Hunting Update

Joe Ten Eyck

Who am I?

- 15 Year Army Veteran
- 8 Years Information Security
  - Red and Blue
- 2 Years Target

The Task

- Significantly improve hunting!
- I don’t know what that is!
- Nobody else does either!

What it’s not.

- Detection
  - Artifact based
  - Known values/behaviors
  - Signature based
- Traditional IR
  - Artifact based
  - Take alert for x, evaluate
    - -good or bad
  - Work thru time

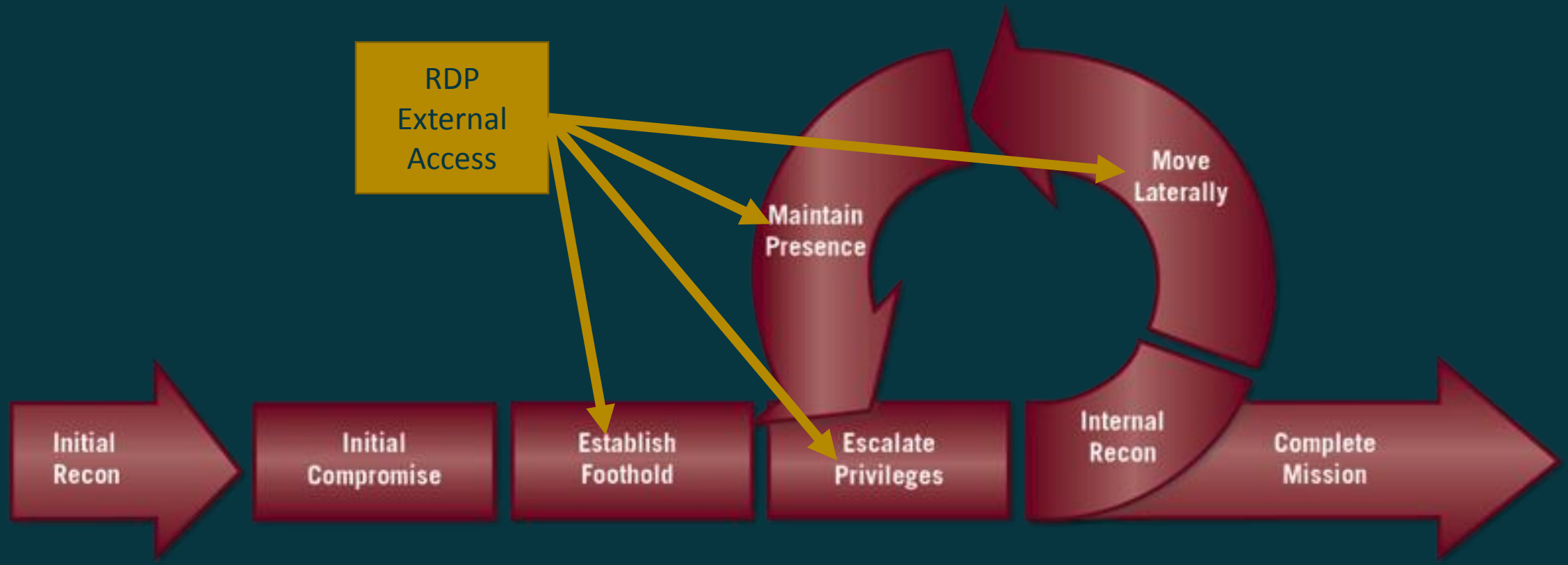
Nothing wrong with either one

- They serve their purpose
- But they don’t find unknown

Needed to fill gaps.

- Look for Unknowns
- Iterative
- Precipitated by need
- Data Analytics

Mapped to Attacker Lifecycle



Hunting is Different…

- Still Artifacts
- In Context
  - Time
    - network
  - Space
    - Host
- Attackers have patterns

