

# Log Aggregation: The Issues with the Solutions

Jonathan Sander  
IAM & Security Analyst  
Quest Software



# Agenda

- ▶ **The Log Situation** ( 8 mins / 3 slides )
- ▶ **What Do Folks Do?** ( 2 mins / 1 slide )
- ▶ **Solution Requirements** ( 30 mins / 8 slides )
- ▶ **Recap** ( 2 mins / 1 slide )
- ▶ **Q&A** (remaining & throughout)

# The Log Situation (1 / 3)

- ▶ Does anyone here not think logs do not contain useful information?

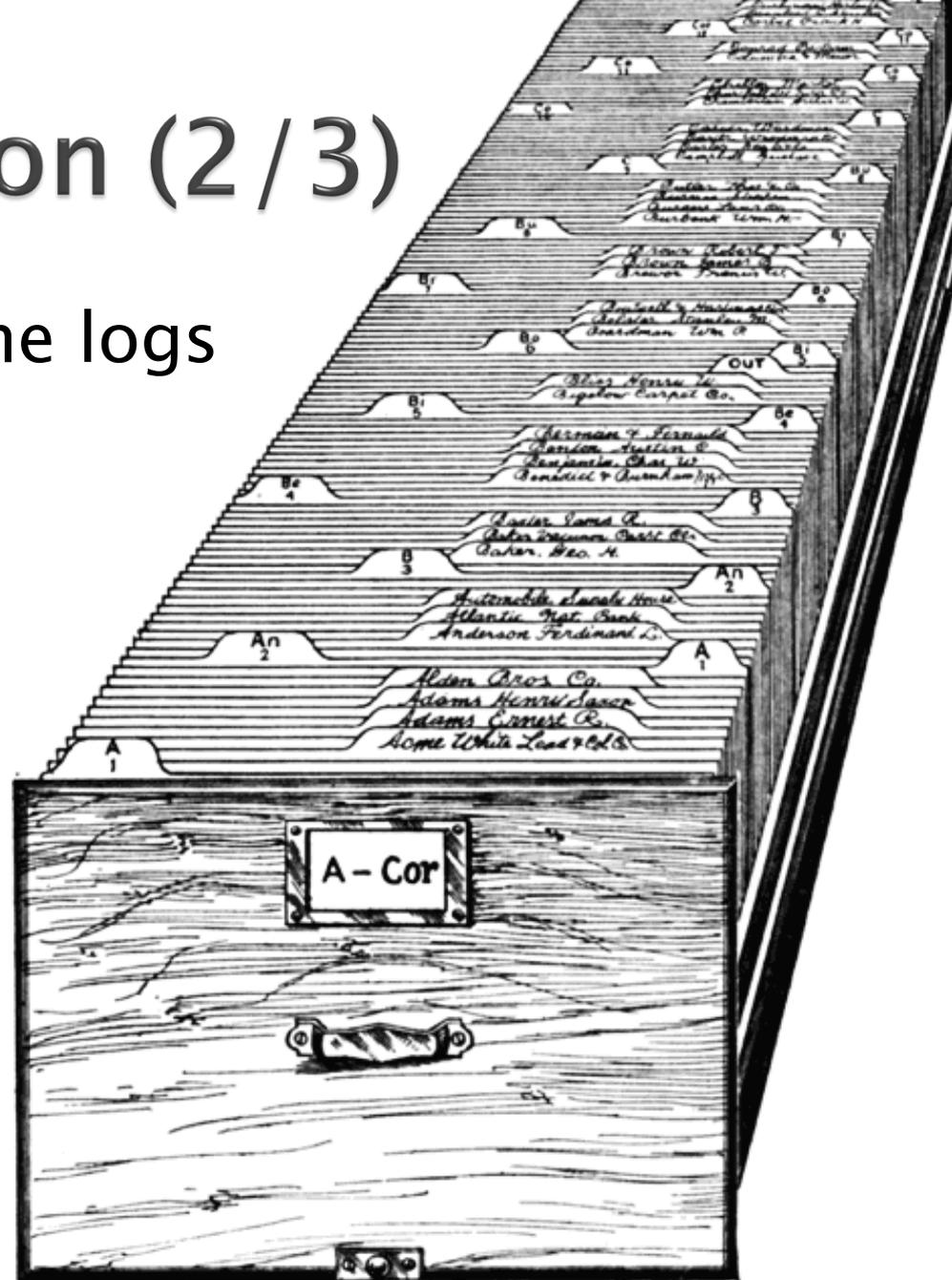
- ▶ Information in logs

- What happened
- When it happened
- What and who did it
- How it was done
- Where it was done from
- Why it was done that way
- Lots and lots of details



