ELK and Sysmon

BLACK HILLS
Information Security
• 2008 •

© Black Hills Information Secur
@BHInfoSecurity

Backdoors & Breaches

MALICIOUS SERVICE/JUST MALWARE
Attacker adds a service that starts every time
DETECTION
TOOLS
HTTPS AS AN EXFIL
This is pretty basic: just use HTTPS. Lots and lots of malware uses this. For example Meterpreter has used this technique for a long time. It can be used in conjunction with other Stego techniques
DETECTION
NetFlow
Zeek/RITA
TOOLS
Metasploit reverse HTTPS payloads
CREDENTIAL STUFFING
Attackers take advantage of third-party breaches to identify and use IDs and passwords for your organization.
DETECTION
Server Analysis
UBEA
TOOLS
Burp
Hydra
Users registering for services with their work email address
WEB SERVER COMPROMISE
Attackers take over an external web server. They then use this to pivot to your internal network.
DETECTION
Server Analysis
SIEM Log Analysis
NetFlow
RITA
Bro/Zeek
TOOLS
Zed Attack Proxy
SQLMap
Burp Proxy
https://www.zaproxy.org
https://portswigger.net/burp
https://www.blackhillsinfosec.com/using-simple-burp-macros-to-automate-testing
TOKEN PASSING
DETECTION
TOOLS
FIREWALL LOG REVIEW
Can your organization analyze and understand firewall logs? Do you regularly run attack scenarios and verify that your procedures work?
TOOLS
SOF-ELK
https://github.com/philhagen/sof-elk
LEAD HANDLER TAKES MATERNITY OR PATERNITY LEAVE
Yea, there is always one person who pretty much runs the whole IR process. That one essential person. Well, now it is time for the IM to silence that person.
NOTES
PROTOTYPE

Incident Response Card Game

Launching in
September 2019

Request a Deck!

Type "Backdoors & Breaches" into the Questions Window

We'll randomly select a few requests to get a deck before the official launch.

