Cyber Threat Intelligence: A Team Sport

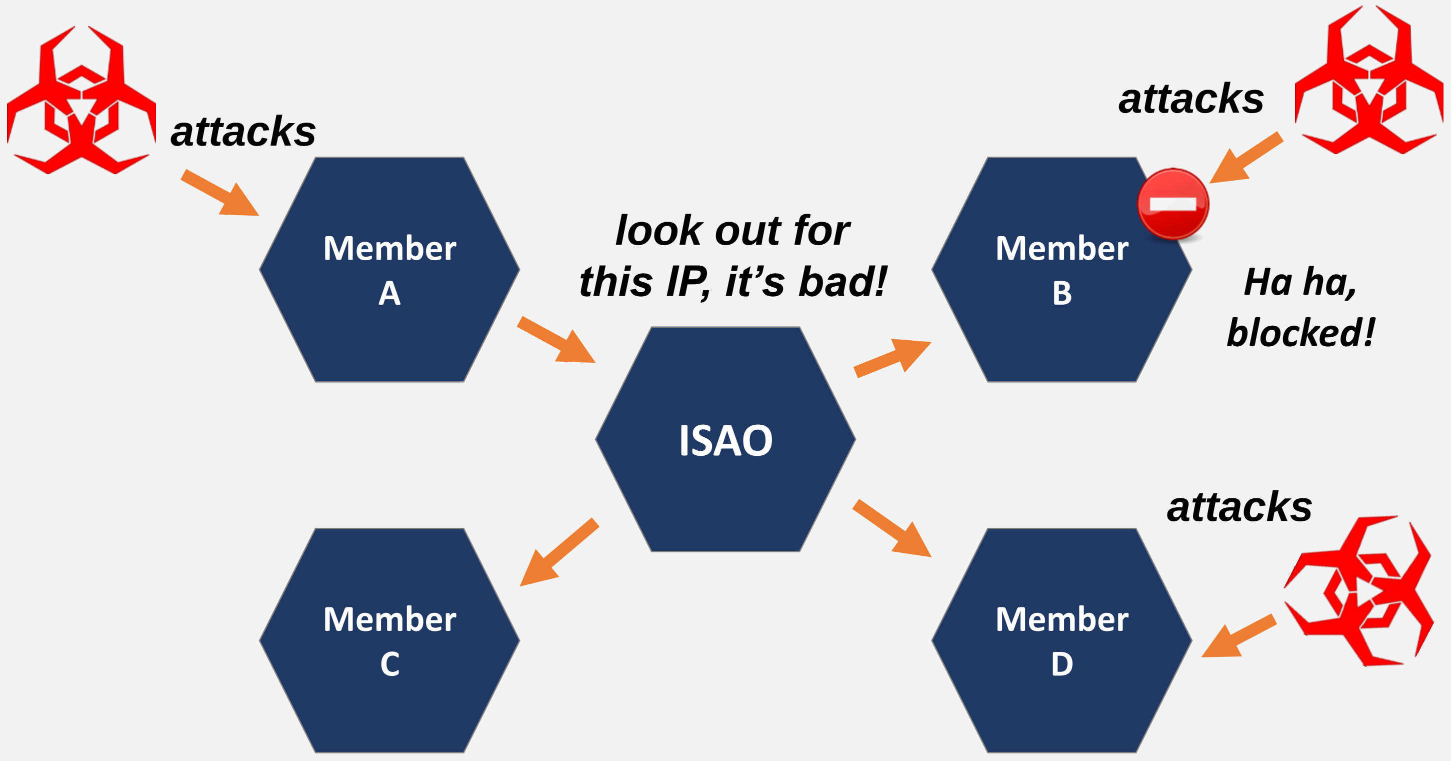
Collaborative Analytic Development

John Wunder

The MITRE Corporation

Approved for Public Release; Distribution Unlimited.
Case Number 17-4328

Indicators of compromise are great



attacks

Member A

look out for this IP, it's bad!

