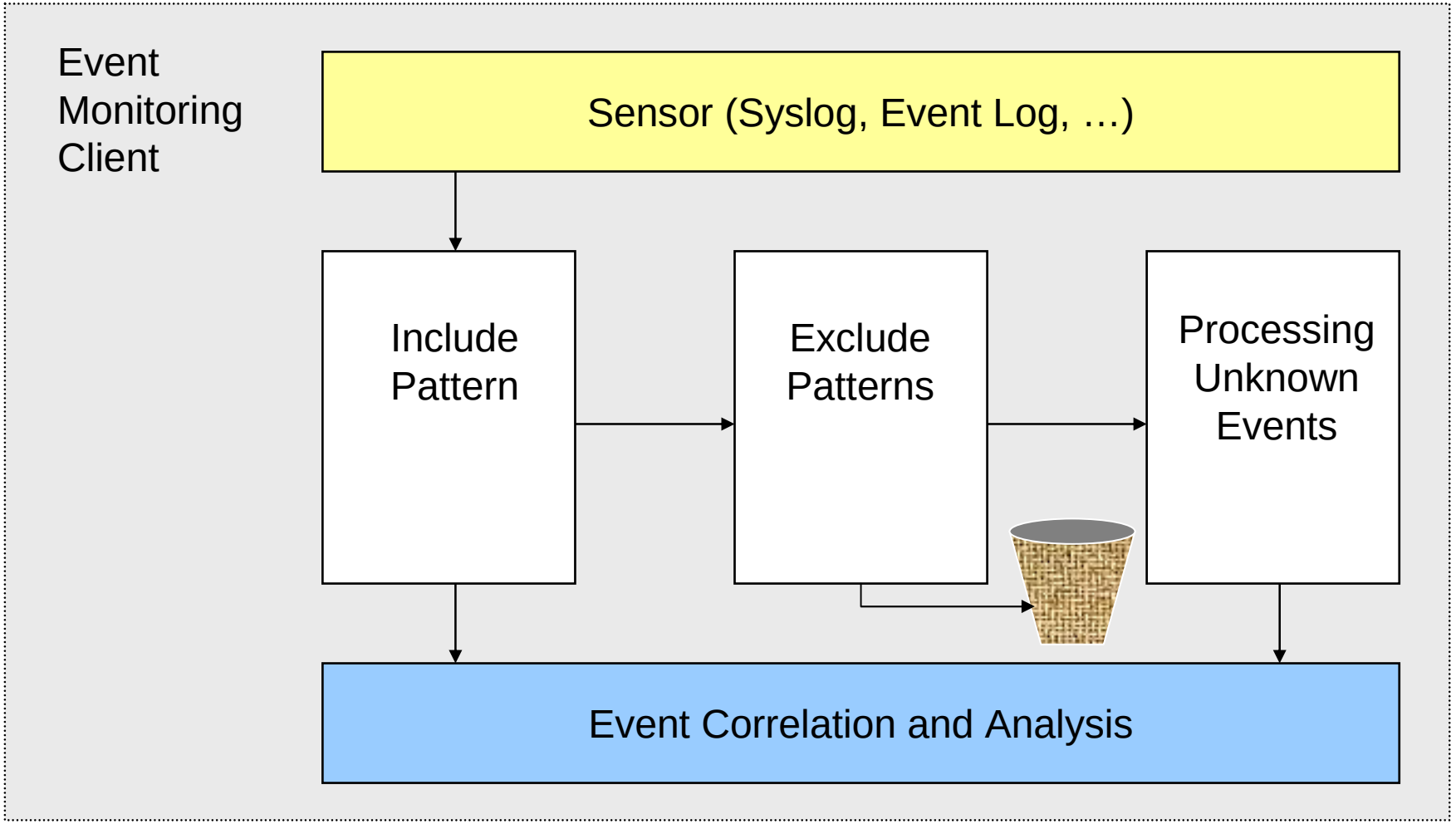


Filter Rules and Correlation Rules show events which require further investigation. Which one to pick?