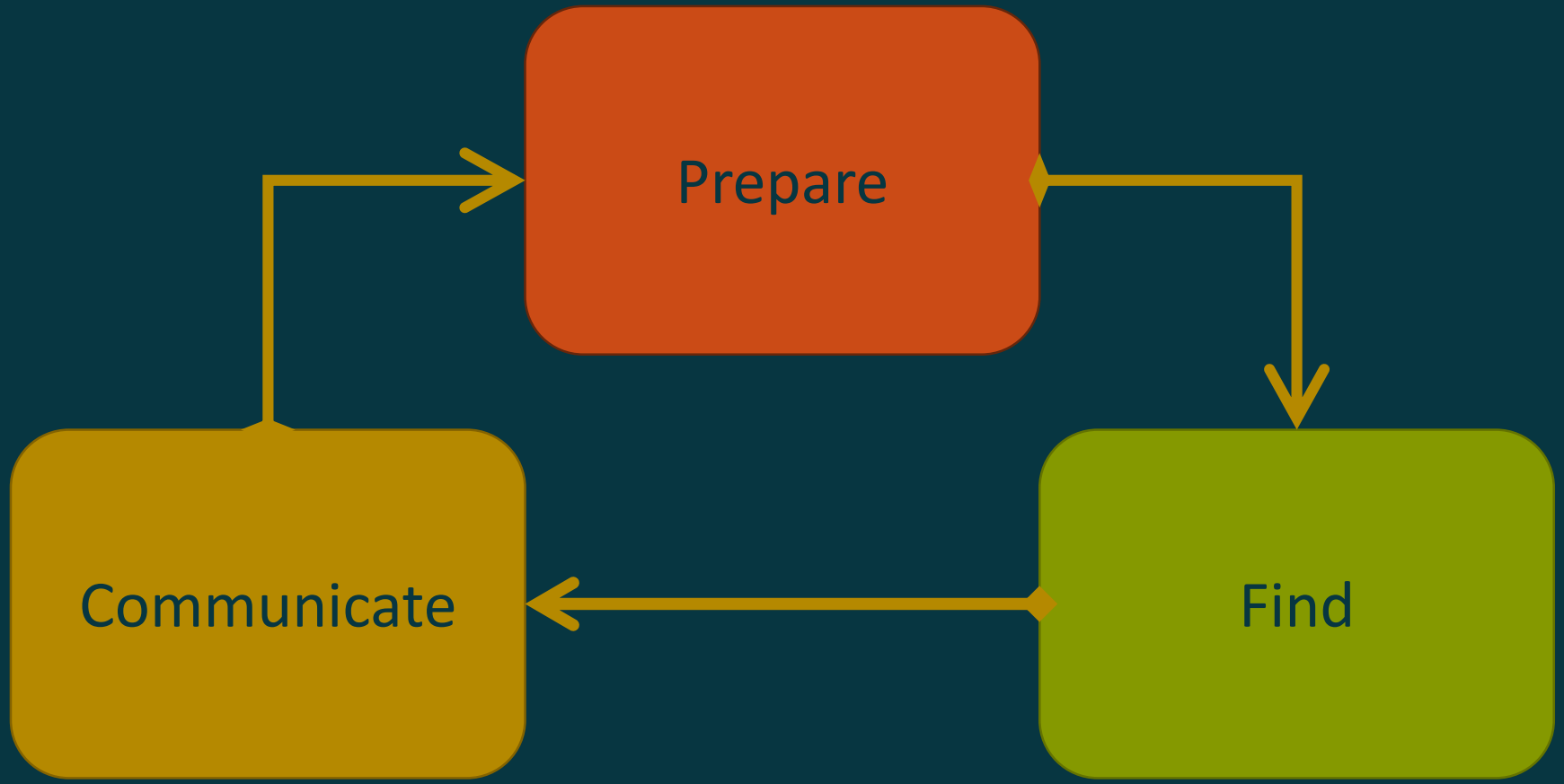
Mission Statement

Hunt team activities will use intelligence driven use cases to iteratively search the enterprise forest for advanced indicators of compromise missed by conventional detection methods. Our goal is to terminate ongoing malicious activity and produce actionable intelligence to improve Target’s security posture. Use cases will be generated using internal and open source intelligence, situational awareness of emerging and current threats, and available data about the current state of the enterprise network. Findings will be utilized to create cases for isolation and investigation, close detection gaps, and create actionable alerting.

