

SIEM: A Critical Component of Information Risk Management

Stefaan Hinderyckx - Security Director Europe

Dimension Data



Infosecurity.be
23-24 March 2011

Friday, April 01, 2011

Agenda



Introduction & definitions

Market drivers

Three Key Objectives

Recommendations

Introduction & definitions

SIM and SEM Definitions

SIM = Security Information Management

Functions

- *Event collection*
- *Event normalization*
- Log record integrity protection
- Event storage and retention management
- Report generation
- Forensic query

SIM and SEM Definitions



SEM = Security Event Management

Functions

- *Event collection*
- *Event normalization*
- Event filtering and aggregation
- Event correlation
- Alert and alarm generation
- Incident workflow support
- Frequent log review support

Source : Burton Group

5

Agenda



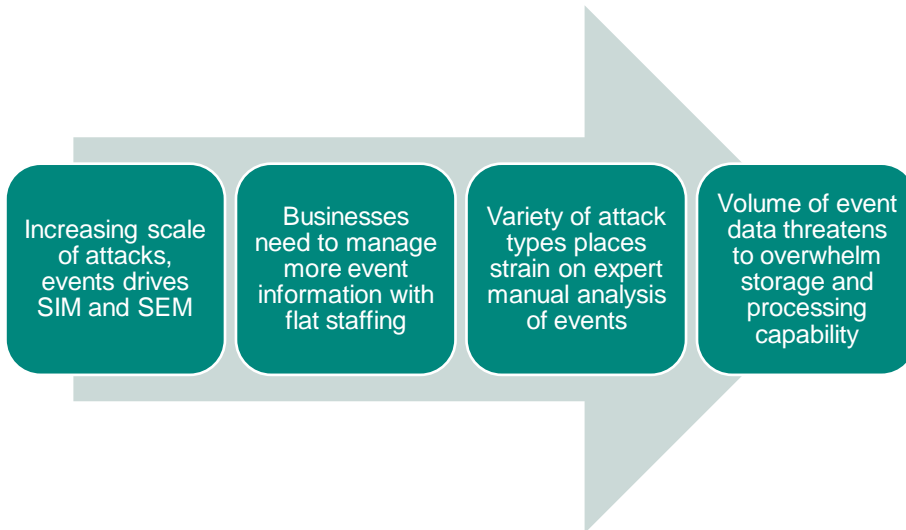
Market
drivers

6

© Copyright Dimension Data 2000 - 2009

1 April 2011

Market Driver – Complexity & Scale



Source : Burton Group

7

Market Driver - Compliance



Compliance - particularly PCI - drives SIM and especially SEM

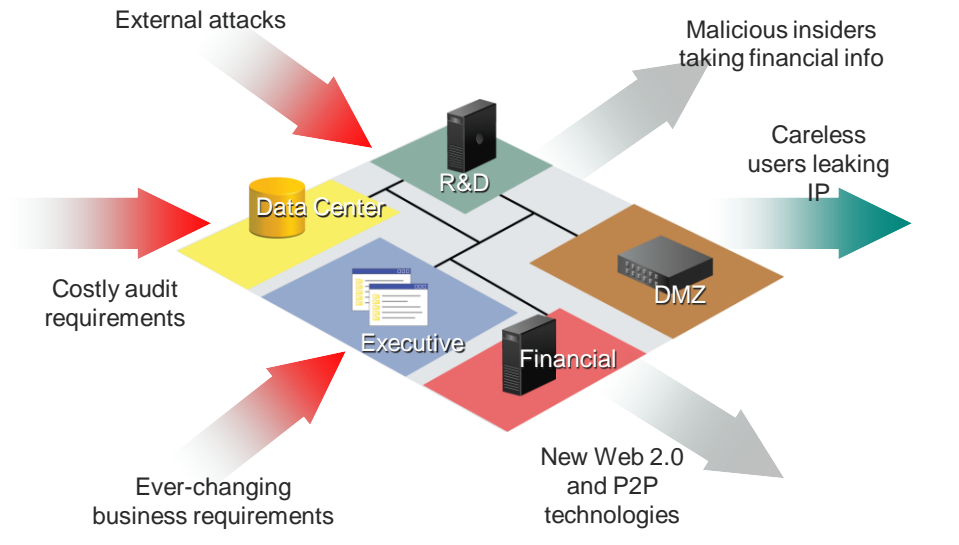
PCI-DSS requirement 10 is the major current driver

