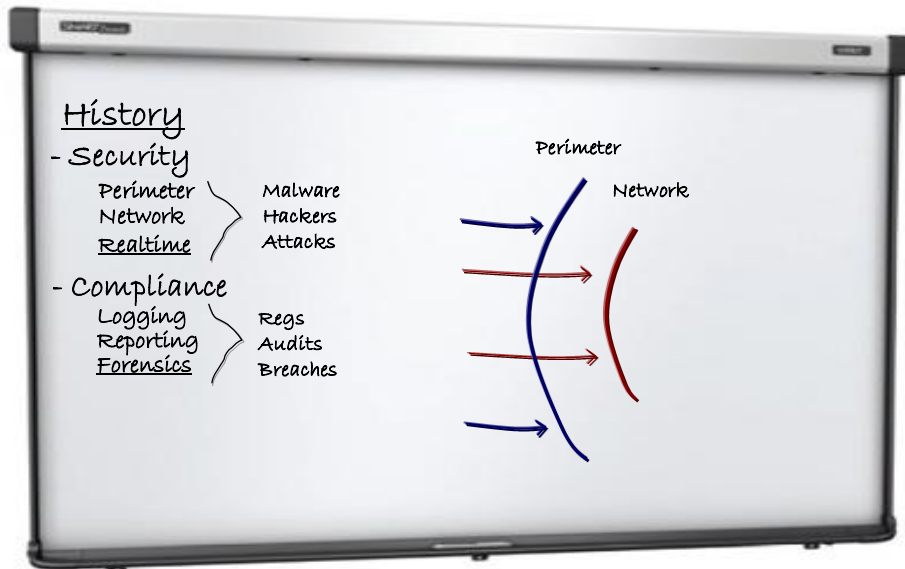
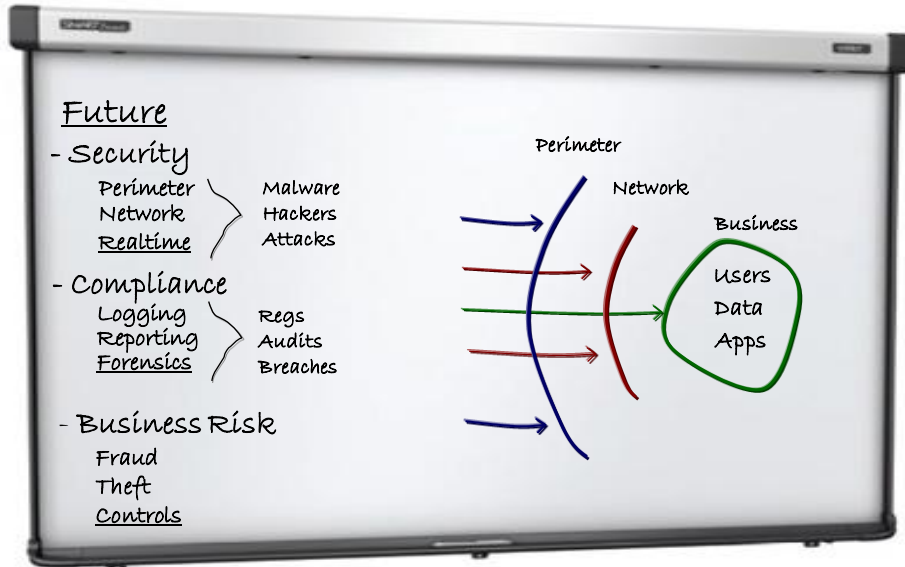


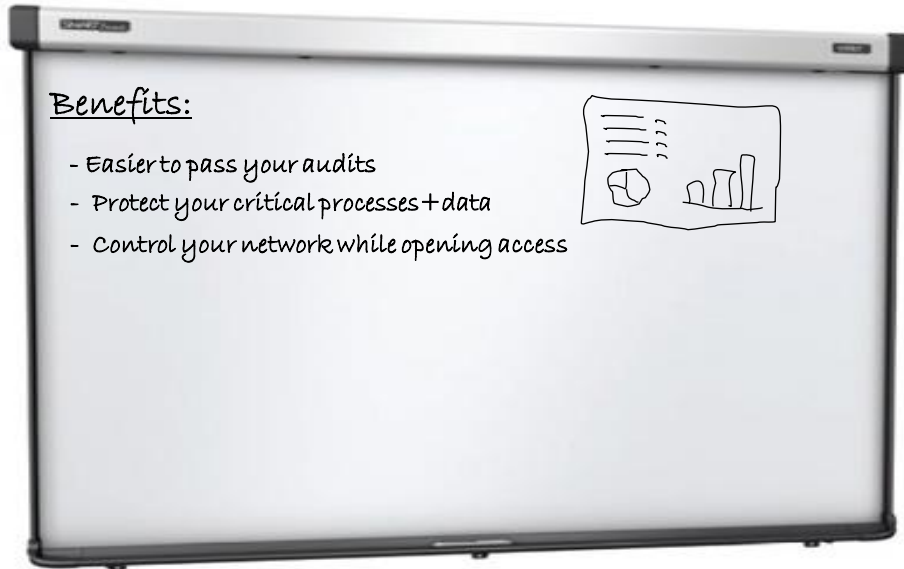
## Beyond IP Addresses. Monitoring Security Risks in Business Processes

Fabian Libeau





- Scenarios:
- Privileged user monitoring
  - Shared account tracking
  - Terminated user activity
  - Separation of duties
  - Online fraud detection