ISAO

attacks

Member B

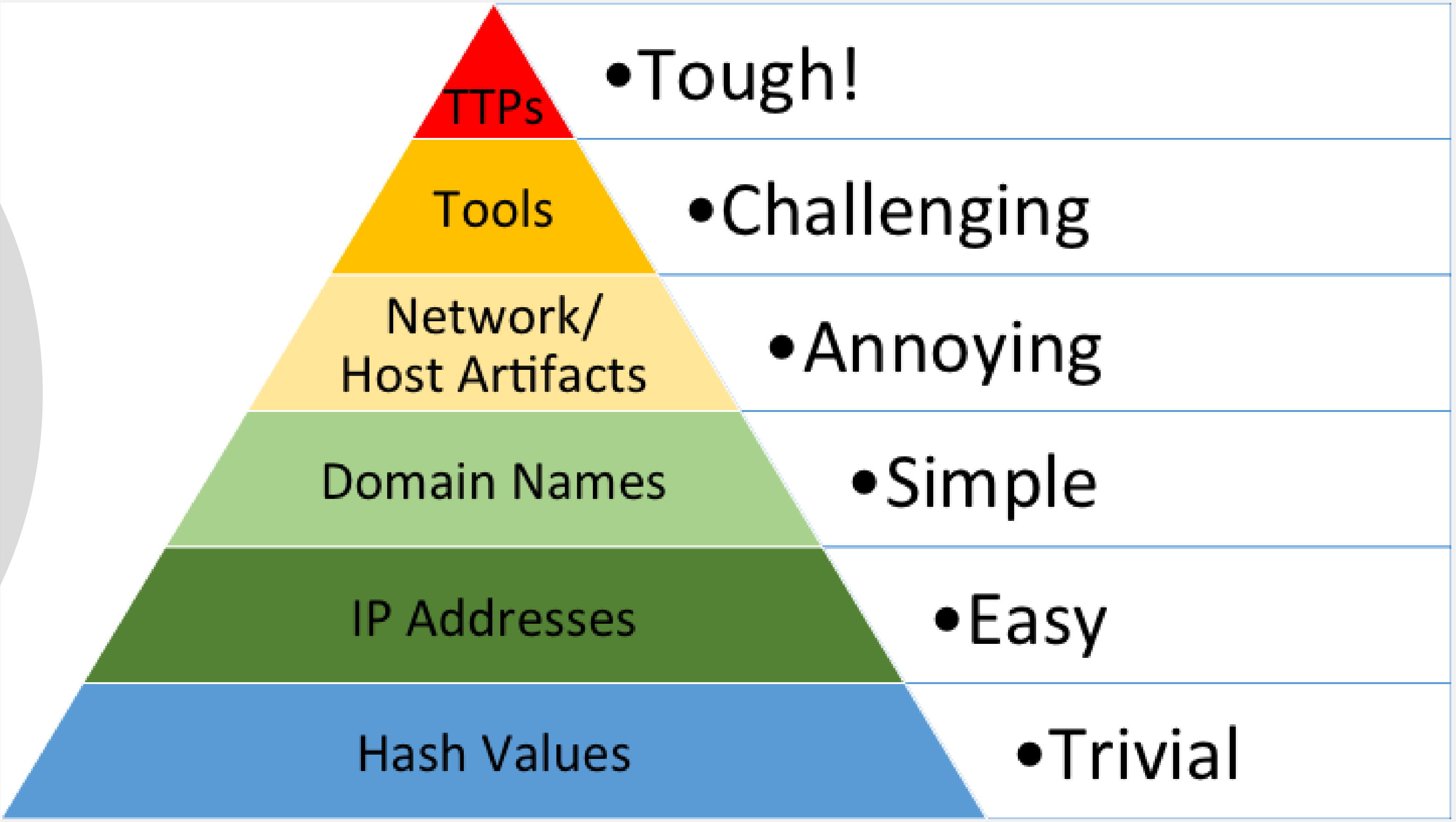
Ha ha, blocked!