- 10.2: Implement automated audit trails for all system components to reconstruct the following events...
- 10.3: Record at least the following audit trail entries for all system components for each event...
- 10.5: Secure audit trails so they cannot be altered
- 10.6: Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS)
- 10.7: Retain audit trail history for at least one year, with a minimum of three months online availability

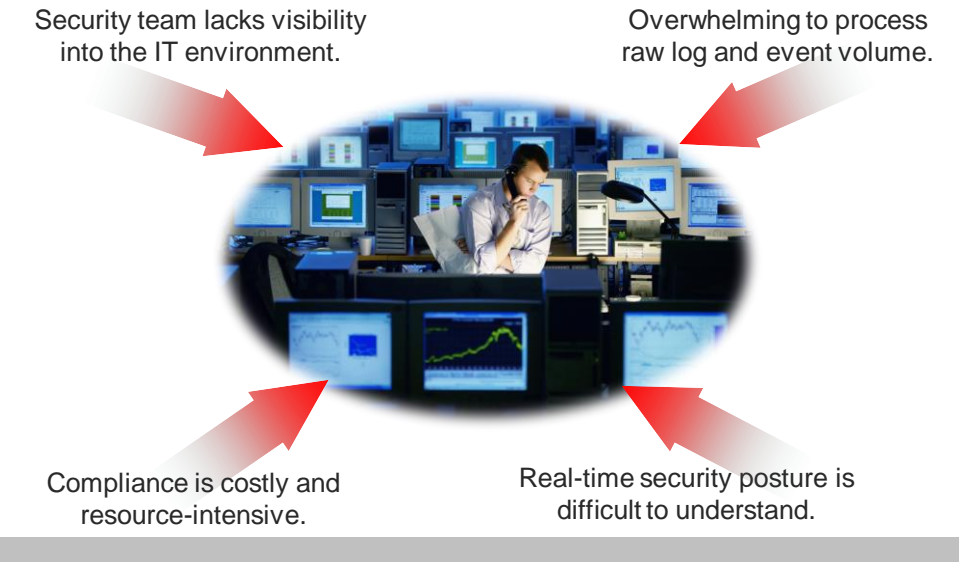
Source : Burton Group

8

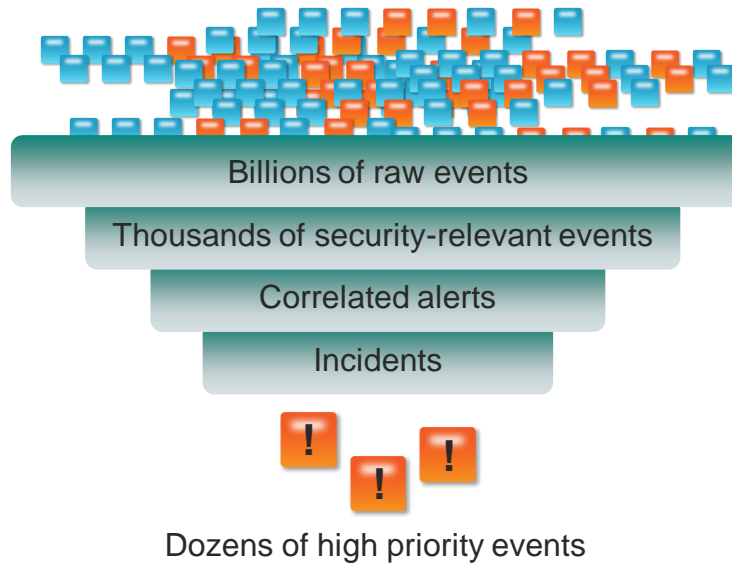
Threats and Regulations



IT Staff Feels the Pressure



Finding a needle in a HUGE haystack

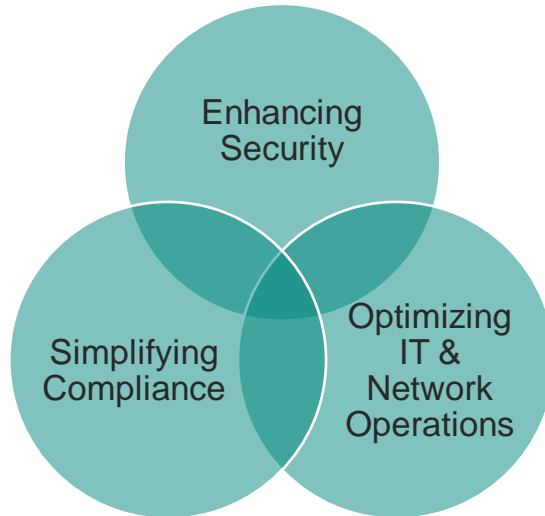


Agenda

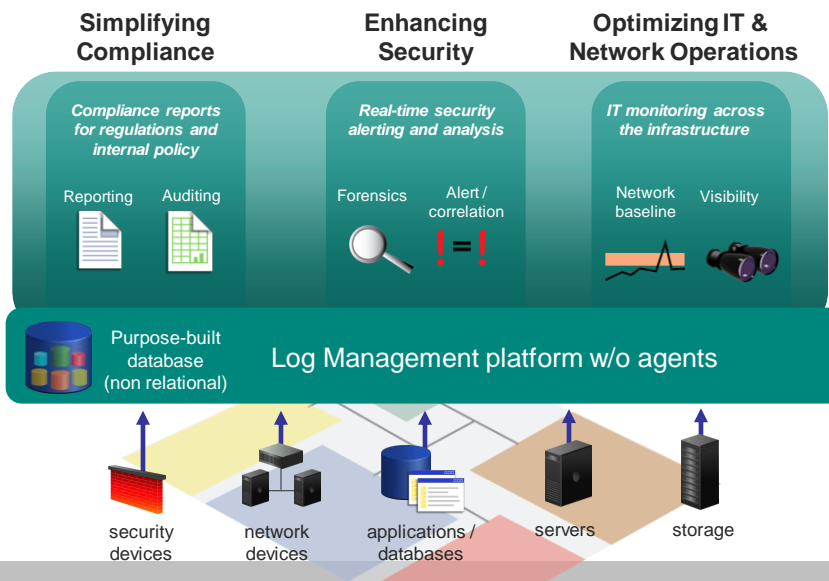


Three Key Objectives