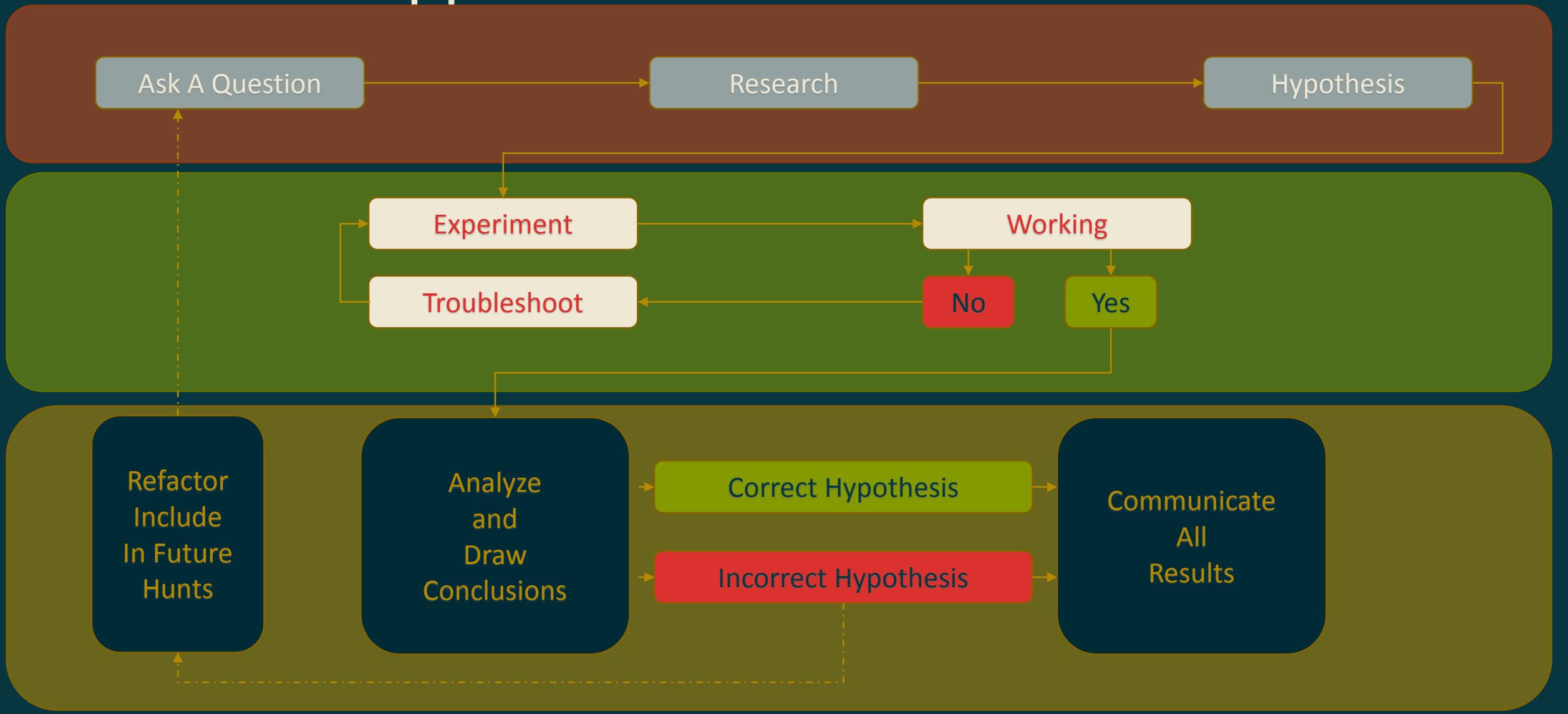
So now we need how?

- Easy to say what hunting is.
- How do I make it into a process for others to easily follow?
- I thought what we are doing is similar to any evidence based questions.

High Process



Process Applied



Relief

- Scientific Method
- Trust process to lead to outcomes
- We just need to communicate

We break communication down as

- Cases:
- Detection Gaps:
- Informational:

Current State

- What Hunting did to improve right now
  - Found x infections
  - This That etc.

