THINGS THAT MAKE YOU GO HMM

Using a Simple Hunting Maturity Model to Establish and Improve Your Threat Hunting Program

David J. Bianco

Principal Engineer, Cybersecurity, Target

@DavidJBianco

Does your organization perform threat hunting?

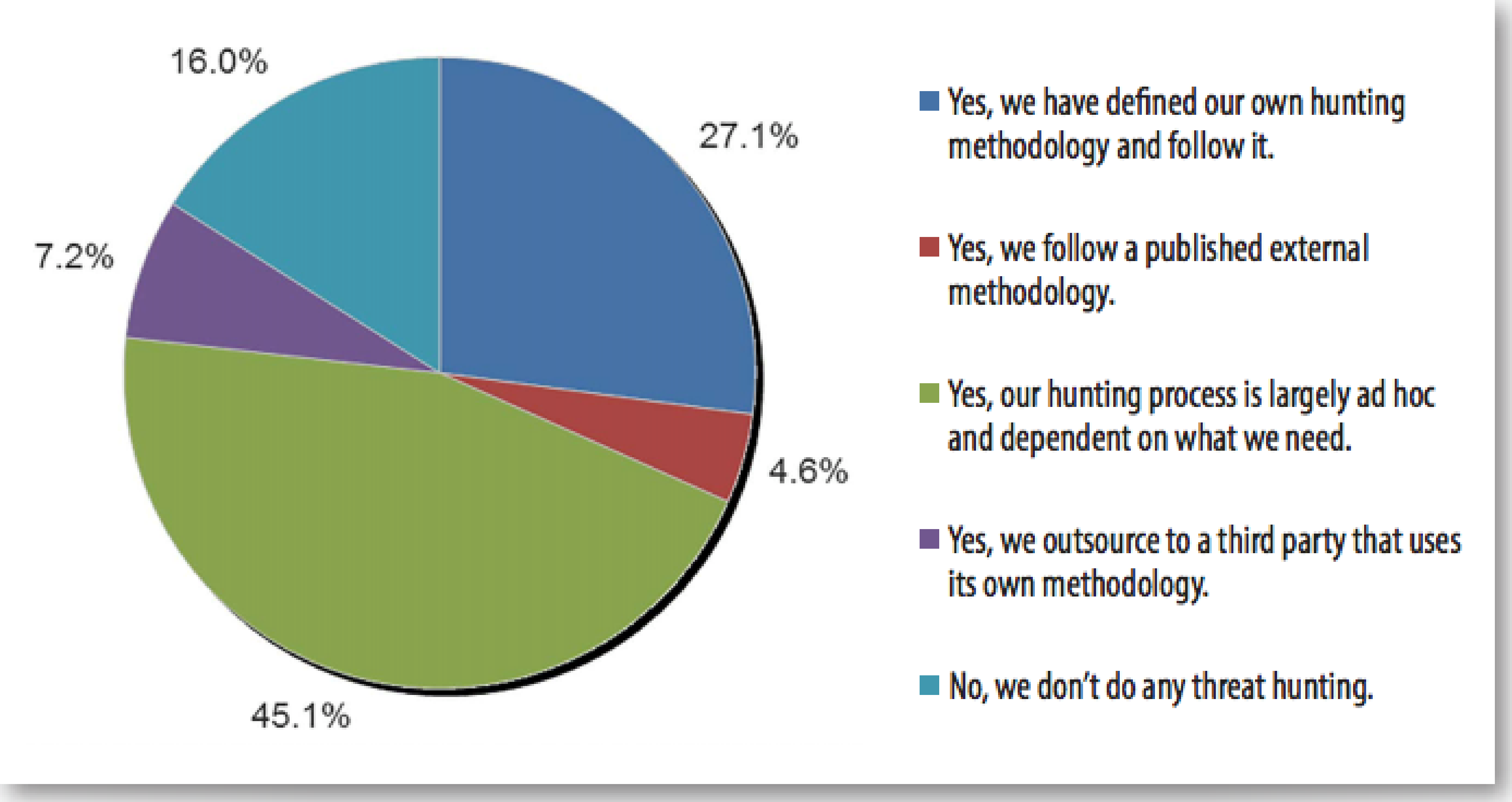


Figure 2. Threat Hunting in Practice

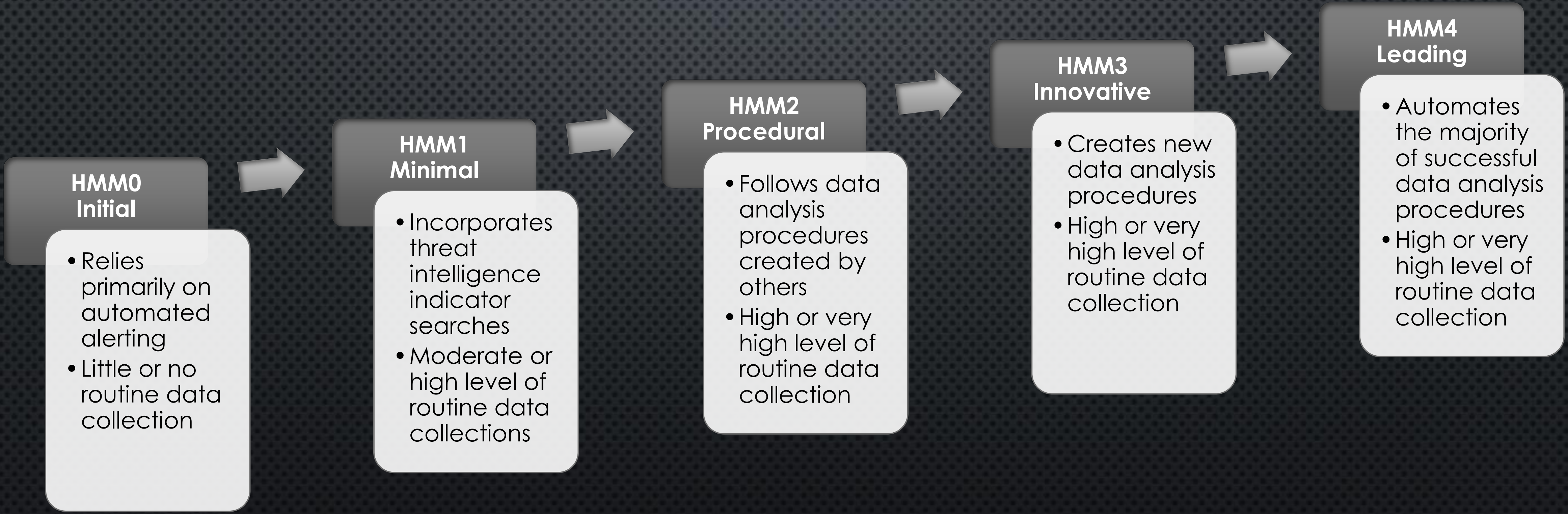
https://www.sans.org/reading-room/whitepapers/analyst/hunter-strikes-back-2017-threat-hunting-survey-37760

> “THE COLLECTIVE NAME FOR ANY MANUAL OR MACHINE-ASSISTED TECHNIQUES DESIGNED TO IDENTIFY SECURITY INCIDENTS [THAT AUTOMATED SOLUTIONS MISSED].”
>
> My definition of Threat Hunting

Key takeaway: a human is always involved. Fully automated “hunting” is just detection, not hunting!

Corollary: The purpose of hunting is not to find security incidents. It’s to find better ways to find security incidents and to drive improvements to automated detection.

