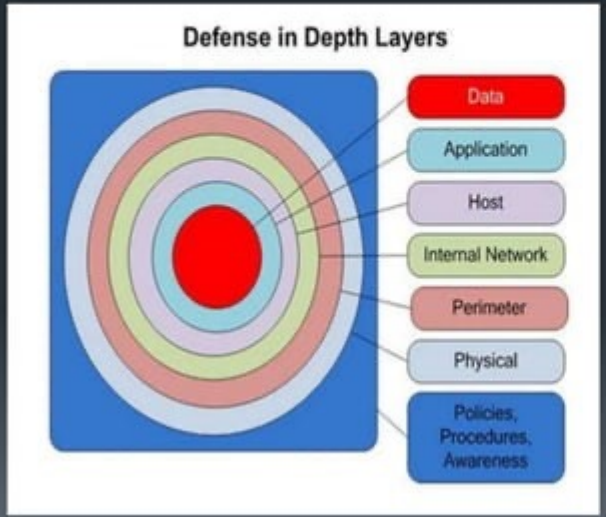
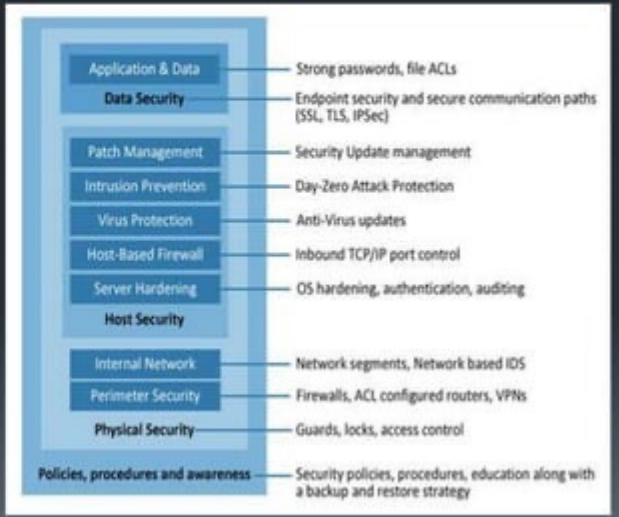
SECURITY INFORMATION & EVENT MANAGEMENT

Background on Network Components

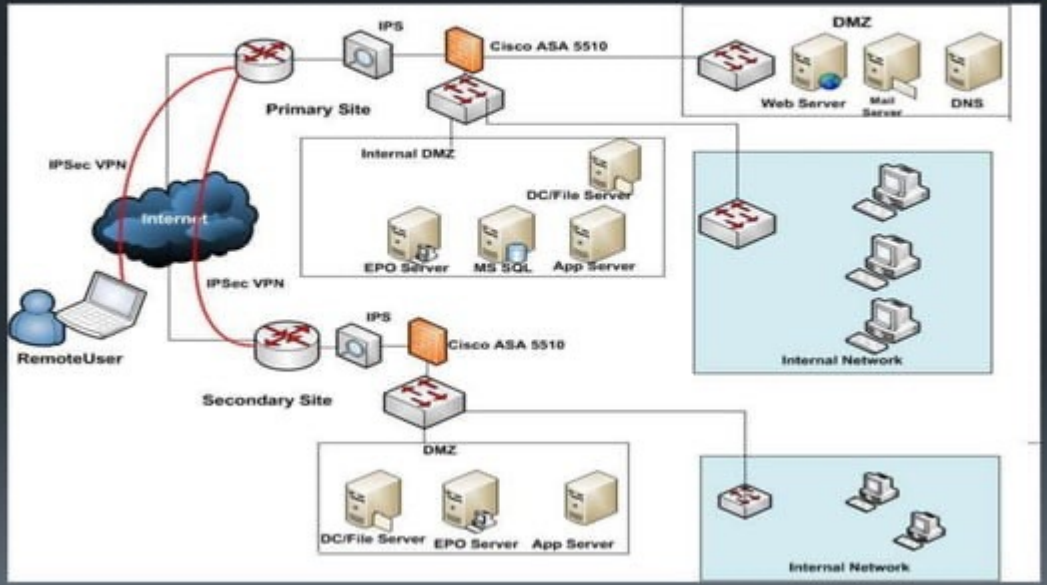
- Router
- IPS/IDS
- Firewall
- Switch (L2 & L3)
- Servers (Application, Database, etc.)
- Demilitarized Zone (DMZ)
- Virtual Private Network

