Evaluating, choosing and implementing a SIEM solution

Dan Han, Virginia Commonwealth University

A little about me

- Worked in IT for about 15 years
- Worked in Application Development, Desktop Support, Server Management, Infrastructure Management and Security
- Worked primarily in healthcare and education settings, with some minimal background in Financial institutions.
- Served as the VCU ISO for the past two years

Knowledge is power

" The greatest enemy of knowledge is not ignorance, it is the illusion of knowledge"

- Stephen Hawking

When I first started to work in Information Security

Illusion of knowledge…

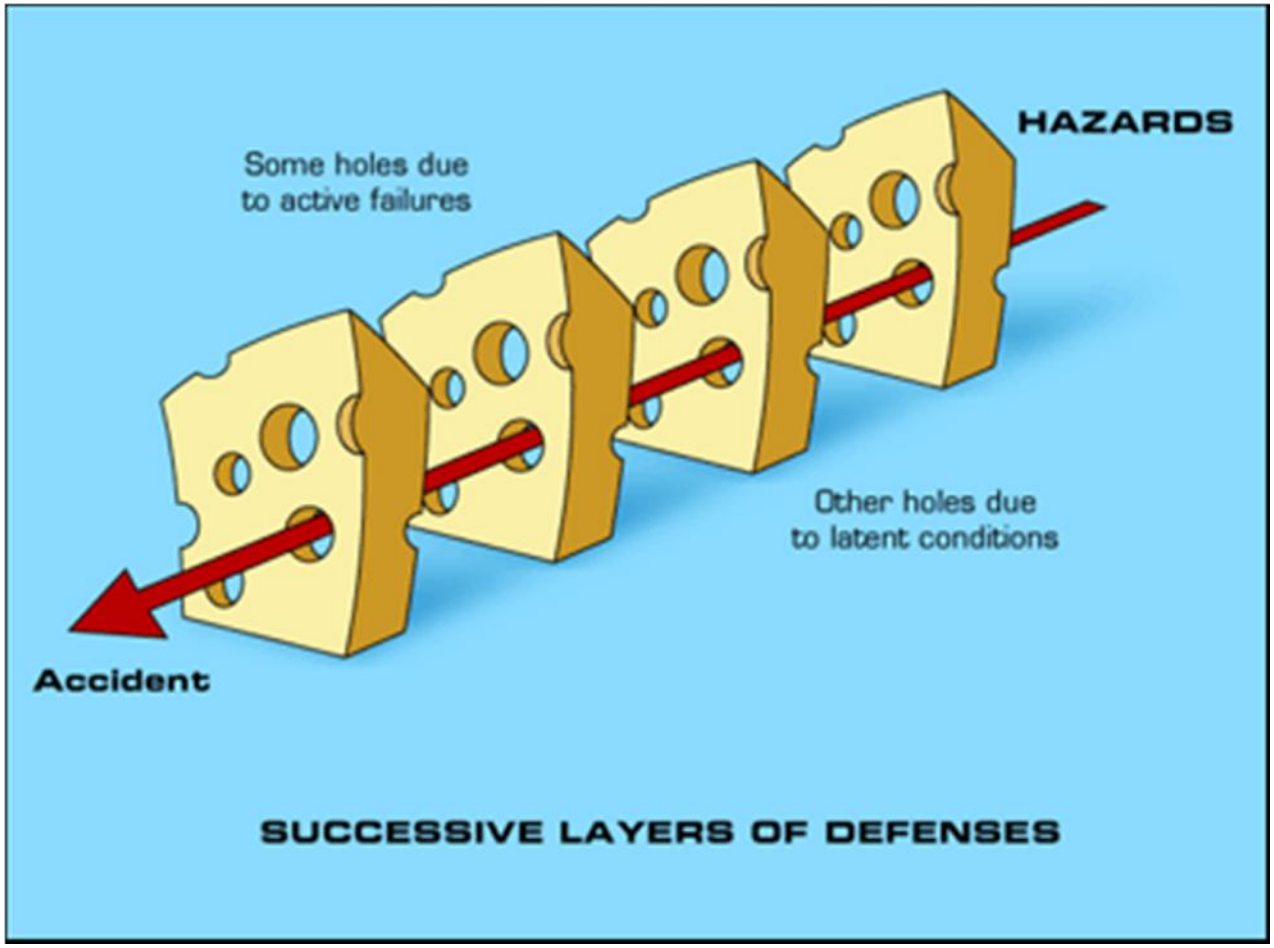
Individual server logs didn’t look too bad…

Besides, we are no three letter agencies, who cares about our data?

