

SIEM City

Luc Doods



Security Information and Event Management

- SIM + SEM = SIEM
- SIEM Architecture
- Market Overview

Security Information and Event Management

- SIM + SEM = SIEM
- SIEM Architecture
- Market Overview

Security Information Management (SIM)

Provides analysis and reports of data from

- network, host ,systems and applications
- security devices supporting
 - policy compliance management
 - internal thread management
 - regulatory compliance initiatives

SIM supports IT security, internal audit and compliance organizations

Common Required ICT Compliance Controls

- Access Control
- Configuration Control
- Malicious Software Detection
- Policy Enforcement
- User Monitoring and Management
- Environment & Transmission Security



Security Information Management (SIM)

Log Data

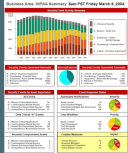
Log Data

Log Data

Log Data

Log Data

Log Data



Compliance Report



Security Event Management (SEM)

Improves security incident response capabilities by

- near-time data processing from
 - security devices
 - network devices
- providing real-time event management for security operations

SEM helps IT security personnel to be more effective in responding to external and internal threats.



Security Event Management (SEM)

Log Data

Log Data

Log Data

Log Data

Log Data

Log Data



Log Data

Log Data

Log Data

Log Data

Log Data

Log Data

SIM + SEM = SIEM



Security Information and Event Management (SIEM)

Log Data

Log Data

Log Data

Log Data

Log Data

Log Data



Security Information and Event Management

- SIM + SEM = SIEM
- SIEM Architecture
- Market Overview

Market Drivers

Customer Need to

- Analyze Security Events Data in Real Time
- Analyze and Report on Log Data

Regulatory Compliance

- SoX, HIPAA, Basel II, ISO 17799 and many more ...

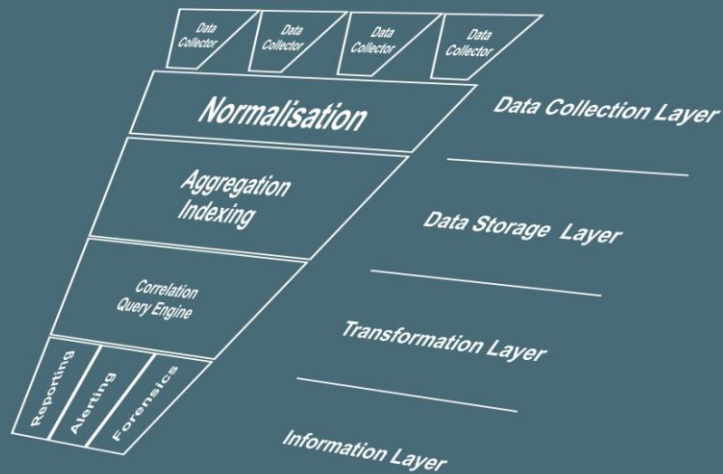
SIEM Requirements

Collection/Capture from heterogeneous data sources
Normalization
Indexing
Advanced Analytics with Data/Filters

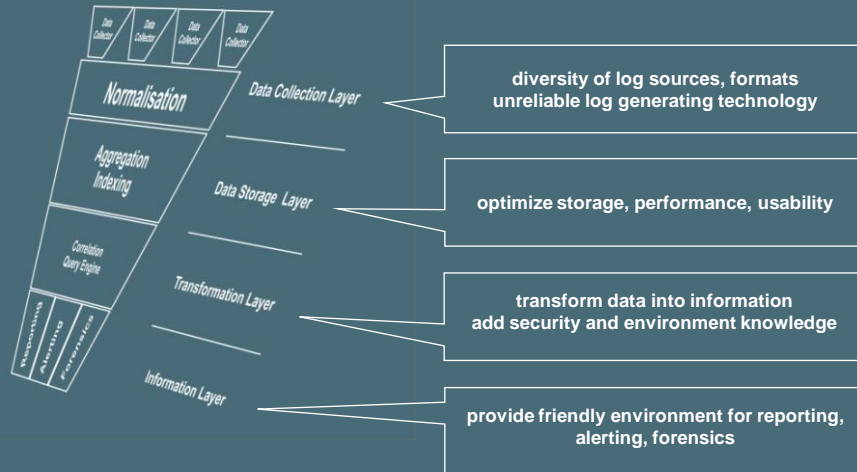
Assets Knowledge
Topological Knowledge
Vulnerability Knowledge



Common SIEM Architecture



Every Layer has its challenges



©CURE

Data Collection Layer

Collect all log information from heterogeneous sources in a constant way

Diversity of 'out-of-the-box' supported log collection

- Security devices, networking devices, OS'es, applications !!!
- Easy parsing technology for non-covered log sources

All Log Data are potentially relevant

- Syslog is UDP based
- Log Buffering on device failure

Agent less vs. Agents

- Agents will Normalize 'on the fly' and send normalized data to the repository
- Agent less systems will store the raw log the repository and work on metadata through indexing

©CURE

Data Storage Layer

Optimize Storage for performance and usability

RDBMS (e.g. ArcSight, High Tower, Log Logic)

- is the most obvious, straight-forward solution for data storage
- are designed for complex datamodels and random read/write operations
- demand a particular database tuning knowledge from the customer
- requires normalization of log data
- tend to be less performing than other systems unless you compensated by filtering out, so called irrelevant data (who are we to decide if data is and will remain irrelevant ...)