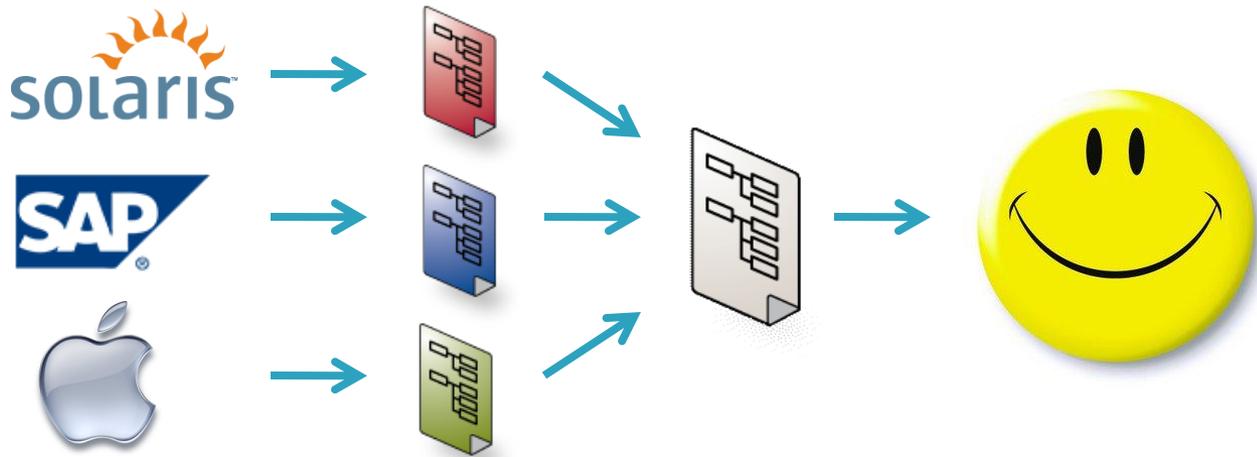
# The Log Situation (2/3)

- ▶ Why not just shove the logs somewhere?
  - Storage
  - Security
  - Indexing
  - Reporting
  - Data retrieval



# The Log Situation (3 / 3)

- ▶ What about data normalization?



- ▶ Lacking in true standards
  - MITRE's CCE has legs (<http://cee.mitre.org/>)
  - Consensus Audit Guidelines may accelerate
- ▶ Doesn't solve other issues

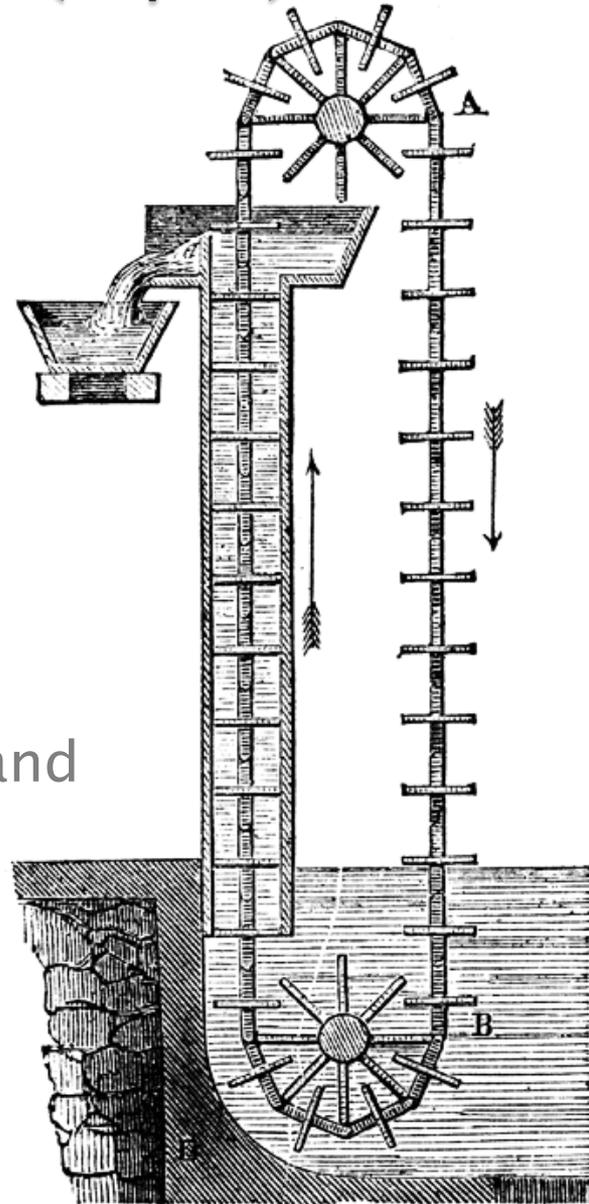
# What Do Folks Do?