We think we know our environment…

No metrics to track results

So what ended up happening…


HAZARDS
Some holes due
to active failures
Other holes due
to latent conditions
Accident
SUCCESSIVE LAYERS OF DEFENSES

Then I grew up…

And realized…

So wake up or ostrich defense?

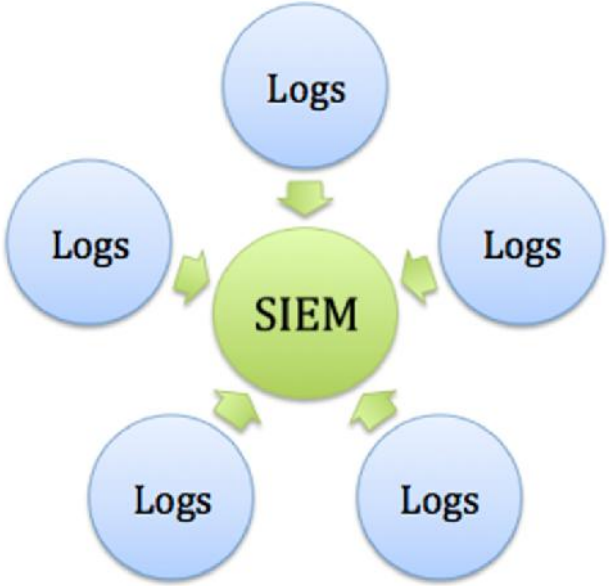
WAKE UP!
AND SMELL
THE
COW POOP!

In order to obtain knowledge of your environment, you must understand your environment as a whole

NetIQ

splunk>

1Labs



LogRhythm
COMPLY. SECURE. OPTIMIZE.

hp ArcSight

Symantec

RSA SECURITY

nitrosecurity
now part of McAfee

What is a SIEM System?

- Common misconception
  - It does not “manage security” for you and let you kick your feet back and relax
  - It is not a plug and play system
  - It doesn’t necessarily reduce the amount of staff or resources needed to manage security
  - It cannot be implemented overnight
  - It is not cheap
  - It will not wash your car and make you coffee

What can a SIEM solution do for an organization

- Provide an organization with unprecedented visibility into its IT environment
- Provide analytical horsepower to correlate, identify and alert on security issues.
- Centrally retain logs for managed IT systems (costly)
- provide compliance testing and reporting across multiple systems
- Allow sight beyond the “White noise”

Why we use SIEM

- Increase visibility into our environment
- Help to collect meaningful metrics
- Prioritize threats against the organization
- Enable sharing of threat intelligence with trusted parties

How did we come to this decision?

- **Business Needs - VCU**
  - Needed more visibility into various IT systems we use to better understand the threat landscape
  - Needed a tool that could help to make sense of volumes of NetFlow and log data and present it in a meaningful manner
  - Needed a centralized log management tool

How did we come to this decision?

- **Evaluation requirements**
  - Must collect and correlate data from LDAP, Network Equipment, Servers, Security Appliances (IDS / IPS, etc), AD, and NetFlow.
  - Must retain information for at least 30 days for correlation and analysis.
  - Must have the ability to define severity of events and alert on those that meet certain severity.
  - Must have search and query capabilities that can allow for detailed incident and forensics analysis.
  - Must provide ability for analysts to quickly drill down from high-level alert to nitty-gritty details
  - Must not eat up the entire security budget for the year.

How did we come to this decision?

