



Some Perspective for Conversation

- 20+ years in game, CISA/ISO27001 Lead Auditor
- Certified by eSecurity in April 2002 after evaluations of leading vendors (NWI, Net Forensics, ArcSight)
- Full Scale SIEM Implementations in Multiple Media, Pharmaceutical, Banking, Telecomm, Cable, & MSSP
- Developed and have continuously operated a Custom SIEM application for one of the worlds largest carrier class networks (to 1Billion events/day)
 - ~ 12 customers currently under Managed SIEM Services contracts
 - Ongoing research initiative in Anomalous Behavior Detection via Security Event analysis

SIEM Early Adopter Woes

- Many Early Projects (pre-2006) have been abandoned resulting in an early “black eye”
 - Immature technology
 - Over hyped and under-delivered
 - Failure to understand commitment from both a vendor/customer perspective
 - Many early adopters are still gun-shy - “Arrows in the Back”

SIEM is Rapidly Evolving

- SIEM has significantly changed for the better the last few years
 - Acquisition of products by established companies has resulted in:
 - > Greater Product Maturity
 - » Stability
 - > Significant Enhancements
 - » Taxonomy
 - » “Agent” Management
 - » Compliance “packages”
 - > Enhanced Services/Support
 - » Channel Partners
 - » 24/7/365 Support Systems
 - Security focus -> Compliance Focus
 - > Demonstrable value for PCI, Sarbox, HIPAA, 27001, etc.



Current SIEM Projects Achieving Success

- SIEM rapidly becoming a mainstream technology
- SIEM success rate much higher post 2006
 - However many still fail to *fully* achieve objectives
 - > In line or better than statistics relating to major IT initiatives (*~16% projects deemed fully successful – Standish group*)
 - > Most current era projects are operational and providing value
 - > Greatest single contributor to improved “success” rates are improved “SIEM practices”

Five Keys to Success

- **Define your Requirements** (*“Log consolidation” is not a requirement*)
- **Align Systems Architecture with Requirements**
(*Communication, Environment Integration, Performance*)
- **Align Database Architecture with Requirements** (*Indexes, Partitions, Storage Architecture*)
- **Commit the Resources Required** (*Device Upgrades, Network Architecture Changes, Evolving Laws/Regulation, Database Administration, Forensic Investigation drive change*)
- **Tightly Scoped Phased Implementation Approach** (*Seek quick wins and minimize early risk*)



Invest Heavily in Requirements Definition

- **Single Most Critical Phase**

- Forms the basis for all future project phases
 - > Not as obvious as it may initially seem
 - » Act four years old – Why? - Why? - Why?
 - > Begin with the end in mind
 - » What audit evidence (e.g., reports) do you need ? (defines systems, event types, event content, data normalization, temporal resolution, incident response, retention requirements, evidentiary requirements, etc.)
 - » Specificity correlates with success
 - > Insufficient Requirements Definition is the root cause of virtually every project failure
- EPS is a critical parameter (*How do I know what I don't know?*)
 - > System/Database Architecture is fully reliant on EPS
 - » Correlation Temporal Resolution
 - » Indexing & Reporting
 - » Factor in growth and 40%+ jump during a security incident
- Bail on the Project if you end up with “half-baked” requirements

Systems Architecture

- Requirements Drive System Architecture - Gotcha's include:
 - Communication Architecture should not be an afterthought
 - > Ensure implications of communications choices are fully understood and aligned with (e.g., syslog, ODBC)
 - Correlation is resource consumptive
 - > Minimize EPS through correlation engine
 - » Eliminate non-essential sources (e.g., Proxy logs)
 - » Eliminate event types (e.g., FW accepts) that are not essential
 - SIEM needs to be “operationalized”
 - > Monitoring of critical system components/processes
 - > Integration with supporting systems/workflows (e.g., trouble ticketing, NMS)
 - > SIEM's need to comply with control environment (e.g., DR, Segregation of Duty)
 - > SIEM's often need their own Policies/Standards/Procedures (What now?)

Database Architecture

- Many people often fail to understand that a SIEM is ultimately a large, relatively complex database
- SIEM Database requirements are very unique
 - Near continuous extremely high inbound TPM with simultaneous queries of same data drive unique considerations:
 - > Indexing – Query performance versus insertion rate & data expansion
 - > Partitioning – Improved Insertion Rates versus slower query performance
 - > “Data Segregation” – Striping data across as many spindles as possible for improved insertion performance and improved query performance (e.g., re-do logs, indexes, raw data, and temporary space to separate spindles)

Resource Commitment

- SIEM's need to evolve with your environment to stay valuable/viable
 - Software updates for devices you are monitoring
 - Changes in Policies, Laws, Regulations
 - Network Changes
- Real World Support Example (18 Month Run-Rate Analysis)
 - 12 Days per Month to run/operate SIEM (400M EPD)
 - > Database Administration (15%)
 - > System Administration (10%)
 - > Special Investigations (15%)
 - > Report Creation & Modification (30%)
 - > Agent Development (15%)
 - > Change Support (15%)



Phased & Focused Project Approach



- Start Small, Grow Big
 - Full Success cycle on a per objective/data source basis
 - > Collector -> Data Source Analysis -> Data Normalization -> Taxonomization -> Correlation -> Workflows -> Reporting
 - Then iterate to the next objective/data source
 - > Too many projects get lost in a “log consolidation” phase
 - Quick Wins create positive momentum and gain political support
 - Lessons learned enhance future phases