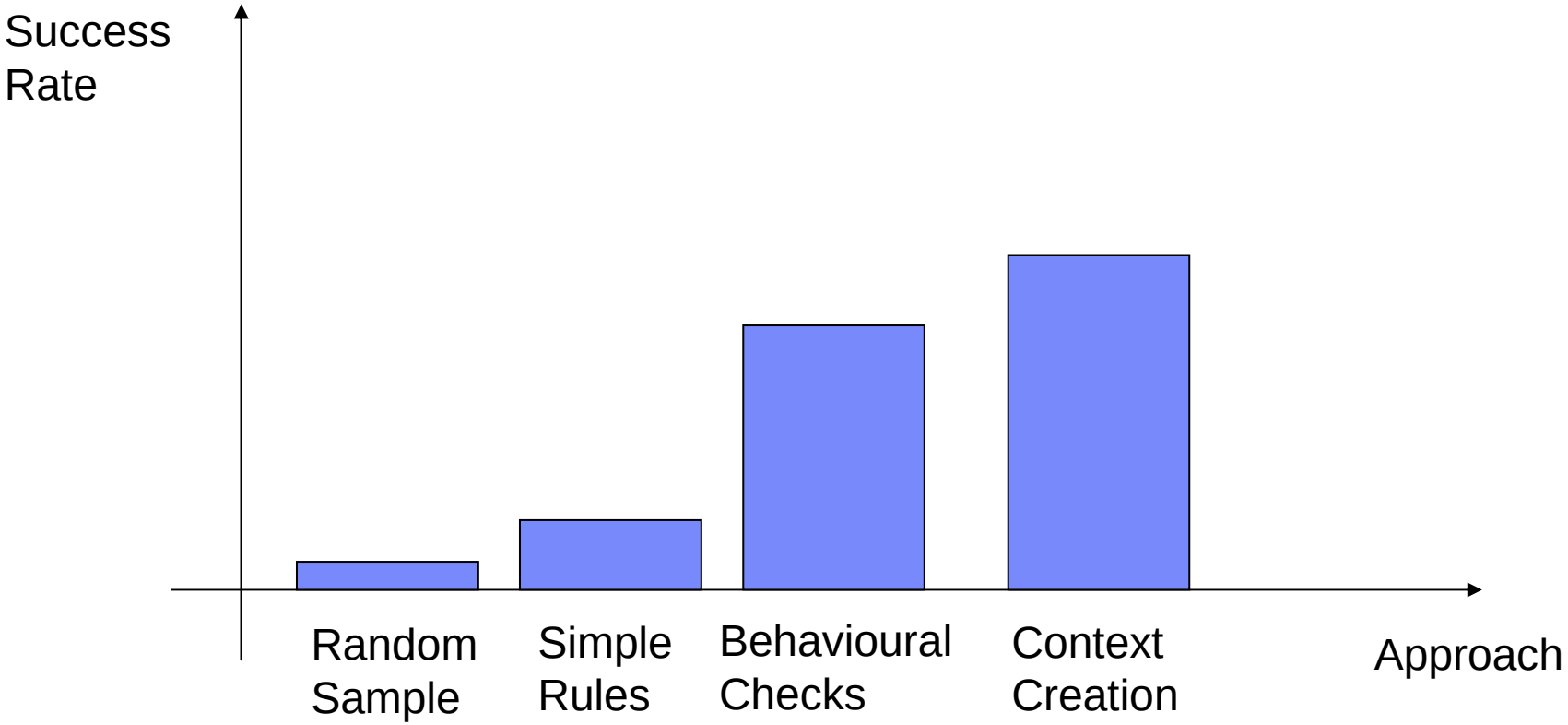
Mid-size production environment



Processing and forwarding unknown events keeps the include and exclude pattterns up-to-date.



The security operator‘s success depends on selecting the right event



Immediate reaction on critical events is key to prevent misuse of access rights.

„17:54:03.00: User us0815 logged in with privileged access on host obaserver1.company.com“

1. Identify user
2. Determine user status and role
3. Security classification of host
4. Access assessment
5. Contact
6. History analysis

Disaster revealed the next day....

Access to multiple data source is required for a comprehensive assessment.