Defense in Depth





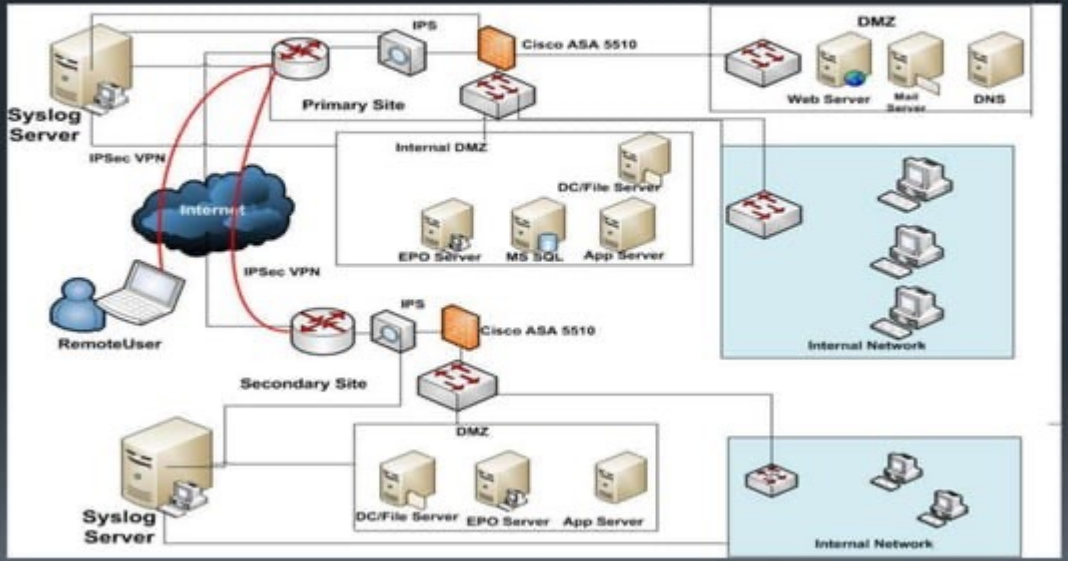
Typical Corporate Environment



Log Management

- Log management (LM) comprises an approach to dealing with large volumes of computer-generated log messages (also known as audit records, audit trails, event-logs, etc.).
- LM covers log collection, centralized aggregation, long-term retention, log analysis (in real-time and in bulk after storage) as well as log search and reporting.

Log Management



Log Management Challenges

- Analyzing Logs for Relevant Security Intelligence
- Centralizing Log Collection
- Meeting IT Compliance Requirements
- Conducting Effective Root Cause Analysis
- Making Log Data More Meaningful
- Tracking Suspicious User Behavior

Introduction to SIEM

- The term Security Information Event Management (SIEM), coined by Mark Nicolett and Amrit Williams of Gartner in 2005.
- Describes the product capabilities of gathering, analyzing and presenting information from network and security devices; identity and access management applications; vulnerability management and policy compliance tools; operating system, database and application logs; and external threat data.

Introduction to SIEM

- Security Information and Event Management (SIEM) is a term for software and products services combining security information management (SIM) and security event manager (SEM).
- The acronyms SEM, SIM and SIEM have been sometimes used interchangeably.
- The segment of security management that deals with real-time monitoring, correlation of events, notifications and console views is commonly known as Security Event Management (SEM).
- The second area provides long-term storage, analysis and reporting of log data and is known as Security Information Management (SIM).

