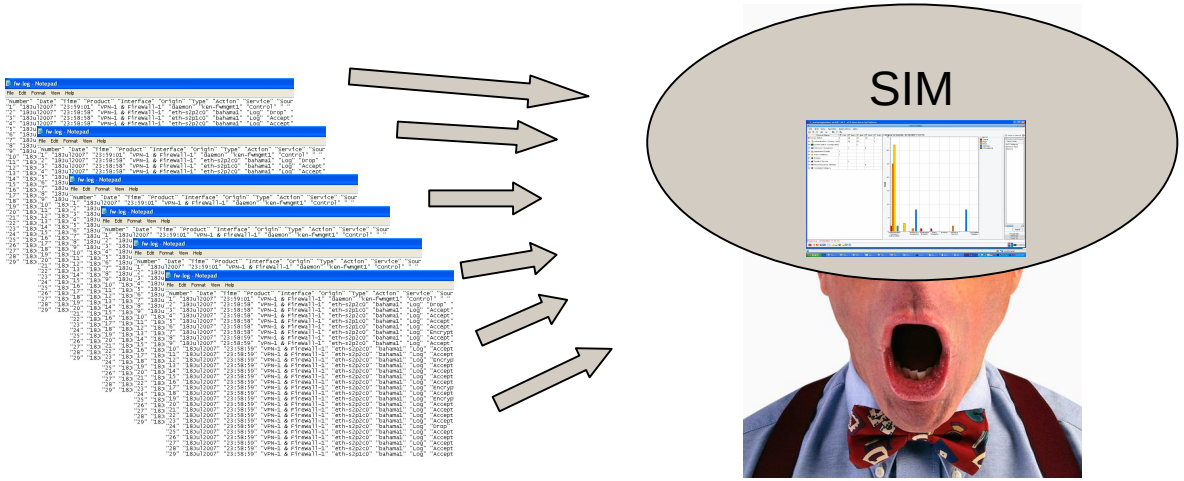
Sasan Hamidi

CISO, Interval International, Inc.



My Background

- CISO at Interval for six years
- Director of Infrastructure & Security – GE Power Systems
- Senior Security Project Mgr. – AT&T Global

- Senior Project Manager – IBM Global Network Security
- Area of interest: *Steganography, applications of Chaos, Complexity, Emergence in security*

- Developed in the late 90's
- Used to be "log and event aggregators"
- Started as simple Unix scripts
- String matching for "failed log-ins"
- Correlation & Intelligence major improvements
-

Why SIM?

- Normalization of logs (many systems with various formats)
- Centralized management of security events – helps build SOCs
- Real-time analysis
- Correlation and intelligence
- Improved forensics analysis of events
- Improved incident response handling
- Foundation for a SOC?

- What is the ultimate goal?
- Deployment Architecture
- Configuration (agents, consoles, etc.)
- Agent Coverage
- Event Filtering (false positives)
- Rules Writing
- Resource Intensive
- Must have patience of an elephant

Interval's Needs

- Public company; subject to:
  - SOX 302, 404
  - California SB1386
  - PCI DSS
  - And a slew of others
- Security Concerns
  - Impossible to review gigs of data manually
  -
  - Scripts are as good as the author
  - Human error
- Resource Issues

- Document & frame the issues
  -
  - Additional resources are needed for status quo
  - May miss important security events
- Build a solid ROI
  - Be unconventional
  - Use the product to justify the product

The ROI

- Be unconventional
  - A good ROI does not hypothesize
  - We used Six Sigma methodology to find out what's measurable
    - Define – what we want to improve?
    - Measure – existing system versus status quoe
    - Analyze – missing links
    - Improve – process, people, etc.
    - Control – policies, procedures

The ROI

- Used SIM pilot information to show
  - Size of information/data
  - Risks
  - Gaps
  - Process improvements
- Get people behind you
  - Talk to directors & administrators
  - Invite them to meetings with vendors

- Get technical (agent vs. agent-less)
- Know your products (leading vendors)
- Talk to your reseller (must represent more than just one vendor)
- Conduct phone interviews
- Be brief and to the point
- Short demos without the marketing junk
- Include training constraints (your site, their site, group v. single)

Pilot Phase

-
- No more than two products
  - SIMs are complex and time consuming
- Pick one flavor of each system/application
- Check support line
- Document issues (no emails, phone calls)
- Update SLAs as pilot progresses