- Look how cool I am

Future State

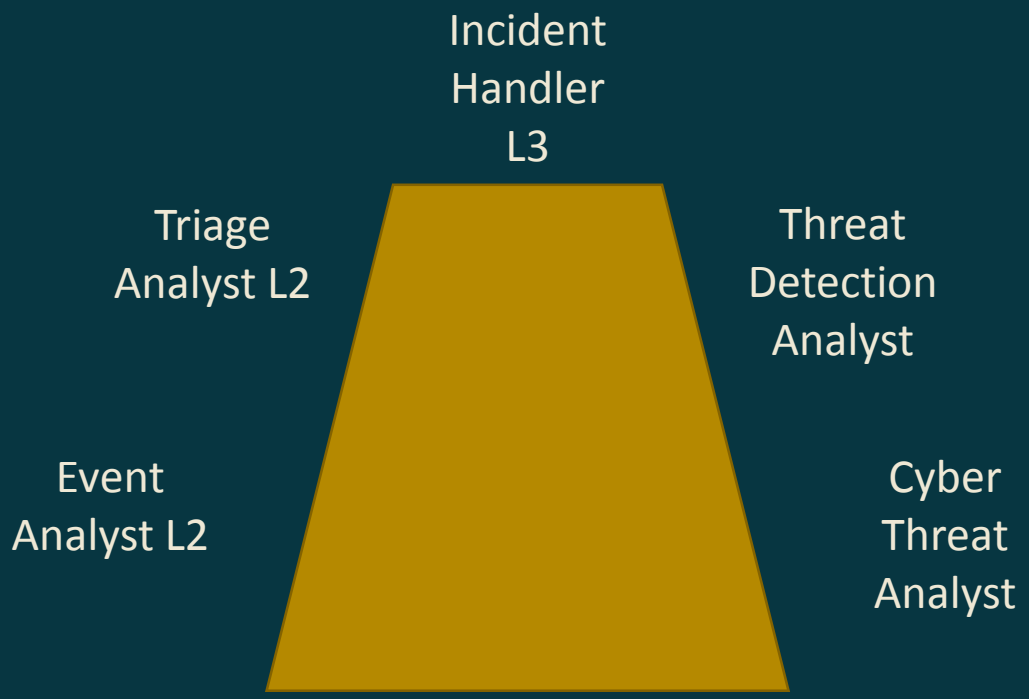
- Our IR is bigger, stronger, faster
- We now know x
- We can now find x

Building the Team

- Knowledge is power
- Not all about us
- Security can influence more than security…maybe

Seats at the table

- Not a function of only IR
- Growth requires the participation of all key-players
- Read-ON
- Read-Off
- Planning



Practical Application

- Playbooks :
  - Threathunting.net
  - Track historical knowledge
  - Reference beginning
- Read-On Read-Off
  - Communicate to future and leadership

Autoruns Analysis

Purpose: Find malware persistence by examining common mechanisms across a netw

HMLO: D=1, A=2, T=3

Hunting Maturity Model

Data Required:

- List of programs configured to start at boot/logon time on each endpoint
- Splunk via Tanium

Collection Considerations:

- Tanium autorun against a specified list of hosts.
- Tanium/Splunk does not different most current from last run (alleged fix)
- No knowledge of hosts coverage, possible null byte issues

Analysis Techniques:

- Stack counting
- string matching
- outlier detection
- Known bad correlations

Description

Gather autoruns data from endpoints across the network and look for:

- Executable starting out of `c:programdata`, recycle bin, appdata area, `%temp%`
- Unsigned executables (not currently in Tanium)
- Shortest / longest filenames
- GUID filenames
- Rare executable filenames or directories
- iPython correlation between bigred and vt