## Top Scenarios



### Identity

- Shared Account Usage Tracking
- Terminated Contractor Activity
- Separation of Duties Monitoring



### Data

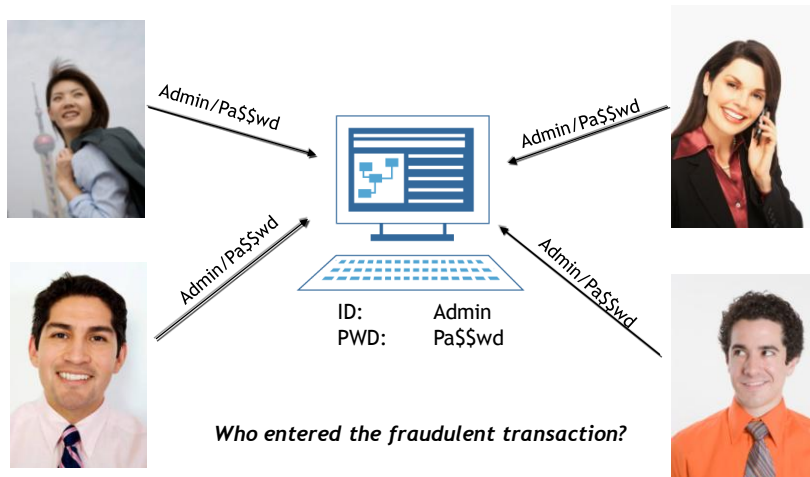
- DBA Activity Monitoring
- SQL Injection
- DB Admin Rights Changes



### Transactions

- Wire Fraud Detection
- Credit Card Number Theft
- Pump and Dump Stock Trades

## Compliance Examples: Shared Account Usage



## Compliance Examples: Terminated Contractor Activity

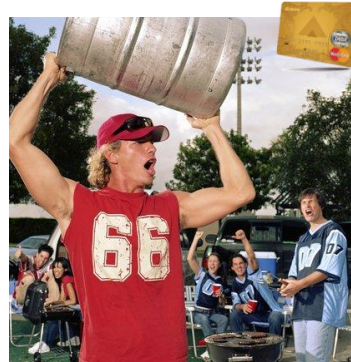


Why is he accessing the finance file server?

## Risk Management Example: Online Fraud Detection



*Is this guy really buying shoes in Brussels?*

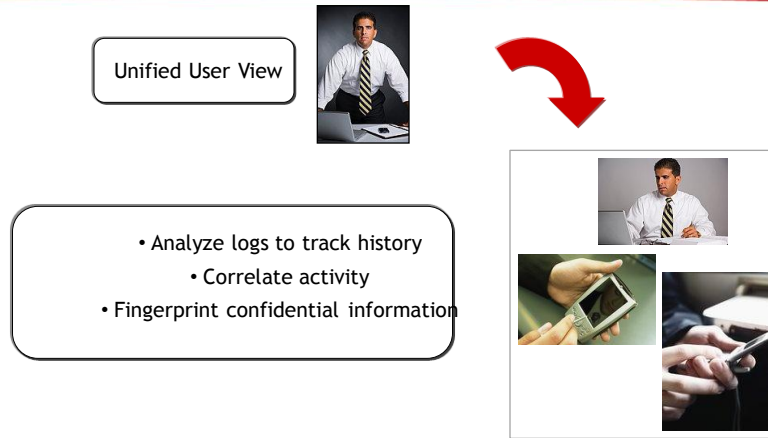


Home Country:	USA	Home Country:	USA
Txn Country:	USA	Txn Country:	Belgium
MCC Code:	5444 (ecomm)	MCC Code:	5444 (ecomm)
Amount:	\$322.10	Amount:	\$96.20

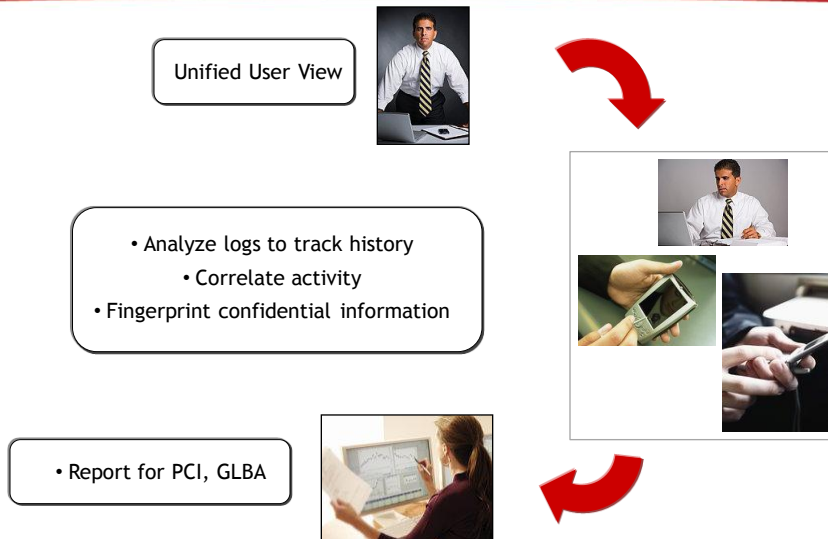
## WHO is Accessing My Systems?



## WHAT Data Are They Seeing?



## WHICH Actions Are They Taking?





ArcSight<sup>™</sup>