

Are you Ready for SIM?

Agenda

- SIM Introduction
- Define Requirements
- Vendor Selection
- Deployment Preparations
- Ongoing Administration
- Understanding SIM ROI
- FOSS Approach
- Case Studies

Value of Central Information

- “Net Video Tape” - What happened and When
- Regulatory Compliance
- IG (Auditor) Requirement
- Support Your SOC or Daily Security Analysis
- Facilitates Incident Response
- Builds Inter-Group Relationships
- Improve Security Posture

Product Space

- Log Management vs. SIM
- SIM, SEM, SIEM, oh my
- SIM Mindset
- SIM Space Is Still Evolving

3 Types

- i. Log Management with some reporting
 - Splunk, Network Intelligence (Now RSA)
- ii. Type 1 + Correlation and Better Reporting
 - Tenable, Q-Labs, LogLogic
- iii. Type 2 + Advanced Correlation – Full Blown SIM (aka Traditional SIM, aka PITA)
 - ArcSight, NetForensics, Intellitactcs

Key Terms

- Many SIM-Specific Terms
- Product Pricing is Term-Critical
- Examples:
 - EPS – Events Per Second
 - Distinct Device Types
 - Event Generators
 - Event (Collection|Normalization|Classification|Aggregation|Correlation)

Define Requirements

- SIM Type
- Reporting Devices
- User Planning/Access
- Hardware Considerations
- Administration Overhead
- Trending
- Disaster Recovery

SIM Type

- Which of the 3 Types?
- Consider Users, Load, and Event Generators

Reporting Devices

- Which Devices
 - All Security-Related Devices
 - All Business-Critical Devices
 - Consider All Publicly-Available Systems
 - Whatever You Can Afford
 - Physical/Logical Separation of Networks
 - Regional or Device-Type Collector
- Will Agents Be Required

Network Map

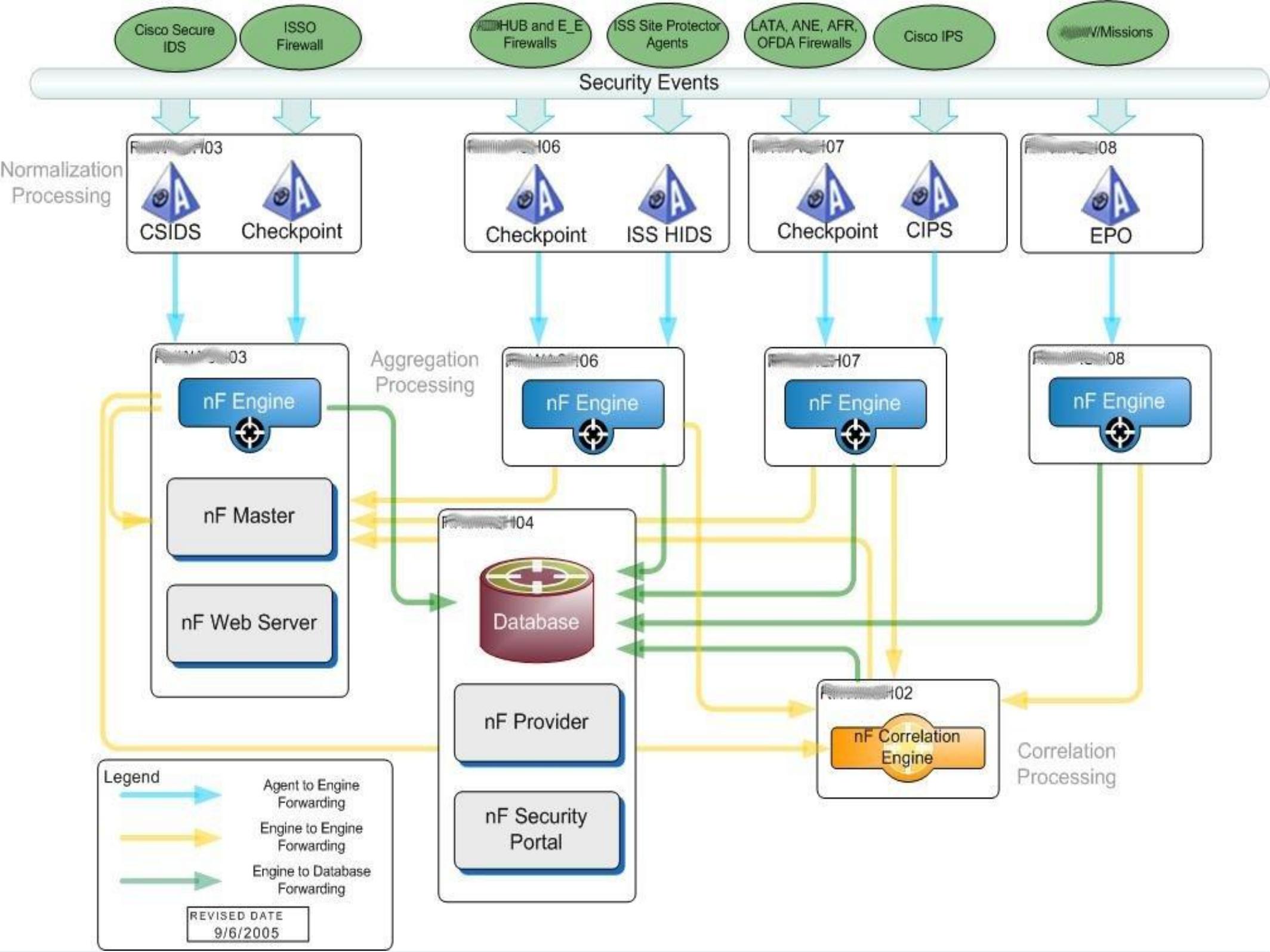
- Physical/Logical Separation of Networks
- Some SIMs Accommodate Regional Collectors
- Group Systems By Type or Region