THE HUNTING MATURITY MODEL (HMM)



HMM0
Initial

- Relies primarily on automated alerting
- Little or no routine data collection

HMM1
Minimal

- Incorporates threat intelligence indicator searches
- Moderate or high level of routine data collections

HMM2
Procedural

- Follows data analysis procedures created by others
- High or very high level of routine data collection

HMM3
Innovative

- Creates new data analysis procedures
- High or very high level of routine data collection

HMM4
Leading

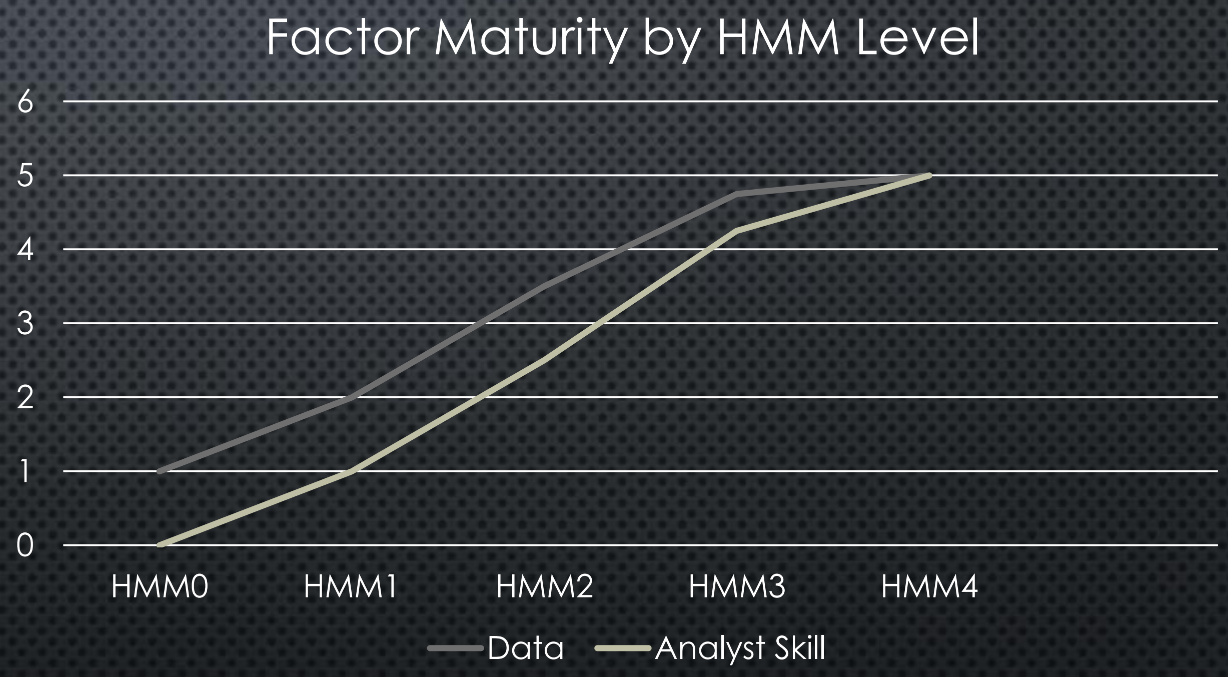
- Automates the majority of successful data analysis procedures
- High or very high level of routine data collection

http://detect-respond.blogspot.com/2015/10/a-simple-hunting-maturity-model.html

MATURITY TRENDING

HMM IS MEASURED ON TWO AXES:

- QUALITY AND AMOUNT OF **DATA** HUNTERS HAVE ACCESS TO
- ANALYTIC **SKILLSET** OF THE HUNTERS ACROSS THE ORGANIZATION



$$HMM = \min(HMM_{data}, HMM_{skills})$$

HMM0: AN ALERT-DRIVEN SOC

HMM0
Initial

- Relies primarily on automated alerting
- Little or no routine data collection

HMM0 orgs focus on **alerts**.

They may incorporate IDS/SIEM rule feeds or vendor detection updates, but are primarily reactive.