Member C

attacks

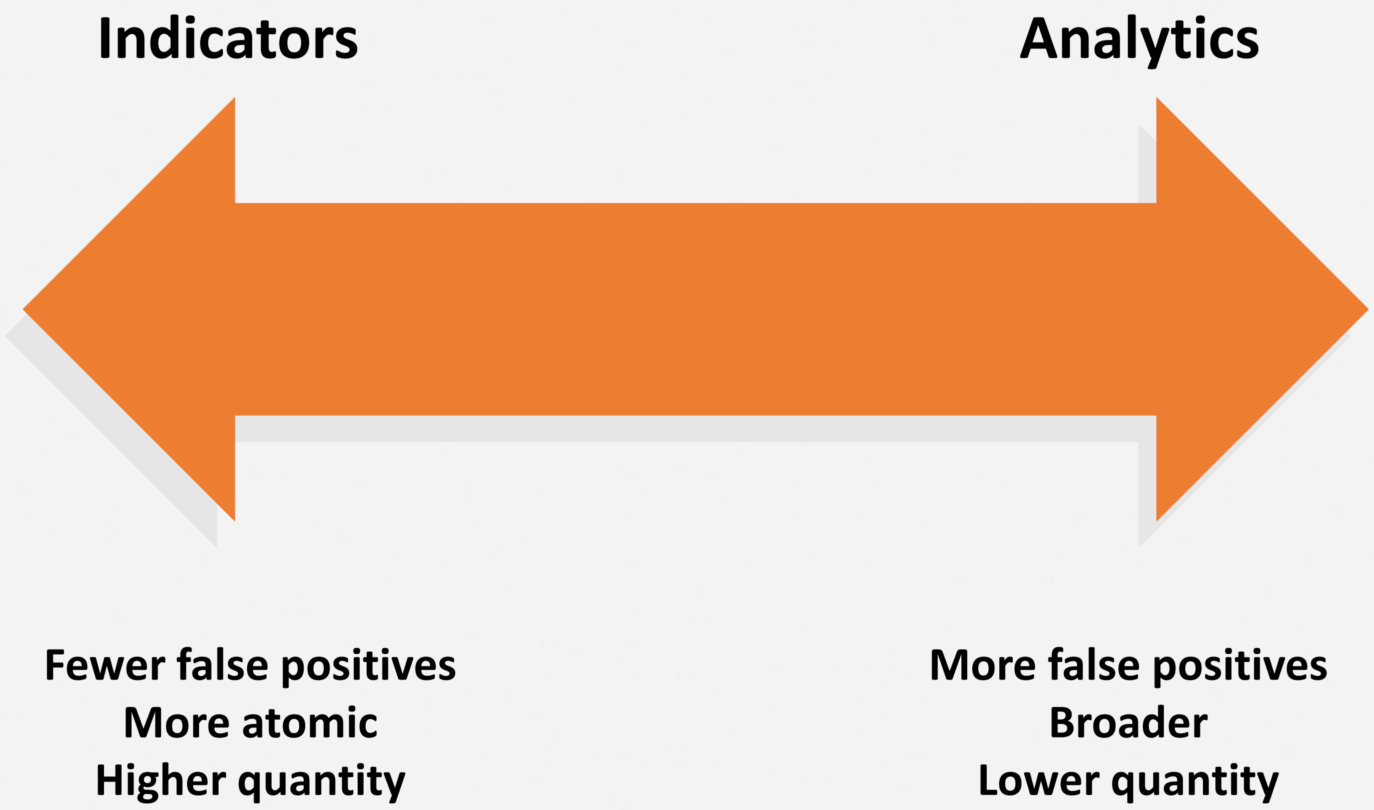
Member D

Analytics move up the (obligatory) pyramid of pain



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

What’s an analytic, *really*?

