Using SIEM for Compliance

- Adrian Lane – Security Strategist
- Securosis.com

Overview

- **SIM/SEM Introduction**
- **Compliance Initiatives**
- **Implementation Examples**
- **Tips**
- **Other Considerations**

Evolution of Terminology

- SIM – System* Information Management
- SEM - Security Event Management
- NBA – Network Based Analysis
- Log Management – Log file capture & storage
- SIEM - SIM & SEM

SIEM: What is it?

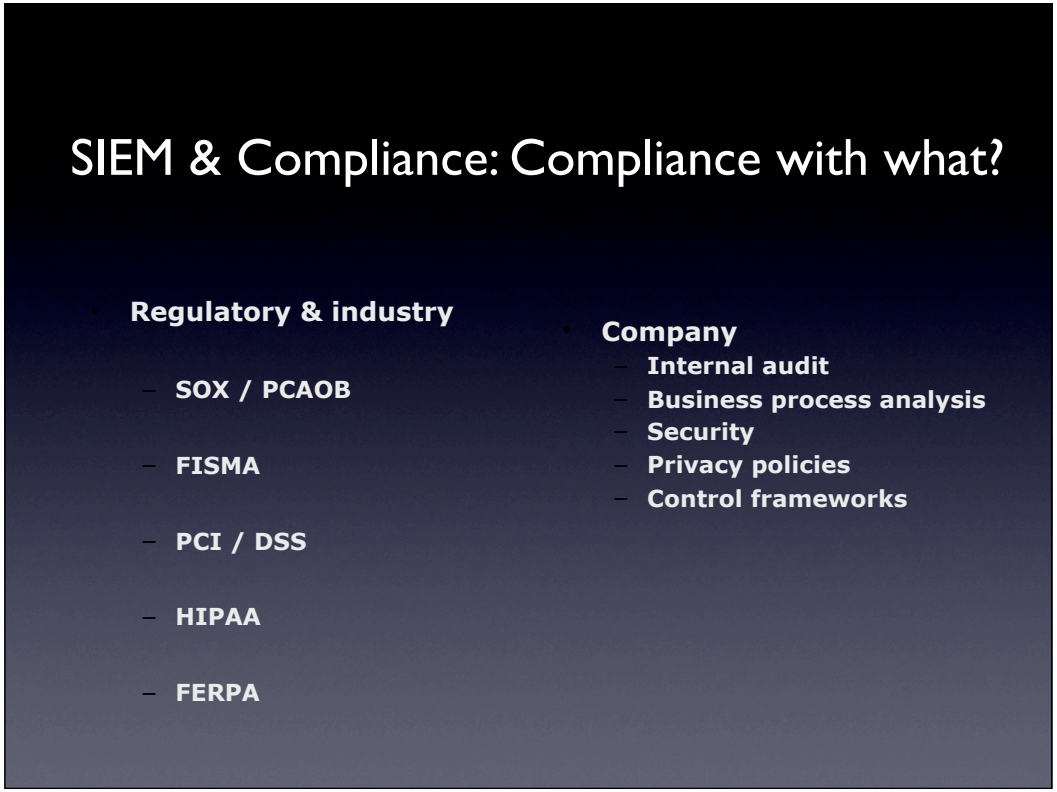
- Diverse Data Collection
- Aggregation & Normalization
- Correlation & Analysis
- Reporting
- Workflow & Integration

SIEM: Data Collection Toolkit

- **System logs & files**
- **Device logs**
- **Network activity**
- **Transactions from apps & database**
- **Change logs**
- **Discovery**

What to do with the Data?

- **The challenge is to map the tools to the compliance initiative:**
  - **What data do I collect?**
  - **What am I responsible for keeping?**
  - **do I implement controls?**
  - **reports do I need to produce?**
  - **w do I react to events?**