BLACK HILLS
Information Security
• 2008 •

PENETRATION TESTING

RED TEAMING

THREAT HUNTING

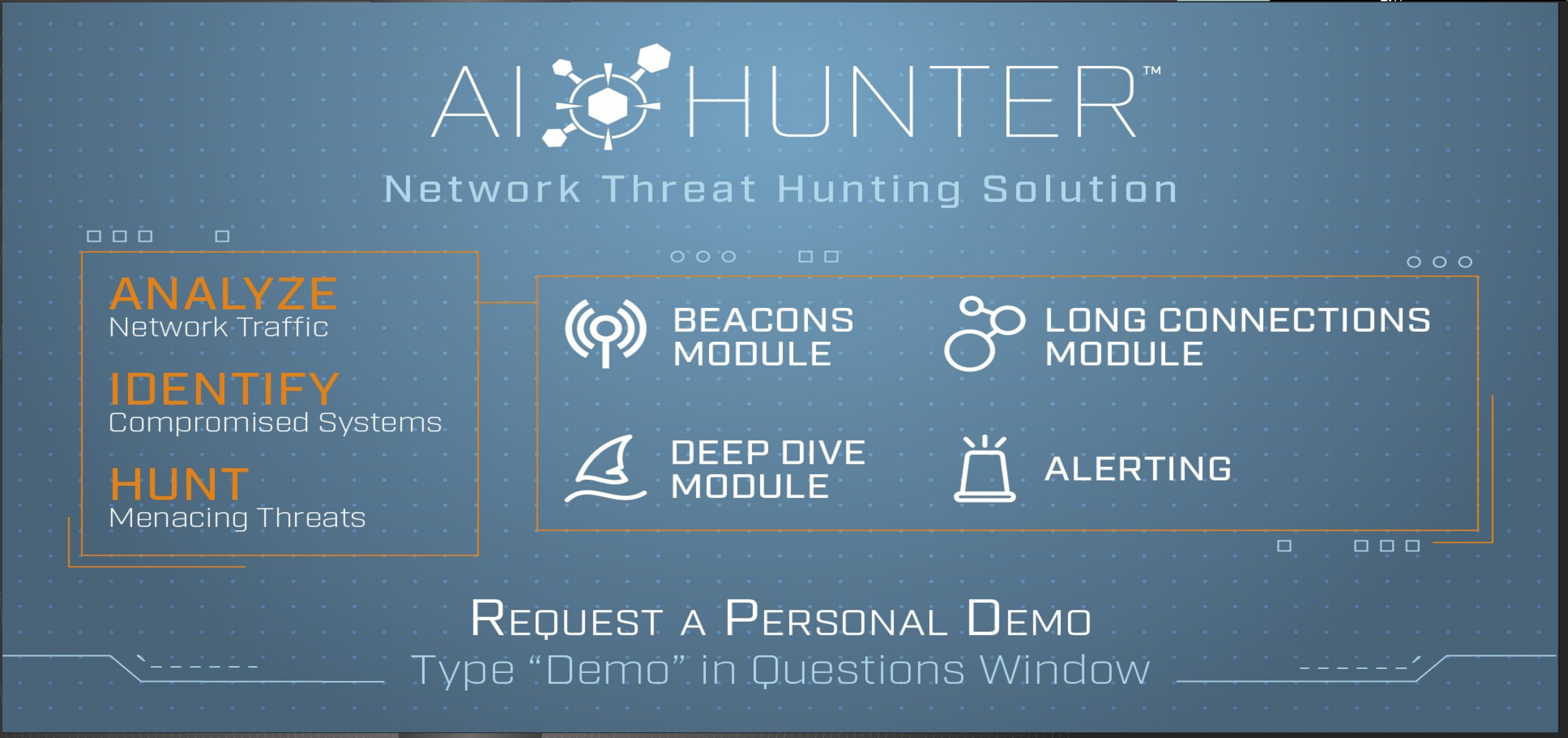
WEBCASTS

OPEN-SOURCE TOOLS

BLOGS

bhis.co

Brought To You By!