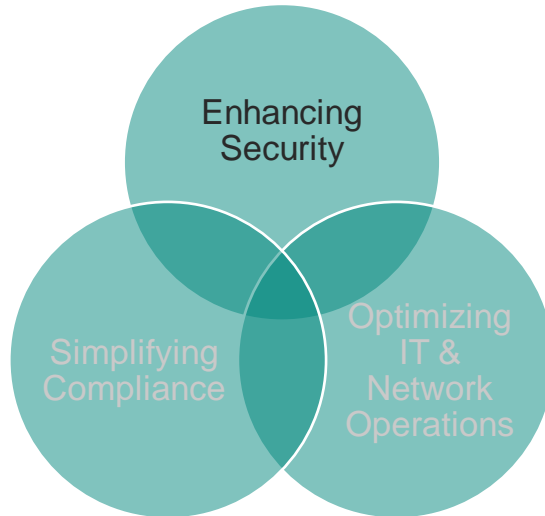
Three key objectives



SIEM Architecture & key objectives



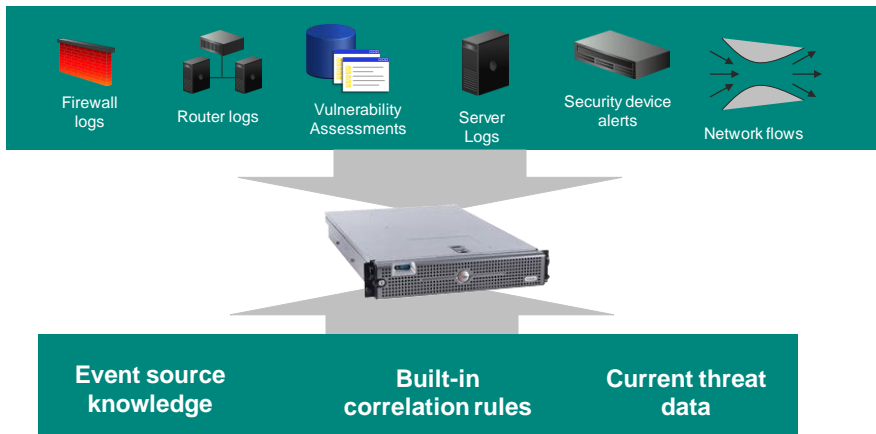
Three key objectives



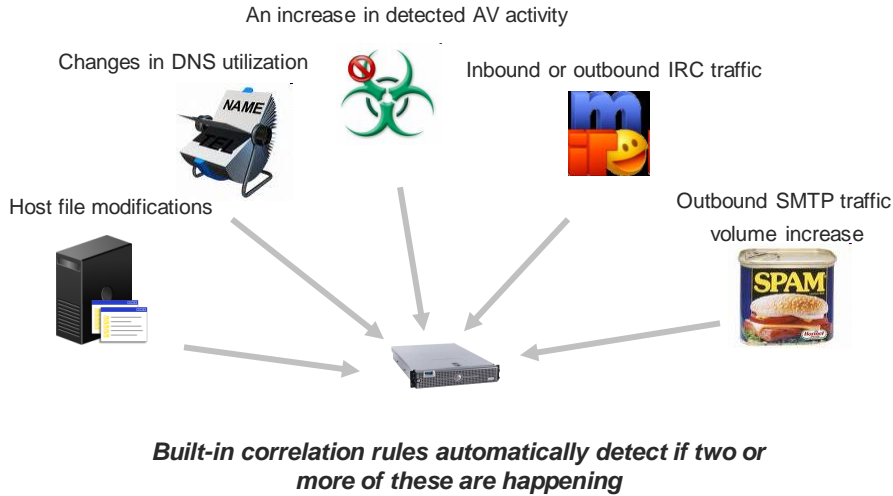
Incident detection and response



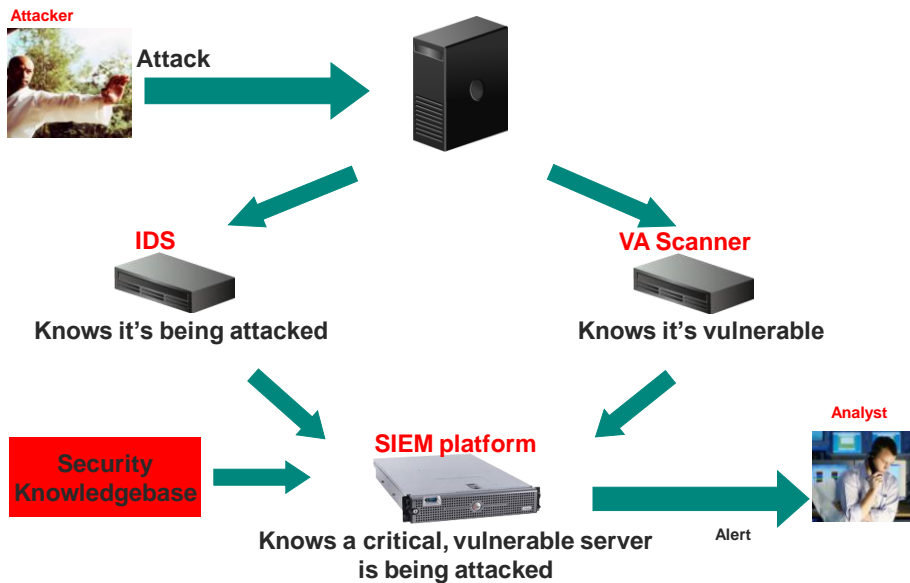
- Combining data from across the network with security knowledge to get the bigger picture