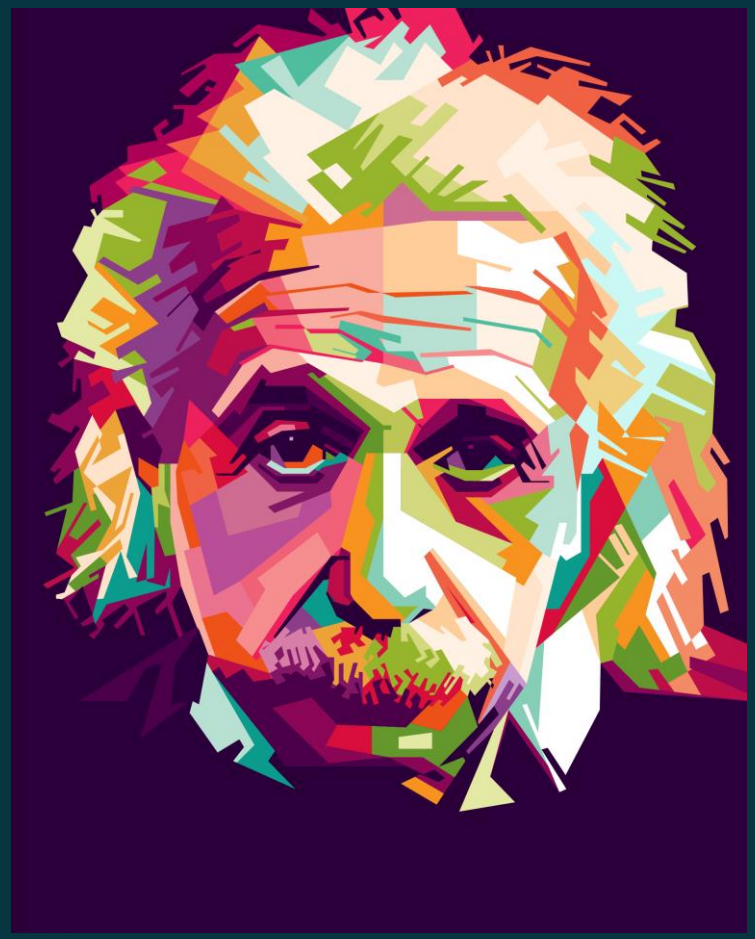
More Info

- **Intrusion Hunting for the Masses**, David Sharpe (HackMiami 2016)

Outside Participation

- Not just IR aanlyst

Einstein vs High School Teacher

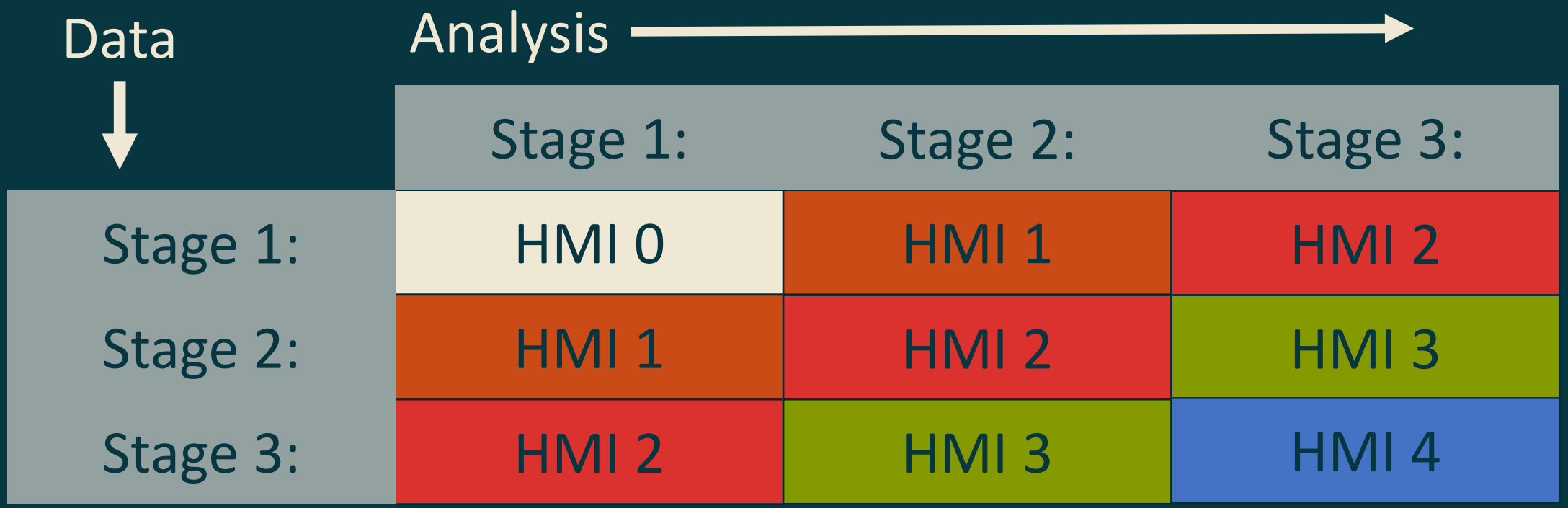


VS

Scientific Process

- Relies on two legs
  - The data used
  - The process/knowledge of analyst

Hunting Maturity Index



Not a Linear measurement

- Data
  - What are we looking at?

- Analysis
  - Who and how are we looking?

