



Experiences from the field and lessons learned. Best Practices in SIEM correlations

Fabian Libeau

© 2009 ArcSight, Inc. All rights reserved.
ArcSight and the ArcSight logo are trademarks of ArcSight, Inc. All other product and company names may be trademarks or registered trademarks of their respective owners.



Three Elements Critical for Success

People



Process



Technology

 ArcSight ESM



 ArcSight NSP



 ArcSight Logger



What is Success?

- Customer: “Make it easier to get more of my job done”

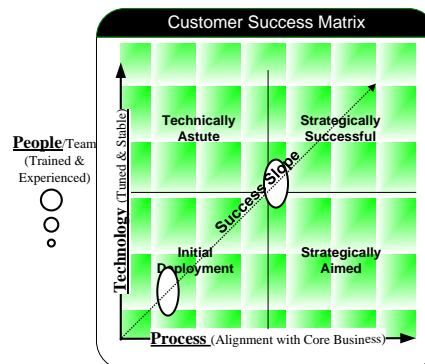
Demonstrate Meaningful Productivity

- What is the mission? How do we get it done?
 - Focus...Process (use cases)
- Who is responsible? Do they have what they need?
 - People (training & experience)
- Can they get it done effectively and efficiently?
 - Technology (tuned & stable)

3

Success: People, Process and Technology

- Enterprise Project**
 - People (size ‘o’)
 - Trained & Experienced
 - Process (x-axis)
 - Focus on Meaningful Business Objectives (use-cases)
 - Technology (y-axis)
 - Tuned and Stable
- Interactions are focused to result in “Strategic Success”**
 - Balanced enterprise approach



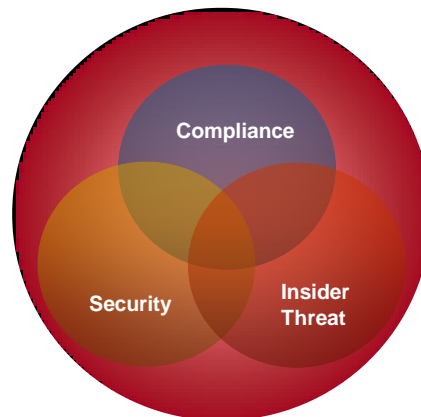
4

SIEM requires a strategy

- Simply installing a SIEM does not inherently “solve” any problem
- SIEM will help automate and improve YOUR security, compliance and incident response program
- SIEM + Strategy + Development = Solution
- An organization must maintain SIEM content (resource planning)
- You will not get what you want unless you know what you want

Define the Use Case

- Regulatory compliance
- Insider threat
- Audit and compliance capabilities
- Other use cases
 - Perimeter security
 - Availability
 - Worm outbreaks





Use Case Overview

Compliance	Identify non-compliant machines and network activities based on corporate or regulatory policy rules	
	Regulatory Compliance	Demonstrate compliance and/or due diligence with respect to federal regulations (SOX, HIPAA, GLB, etc.) Account management, Configuration Management, Authentication, Vulnerability Management
	Corporate Policy Compliance	Identify and respond to organizational policy violations. Web Policies of explicit material, use of clear text protocols, or Access policies.
Security	Risk management of threats and exposed vulnerabilities. Identify and respond to attacks against the organization's information systems from external threats. This includes monitoring for worms, viruses, denial-of-service, and other similar attack vectors.	
	Outbreaks	Compute activity trends and raise alarms for potential outbreaks (e.g., from worms)
	Intrusions	Isolate actual breaches while recording and suppressing false positives
	Suspicious	Monitor and record potentially malicious activity and raise alarms on thresholds
	2. Denial of Service	Identify networks being subjected to potential denial of service attacks
Insider Threat	Identify and respond to attacks against the organization's information systems from internal threats. The focus is to identify activities that could result in theft of intellectual property and/or intelligence.	
	Data Leakage	Track and reconstruct insider activities and identify exceptions
	Early Warning	Track @Risk User Activity with early warning indicators
	Sabotage	Track Denials of Service by Insider Activity



Non-Security Centric Use Cases

Network Operations	Monitor the health of core network infrastructure	
	Availability	Monitor critical status and raise alarms for network outages (business continuity) and Security Device outages
	Utilization	Monitor device vital signs and raise alarms for potentially critical conditions. CPU, Disk utilization of critical systems.
Workflow and RESPONSE	Closed Loop Management of Incidents and Response	



Compliance: Regulatory

Secondary Use Case	Specific Requirement	SIEM Content
Authentication Monitoring	Review Weekly, all Authentications against SOX Regulated Systems	Scheduled Weekly Report
Anti-Virus Signature Compliance	High-level report that shows my Signature compliance on my PCI Regulated Systems.	Scheduled Report
	Alert when Anti-Virus software is disabled and flag system as Out of compliance.	Rule, Notification, Data Monitor
Potential Virus Outbreak Uncontained	Alert when there is an unquarantined spread of virus activity across multiple systems in 5 minutes	Rule, Notification
Configuration Management	Reports that monitor for changes in infrastructure.	Scheduled Weekly Report
Account Management	Reports that monitor for changes in accounts.	Scheduled Weekly Report
Vulnerability Management	Alert when new vulnerabilities are found on PCI Regulated System	Rule, Notification