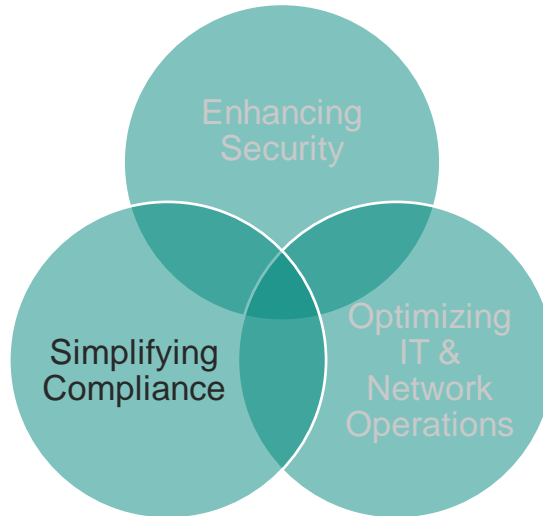
Example : Detecting Botnets



Example : Vulnerable Server Attacked



Three key objectives



Top 5 Things SIEM must do to Simplify Compliance



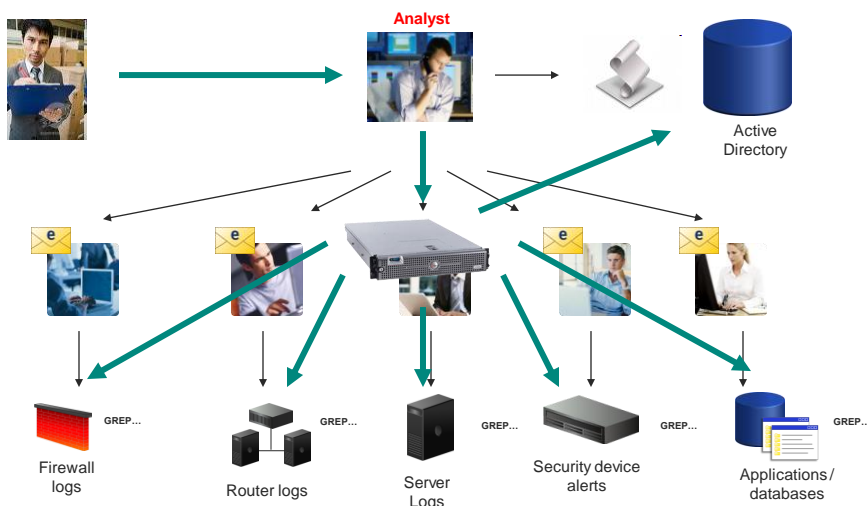
- 1 Collect ALL the event log data, ALL the time!
- 2 Store the data from across the organization in a secure common data repository for global analysis
- 3 Ensure that the data is not filtered, edited, or changed in anyway
- 4 Ensure that the data is verifiable and authentic
- 5 Maintain an audit trail of all activity

Compliance - Alerting & Reporting

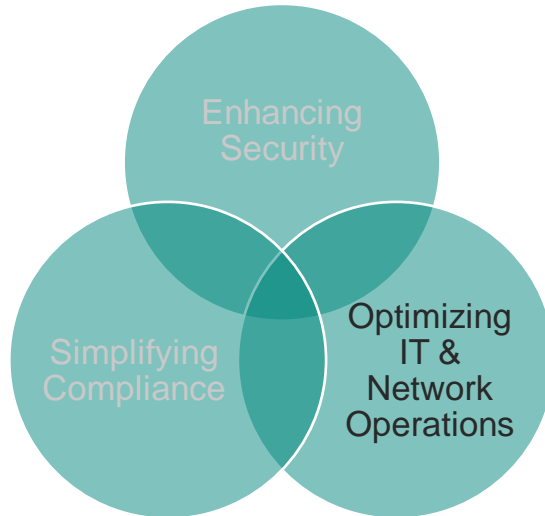


- ▶ Canned reports for easy response to auditors
 - Mapped to common regulations
 - Reports against common controls frameworks (e.g. ISO-17799)
- ▶ Asset grouping to identify in-scope event sources
 - Prioritize alerts based upon regulatory or contractual requirements