Challenges

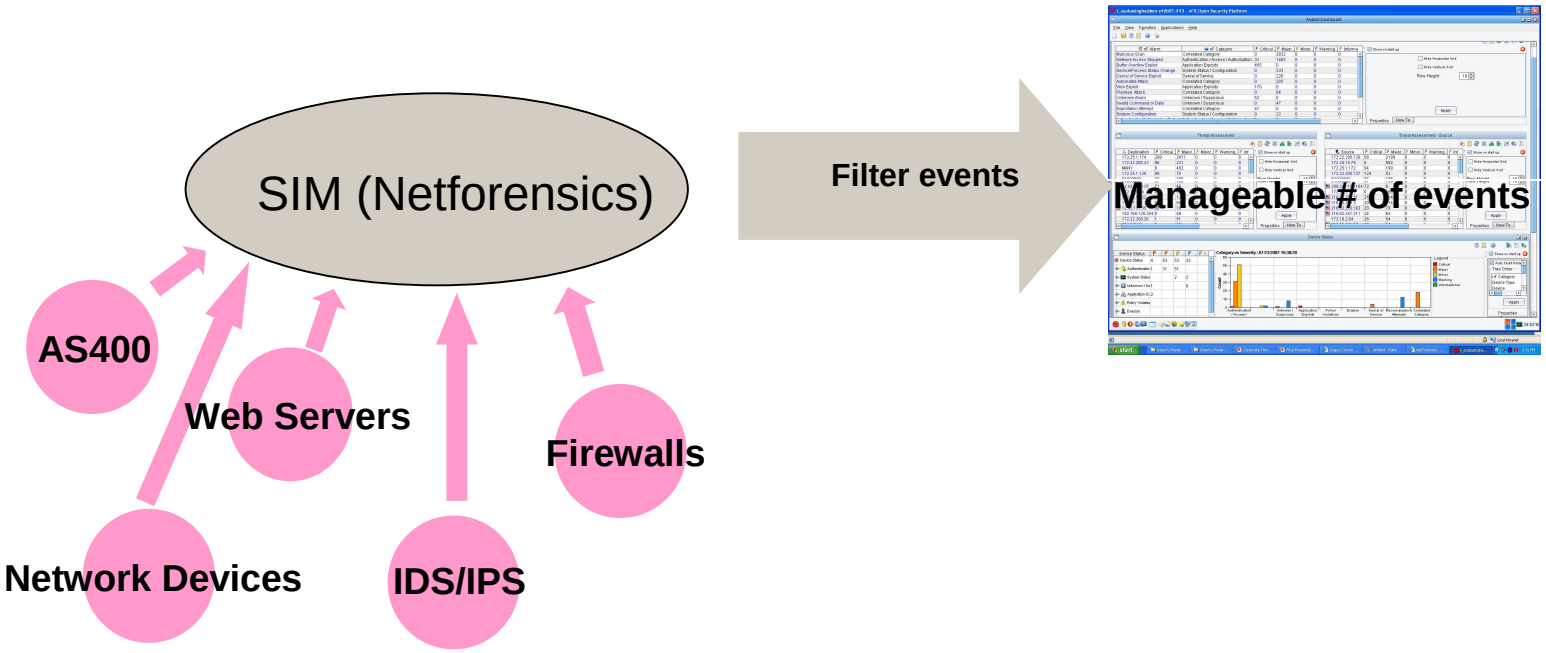
- Too many alerts in one place!
- Need dedicated resource
- Technically challenging
- Training takes too long
- Tweaking the system
  - Eliminating false positive
  - Finding false negatives
- Updating policies & procedures

Challenges

- Placing effective controls in place
  - How can you make sure devices are
- Measuring performance against ROI
  - Validating results for the boss
  - Validating results for IT
  - Convincing yourself that it was all worth it!

Managing SIMs

- Requires extensive training of personnel
- Requires constant filtering of events
- Must provide 24 x 7 support
- admins
- Master art of generating reports
  - Daily Information Security Report



He Who Masters the Filter will Master the SIM Universe!