AI HUNTER™

Network Threat Hunting Solution

ANALYZE Network Traffic

IDENTIFY Compromised Systems

HUNT Menacing Threats

BEACONS MODULE

LONG CONNECTIONS MODULE

DEEP DIVE MODULE

ALERTING

REQUEST A PERSONAL DEMO

Type "Demo" in Questions Window

Hands On

Chuck Wagon Feast

Adventure

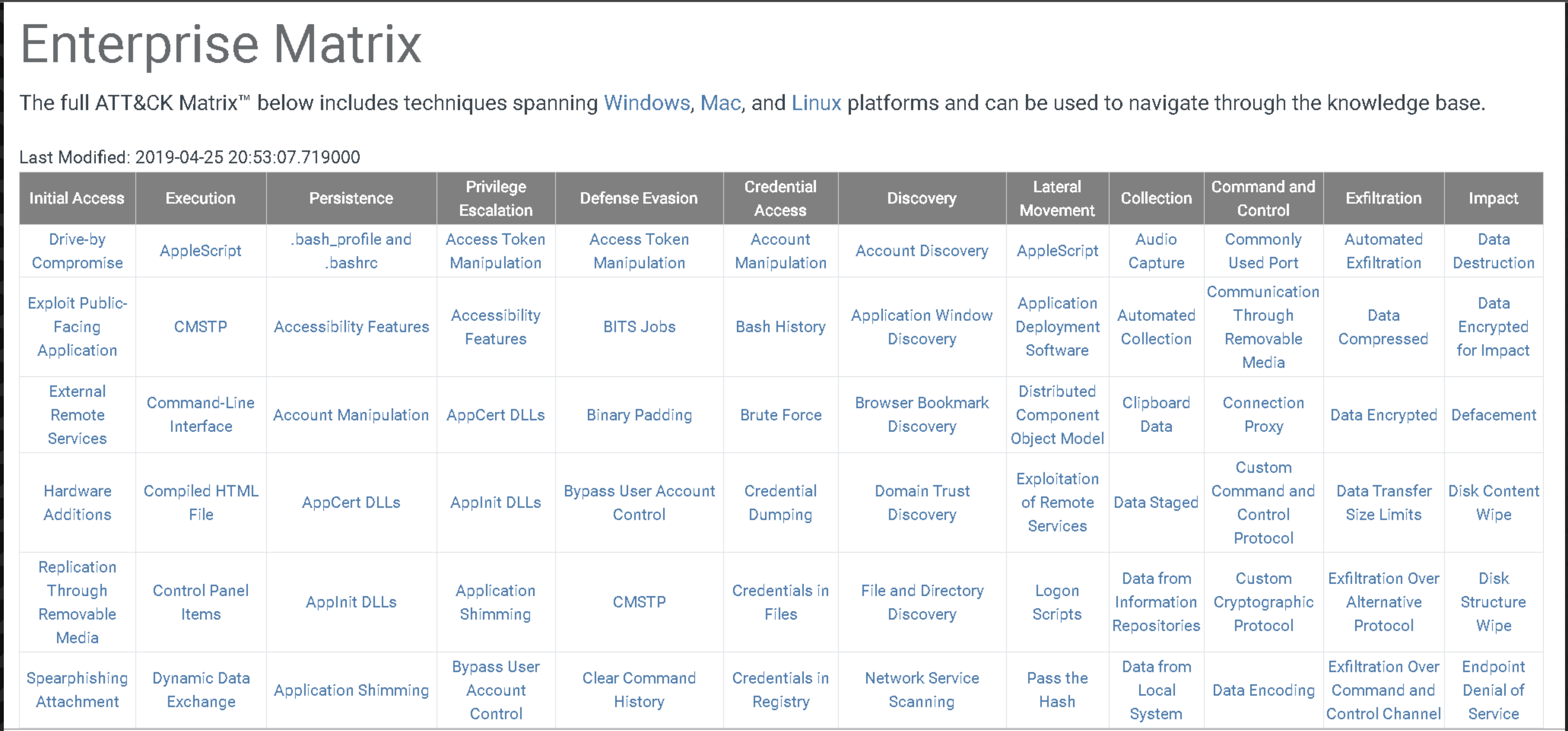
Wild West Hackin' Fest 2019

Training 10/22 - 23
Conference 10/23 - 25

Deadwood, SD

wildwesthackinfest.com

Problem Statement



Enterprise Matrix

The full ATT&CK Matrix™ below includes techniques spanning Windows, Mac, and Linux platforms and can be used to navigate through the knowledge base.

Last Modified: 2019-04-25 20:53:07.719000

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data Staged	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service

Executive Problem Statement

Basic Questions:

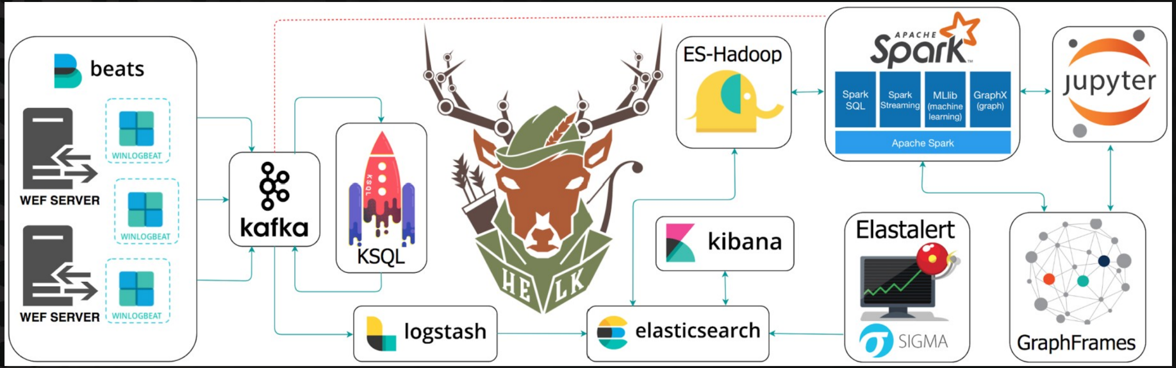
- Is logging working?
- Are we logging too much?
- How much does logging cost?
- What the hell is a Data Lake?
- What is my team actually doing?
- Things are not getting better...