Key Objectives

- Identify threats and possible breaches
- Collect audit logs for security and compliance
- Conduct investigations and provide evidence

SIEM vs LM

Functionality	Security Information and Event Management (SIEM)	Log Management (LM)
Log collection	Collect security relevant logs + context data	Collect all logs
Log pre-processing	Parsing, normalization, categorization, enrichment	Indexing, parsing or none
Log retention	Retail parsed and normalized data	Retain raw log data
Reporting	Security focused reporting	Broad use reporting
Analysis	Correlation, threat scoring, event prioritization	Full text analysis, tagging
Alerting and notification	Advanced security focused reporting	Simple alerting on all logs
Other features	Incident management, analyst workflow, context analysis, etc.	High scalability of collection and storage

Why is SIEM Necessary?

- Rise in data breaches due to internal and external threats
- Attackers are smart and traditional security tools just don't suffice
- Mitigate sophisticated cyber-attacks
- Manage increasing volumes of logs from multiple sources
- Meet stringent compliance requirements

Elements of SIEM

- Monitored Events
- Event Collection
- Core Engine
- User Interface

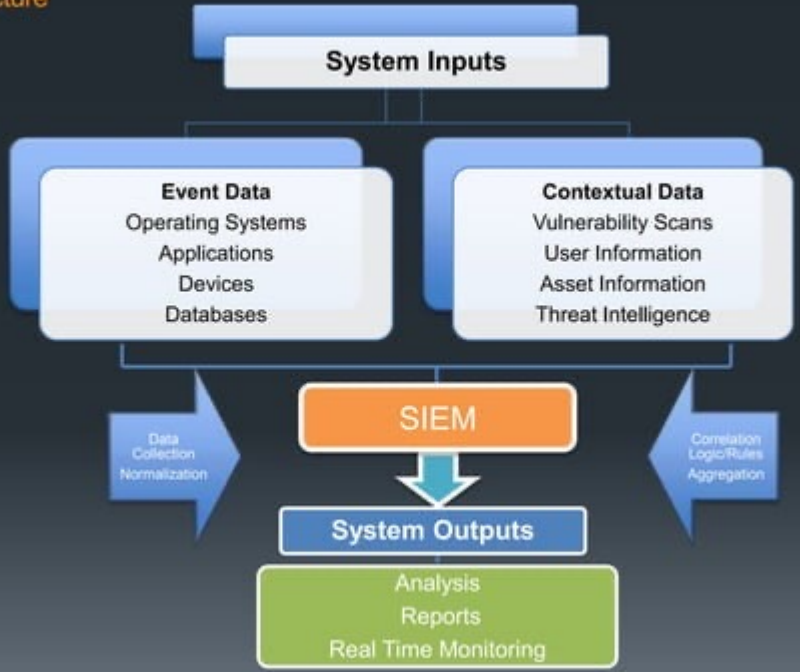
Typical Features of SIEM

BIG 3 for SIEM

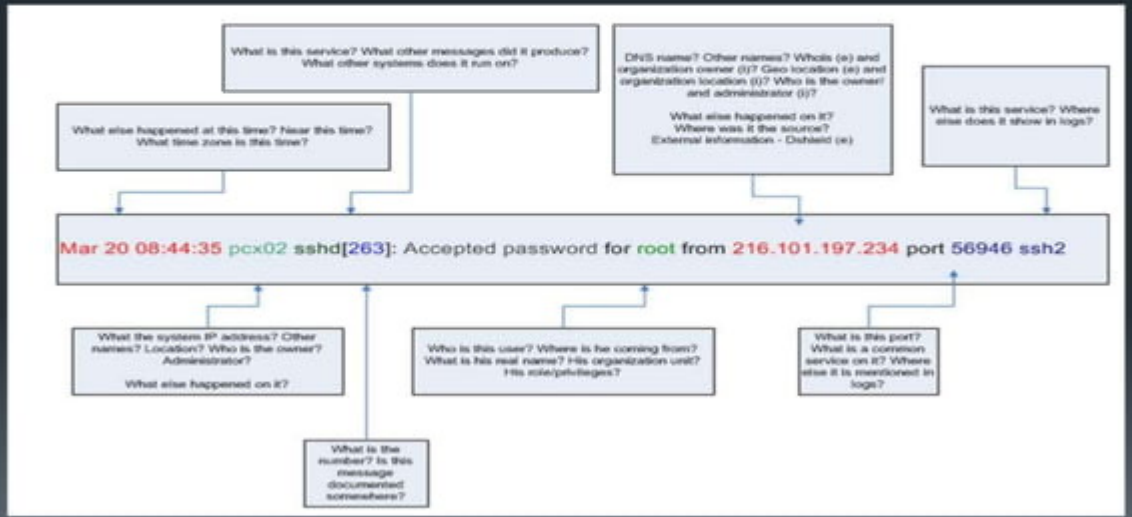
SIEM Process Flow

Typical Working of an SIEM Solution

SIEM Architecture



Context


What is this service? What other messages did it produce? What other systems does it run on?
What else happened at this time? Near this time? What time zone is this time?
DNS name? Other names? Whois (e) and organization owner (i)? Geo location (e) and organization location (i)? Who is the owner and administrator (i)?
What else happened on it? Where was it the source? External information - Dshield (e)
What is this service? Where else does it show in logs?
Mar 20 08:44:35 pcx02 sshd[263]: Accepted password for root from 216.101.197.234 port 56946 ssh2
What the system IP address? Other names? Location? Who is the owner? Administrator?