Sasan Hamidi, battered veteran of a recent SIM deployment

- Perhaps the most challenging of all SIM activities
- Events can be complex and vague
- High degree of false positives
- Difficult to train personnel
- Rules can be even more challenging
- Very time consuming – requires dedicated resource
  - Interval used summer interns

Filtering Strategy

- Break down each device group
  -
  - Host-Based IDS (CSA)
  - Network-Based IDS (SourceFire)
  - Network Devices (Routers, switches)
  - Servers
    - Unix (Solaris, Linux)
    - Windows (2003)
  - Mainframe (AS400)

Windows Alarm Summary (MOM)

nF Alarm	nF Severity	Device Alarm Description	Process	Event Ct.	IS Action
Application Configuration	Warning (2)	Printer error	TermServDevices	112	DO NOT FILTER
Unknown Alarm	Critical (5)	NO DATA	MSExchangeIS Public Store	90	DO NOT FILTER
Unknown Alarm	Critical (5)	NO DATA	Exchange MOM	29	DO NOT FILTER
Unknown Alarm	Critical (5)	NO DATA	Service Control Manager	14	DO NOT FILTER
Suspicious Activity	Major (4)	File transfer response - Failed to transfer files	Microsoft Operations Manager	12	DO NOT FILTER
Unknown Alarm	Critical (5)	NO DATA	Userenv	11	DO NOT FILTER
Service/Process Status Change	Minor (3)	The service terminated unexpectedly.	Service Control Manager	5	DO NOT FILTER
Invalid Command or Data	Warning (2)	"Error 500: Internal Server Error"" - Alert"""	NO DATA	4	DO NOT FILTER
Exceed Threshold or Limit	Minor (3)	A script hung or exceeded its specified timeout	Microsoft Operations Manager	3	DO NOT FILTER
Unknown Alarm	Critical (5)	NO DATA	MSExchangeSA	3	DO NOT FILTER
System Failure	Minor (3)	Agent Install Failure - Push Install Failed	Microsoft Operations Manager	3	DO NOT FILTER

Netscreen Alarm Summary

nF Alarm	nF Severity	Device Alarm	Alarm Ct	Comment	Conclusion	Comments
Network Access Stopped	Informational (1)	traffic log - pckt dropped	61791	Default denary rule for all out bound traffic. Does not clearly distinguish a threat as the packet is dropped. Most events were caused by XXX which is a server running an IP address connectivity monitoring tool named "Smarts Applications suite" . Most of the other traffic which triggered this event were internal to internal.	Can safely filter the events from NFx	Also the second heights event generator is from XXX (external IP address not belongs to II) to XXX (Uninet S.A. de C.V Mexico), UDP traffic. It is not sure why this traffic is coming through II; Probably a bad IP routing or BGP configuration.
DNS Reconnaissance	Critical (5)	screen - ids port scan	334	XXX (outside IP for Internet access for II) and some web server IP addresses. Looks like a the regular port scan	Juniper recommends to filter these events as these scans looks pretty normal.	

Unix Alarm Summary

nF Alarm	nF Severity	Device Alarm Description	Protocol	Event Ct	IS Action
System Status	Minor (3)	Connection closed	SSH	27059	Filter
Authentication Succeeded	Major (4)	The superuser performed on login with terminal ttyname	NONE	8679	Filter
Authentication Succeeded	Minor (3)	Accepted password	SSH	7727	Filter
FTP Access	Minor (3)	FTP session closed by the client	FTP	7475	Filter
Unknown Alarm	Critical (5)	Mail function error	SMTP	233	Needs Analysis
Authentication/Authorization Failed	Minor (3)	Failed password	SSH	68	Filter
Unknown Alarm	Critical (5)	SUDO allow restricted root access	NONE	41	DO NOT FILTER
Service/Process Status Change	Critical (5)	Syslogd service is shutdown	UDP	27	DO NOT FILTER
Service/Process Status Change	Critical (5)	Syslogd service is started	UDP	21	DO NOT FILTER
Authentication Succeeded	Minor (3)	User performed a login from client host	SSH	14	Filter
Unix / Linux Access	Warning (2)	Login session closed for user	SSH	14	Filter
Authentication/Authorization Failed	Critical (5)	The login by superuser on terminal ttyname is refused	NONE	8	DO NOT FILTER
Mail Access	Minor (3)	Null connection from the client host	SMTP	6	Filter

Filtering Strategy

- Work with SIM vendor to sort through alerts
  - Requires great deal of time & patience
  - Expertise
- Provide alert detail to CISO
  - Which alerts to suppress
- Provide alert detail to system admins
  - Normal chatter?
  - Cut off from source