Users

- User Planning
 - User/Role Permissions
 - Technical Vs Decision Maker
 - Security Implication of Providing Access
- User Access
 - Java and Web Clients Are Big In This Market
 - Will the Client Pass Your Software Requirements?
 - Consider Server Resources (i.e. Proc/Query)
 - Java Java Java Java Java

Hardware

- Prepare for Several/Many Systems
- Most Benefit From High CPU/Memory
- Databases Require High Reliability
- Expect to Deploy a SAN or Storage Array



Appliance Vs Installable Software

- Appliance is Easier, But at What Cost?
- What is the Analytic Requirement?
- What is the Expected Load/Event Counts?
- Price
- Extensibility

Admin Overhead

- Dedicated Admin is Recommended
- For Type3 - You Might Want to Buy Them a Headset For The Long Support Calls
- Type2/3 - Professional Services are Usually an Unfortunate Necessity
- Custom Solutions (Both Customer and Vendor)
- Most SIMs are Unix/Linux-Based

Trending

- Review Trends From Collected Devices
- Long Term Trends (Years)
- Must Collect Metadata From Stored Logs
 - Almost no SIM Vendor Does This
- Most SIMs Display Trends Only On Currently-
Stored Logs

Disaster Recovery

- Defer to Management Direction
 - Full System
 - Configs
 - Data (Raw, Parsed, Summaries, etc.)
- Vendor Will Provide Method to Backup/Restore Their Application

Vendor Selection

- Market Survey
- Reputation (Gartner and Others)
- Not Apples-to-Apples
- Get Vendor-Referrals
- Demo, demo, demo
 - One Product Failed During Demo
 - Another Should Have

Deployment Preparations

- NTP – Network Time Protocol
- Considerable Administrative Overhead
- Vendor's Preparation Guides
- Pre-Configure What You Can
- Things Will Go Wrong, Expect This
- Contract

NTP

- Network Wide NTP (Deploy And Force Usage)
- Without Central Time SIM Provides Little Value

Vendor's Preparation Guides

- Steep Learning Curve for SIM
- Additional Learning Curve for Each Vendor
- This Will Not be a Seamless Implementation
 - Should it Be?

Pre-configure What You Can

- Build Your Systems (Install, Patch, Harden)
- Prep The SAN, HBAs, LUNs
- Get Device Connection Info Ready (e.g. DB Accts, FW Info, etc.)
- Preparation Will Save You Professional Services Dollars

Things will go wrong, expect this

- A Good Vendor Will Overcome the Hurdles
- These Have Happened During Install
 - Reinstall during install
 - Dozens of OOM (Out of Memory) Crashes the First Week
 - Millions of Events Lost in First Few Days

Deployment Preparations - Contract

- What determines a successful install?
- How Is This Measured?
- What Do You Do If There Are Problems?
- Deployment Agreement/Statement of Work
- Ensure the SOW Meets Your Requirements