Change Data

Change-ID	Hostname	Description	Person
Change-45	messaging.company.com	Install patch	Oliver James
Change-47	obaserver1.company.com	Delete db instance #23	John Admin

Asset Data

***Asset-id*;hostname;owner;os;sla**

Asset-86; obaserver1.company.com; J. Admin;Unix;8x13
Asset-87; online.banking.com;Jason;Unix;24x7
Asset-88; messaging.banking.com;Windows;8x5

User ID Management

System	login	real_name
Windows	delivery7	Oliver James
Unix	stephanSec	Stephan Verne
Unix	us0815	John Admin

HR Data

Person-ID	Name	Telefon
Person-17	Oliver James	2457
Person-18	John Admin	3526
Person-19	Michael Jones	3334

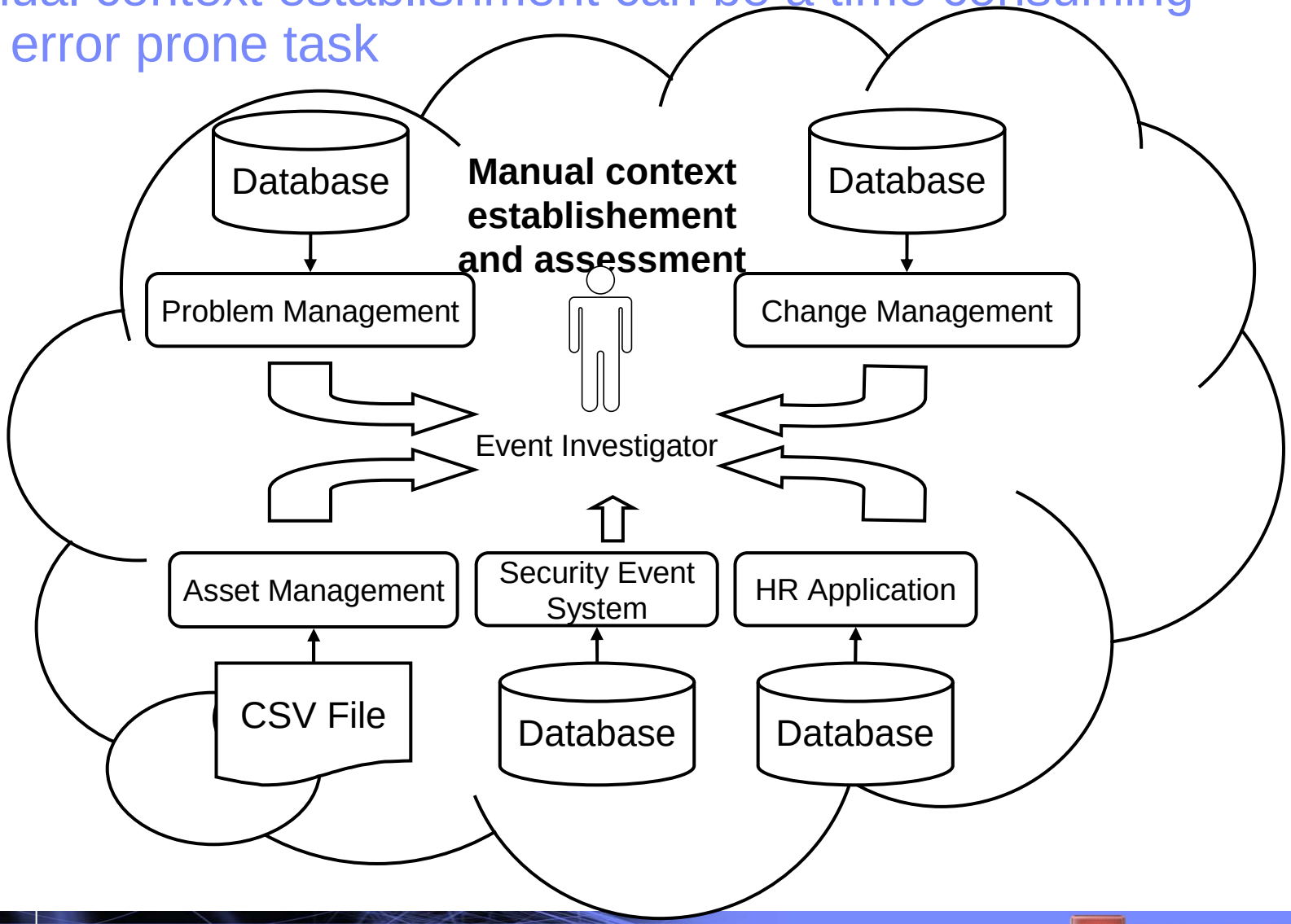
Event Data

Event-ID	Hostname	Event description
Event-123	obaserver1.company.com	us0815 logged in on obaserver1.company.com
Event-124	Messaging.company.com	3 x false password by george27
Event-125	obaserver1.company.com	us0815 performed a 'sudo' on host obaserver1.company.com .