Data Storage Layer (.)

Proprietary Database

- are designed for performance
 - write once/read many operations
 - no expensive record locking mechanisms
- not necessarily require normalization
- raw data is stored
- focus is on indexing and producing meta-data



Transformation Layer

Transforms Data into Information

Query Engine

- most straight-forward ways to gather information
- mostly QBE, SQL, ...
- performance will depend upon the DB

Correlation Engine

- tool that supports the search for 'causal structural or functional relationships between events'
- watch out for 'cheap trick' counting tools
- rule base driven
- it is the population of the rule base that determines the real-added value of the SIEM system



Transformation Layer (.)

Watchdog System

- rules or queries in combination with a threshold to generate alerts



Information Layer

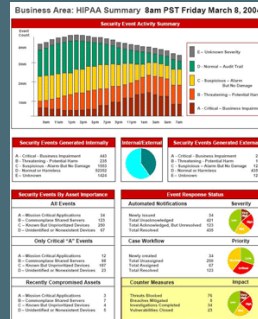
Delivers Structured Information to Customer

Reports

- compliance reports
- your compliance regime needs to be available out-of-the-box
- security reports
- check the intelligence of the security reports
- user-defined reports for company specific

Alerting

- quality depends upon the completeness of the correlation rule base
- filter out false-positives
- integrate with your Trouble Ticketing System



Information Layer (.)

Forensics

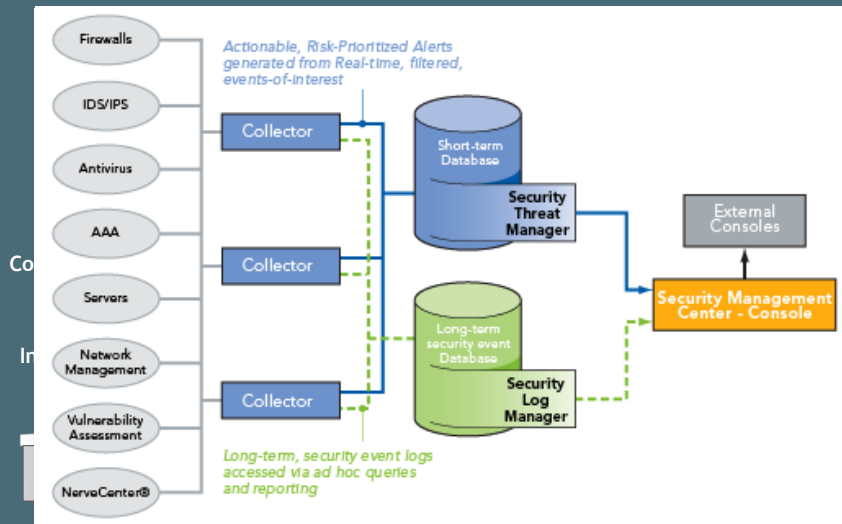
- you don't know what you are looking for
- think like a detective
- look for smoke signals
- assumption -> consequences -> reality check -> keep, adapt, remove
- eliminate all the impossible, whatever remains, must be the truth
- you need a set theory based system
- has room to improve in ALL current systems



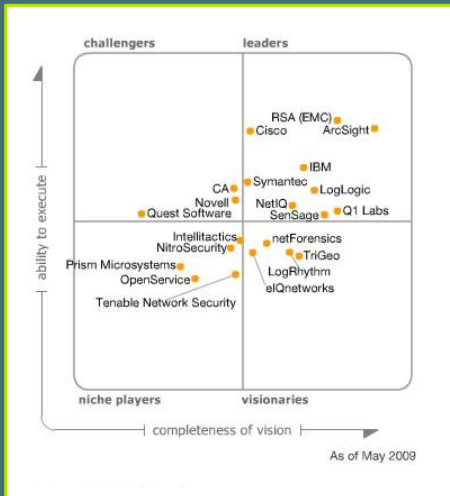
Security Information and Event Management

- SIM + SEM = SIEM
- SIEM Architecture
- Market Overview

Some SIEM Architectures



Market Overview – Gartner



Eliminate vendors:

1. poorly distributed in Europe
2. only decently handling their own log
3. compensating discussable technological choices with marketing tricks (A/FUD)