Device Coverage:

- Firewall
- Router
- Operating System
- Application
- Database
- Mainframe
- Policy Management
- Anti Virus
- NIDS, NIPS
- HIDS, HIPS



Compliance: Corporate Policy

Secondary Use Case	Specific Requirement	SIEM Content
Protocol/Weak Service Policy	Alert each time a clear text protocol (unencrypted) is used on the DMZ.	Rule, Report
Internet Usage Policy	Generate a weekly report of all systems that attempted to use a peer to peer application.	Schedule Report
	Alert when Instant Messaging (AOL, MSN, and Yahoo) occurs. Weekly Review of violators	Rule, Report
Security Policies	Alert when root directly logs onto a system not using trusted golden host	Rule

Device Coverage:

- Firewall
- Router
- Operating System
- Application
- Database
- Mainframe
- NIDS, NIPS
- HIDS, HIPS



Security: Intrusions

Secondary Use Case	Specific Requirement	SIEM Content
Perimeter Monitoring	Alert when there are attacks against multiple Internet gateways from the same source IP.	Rule, Notification
	Alert and manage incident each time a DMZ system is compromised using a buffer overflow exploit.	Rule, Notification, Case
	Alert when reconnaissance activity is detected from DMZ.	Rule
Authentication Monitoring	Alert when there is a successful authentication after brute force attempt.	Rule

Device Coverage:

- AV
- Firewall
- NIDS/ HIDS
- Authentication
- VPN
- OS
- DAM
- WAF



Security: Outbreaks - Virus/Worm/Malware Activity

Secondary Use Case	Specific Requirement	SIEM Content
Worm Monitoring	Alert on a worm outbreak within 30 minutes of the onset	Rule, Notification
	Alert and Track on each new virus that is identified in the environment.	Rule, Notification, Case, Active List
	Generate a report all systems infected with a new virus on a weekly basis	Report
	Alert when there is 200% spike in activity against a particular port.	Statistical Datamonitor, Rule

Device Coverage:

- AntiVirus
- Network-based Intrusion Detection and
- Intrusion Prevention Systems
- Network Monitoring Policy Management



Security: Anomaly Detection

Secondary Use Case	Specific Requirement	SIEM Content
Baseline "Normal" Activity	Review baseline known patterns in the environment and alert on newly discovered patterns.	Pattern Discovery, Rule, Event Graph
Activity Monitoring	Alert when a known pattern reoccurs	Pattern Discovery, Rule
Forensic Analysis	When a critical alert occurs, Investigators need to analyze history for anomalies.	Interactive Discovery

Device Coverage:
Any



Insider Threat: Early Warning Indicators

Secondary Use Case	Specific Requirement	SIEM Content
EW Activity	Alert when scans or other activity from @risk users such as former employees, contractors, disgruntled employees	Rule, Notification, Active Lists
	Review user activity targeting known job websites.	Reports, Active Lists
	Alert when audit logs have been cleared on a High-Value Target.	Rule



Insider Threat: Information Leak

Secondary Use Case	Specific Requirement	SIEM Content
Emails to Competition	Monitor for emails being sent from Internal to known competition	Rule, Notification, Active Lists, Reports
Large Transfers to External Sites	Display the top 10 systems based on bytes transferred the last 2 hours.	Dashboard, Datamonitor, Rule
Removable Media on High Value Target	Alert each time a removable media device is used between the hours of 6pm and 6 am and add account to suspicious list.	Rule, Active List



Insider Threat: Sabotage

Secondary Use Case	Specific Requirement	SIEM Content
Denial-of-Service	Alert when there more than 20 unique account lockouts in a 5 minute window.	Rule, Notification, Active Lists, Reports

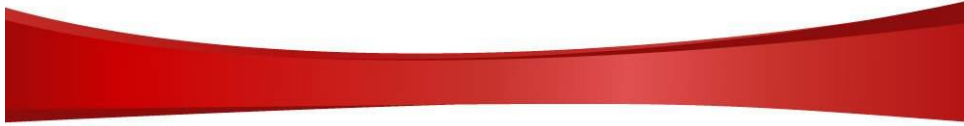
Network Operations: Utilization/Disruptions/Availability

Secondary Use Case	Specific Requirement	SIEM Content
ArcSight Monitoring	Alert when there a drop or stop in data feeds from a monitored security device or Agent.	Rule, Datamonitor, Notification
Firewall Utilization	Alert when processor utilization is greater than %50 for a period of 2 hours and Display System Critical.	Rule, Dashboard
Network Monitoring	Alert when a router Interface indicates down.	Rule, Notification, Dashboard
Critical System Monitoring	Alert and report on critical systems that have reboot	Rule, Report, Activelist

Device Coverage:
Operating System,
IOS,
ArcSight Internal Events

Solution Process





ArcSight[™] 

The logo consists of the word "ArcSight" in a sans-serif font, with "Arc" in red and "Sight" in black. To the right of the text is a stylized logo symbol: a red arc on the left, a black vertical line in the middle, and a black diagonal line on the right that crosses the vertical line. A small "TM" trademark symbol is located at the bottom right of the logo symbol.