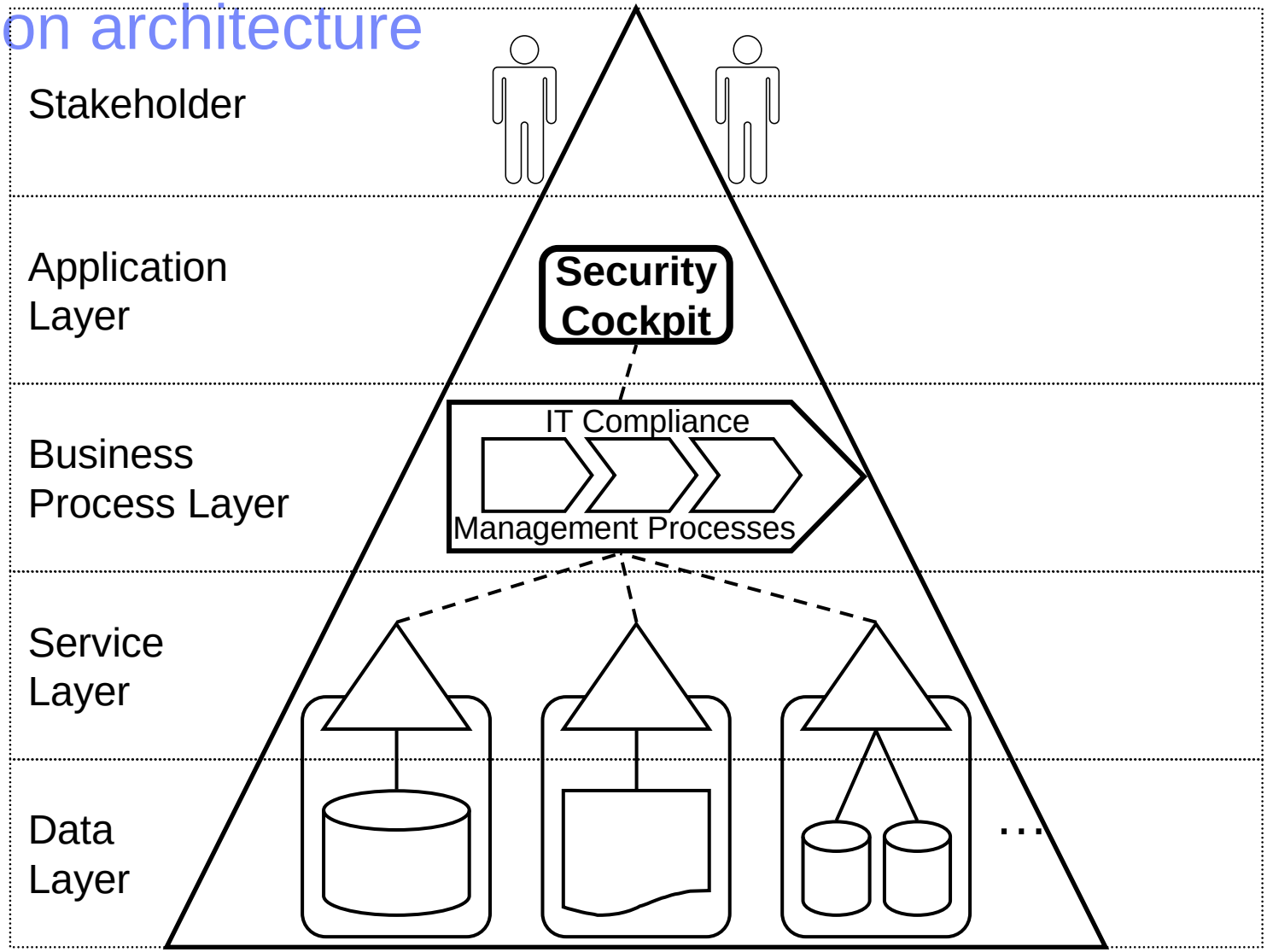
Data Access

- 5 x HR Data
- 2 x Event Data
- 1 x Change Data
- 1 x Problem Ticket System
- 1 x Brokering System
- 1 x Asset Data
- 1 x SOX Liste
- 1 x User ID Management System