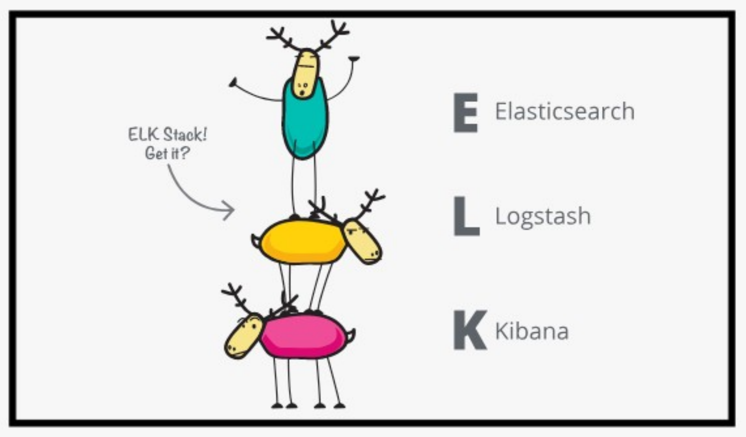
“I am a Youngblood! I will avenge my fallen classmates!”

Sysmon

- Basically…
    - Windows logging is just bad
    - Finding anything is tough
- Sysmon makes it better
    - In like.. Five minutes
    - See last webcast

Something Different Now.. ELK



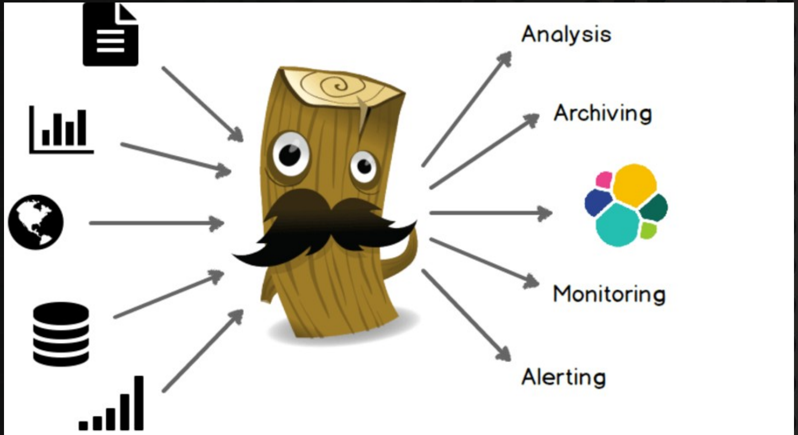


Why ELK?

- Let’s talk about data for a moment
- Structured data vrs lots of different documents/data
- A different type of “database” is needed
- The right tool for the right job

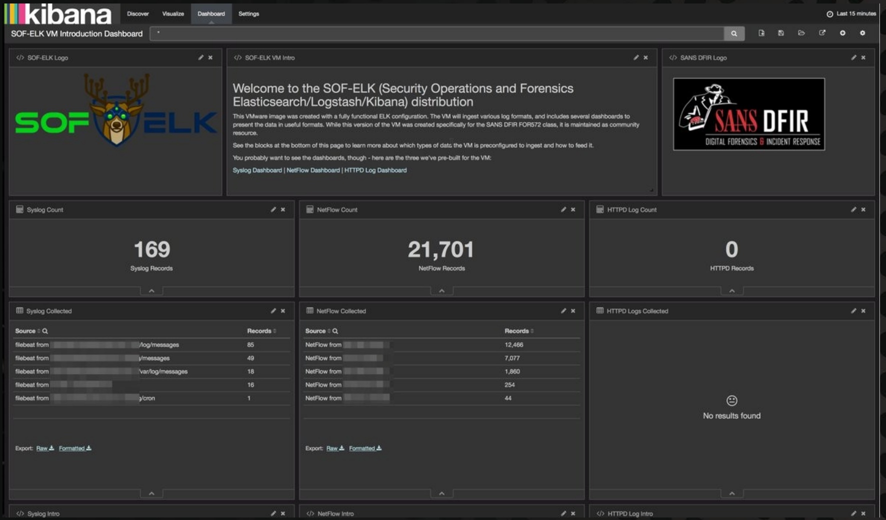
But Why ELK?