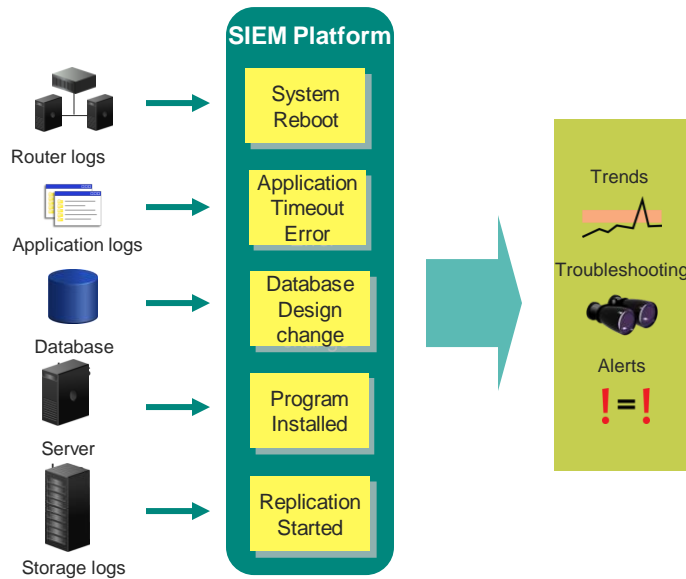
Example: privileged users logs



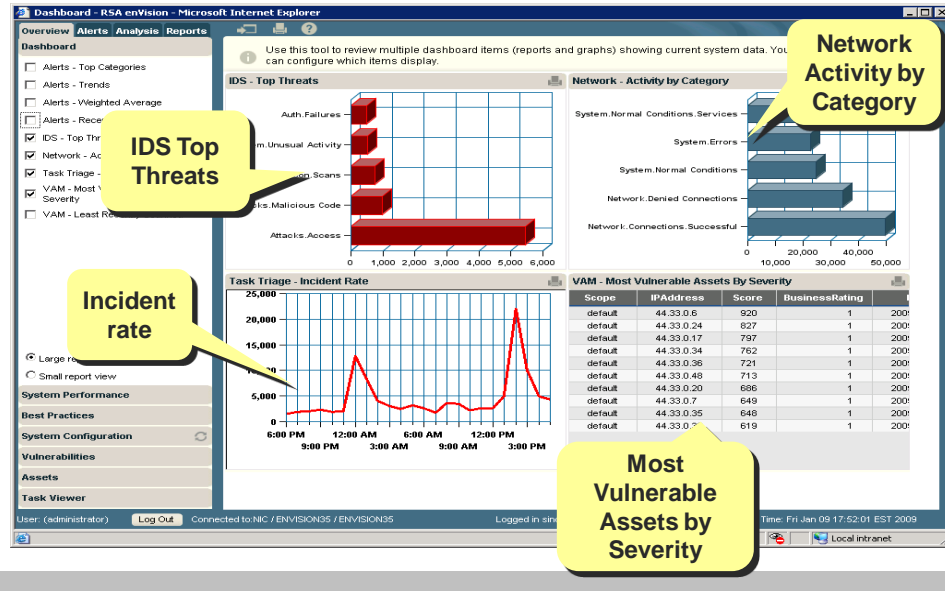
Three key objectives



Streamlining IT & Network operations



Single dashboard for security, compliance and IT operations issues



Agenda



Recommendations

Recommendations



Avoid agents

Validate scalability in terms of events per second

Beware of data explosion

Data integrity is absolutely critical

Don't underestimate the complexities of correlation

Be realistic about your in-house capabilities – outsource if required

Thank You

Stefaan Hinderyckx - Security Director Europe

Dimension Data