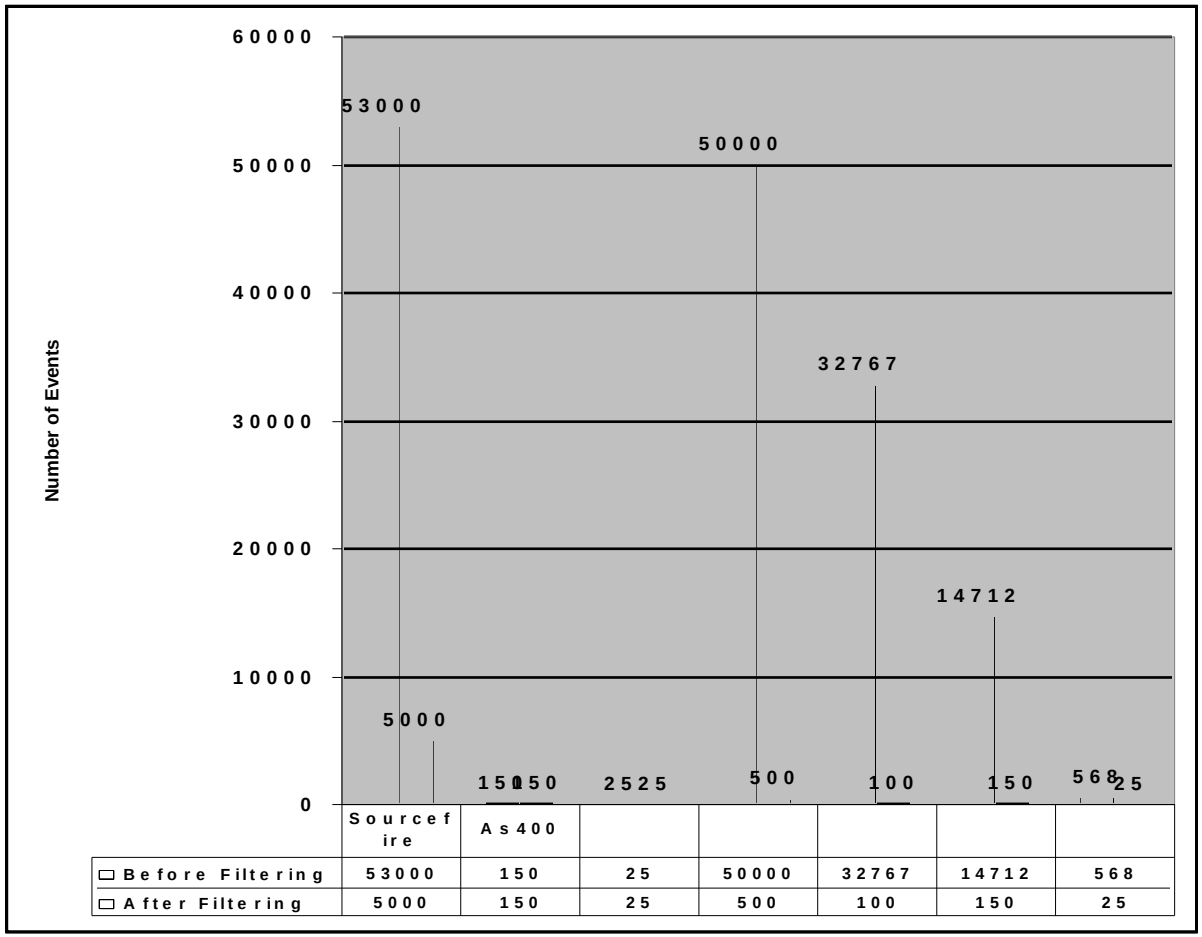
Filtering Strategy

- Stop message flow from the source
  - Sys admin will turn off messaging for a specific event at the source
- Stop message flow at SIM
  - rules can be written to ignore the message
  - Action can be “drop” - eliminates the message all together from the database;
  - or “store” - ignore the message but keep it in the database for future use. Future use could include forensics and compliance.
- Examine “canned” rules & write rules customized for your environment

Statistics

- Servers, Network Devices, Firewalls, etc.)
-
- Four Thousand Nodes
- More than Four Million Events per day (average - 45 events per second !!)
- One dedicated person

Over 90% Reduction of Events



- Create “compartments” for other groups
- Give department heads access to console
- Create knowledge base
- Leverage Help Desk support
- Provide regular feedback to senior management
- Watch system growth – budget properly for future agents

"*The single most important and lasting accomplishment of a CISO is not how many complex projects he or she*

she manages to bring everyone together"

Contact Information:

Sasan.hamidi@intervalintl.com

305-666-

407-566-0250, ext. 18