Security Incident and Event Management (SIEM) Solutions

Event Code: TECH12

Session Presenters:

Eric Maher
Information Security Manager
Foley & Lardner LLP

Jason Preu
Information Security Manager
Lathrop & Gage LLP

Ted Theisen
Director, Cyber Investigations
Kroll Advisory Solutions

Security Incident and Event Management (SIEM) Solutions

Eric Maher
Information Security Manager
Foley & Lardner LLP

i/+\ 2013
the catalyst

Foley & Lardner LLP SIEM Deployment

- Started deployment in 2012
- Chose LogRhythm; also evaluated Q1 and ArcSiht
- Initially focused on DMZ and Active Directory
- Currently deploying to the remainder of our infrastructure, and tuning the advanced intelligence and correlation functions

Why Now?

- Client Demands – more and more questions on how we keep and process logs and react to events
- Normalizing our desperate system logs for reporting and incident tracking
- Compliance*
  - HIPPA (Security Management Process~164.308(a)(1) (Activities 7, 8, and 9)
  - PCI (Requirement 10)
  - ISO (27002 – 15.3.2 Info System Audit Control)

* None of these specifically require SIEM, but log management in general.

What were we looking for?

- Improved visibility of events across multiple systems in a single pane of glass
- Go from logs as reactive controls to proactive alerts
- Event correlation across multiple systems
- Usefulness across technology (not just security) and beyond
- The ability to positively respond to client requests and regulatory requirements

Did we find it?

YES! But it is not that straight forward . . .

- We have improved visibility across systems. . .now we need to really figure out what we need to look at
- Event correlation works and has provided some very useful data that our other security tools did not see . . . but we needed to sift through a lot of alerts to get that info
- Other departments come to us for reports, but we would have liked to have their requirements better defined ahead of time

What *should* we have been looking for?

- Better requirement guidance from outside of security team. *We seem to be stuck on the "**S**" in SIEM*.
- Finding stakeholders outside of security
- How does SIEM fit into our current response processes, and how will alerts be incorporated?
- Stronger ties to risk management – identifying specific risks that SIEM could help mitigate in security and other departments

What SIEM is NOT

- SOC in a Box; or ESM in a Box; Analyst in a Box; or Compliance in a Box
- Plug and play. No training needed!
- Out of the box event correlation. Just like IPS/IDS, can be very noisy. Tune…tune…tune.

What SIEM can do that we did not consider.

- Monitor for file integrity and access - DLP lite
- Monitor system status and raise alarms
- Configuration management auditing
- Internet usage monitoring - Lite

Advise I wish we had 18 months ago

- Start small. Target the systems that require advanced log management
- Fully define use cases across technology. List regulations and requirements you are looking to meet. “You will never get what you want until you know what you want!”
- Take hard look at what you already have. . . Can you meet these requirements with your current log management solutions?
- If not, work with vendors to map out features to meet these goals

Going Forward

- We believe SIEM is a valuable tool in our security environment
- We continue to deploy agents, adjust reporting and alerting, and tune correlation
- Do some internal marketing for SIEM. Make the tool useful to other groups
- Outsourcing????

Security Incident and Event Management (SIEM) Solutions

Jason P. Preu
IT Security Manager
Lathrop & Gage LLP

i/+^ 2013 the catalyst

Why Did We Do This?!

- Verizon 2010 Data Breach Investigations Report*: “Almost all victims have evidence of breach in their logs."

*http://www.verizonenterprise.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf

Lathrop Prior to SIEM

- 7.5 million events/day
- Number of staff devoted to log management and review?
  - .01 (on a good day)

Lathrop Prior to SIEM (cont'd)

- The Milli Vanilli Approach

- "Gotta blame it on something. Blame it on the rain."

Lathrop Approach

- The School of Johnny Nash: “I can see clearly now the rain is gone.”
- Initial problems we (IT) wanted to solve:
  - Anything IT-related (reboots, failed admin logins), AD changes
- After 3 years, we now receive SIEM review requests from all areas of the business

SIEM vs. Log Management

- Log Management = No threat identification
- Log Management = No active response
- SIEM = Time-based security
- SIEM = Normalized data

5 Steps Toward Building a SIEM Engine of Awesome

- Collect
- Supplement
- Correlate
- Follow-up
- Document

SIEM Engine of Awesome Collect

- Get the biggest net you can
- Cast that net wide
- Reel that net in and throw nothing back (yet)
- Then get 3 or 4 more nets and repeat
- Then get 1 or 2 more nets and repeat for good measure

Note: If you are going to outsource, try to keep local copies of your logs

SIEM Engine of Awesome Supplement

- Gather non-system data:
  - HR
    - Current Employee List
    - LAA assignments
  - Records
    - Members of ethical walls
  - Practice Area Data Custodians
    - Approved ACLs