- ▶ Most do not go it alone
  - At the very least they leverage standards
- ▶ Many go for real time search like solutions
- ▶ Just as many go for log movement
- ▶ A smaller group of larger firms opts for SIEM

*We are here today to explore what you should look for in any solution you choose.*

# Solution Requirements (1 / 8)

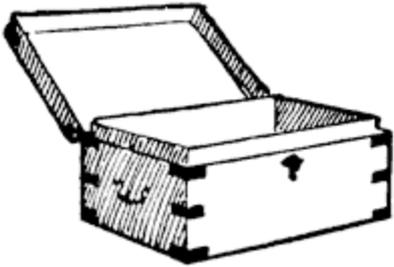
- ▶ Collection methods
  - Must exist for all platforms
    - SYSOG & evt collection is minimum
    - Best if adaptable
    - Make a list of all your formats
  - Streaming vs. move files
    - Streaming often strips data that is “extraneous” – be mindful
    - Moving files can bloat infrastructure and storage



# Solution Requirements (2 / 8)

## ▶ Storage methods

- Single tier vs. multi tier
  - Single tier puts many conflicting demands on store (reporting, long term, real time)
  - Multi tier can be more complex to set up at first, may take time to settle in
- Make sure to get numbers for long terms needs
  - Not only projections of size, but cost
  - Get your whole long term your whole long term cost estimated up front



# Solution Requirements (3 / 8)

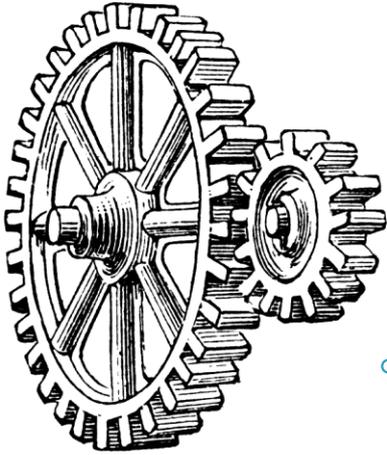
## ▶ Flexible delivery options

- Understand all your audiences for log data
  - Auditors need simple interfaces and pre-populated reports
  - IT Admin staff need flexible querying to do ad hoc digging through data
  - Who else?
- Where will they access?
  - Bandwidth?
- Very often ignored



# Solution Requirements (4/8)

- ▶ **Agent based vs. agentless architecture**
  - Agents often get bad first reaction
  - Most tools will offer both types of operation
  - Agent based will always offer enhancements
    - Agents can often protect against log rolling
    - Agents can ensure strong authentication in the agent structure vs. relying on network protocols or remote access
  - Find out exactly what each mode of operation offers and compare to what you require



# Solution Requirements (5 / 8)

## ▶ Log tampering

- The value of log data is accuracy
  - Log integrity
  - Administrators, and hackers, can cover their tracks
- Determine exactly how the data is protected
  - Real time systems are less vulnerable
  - Log movement systems will need to use special methods
  - Both collection types will have an agent required to provide this widely
    - Facilities like SYSLOG can provide good solution