They often collect very little additional data beyond what is required to drive the alerting.

Analyst access to the data may or may not be easy & quick.

Detection is totally automated, and priorities often driven by outside forces (vendors or ruleset providers).

HMM1: INDICATOR SEARCH

HMM1
Minimal

- Incorporates threat intelligence indicator searches
- Moderate or high level of routine data collections

HMM1 orgs focus on **searching for IOCs**.

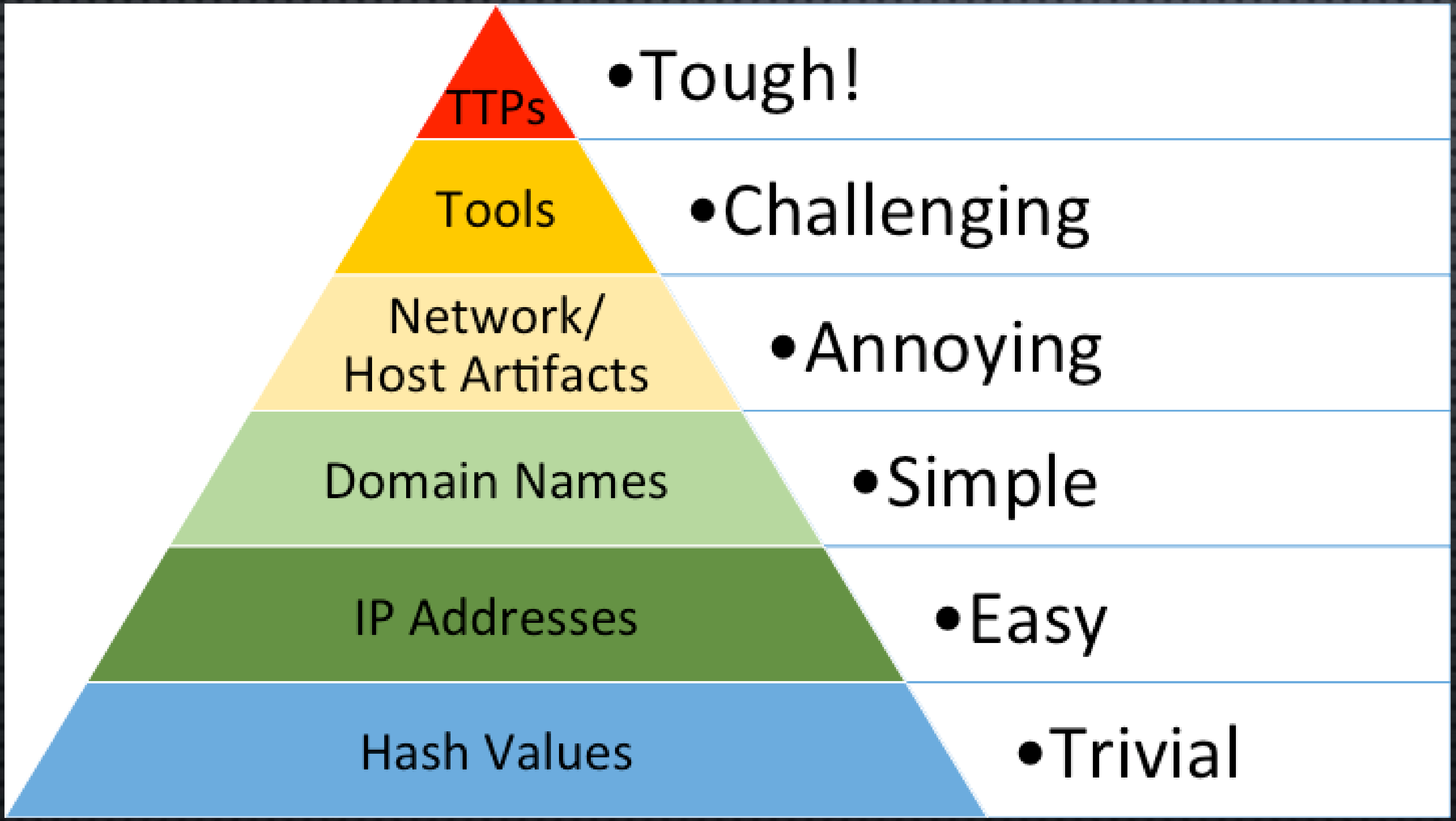
Automated indicator matching (technically HMM0), plus manual searches for indicators from vendor reports or other sources.