SIM Administration 101

- Backups
- Monitoring
- Configuration Management
- Device Support
- Maintenance
 - Patching, Signature Updates, Etc.
 - Full-Time Admin In Some Organizations
 - Database Pruning/Purging

Backups

- Implement Backup Plan
- Vendor Will Provide Backup Procedure
- Consider Impact of Backups on SIM DB

Monitoring

- SIM Systems (resources, network, etc.)
- SIM Processes (db, correlation, web, etc.)
- Reporting-devices
 - Which Devices Are Really Reporting In?
- Number of Incoming Events
 - GREAT Trending Data...When It Is There

Configs

- Many initial configurations
- Change Management Policy Model
- SIMS Require a lot of Tweaking

Alternatives To A Commercial SIM

- MSP (Managed Service Provider)
 - Have Experts Do It (Questionable??)
 - Security Concerns
 - IT Staff Can Lose Motivation and Abilities
- Roll Your Own
 - Central Syslog (More on FOSS In a Few Slides)
 - Open Source SIM - <http://ossim.org>
 - Prelude IDS <http://prelude-ids.org>

One Possible Approach

- Determine Devices
- Build syslog-ng Host
- One (or more) of these Three:
 - Type1 SIM
 - Type2 SIM
 - FOSS Analytic Farm

Determine Devices

- Determine Type and Quantity of Devices
- Many Devices Log as Syslog
- Some Devices Log Special
 - Determine if this is the Case
 - Find a Solution (e.g. Checkpoint's Opsec Lea Encrypted Log Has Several Free Alternatives)
 - Don't forget to Sync Time!!!!

Build Central Log-Host

- Log-Host Will Help: Inventory Devices and Data, Validate Data, Repository of Raw Data
- Install Pre-Fork Syslog-ng on Linux
- Plan For Storage/Space
- Is HA Necessary?
- Sync Logs Or Collect Syslog
- Rsync Log Files From Remote NIX Systems

Deploy Type1 SIM or

- Go Through Steps Outlined In this Presentation
- Market Survey/Demo Candidates
- Retransmit Your Syslog Feed to SIM
 - This Step Typically Shortens Initial Install Time
- Consider Using Splunk (Free/Easy Trial)
- Pros: Easy, Fast, Cheaper Than Type2, Frequently Appliances, Relative-Low Overhead
- Cons: Not Flexible, Little to No Correlation, Few Reports/Graphs/Trends, No Open DB?

Deploy Type2 SIM

- Go Through Steps Outlined In this Presentation
- Market Survey/Demo Candidates
- Retransmit Your Syslog Feed to SIM
 - This Step Typically Shortens Initial Install Time
- SIM Will Also Allow For
 - Anti-Virus Data
 - Vulnerability Assessment Data
- Con'td -->

Deploy Type2 SIM Cont'd or

- Validate SIM By Comparing Syslog Data
- Spend Next Few Months Configuring
- Pros: Vendor Provides Integration, Correlation, Aggregation, Trending, Good Data per Dollar with relative little time investment
- Cons: Little Flexibility, No Open DB?

Deploy Analytic Farm

- Configure One or More Systems Dedicated to Analytics With a Mount Point to Syslog-data
- Install FOSS Utilities Specially Made to Churn Through Collected Data
- Determine Trends and Values To Monitor
- Install FOSS Graphing Utilities
- Pros: Low Cost, Flexible, Raw Data Access
- Cons: All Manual, Self-Service Device Integration, Can Be Very Complicated

What About Windows Logs

- Windows Logs Can Be Very Valuable
- Most Granular Auditing of **Any OS**
- Windows Logs Are Notoriously Hard To Collect
- DAD – Distributed Analyst Database
 - FOSS WAMP Based – Search for “DAD” on SF
 - Agentless by Using RPC DCOM; Collects, Aggregates and Reports on Windows LOGS
 - Can Retransmit as Syslog Feed to SIM
- Many SIMs Will Collect Windows Logs

“Where Is My ROI?” OR “Getting The Most Out Of Your SIM”

- Daily Usage Quickly Reveals Problems
- Can Help Determine Network and System Fault
- Track Infection Spread (e.g. Worm Spread)
- Discover Internal attackers
- Trends in Attacks and Service Usage
- Improve Security Posture