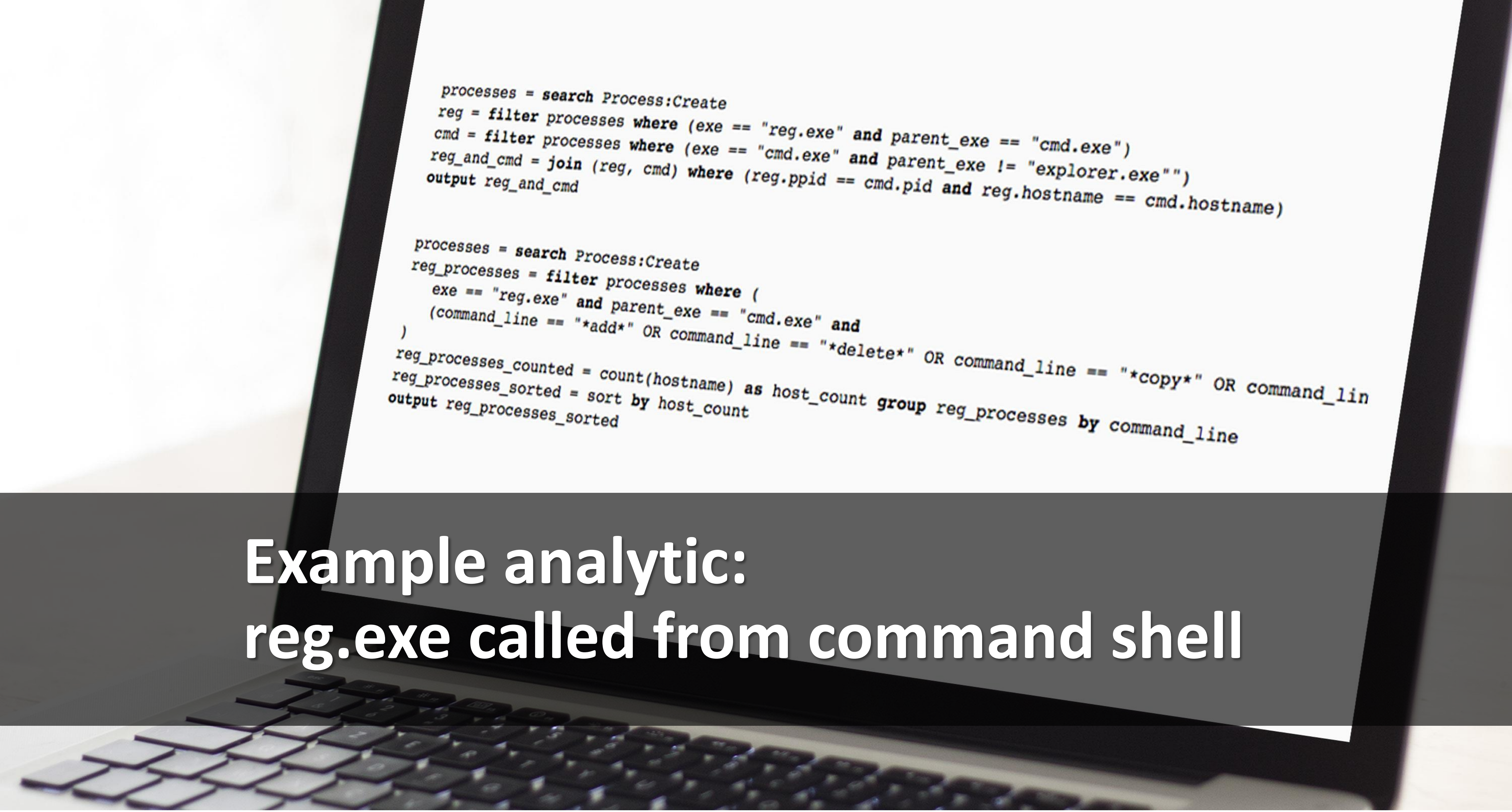


Indicators

Analytics

Fewer false positives
More atomic
Higher quantity

More false positives
Broader
Lower quantity



```
processes = search Process:Create
reg = filter processes where (exe == "reg.exe" and parent_exe == "cmd.exe")
cmd = filter processes where (exe == "cmd.exe" and parent_exe != "explorer.exe"")
reg_and_cmd = join (reg, cmd) where (reg.ppid == cmd.pid and reg.hostname == cmd.hostname)
output reg_and_cmd


processes = search Process:Create
reg_processes = filter processes where (
  exe == "reg.exe" and parent_exe == "cmd.exe" and
  (command_line == "*add*" OR command_line == "*delete*" OR command_line == "*copy*" OR command_lin
)
reg_processes_counted = count(hostname) as host_count group reg_processes by command_line
reg_processes_sorted = sort by host_count
output reg_processes_sorted
```