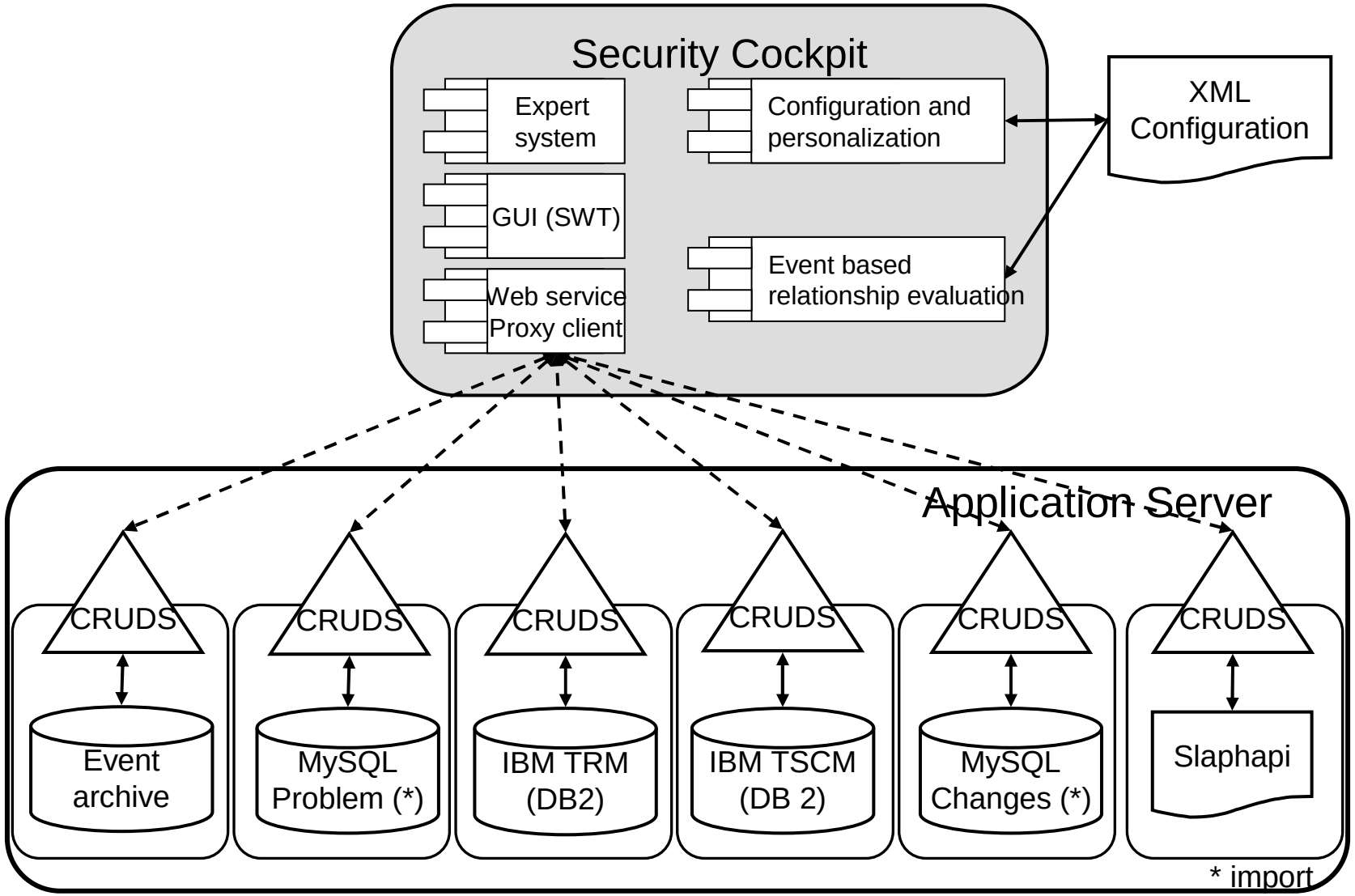
Manual context establishment can be a time consuming and error prone task