Rewrite

Security Management

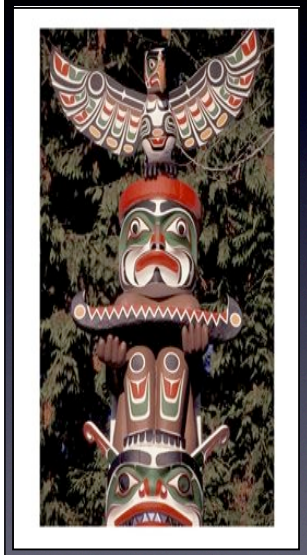
Security management includes risk management, information security policies, procedures, standards, guidelines, baselines, information classification, security organization, and security education. These core components serve as the foundation of a corporation's security program. The crux of security, and a security program, is to protect the company's assets. A risk analysis will identify these assets, discover the threats that put them at risk, and estimate the possible damage and potential loss a company could endure if any of these threats become real. The results of the risk analysis help management construct a budget with the necessary funds to protect the recognized assets from their identified threats and develop applicable security policies that provide direction for security activities. Security education takes this information to each and every employee within the company so that everyone is properly informed and can more easily work toward the same security goals.

Security management has changed over the years because networked environments, computers, and the applications that hold information have changed. Information used to be held in mainframes, which is a more centralized network structure. The mainframe and management consoles used to access and configure the mainframe were placed in a centralized area instead of the distributed approach we see today. Only certain people were allowed access and only a small set of people knew how the mainframe worked, which drastically reduced security risks. Users were able to access information on the mainframe through dumb terminals (they were called this because they had little or no logic built into them). This also drastically reduced the need for strict security controls to be put into place. However, the computing society did not stay in this type of architecture. Now most networks are filled with personal computers that have advanced logic and processing power, users know enough about the systems to be dangerous, and the information is not centralized within one "glass house." Instead, the information lives on servers, workstations, and other networks. Information passes over wires and airways at a rate that was not even conceived of 10 to 15 years ago.

The Internet, extranets (business partner networks), and intranets not only make security much more complex, they make security even more critical. The core network architecture has changed from being a stand-alone computing environment to a distributed computing environment that has increased exponentially with complexity. Although connecting a network to the Internet adds more functionality and services for the users and gives more visibility of the company to the Internet world, it opens the floodgates to potential security risks.

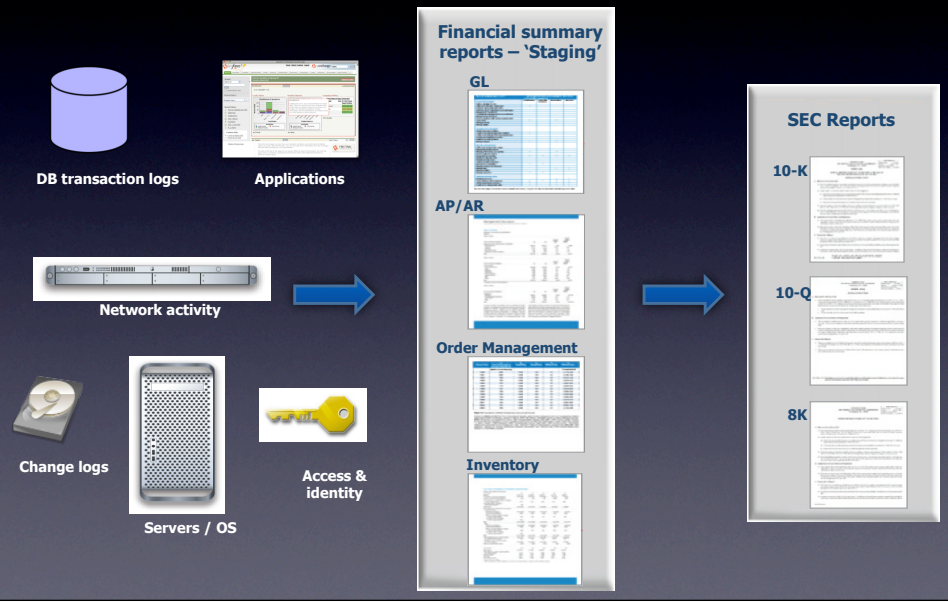
Today, a majority of organizations could not function if they lost their computers and computing capabilities. Computers have been integrated into the business and individual daily fabric and would cause great pain and disruption if they were suddenly unavailable. As networks and environments have changed, so has the need for security. Security is more than just a firewall and a router with an access list; these systems have to be managed and a big part of security is the actions of users and the procedures they follow. This brings us to security management practices, which focus on the continual protection of company assets.