Example analytic:
reg.exe called from command shell

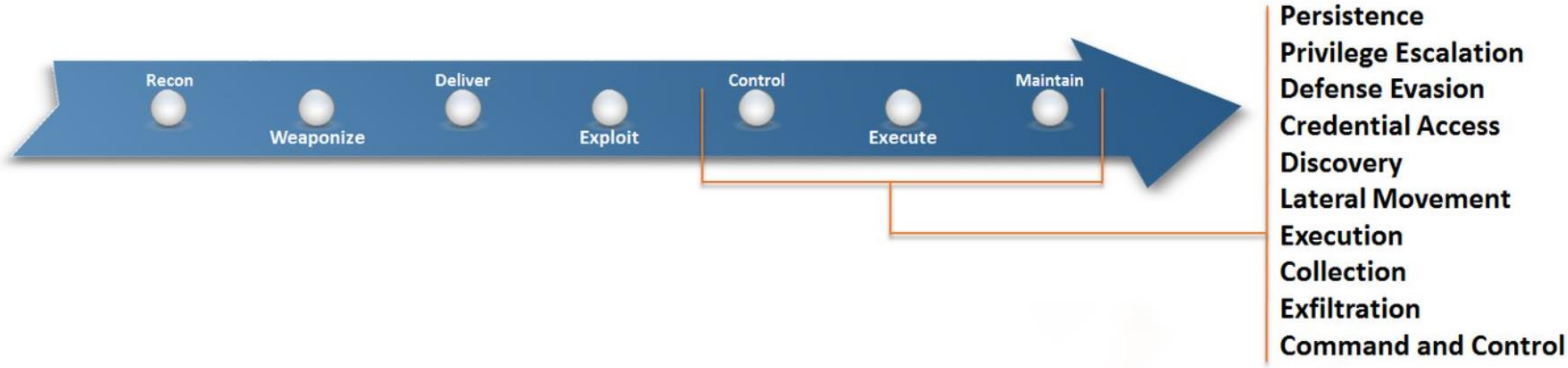
We need an organizing framework.

Analytics are great, but they need to be put into the context of which adversary technique they detect

- How do you know which ones you need?
- If you have some analytics shared with you, how do you know whether they’re additive or duplicative?
- If you see a new technique being used in a threat report, how do you know if your current set of analytics will cover it?

ATT&CK™

ATT&CK™ is a MITRE-developed, globally-accessible knowledge base of adversary tactics and techniques based on real-world observations of adversaries’ operations against computer networks.



Recon
Weaponize
Deliver
Exploit
Control
Execute
Maintain

Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Execution
Collection
Exfiltration
Command and Control

What's in ATT&CK™

1. List of techniques used by adversaries for each phase of the kill chain

2. Possible methods of detection and mitigation

3. Published references of adversary use of techniques

Image source: www.hasbro.com

Mr. Potato Head is a registered trademark of Hasbro Inc.