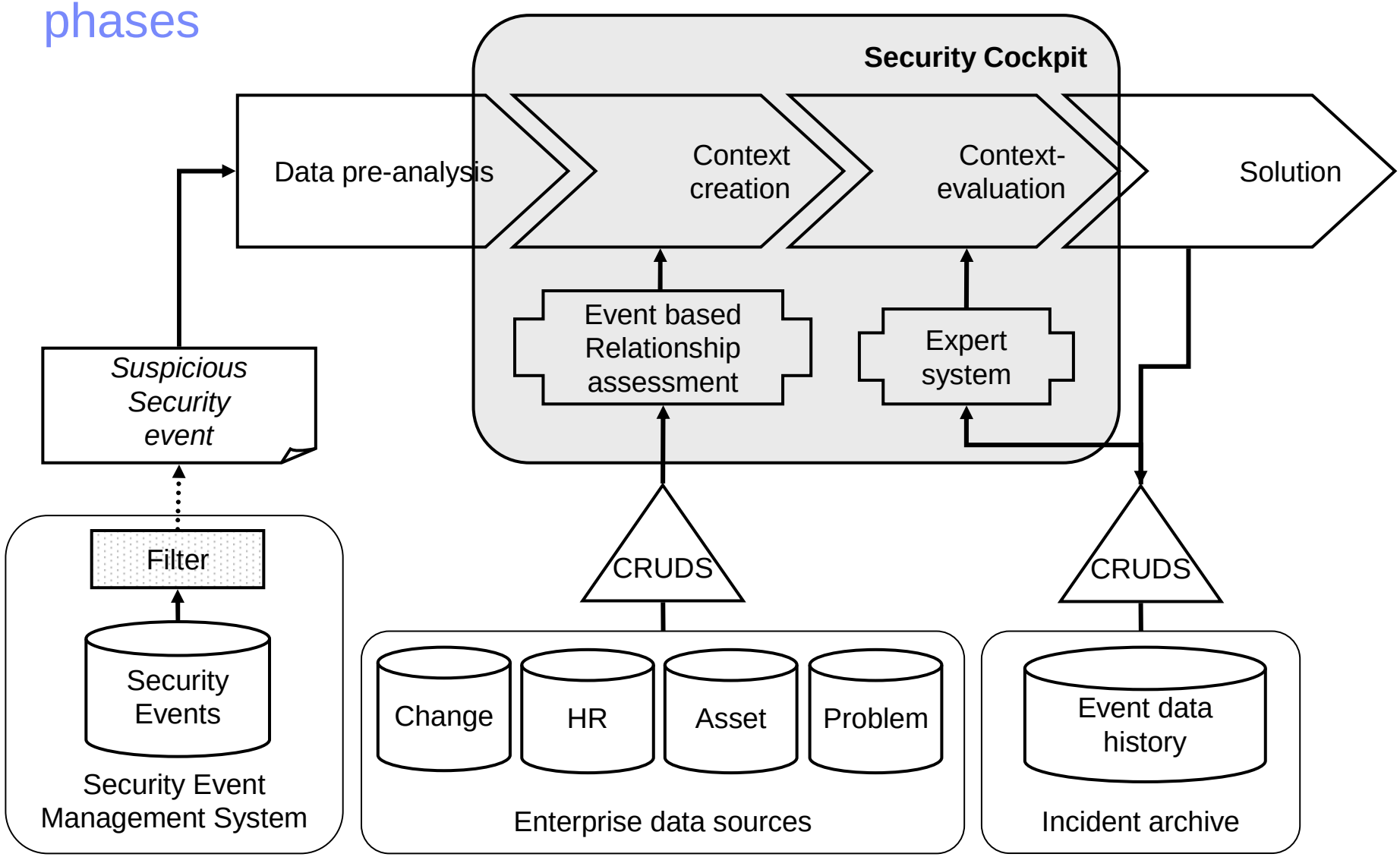
Solution architecture



The Component Model



Our solution supports users in all incident processing phases



First prototype promises improved reaction on security events with regards to time and contents.

- Security event assessment is mandatory part of compliance management
- Helps to reduce risk of unauthorized access
- Event context creation is an essential part of the process
- Our prototype improved the event reaction time and quality of investigations during the pilot phase
- Next steps include further automation of event assessment, for example by integrating „patterns of behaviour“ in the context of change management