May collect a significant amount of data, since you never know where those IOCs will show up.

Usually offers quick, convenient search platform.

Most common HMM level right now.

Technically proactive, therefore the first level where true hunting occurs.



http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

HMM2+

HMM1 IOC Search

HMM0 Automated indicator matching

HMM2: FOLLOWING ESTABLISHED HUNT PROCEDURES

HMM2 Procedural

- Follows data analysis procedures created by others
- High or very high level of routine data collection

HMM2 orgs **collect hunting procedures from external sources**.

Enterprise visibility is a priority, therefore collecting lots of data for hunting.

Often has an organizational hunting strategy, backed up by hunts collected from peers, conference presentations, blogs or other sources (**ThreatHunting.net**).

Hunters adapt recipies to their environment and interpret results.

The most appropriate first goal for many orgs.

HMM3: CREATING ORIGINAL HUNTS

HMM3 Innovative

- Creates new data analysis procedures
- High or very high level of routine data collection

HMM3 orgs **create their own hunts**.

Very high level of data collection, giving hunters a wide variety of choice in what to hunt and where they can pivot.

May begin to incorporate data science, machine learning or other advanced analysis disciplines.

Often the source of published hunts used by HMM2 orgs.

I'd like to see these orgs to **publish more**!

HMM4: AUTOMATED DETECTION IMPROVEMENT

HMM4
Leading

- Automates the majority of successful data analysis procedures
- High or very high level of routine data collection

HMM4 orgs **automate successes**.

Most hunting orgs operate at a scale that makes manual processes impractical for detection. Automation is critical for defensible networks.

Suitable automation (or semi-automation) may include:

- Signatures (!!)
- Analytics which create alerts
- Dashboards & reports
- Risk/reputation scoring

Hunting is the engine which drives improvements to the automated processes.

IT'S THE JOURNEY, NOT THE DESTINATION

There's no single starting point that works for everyone.

The HMM is your map.

Figure out where you already are, then make a plan to get to the next level.

There's no rush! Feel free to get off the bus for a while and hop back on later.

Each level is a victory. Celebrate your successes along the way!

EXAMPLE/MADE-UP CASE STUDY #1

Current State	Level Up
Consumes both feeds and relevant intel reports for detection and response. Good perimeter visibility: • Netflow or equivalent • HTTP proxy logs • DMZ/exposed server process creation logs Easy access to collected data via ELK.	Set hunting/detection priorities. Find relevant hunts via **ThreatHunting.net** or other sources. Expand visibility to support priorities: • More endpoint monitoring on infrastructure and key assets • Deploy internal NSM sensors Establish hunting function with regular rhythym.
HMM1	**HMM2**

EXAMPLE/MADE-UP CASE STUDY #2

Current State	Level Up
Regular hunting with established playbooks.	Modify/extend existing hunts to cover additional detection requirements.
Extensive internal and perimeter visibility, both network and endpoint.	Mix & match familiar analysis techniques to create new hunts.
Starting to come up with custom detection requirements.	Train hunters for analysis and/or partner with data scientists.
HMM2	**HMM3**

“

I HAVE A QUESTION AND/OR WISH TO MAKE A SHORT SPEECH…

”

DAVID J. BIANCO

@DavidJBianco

ThreatHunting.Net

Detect-respond.blogspot.com