What else happened on it?
Who is this user? Where is he coming from? What is his real name? His organization unit? His role/privileges?
What is this port? What is a common service on it? Where else it is mentioned in logs?
What is the number? Is this message documented somewhere?

Adding Context

- Examples of context
  - Add geo-location information
  - Get information from DNS servers
  - Get User details (Full Name, Job Title & Description)
- Add context aids in identifying
  - Access from foreign locations
  - Suspect data transfer

8 Critical Features of SIEM

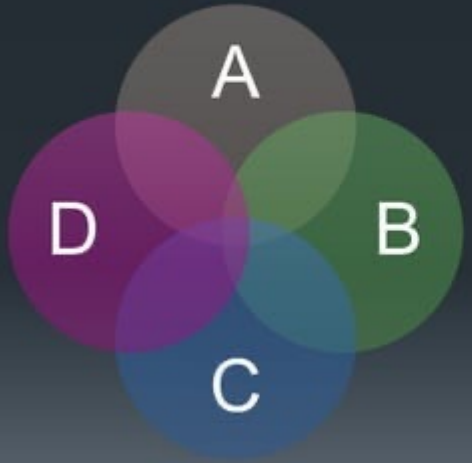
#1. Log Collection

- Universal Log Collection
  - To collect logs from heterogeneous sources (Windows systems, Unix/Linux systems, applications, databases, routers, switches, and other devices).
- Log collection method - agent-based or agentless
  - Both Recommended
- Centralized log collection
- Events Per Second (EPS) – Rate at which your IT infrastructure sends events
  - If not calculated properly the SIEM solution will start dropping events before they are stored in the database leading to incorrect reports, search results, alerts, and correlation.

#2. User Activity Monitoring

- SIEM solutions should have Out-of-the-box user activity monitoring, Privileged user monitoring and audit (PUMA) reporting feature.
- Ensure that the SIEM solution gives the **'Complete audit trail'**
  - Know which user performed the action, what was the result of the action, on what server it happened, and user workstation/device from where the action was triggered.

#3. Real Time Event Correlation



- Real-time event correlation is all about proactively dealing with threats.
- Correlation boosts network security by processing millions of events simultaneously to detect anomalous events on the network.
- Correlation can be based on log search, rules and alerts
  - Predefined rules and alerts are not sufficient. Custom rule and alert builder is a must for every SIEM solution.
  - Ensure that the process of correlating events is easy.