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
DLL Search Order Hijacking			Brute Force	Account Discovery	Windows Remote Management		Audio Capture	Automated Exfiltration	Commonly Used Port
Legitimate Credentials			Credential Dumping	Application Window Discovery	Third-party Software		Automated Collection	Data Compressed	Communication Through Removable Media
Accessibility Features		Binary Padding			Application Deployment Software	Command-Line	Clipboard Data	Data Encrypted	
AppInit DLLs		Code Signing	Credential Manipulation	File and Directory Discovery		Execution through API	Data Staged	Data Transfer Size Limits	Connection Proxy
Local Port Monitor		Component Firmware			Exploitation of Vulnerability	Execution through Module Load	Data from Local System	Exfiltration Over Alternative Protocol	Custom Command and Control Protocol
New Service		DLL Side-Loading	Credentials in Files	Local Network Configuration Discovery			Data from Network Shared Drive		
Path Interception		Disabling Security Tools	Input Capture		Logon Scripts	Graphical User Interface		Exfiltration Over Command and Control Channel	Custom Cryptographic Protocol
Scheduled Task		File Deletion	Network Sniffing	Local Network Connections Di	Pass the Hash	InstallUtil	Data from Removable Media		
File System Permissions Weakness		File System Logical Offsets	Two-Fa						
Service Registry Permissions Weakness									
Web Shell		Indicator Blocking							
Authentication Package	Exploitation of Vulnerability								
	Bypass User Account Control								
Bootkit	DLL Injection								
Component Object Model Hijacking		Component Object Model Hijacking							
Basic Input/Output System		Indicator Removal from Tools							
Change Default File Association		Indicator Removal on Host							
Component Firmware		Install Root Certificate							Protocol
External Remote Services		InstallUtil							
Hypervisor		Masquerading							
Logon Scripts		Modify Registry							
Modify Existing Service		MSBuild							
Netsh Helper DLL		Network Share Removal							
Redundant Access		NTFS Extended Attributes		System Time Discovery					
Registry Run Keys / Start Folder		Obfuscated Files or Information							
Security Support Provider		Process Hollowing							
Shortcut Modification		Redundant Access							
Windows Management Instrumentation Event Subscription		Regsvcs/Regasm							
		Regsvr32							
		Rootkit							
Winlogon Helper DLL		Rundll32							
		Scripting							
		Software Packing							
		Timestomp							

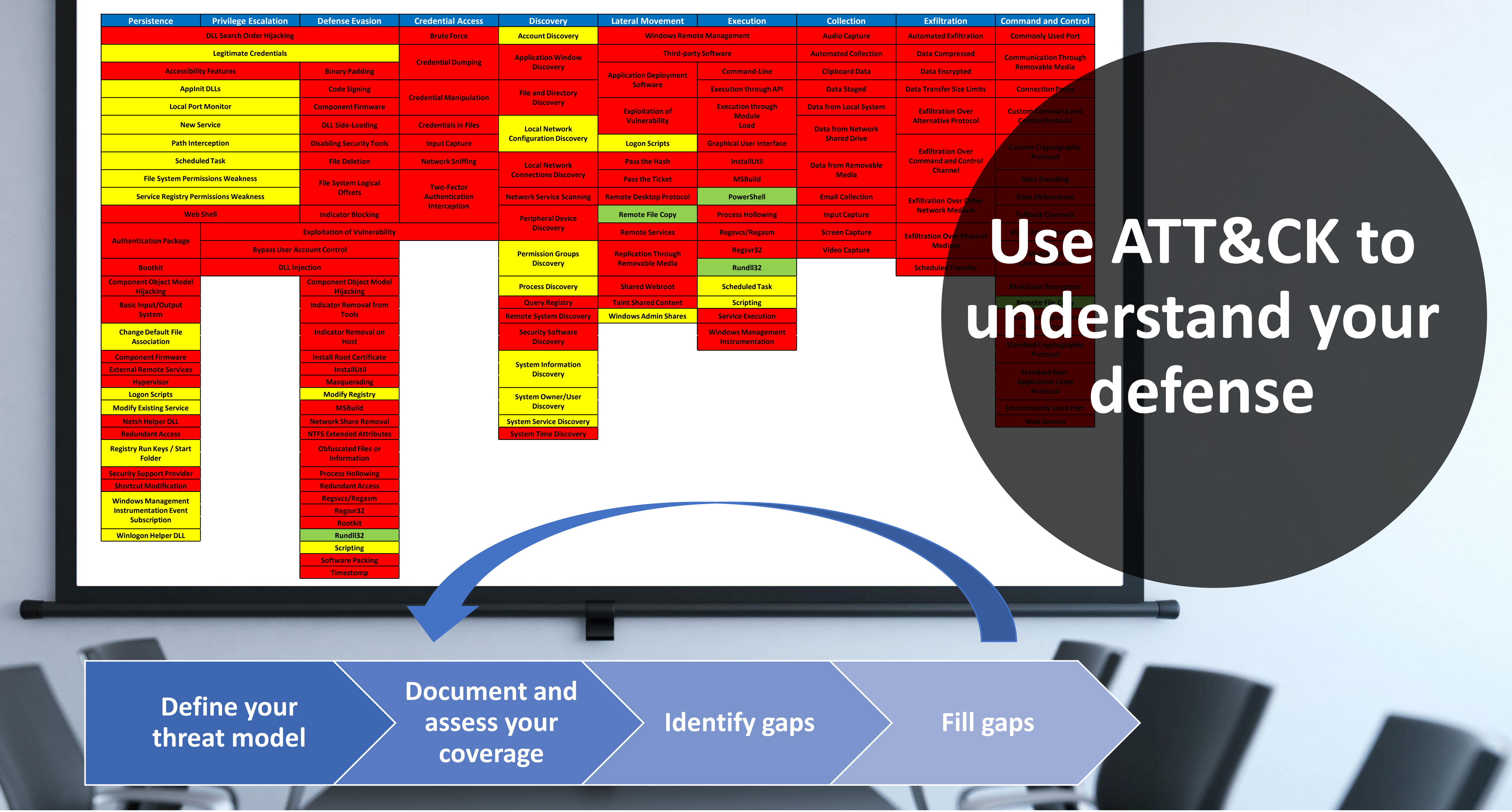
Enables pivoting between red team and blue team