Three Stages Each Way

- Reflects growth of People
  - Analysis
    - From uninformed to highly knowledgeable

- Reflects growth of Technology
  - Data
    - From standard to use specific

Data Stage 1:

- Standard byproduct data sets
  - Not specific
  - Functional data
  - Think Firewall logs

Data Stage 2:

- Data Collection
  - SIEM
  - Data for data’s sake
  - Correlation

Data Stage 3:

- For hunting
  - Data that is only valuable for pattern based big picture searches
  - Not useful for alerting
  - Probably difficult and expensive

Analysis Stage 1:

- Others automation
- Entry level
- Often tied to vendor solutions

Analysis Stage 2:

- Research based
  - What do we know?
  - How do we identify?
  - What is it in my environment?
    - Allow investment in analyst!!!!

Analysis Stage 3:

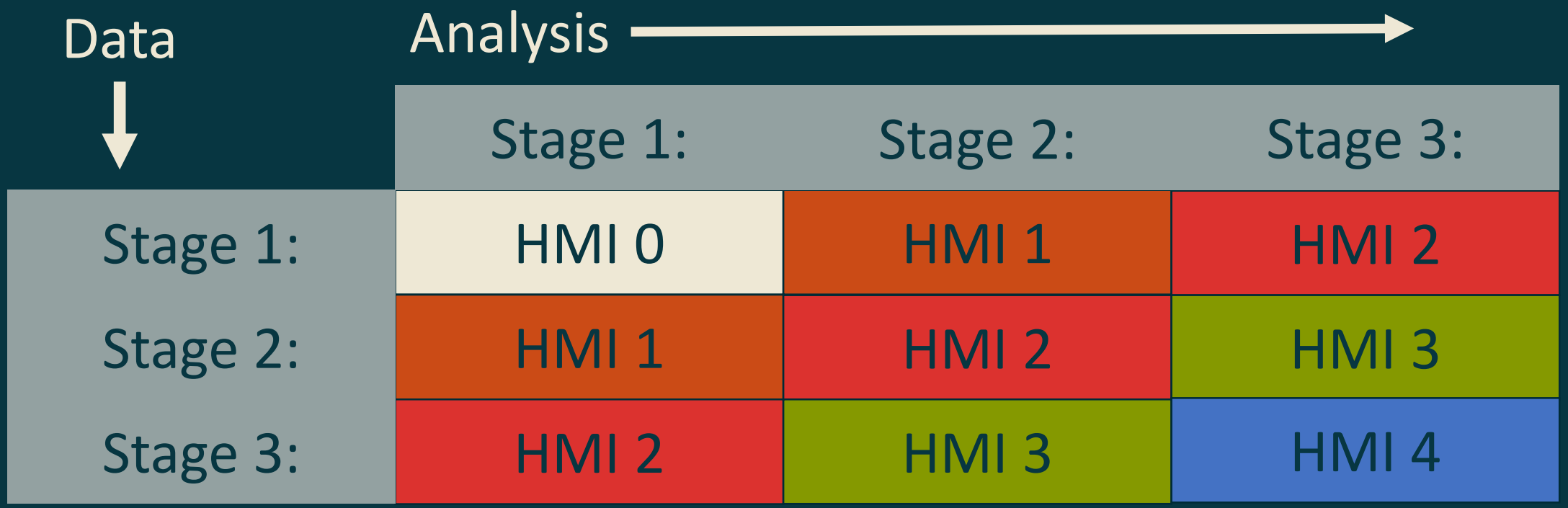
- Heavy investment in analyst!!!
- Self made automation.
- Allows rapid iteration.