# Solution Requirements (6 / 8)

- ▶ Native data is often isn't sufficient or clear
  - If you can't understand the data, it's useless
    - GPO changed, does not say which
    - Same event for calendar open and free/busy check
    - Logon failed – for who? from what?
    - File not found.
  - Some solutions offer enhanced data
    - Agent is always required
    - Can be difference between success and failure of a project with some audiences – auditors
    - Make sure you know events content
      - Make a list of key events



# Solution Requirements (7/8)

## ▶ Security

- This is a huge amount of sensitive data
  - SoD for administration
    - For every part of the technology stack
  - Encryption, at rest and in transit
  - Good authentication practices
  - Secure backup & recovery
- If they aren't already, get IT security involved

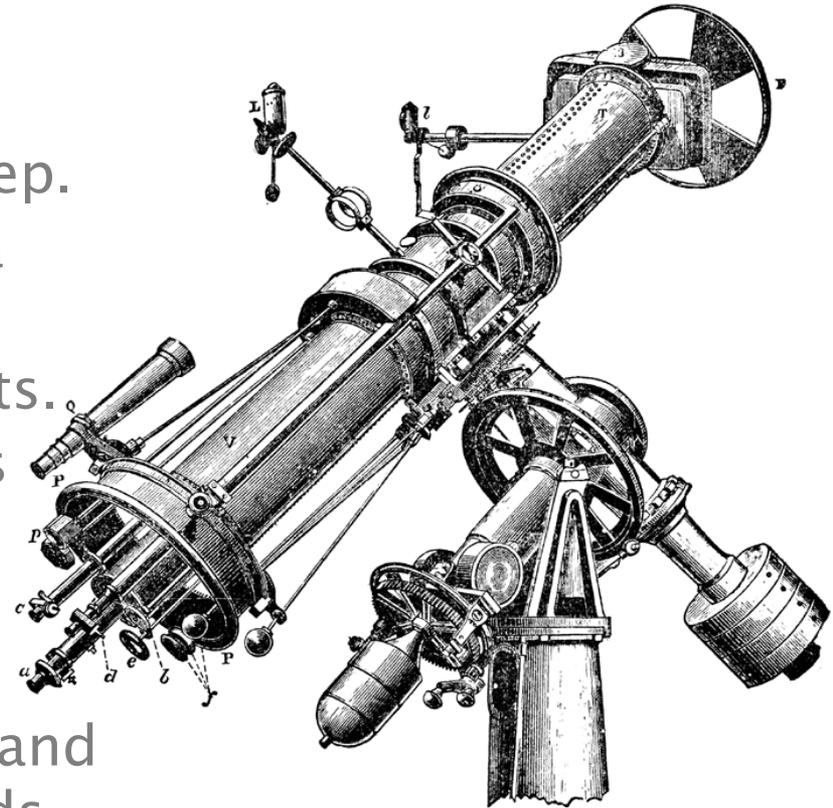


# Solution Requirements (8/8)

- ▶ **Do they eat their own dog food?**
  - If they have a suite of products, can they get all the logs into their own logging platform?
  - Do they have reports built for their products data?
  
- ▶ **Normalization**
  - This is in vogue right now
  - CEE from MITRE is the best to ask about
    - Could change quickly, though

# Recap

- ▶ To get the right solution:
  1. Know what you need to collect.
  2. Know how much you need to keep.
  3. Know who needs to use the data and how.
  4. Figure out if you can allow agents.
  5. Understand how data integrity is maintained.
  6. Make sure the information is usable.
  7. Make sure the product is stable and keeping up with innovative trends.



# Q&A



# Contact Info

Jonathan Sander

Email:

[jsander@quest.com](mailto:jsander@quest.com)

Cell:

+1.973.746.0182

Blog:

<http://theexpertscommunity.com/users/blog/33>

Twitter:

@jonathansander

Profile:

<http://www.linkedin.com/pub/0/901/689>

너를 감사하십시오

Thank You

Gracias

有難う御座いました

Merci

Grazie

谢谢

Danke Schön

Obrigado

спасибо