Case Study – 6 Months and No SIM

- Gov't Agency Deployed Type3 SIM in 2003
 - Good at the Time, but Became Outdated
- Nov. 2006 Market Survey For new Type3 SIM
- Considered 6 Products Demoed Several
- Ultimately Chose A Recently-Redesigned SIM
- Merrily Deployed New SIM in Jan 2007
- 5 Months of Chaos and Failure
- May 2007 Gave Ultimatum To Vendor

Installation Timeline 5.6

May

5/29 - Begin 5.6 Install; applied hotfix1 and hotfix2

5/31 - Rebuild

June

6/1 - Installed hotfix3; logic bug in reports impacting performance; FW events hung; no EPO data

6/2 - Reports won't Run and other Problems occur

6/4 - ~~Issue~~ realizes critical problem; we have many crashes

6/7 - ~~Issue~~ onsite to fix DB corruption; reinstalled ~~Issue~~; purged all events

6/8 - Provided fix for mysql (which caused previous crashes)

6/11 - Report OOM crashes; provided memory adj fix

6/13 - Most probs worked out; need to cleanup data and re-import fresh data

6/18 - We report another crash

6/19 - No response from ~~Issue~~ on crash; finally provided cleanup script

6/20 - We run cleanup script

6/21 - Onsite; fix problems caused by cleanup script

6/27 - More failures reported

6/28 - ~~Issue~~ onsite to fix problems; applied hotfix 4; fixes broke ISS collection

6/29 - Fix for ISS; didn't work

July

7/3 - Provided fix for the ISS fix

7/9 - System queuing events; more failures

7/10 - We report rapidly growing mysql.log; support says testing config mistake; check all tiers and comment out log line

7/11 - More problems; ~~Issue~~ says problems caused by disk space issue (caused by their "testing" version of mysql config)

7/12 - Things are a mess; still queued up; still seeing errors; all stop



Installation Timeline 5.6

May

Rebuild
Onsite

5/29 - Begin 5.6 Install; applied hotfix1 and hotfix2

5/31 - Rebuild

Rebuild
Onsite

June

Onsite

6/1 - Installed hotfix3; logic bug in reports impacting ~~SQL~~ performance; FW events hung; no EPO data

6/2 - Reports won't Run and other Problems occur

6/4 - ~~Team~~ realizes critical problem; we have many crashes

6/7 - ~~Team~~ onsite to fix DB corruption; reinstalled ~~SQL~~; purged all events

Rebuild
Onsite

6/8 - Provided fix for mys ql (which caused previous crashes)

6/11 - Report OOM crashes; provided memory adj fix

6/13 - Most probs worked out; need to cleanup data and re-import fresh data

6/18 - We report another crash

6/19 - No response from ~~Team~~ on crash; finally provided cleanup script

6/20 - We run cleanup script

Onsite

6/21 - Onsite; fix problems caused by cleanup script

6/27 - More failures reported

Onsite

6/28 - ~~Team~~ onsite to fix problems; applied hotfix 4; fixes broke ISS collection

6/29 - Fix for ISS; didn't work

July

7/3 - Provided fix for the ISS fix

7/9 - System queuing events; more failures

7/10 - We report rapidly growing mys ql.log; support says testing config mistake; check all tiers and comment out log line

7/11 - More problems; ~~Team~~ says problems caused by disk space issue (caused by their "testing" version of mys ql config)

7/12 - Things are a mess; still queued up; still seeing errors; all stop



Trends?

- SIM Type 1 & 2 Space Steadily Growing
- SIM Type 3 Space Shrinking
- Well-developed Security Teams Ditching SIMs
- Analysts Turning Toward Extrusion Detection
- Flow Analysis an Increasing Player
- Regulatory/Auditors Require Central Log Mgmt

Closing

- A SIM Is Not Just Software, But A Change In Your Information Security Strategy
- Great Network, System, and Time Overhead
- Garbage In Is Garbage Out, Not Auto-Secure
- SIM Can Be A Considerable Asset To A Well-Honed Information Security Program
- A SIM, no matter what the cost, DOES NOT replace the Skills of a Good Analyst

Resources

- Gartner Report Security Information and Event Management Solutions June 2006
- Review: Security Information Management Products
<http://www.networkcomputing.com/article/printFullArticle.jhtml?articleId>
- Market Analysis: Security Information Management
<http://www.networkcomputing.com/article/printFullArticle.jhtml?articleId>
- Too Much Information
<http://www.networkcomputing.com/article/printFullArticle.jhtml?articleId>