Maturity Phases PCR Example

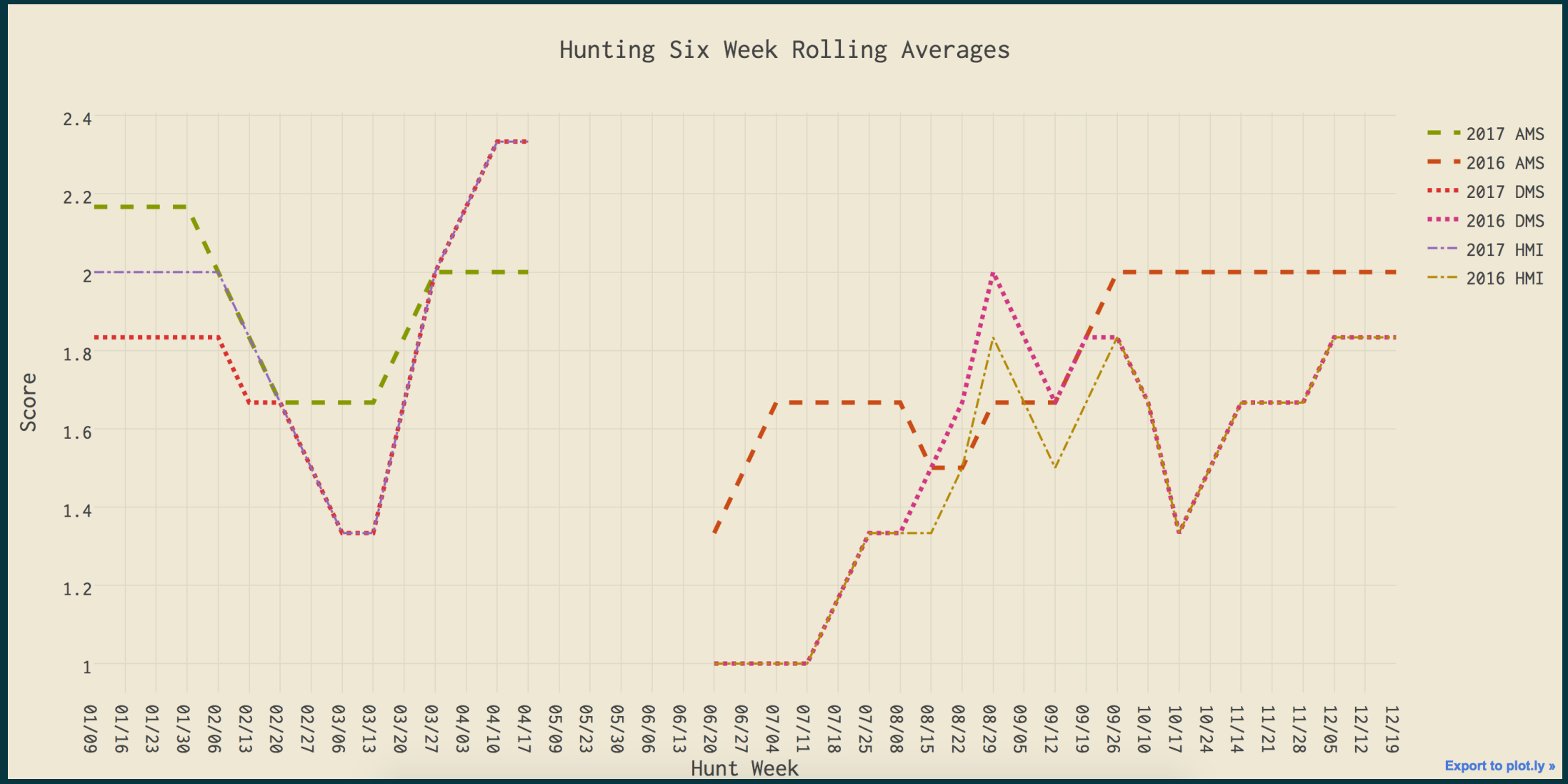
Data Stages: Proxy Logs	Analysis Stages:
Examine Logs, Compare Singular Events - Bytes in vs Bytes out but only on single connection	Just evaluating individual connections.
Examine Groups of Logs - Group by user - Bytes in vs Bytes out over period of time - Virus Total and Alexa to Reduce Data Set	Requires Analyst to engage in data and develop plan for processing larger datasets.
Weigh Data against Itself - 30 day average of PCR - 24 hr as change against 30 day average	Requires the analyst to develop a plan to look at large data sets and plan an evaluation technique. Reduces the hunt to what is critical. Use of visualization for rapid iteration.

Which left us with

Hunting Maturity Index



Overtime


Hunting Six Week Rolling Averages
Score
Hunt Week
2.4
2.2
2
1.8
1.6
1.4
1.2
1
01/09
01/16
01/23
01/30
02/06
02/13
02/20
02/27
03/06
03/13
03/20
03/27
04/03
04/10
04/17
05/09
05/23
05/30
06/06
06/13
06/20
06/27
07/04
07/11
07/18
07/25
08/08
08/15
08/22
08/29
09/05
09/12
09/19
09/26
10/10
10/17
10/24
11/14
11/21
11/28
12/05
12/12
12/19
2017 AMS
2016 AMS
2017 DMS
2016 DMS
2017 HMI
2016 HMI
Export to plot.ly »