- Logstash
- Multiple different types of “log” feeds
- Sysmon, Netflow, etc.
- Need some way to get it all to the same place



But Why ELK?

- Kibana
- Need for a dashboard that has crazy cool (and useful visualizations!)
- Ability to create and save dashboards
- Ability to create and save searches



Welcome to the SOF-ELK (Security Operations and Forensics Elasticsearch/Logstash/Kibana) distribution

This VMware image was created with a fully functional ELK configuration. The VM will ingest various log formats, and includes several dashboards to present the data in useful formats. While this version of the VM was created specifically for the SANS DFIR FOR572 class, it is maintained as community resource.

See the blocks at the bottom of this page to learn more about which types of data the VM is preconfigured to ingest and how to feed it.

You probably want to see the dashboards, though - here are the three we've pre-built for the VM:

Syslog Dashboard | NetFlow Dashboard | HTTPD Log Dashboard

169
Syslog Records

21,701
NetFlow Records

0
HTTPD Records

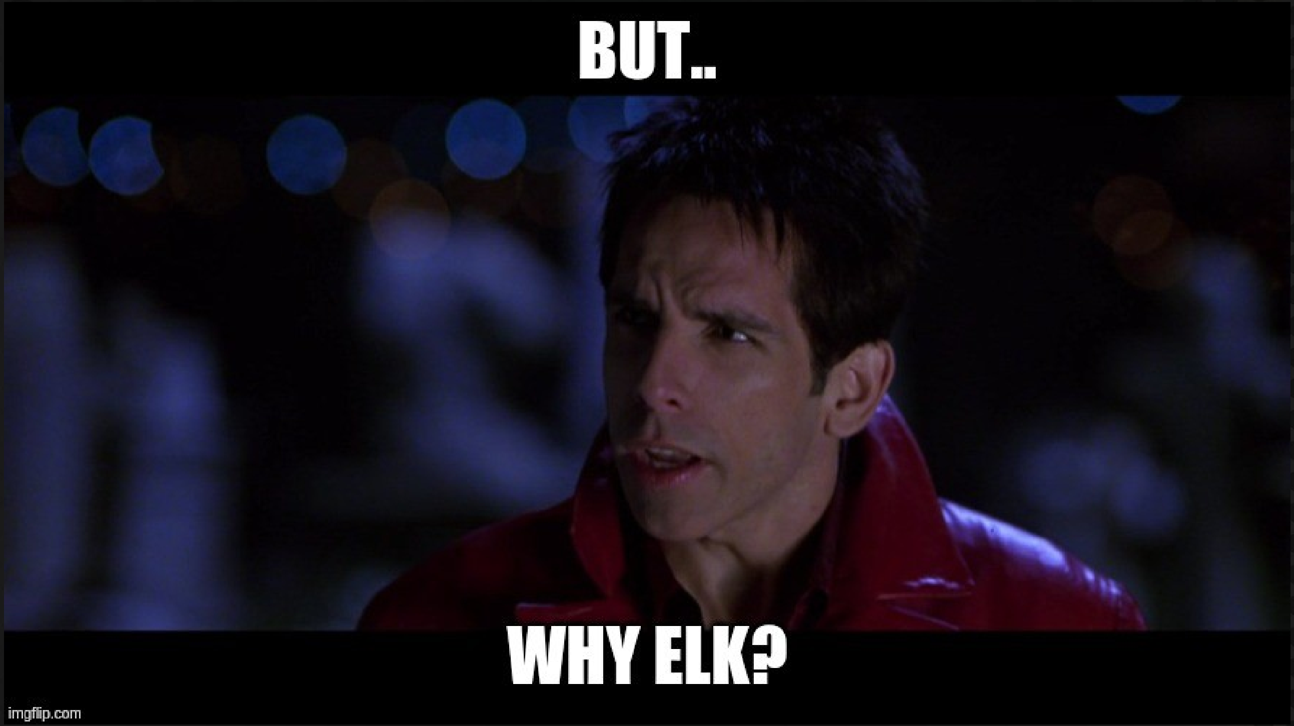
Source	Records
filebeat from [redacted] /log/messages	85
filebeat from [redacted] /messages	49
filebeat from [redacted] /var/log/messages	18
filebeat from [redacted]	16
filebeat from [redacted] /cron	1