SIEM Engine of Awesome Correlate

- Maturity means comparing logs from disparate sources and establishing a narrative from the data
- Most third-party SIEMs have many avenues toward normalization and subsequent event correlation
- Failed logins are good but successful logins are better
- CVE to IDS events

SIEM Engine of Awesome Follow-up

- Defenses must be monitored and alarms heeded
- All defenses fail
- SIEM helps with the timeliness of our response(s)
- Goal expands to become: Not only to prevent but to detect with precision and speed then RESPOND accordingly

SIEM Engine of Awesome Follow-up (cont'd)

- Analyze reports to reduce signal to noise
- Hygiene

SIEM Engine of Awesome Document

- Scope of protection
- Service Level Agreements
- Change Management
- Response procedures

SIEM Engine of Awesome Document (cont'd)

- Sample SIEM Rule to Procedure Matrix

Rule	Procedure/Action	SLA	Priority
High Threat/Vulnerable Asset	Malware check	1.5 hours	1
Outbreak	Malware check	1.5 hours	1
No response from log source	Security Review	2 hours	2
Attack-Suspicious Login	Security Review	4 hours	3
Attack-Firewall	Security Review	8 hours	5

Recap

- Use highly-focused rules at first to establish and refine uses
- Pick a good musical metaphor
- Cast a wide net when gathering data
- Supplement your system data sources
- Act on your findings

Security Incident and Event Management (SIEM) Solutions

Don't Be SIEM-Less

Ted Theisen
Director, Cyber Investigations Practice
Kroll Advisory Solutions

i/+^ 2013 the catalyst

Ted Theisen

- Systems Engineer at an online Brokerage
- Special Agent, FBI
- Branch Chief of Cyber Integrity, Executive Office of the President, White House
- Director at Kroll Advisory Solutions, Cyber Investigations Practice

i/+\ 2013 the catalyst

Overview

- (Ir)Rationalizations for not having a SIEM / Log Aggregation / Event Correlation tool?
- Case examples – Real World Intrusion Incidents
- SIEM effects on Incident Response

SIEM-less Rationalizations

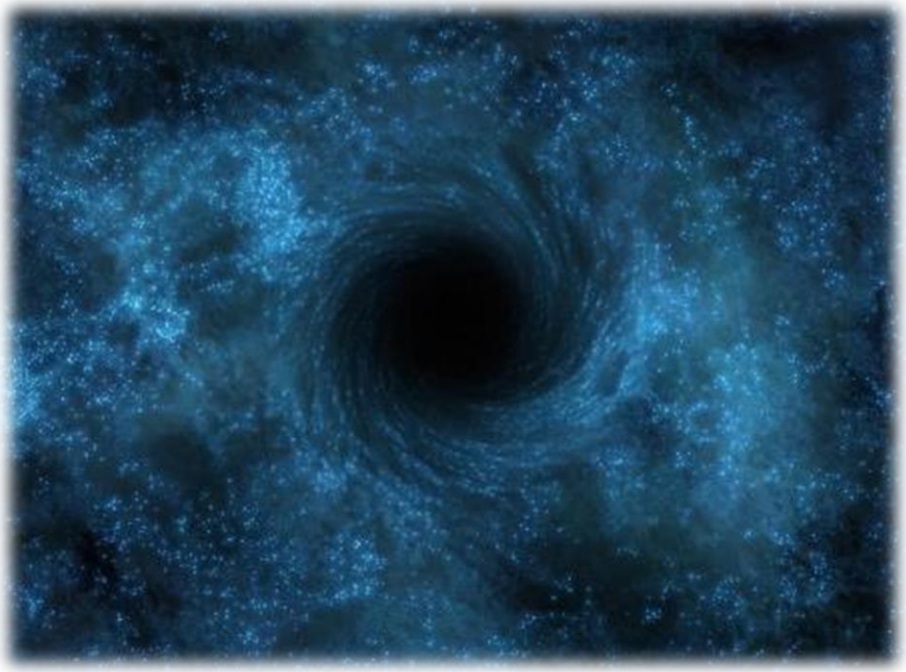
"I cannot imagine any condition which would cause a ship to founder. I cannot conceive of any vital disaster happening to this vessel. Modern ship building has gone beyond that."