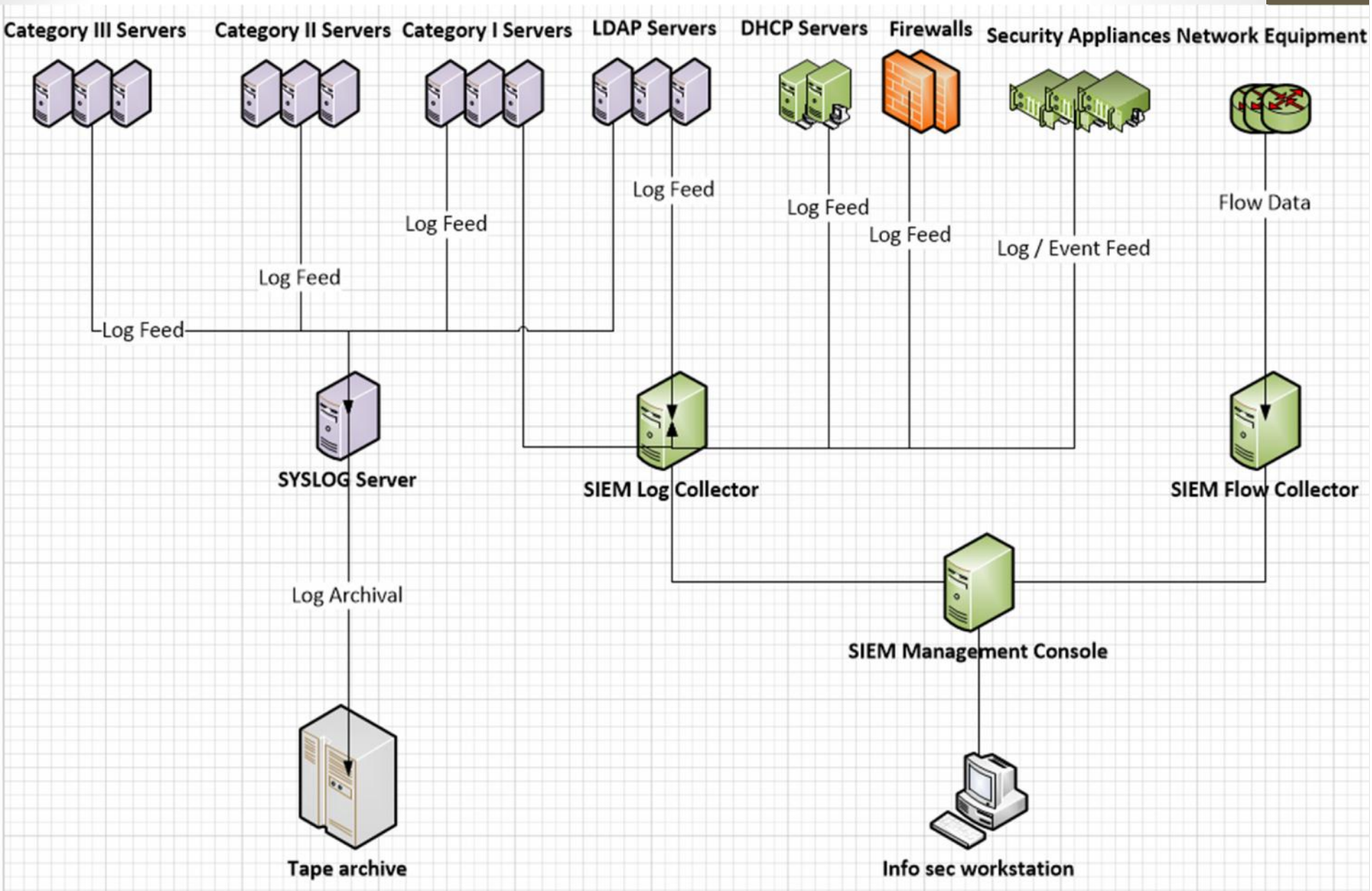
- **Compliance requirements**
  - System access record retention requirements (COV § 2.2-3803.7)
- **Visibility requirements**
  - AD / LDAP
  - NetFlow
  - Firewalls
  - Sensitive Servers
  - Security Appliances
  - Needed log retention and data correlation / analysis capabilities

The product we chose

How did we come to this decision?

- **Architecture design**
  - SIEM for collection and correlation of critical servers and network / security device logs.
  - Syslog for server log collection and short term retention
  - Tape archive for long term retention of server logs

Architecture



Current implementation

- 1x Management console
- 1x Flow collector
- 1x Log collector
- System partially tuned with average of around 1000 - 2000 correlated offenses per week
- At current log and flow volume
  - Average of over 2,000 events per second, with spikes that can exceed well over 10,000 events per second
  - Average of around 400,000 flows per minute

Next Steps

- Continue the implementation efforts
  - Additional tuning
  - Capacity adjustment for additional flows and events
  - Better incident response integration and potential integration with MSSP

Lessons Learned

- Large financial investment
  - Price of SIEM appliance and support
  - FTE required to effectively manage / monitor SIEM
  - Additional FTE hours needed for incident handling and response
  - Additional efforts required for source connection maintenance and system administration
  - Increased investments to incident response
  - Data storage costs

Lessons Learned

- Define the scope of protection
  - Too expensive as a log collector
  - What do you expect from the SIEM, and what do you want to monitor? Determine the scope of surveillance
    - Data center
    - NetFlow
    - Sensitive servers
    - Other servers
    - Endpoints
    - Firewalls
    - IDS / IPS
    - Networking equipment
    - LDAP / AD
  - Scope of response – Risk based management

Lessons Learned

- Plan your capacity
  - Base on defined scope
    - Determine the licensing model and “Events per Second” (EPS) cost
    - If collecting NetFlow data, understand your capacity needs and plan for the appropriate capacity
    - Understand the various charges around Log sources, Flow Per Minute cost for NetFlow, and EPS cost for log events, etc.