#4. Log Retention

- SIEM solutions should automatically archive all log data from systems, devices & applications to a **'centralized'** repository.
- Ensure that the SIEM solution has **'Tamper Proof'** feature which **'encrypts'** and **'time stamps'** them for compliance and forensics purposes.
- Ease of retrieving and analyzing archived log data.

#5. IT Compliance Reports

- IT compliance is the core of every SIEM solution.
- Ensure that the SIEM solution has out-of-the-box regulatory compliance reports such as PCI DSS, FISMA, GLBA, SOX, HIPAA, etc.
- SIEM solutions should also have the capability to customize and build new compliance reports to comply with future regulatory acts.

#6. File Integrity Monitoring

- File integrity monitoring helps security professionals in monitoring business critical files and folders.
- Ensure that the SIEM solution tracks and reports on all changes happening such as when files and folders are created, accessed, viewed, deleted, modified, renamed and much more.
- The SIEM solution should also send real-time alerts when unauthorized users access critical files and folders.

#7. Log Forensics

- SIEM solutions should allow users to track down a intruder or the event activity using log search capability.
- The log search capability should be very intuitive and user-friendly, allowing IT administrators to search through the raw log data quickly.

#8. Dashboards

- Dashboards drive SIEM solutions and help IT administrators take timely action and make the right decisions during network anomalies.
- Security data must be presented in a very intuitive and user-friendly manner.
- The dashboard must be fully customizable so that IT administrators can configure the security information they wish to see.

Deployment Options

Self-Hosted, Self-Managed

	Cl	Ag	Cr	Vz	Al	An	Rp	Re
In-house	■	■	■	■	■	■	■	■
MSSP								

Self-Hosted, MSSP-Managed

	Cl	Ag	Cr	Vz	Al	An	Rp	Re
In-house	■							
MSSP		■	■	■	■	■	■	■

Self-Hosted, Jointly-Managed

	Cl	Ag	Cr	Vz	Al	An	Rp	Re
In-house	■	■	■	■	■	■	■	■
MSSP		■	■	■	■	■	■	■

Cloud, MSSP-Managed

	Cl	Ag	Cr	Vz	Al	An	Rp	Re
In-house								
MSSP	■	■	■	■	■	■	■	■

Cloud, Jointly-Managed

	Cl	Ag	Cr	Vz	Al	An	Rp	Re
In-house				■	■	■	■	■
MSSP	■	■	■	■	■	■	■	■

Cloud, Self-Managed

	Cl	Ag	Cr	Vz	Al	An	Rp	Re
In-house			■	■	■	■	■	■
MSSP	■	■						

Hybrid-Model, Jointly-Managed

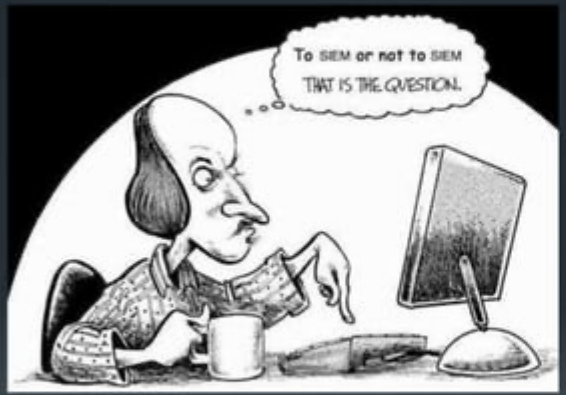
	Cl	Ag	Cr	Vz	Al	An	Rp	Re
In-house	■	■	■	■	■	■	■	■
MSSP	■	■	■	■	■	■	■	■

Why SIEM implementation fails?

- Lack of Planning
  - No defined scope
- Faulty Deployment Strategies
  - Incoherent log management data collection
  - High volume of irrelevant data can overload the system
- Operational
  - Lack of management oversight
  - Assume plug and play

"Security is a process, not a product"

Business Benefits



- Real-time Monitoring
  - For operational efficiency and IT security purposes
- Cost Saving
- Compliance
- Reporting
- Rapid ROI

Q & A

THANK YOU