- Captain Smith, Commander of the Titanic

Justifications

- “We’re not a target”
- “We’re too small”
- “It’s too expensive”

SIEM-less Impact



SIEM-less Impact

- No SIEM?
- You have a void of comprehensive insight into multiple areas of your infrastructure during an intrusion incident

This can be problematic

SIEM-less Impact

- Without a SIEM, it is difficult to rapidly pinpoint:
  - Affected hosts
  - Compromised data
  - Impacted processes
- Can dramatically increase duration of troubleshooting
- Root cause analysis becomes challenging

SIEM-less Case Studies

We'll review two examples:

- Financial Institution
- Educational Institution

Financial Institution

- The institution was notified by a ***customer*** that their PII was posted on pastebin.com
- ‘nuff said…
- Identification of the attack vector took an inordinately long amount of time

Financial Institution

- Harvesting logs from multiple devices was arduous
- Investigators and institution had difficulty identifying the impact to downstream devices and associated processes
- Due to the inability to conclusively show what had/had not been compromised, an inordinately large notification process resulted

Educational Institution

- The institution was infested with malware through an e-mail attachment; this was isolated and quarantined in a reasonable amount of time
- Infected hosts included a file server with numerous student records
- Due to the absence of event correlation, log aggregation, netflows, pcaps, etc. the infected hard drives were the only evidence available to analyze
- The victim organization was prepared for a very large notification process until…

Educational Institution

- Although we were told that there were no logs available, thorough investigation revealed that one of the IT Engineers had been archiving netflows
- Subsequent analysis resulted in being able to conclusively show no exfiltration of data for the duration of the malware outbreak
- ***No notifications were necessary***

SIEM Case Studies

Intrusion cases encountered where victim company implemented a SIEM?

- Almost **NONE!**
- In all seriousness, there have been cases… but due to the rapid identification and isolation of affected data and systems, outside investigation is minimal

SIEM Case Studies

Intrusion cases encountered where victim company implemented a SIEM

- Based upon the respective alerts generated, evidence was easier to identify and search
- Archived evidence was in a central location
- Log aggregation resulted in reduced inadvertent tampering of logs when data was accessed from multiple locations
- Event correlation improved triage of affected hosts

SIEM and Incident Response

- Assess the Exposure, Access and Acquisition
  - Part of a larger Incident Response Process (NIST 800-61 rev 2)
    - Preparation
    - Detection and Analysis
    - Identification
    - Containment
    - Eradication
    - Recovery

“Proactiveness” of SIEM Implementations

- Examples:
  - Services stopping and starting on multiple devices
  - Multiple hosts establishing connections to certain IP addresses
  - Various applications crashing on multiple devices
  - Account logon anomalies
    - Many usernames connecting over remote access from same IP

“Proactiveness” of SIEM Implementations

- Examples:
  - Unexpected Network Traffic To/From Perimeter Devices
    - Encrypted Files
    - Remote Shells (Remote Desktop Protocol (RDP)
    - “Grayware” – PSTOOLS, nmap, etc.
    - Network reconnaissance scans
  - System Anomalies
    - Firewall modifications
    - Disk space spikes upward and downward
    - Log deletion messages
    - Unknown files on webservers

Attacks from Insiders

- Insider threats are becoming much more common!
- Carnegie Mellon determined:
  - 58% of Insider Threat cases occurred outside of normal business hours
  - 66% were executed via remote access
  - Common ports used for remote attacks were port 22 (SSH), 23 (Telnet) and 3389 (Terminal Services, or RDP)

Source: CERT/DHS April, 2011 publication: “Insider Threat Control: Using a SIEM signature to detect potential precursors to IT Sabotage”

Attacks from Insiders

The subsequent signature developed was as follows:

Detect <username> and/or <VPN account name> and/or <hostname> using <ssh> and/or <telnet> and/or <RDP> from <5:00 PM> to <9:00 AM>

Source: CERT/DHS April, 2011 publication: “Insider Threat Control: Using a SIEM signature to detect potential precursors to IT Sabotage”

Attacks from Insiders

This type of signature can be applied to targeted individuals:

- Disgruntled employees
- Probationary employees
- Off-boarded employees
- Temporary Employees
- Contractors

Limitations

- This is not a *replacement* for sound Incident Response, but will enhance your existing IR plan
- This is an information aggregator, so proper administration of the SIEM and the corroborated data is essential

Conclusions

- Consider implementation of a SIEM
- Even if you're a small organization, consider third party "SIEM as a service" offerings
  - Take baby steps… *turn on logging!*
  - Start with log aggregation...
- Regardless of your industry or the size of your company, your data is always a target to the hacker community

Questions?

Thank you!

Eric Maher
Information Security Manager
Foley & Lardner LLP
emaher@foley.com

Jason Preu
Information Security Manager
Lathrop & Gage LLP
jpreu@lathropgage.com

Ted Theisen
Director, Cyber Investigations
Kroll Advisory Solutions
ttheisen@kroll.com