Lessons learned

- Fortify your incident handling capabilities and define the "Actionable incident"
  - Define how you will handle each type of incident based on system categorization, incident type, and other risk factors
  - We cannot triage every single incident
  - Allocate enough resources for the triage and handling of incidents
  - Define a good incident handling process that involve other units such as help desk and network operation centers
  - Try not to be overwhelmed by the shear amount of data coming from the SIEM.

Lessons Learned

- Ensure ability to collect logs and Flow data
  - Determine whether a log collection agent will be required to collect logs from any of your log sources
  - Ensure that the log collection agent will work with your architecture
    - Log agent can properly and correctly forward logs from all monitored devices to SIEM and any other collection devices
  - LOGS ALONE ARE NOT ENOUGH

g18

g18

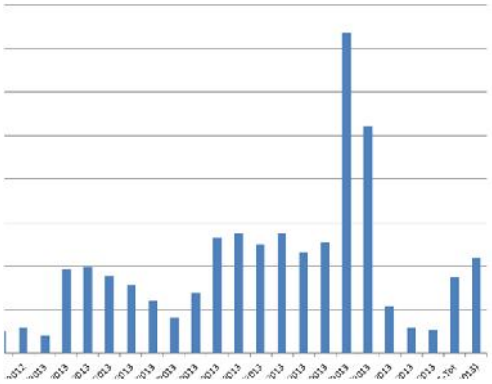
- Determine whether a log collection agent will be required to collect logs from any of your log sources.
- Ensure the supported log collection agent(s) will work with your architecture.
>>etc...

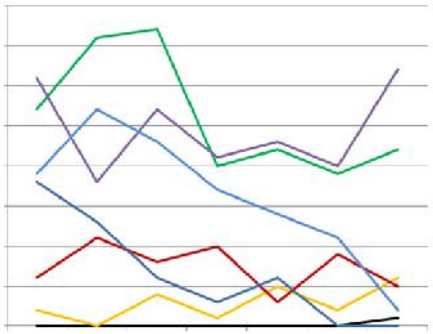
LOGS ARE NOT ENOUGH
- If you're not collecting flow data (NetFlow, JFlow, SFlow), you've only got one eye open.
>>If your SIEM can't correlate flow data with log data, you still don't have the full picture.
>>>Some SIEM vendors will claim to support flow data. But not all of them can correlate it with event data. Be careful here.
- Logs provide the microscopic view of an event. Flow data gives you the macroscopic view of the issue.
>> This may be the only way you have to know where the attacker went after an initial compromise.
>> It may also be the only way to show that data didn't leave the building.

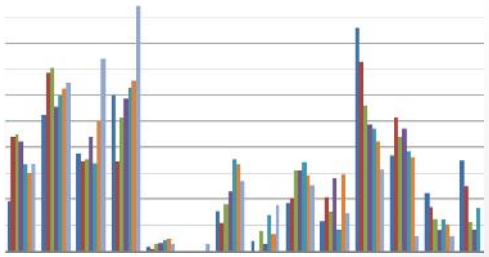
gnpadmin, 9/24/2012

Lessons Learned

- Use the collected data
  - Establish security metrics for your organization based on the data you collect, compare your data with industry statistics, determine patterns that are hidden within the data
    - Number of offenses per week
    - Most targeted systems
    - Most prominent attack types
  - Re-define risks and refine protection tactics that align with the threat landscape







Lessons Learned

- Resources, Resources, Resources
  - You will need at least 1 FTE and proper training for to properly tune and manage a small to medium SIEM implementation
  - Ensure adequate FTE or consultant is assigned to the tuning of the SIEM
  - Ensure incident response procedures are updated with the triage and handling procedures for SIEM events
  - Ensure adequate FTE is assigned to manage the SIEM appliance and incidents
  - Ensure that your human capital is properly trained to handle the SIEM appliance

Bottom Line

- Choose ignorance, illusion of knowledge, or knowledge
- If you choose knowledge, remember that great power comes with great responsibility, and due diligence must be paired with due care
- Be sure to plan the scope and adequately fund the project.
- Assign adequate resources to the project.

THE END

THANK YOU