SOX Totem Pole of Clarity



Sarbanes-Oxley	• SOX & ICOFR • Executives must tell the truth • Prove your financials are accurate
PCAOB	• Auditing Standard #5 • How auditors prove financials are accurate
COSO	• "Cookbook' on what and how to investigate • People & Process, not Technology
COBIT	• IT control objectives • Process and checklist for technology
IT Infrastructure	• Systems to be queried & monitored
You & SIEM	• How the work gets done

IT's Role in Producing Financial Statements



SOX – The ‘Show Me’ Regulation

- Your financial statements are accurate?
- Show me!
- What happened?
- Explain what should not have happened
- Reconciliation

Control Examples: Identity Management

- Objective:

Show that all accounts in relation to financial reporting have not been altered to allow unwanted access.

Check for unreasonably escalated privileges that allow access to accounting and reporting functions.

Data source:

Access & identity

Corresponding guideline:

COBIT:
AI2.4
DS5.3, DS3.5, DS5.4

Examples:
Failed Application Use,
Failed Application Logins

Objective:

Attempted access to financial applications or reporting systems should be reviewed for signs of potential misuse.

Failed transactions should be accounted for, both as an indicator of potential fraud, and as a KPI for efficiency.

Data Sources:

Access logs

Application logs

Network activity

Corresponding regulation:

COBIT:
DS10.1

Examples:
End of Period Adjustments;
Prior Period Remediation

Objective:

Changes to General Ledger, Accounts Payable, Accounts Receivables after the account period need to be documented and explained.

Alterations and remediation entries need to be provided to auditors.

Data Sources:

DB transaction Logs

Application logs

Corresponding regulation:

COBIT:
AI 2.3
PCAOB:
Section A-38

Examples:
Transaction Verification (Application Logs, Transaction Logs, Service Accounts)

Objective:

Provide an auditor the ability to review transactions and verify that what should have happened actually did happen.

Reports should provide insight as to the effectiveness and efficiency of the controls. Aggregation of information from multiple points provides proof of activity.

Data Sources:

Access logs

Applications

Network activity

DB transaction logs

Corresponding regulation:

COBIT:
DS 3.5, 5.5, 13.3
PCAOB:
Section 50

Examples: Anomaly Detection & Reporting

Provide a suitable explanation of anomalous events, with sufficient detail, proving that there are no deficiencies or errors in transaction reports.

Detection and reporting for system outages, database restoration, alteration of audit data collection, failed transactions and other events should be recorded and reported to auditors.

Data Sources:

Servers / OS

Change logs

DB transaction logs

Network activity

Corresponding regulation:

COBIT:
AI 7.11, DS 4.8, 5.5, 10.1
PCAOB:
Section 85

PCI DSS
Security & Privacy

- **Secure Credit Card Data**
- **Monitor Use of Data**
- **Detective Controls**

Monitor all Network Access to Credit Card Data

Objective:

Monitor all electronic access to credit card data, not just the network. Watch the use of service and admin accounts for obtaining access rights, and monitor network access and DB transaction logs to provide detailed access and use reports of relevant data.

Behavioral Monitoring and Policy Development are very useful in filtering activity records.

Data Sources:

DB transaction logs

Access logs

Network activity

Corresponding regulation:

PCI DSS – Req. 10

Audit: Activity Verification & Remediation Reports

Objective:

Provide reports that show activity and summarize normal use behavior such as updates to AV.

Detailed reports on anomalous events that indicate fraud or system misuse are also recommended.

Data Sources:

Change Logs

Access logs

Application Logs

Network Activity

Corresponding regulation:

PCI DSS – Requirements 5, 6, 7

Other Compliance Regulations …

- **FISMA**
- **FIPS**
- **FERPA**
- **FRCP**
- **HIPAA**

Examples: Controls, Monitoring & Data Retention

Objective

Discovery and continuous monitoring of usage of systems and data; verify compliance of policies. (Example: FISMA, HIPAA)

Attempted alterations to students records should be reviewed for signs of potential misuse. (Example: FERPA)

Collect and filter in accordance to policy and data retention requirements. (Example: FRCP)

Data Sources:

Access logs

Application logs

Network activity

Corresponding regulation:

FISMA – Continuous monitoring & system certification
NIST - SP-800 series

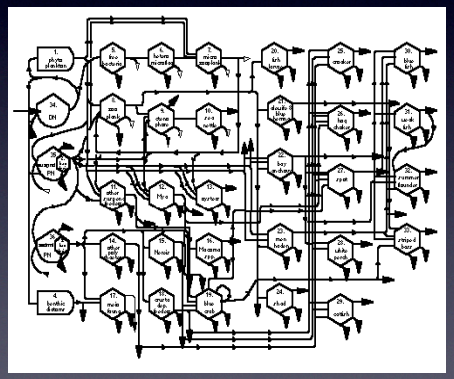
Tips & Tricks

Tip #1: Canned Compliance

- **Using Canned Reports and Controls is like wearing someone else's clothes … the fit is often poor and the style is just not quite right.**

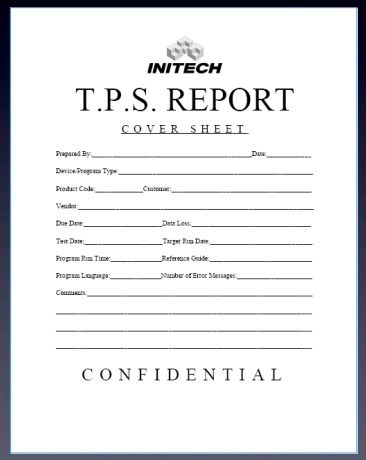
Tip #2: Complete Picture

- **Make sure you are aware of all your applications -- or risk missing the whole picture.**
- **Consider how virtualization, outsourcing and partnerships will effect Controls and Data Collection.**



Tip #3: Normalized Data

- **Use meaningful reports to balance the need for efficient data collection & storage. You can normalize relevant data right out of reports.**



INITECH

T.P.S. REPORT

COVER SHEET

Prepared By:_____Date:_____

Device/Program Type:_____

Product Code:_____Customer:_____

Vendor:_____

Due Date:_____Data Loss:_____

Test Date:_____Target Run Date:_____

Program Run Time:_____Reference Guide:_____

Program Language:_____Number of Error Messages:_____

Comments:_____

_____

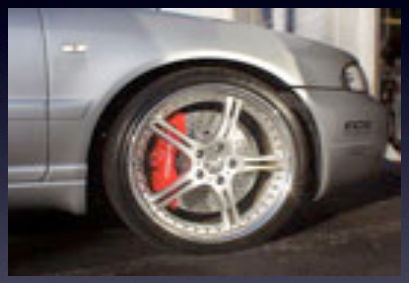
_____

_____

CONFIDENTIAL

Tip #4: Efficiency

- **Remember, this effort is about efficiency & automation. If your controls and reports are not making your job easier, you probably have the wrong ones.**



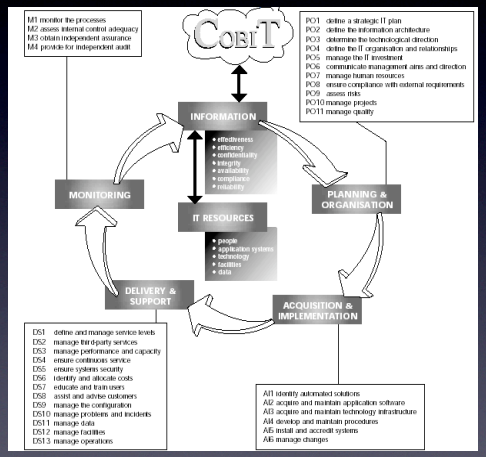
"The brakes on my car don't make me go slower, they allow me to go faster and still maintain control" – Unattributed.

Tip #5: Get to Know Your Auditor

- **The auditor can help you understand the compliance requirements, what is important and what is not.**

Tip #6: People & Process

- **Compliance is more about people & process than technology.**
- **Process is what you make it out to be … so choose a process that works for your organization.**
- **Do not forget training!**



Additional Recommendations

- **Vulnerability assessment & risk assessment for preventative controls and configuration management**
- **Discovery tools assist with location of assets and data.**

SIEM Value

- Broad array of data collection, analysis, storage and reporting options
- Excellent for Detective Controls
- Acceleration of compliance deployment (with vendor canned reports and controls)
- Tailored controls of your processes and systems
- Enhancing the process: Monitor to help discover what is going on, then adjust reports and data collection
- Can feed events to other workflow and management

Adrian Lane

Securosis, L.L.C.

alane@securosis.com

http://securosis.com

AIM: securosis