Logging

You’re not doing it enough

Me (Travis Friesen)

- Previously, InfoSec ‘Guy’ at MERLIN
  - TLDR, IT Provider in Education in Manitoba
- Now: Infrastructure (AWS) Security at Neo Financial
- GXPN, GSTRT, GWAP, etc, no-one cares

OLD MAN YELLS AT CLOUD

NIST Pillars

Identify

Protect

Detect

Respond

Recover

The Problem

- Focus on Prevention makes sense
- BUT
- Can **never** reach 100% Protection
    - Yet Vendors will happily sell that

WHAT IF I TOLD YOU
WOW

But I have logs!

- Muh firewall logs DNS!
    - No, it logs TLS SNI
        - And only until Encrypted Client Hello becomes common

- I can tell which machine hit up evilsite.com!

Yes, but can you tell

- Which
  - User (or was it SYSTEM?)
  - Process
    - And its command line args
    - And its file hash
  - Process’s parent
    - And its command line args
  - What files that process opened
  - What other processes it spawned
  - Which other machines on the network that process has connected to
    - And so might also be compromised
  - etc

But I have logs!

- Ain’t their lawgs on muh endpoints? I got syslog and Event Viewer!

No you don’t

- Integrity
  - Logs on a compromised machine can’t be trusted
- Availability
  - Machines turn *off*, or crash (or are DoSed)
- Manually searching the logs on 100s of different hosts = no_fun
- Also, Event Viewer fucking SUCKS

Threat hunting made easy

- ‘Fictional’ TravWorm.exe
- What are its IoCs?
  - Hashes, CnC IPs, etc
- A quick search and you’re done

Threat alerting made easy

- Why is \\MarketingTeam\Debbie executing powershell on $sqlServer03?
    - ALERT
- Maybe it’s actually legit?
    - How are you supposed to know without the log trail to back that up?

Recover with Confidence

- Servers X, Y, and Z or User ABC was pwned
  - It happens
- So you cleanup Servers X, Y, Z and and reset User ABC’s password
- Are you SURE those were the only servers and compromised?
  - What other hosts were connected to? What all did that user *do?*
  - Pave your whole environment?

- How did they get in the first place?
- Lest they get in again….

LOGS
OTHER SHIT
imgflip.com

SIEM vs Log Aggregator

- Difference?
    - Not a lot

- Both
    - Gather, centralize and index ‘events’ or ‘logs’
    - Allow for rapid searching and alerting

SIEM

- Focus is on SECURITY
- Include threat feeds, security-focussed alerts
- Integrate with or include incident response platforms
- ‘SECURITY’ tax
  - More expensive for same features

Log-Aggregator

- General-purpose
- Can answer questions a SIEM cannot
  - Eg Website analytics
  - Performance metrics
- Get the logs, THEN do the thing

SIEM vs Log Aggregator

- Easier to add Security- and SIEM-like features to a General-purpose logger than the other way around

- Use the term (and the tool) interchangeably

How can has Log Aggregation?

SHUT UP AND TAKE MY MONEY

SLOWWWWW
DOWWWNNN

“Free”/Open source vs Commercial/Paid

- IBM+QRadar
- LogRhythm
- Splunk
- Forti~~Shit~~SIEM

Why paid?

- My time is worthwhile
- Support
- Edge-cutting features
- Proprietary pixie dust

The problem with paid

- Not just expense
  - And I’m cheap!
- Pricing model is *perverse*

Moar logs

- The more you log, more valuable the logging data
- More ‘types’ of logs or ‘facets’
    - DNS, process creation, network connections, file creation, etc
- More hosts
    - Especially your endpoints

Pricing model

- Commonly: Charge for how much you use it
  - Events per Second
  - # of devices sending logs
    - Or both

- The more you use it, the more you should pay, right?

- Financially disincentivizing customers from maximizing the value they derive from your product

- ‘Crown Jewels’
- “How about I only gather logs from my Domain Controllers and SQL Servers?”
  - Or get stingy about what is logged
- Valuable logs

Better way?

- Flat license charge based on org size
    - # of users
    - Total # of hosts
        - (Ir)Regardless if they’re sending logs or not
- Use it as much as you like
- Can I afford to log this? YES

How to ship logs

- Log-forwarding or Agent
    - Frequently: some combination

Log-forwarding

- Almost everything supports log-forwarding out-of-box
  - Syslog, Windows Event Forwarding
  - Not all logs are usable or useful

- Log-forwarding is lean
  - Not 1997 anymore

Agents

- Agents can often provide additional detail and context
  - Eg which process, what was its parent and command lines
- Or logs which simply aren’t provided by the OS
- Sysmon on Windows - log enhancer
  - It’s like an agent, that you have to forward

Why not both?

- Forward logs *to* an agent
  - Which then forwards to collector
  - Useful for endpoints that can’t run the agent

Which logs to ship?

- ‘Use cases’

- What do I need the logs for? Get the logs necessary to meet that need

- eg Who is going to evilsite.com?
  - Get DNS logs

- Minimizes unnecessary logs

Which logs to ship?

- Deriving all use cases takes time
  - Time that could be spent gathering logs
- Expectation: you know all your use cases ahead of time
  - Often don’t realize you needed a particular log until too late

Essential logs

- Detailed Process logs
    - Creation, parent, command line, children, files opened
- Network logs
    - East-west traffic visibility
    - DNS logs
- Other
    - Registry modifications
    - Auth logs

Logging on the cheap

- Graylog
- Logging Made Easy
- Security Onion
- Wazuh

Personal Experience

- Elasticsearch
  - Went agent-based in v8
- ‘Free’ version still has pretty good security tooling
  - Sane-ish pricing model
- Great homebrew community