Export: Raw Formatted

Source	Records
NetFlow from [redacted]	12,466
NetFlow from [redacted]	7,077
NetFlow from [redacted]	1,860
NetFlow from [redacted]	254
NetFlow from [redacted]	44

Export: Raw Formatted

No results found


BUT..
WHY ELK?
imgflip.com

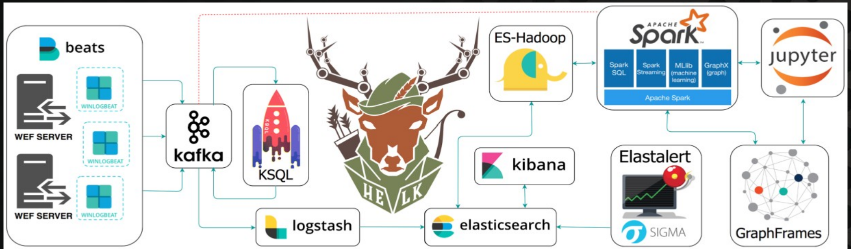
But all this is only as good as the data you feed it!

- Enter Sysmon
- The data you actually want
- Yes, there are some other Windows logs you would want as well
- Easy to get to Elasticsearch
  - Via Winlogbeat

Any time I can work Weird Al in…. It's a good time.

We Will Be Using HELK Today

- Still Alpha
- Still Alpha
- Pretty darn good
- Data normalization (we will be looking at some log files)
- Would not recommend for production
- Let’s begin!



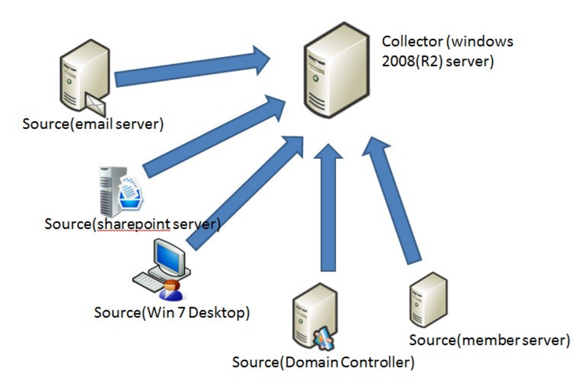
So many things… All the things...

Moving Forward

- Bringing in Mick for this…
- He will be showing us all the ELK rock
    - And the suck…
- So many variants
- You will most likely be mixing and matching

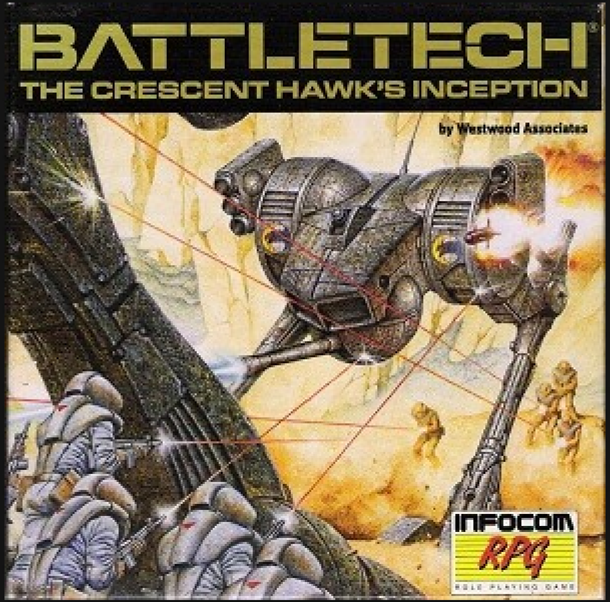
graylog

NXLog


Collector (windows 2008(R2) server)
Source(email server)
Source(sharepoint server)
Source(Win 7 Desktop)
Source(Domain Controller)
Source(member server)

Questions?

Answer!!


BATTLETECH®
THE CRESCENT HAWK'S INCEPTION
by Westwood Associates
INFOCOM
RPG
ROLE PLAYING GAME