Decouples the problem from the solution

Transforms thinking by focusing on post-exploit adversary behavior

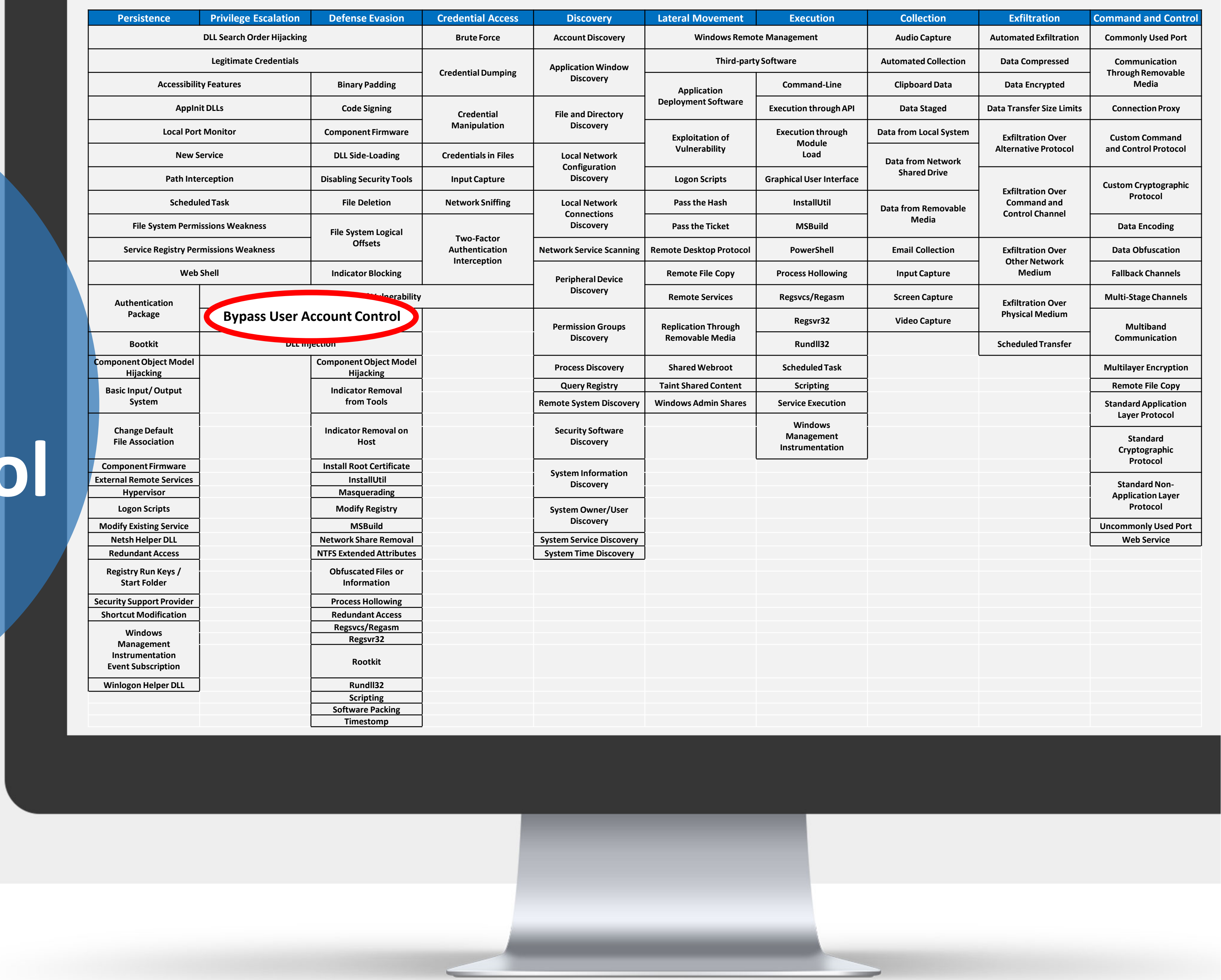
MITRE

Use ATT&CK to understand your defense



Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
DLL Search Order Hijacking	DLL Search Order Hijacking	DLL Search Order Hijacking	Brute Force	Account Discovery	Windows Remote Management	Windows Remote Management	Audio Capture	Automated Exfiltration	Commonly Used Port
Legitimate Credentials	Legitimate Credentials	Legitimate Credentials	Credential Dumping	Application Window Discovery	Third-party Software	Third-party Software	Automated Collection	Data Compressed	Communication Through Removable Media
Accessibility Features	Accessibility Features	Binary Padding	Credential Manipulation	File and Directory Discovery	Application Deployment Software	Command-Line	Clipboard Data	Data Encrypted	Connection Proxy
AppInit DLLs	AppInit DLLs	Code Signing	Credentials in Files	Local Network Configuration Discovery	Exploitation of Vulnerability	Execution through API	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Local Port Monitor	Local Port Monitor	Component Firmware	Input Capture	Local Network Connections Discovery	Logon Scripts	Execution through Module Load	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
New Service	New Service	DLL Side-Loading	Network Sniffing	Network Service Scanning	Pass the Hash	Graphical User Interface	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Path Interception	Path Interception	Disabling Security Tools	Two-Factor Authentication Interception	Peripheral Device Discovery	Pass the Ticket	InstallUtil	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Scheduled Task	Scheduled Task	File Deletion	Exploitation of Vulnerability	Permission Groups Discovery	Remote Desktop Protocol	MSBuild	Email Collection	Exfiltration Over Physical Medium	Fallback Channels
File System Permissions Weakness	File System Permissions Weakness	File System Logical Offsets		Process Discovery	Remote File Copy	PowerShell	Input Capture	Scheduled Transfer	Multi-Stage Channels
Service Registry Permissions Weakness	Service Registry Permissions Weakness	Indicator Blocking		Query Registry	Remote Services	Process Hollowing	Screen Capture		Multiband Communication
Web Shell	Web Shell	Exploitation of Vulnerability		Remote System Discovery	Replication Through Removable Media	Regsvcs/Regasm	Video Capture		Multilayer Encryption
Authentication Package	Exploitation of Vulnerability	Bypass User Account Control		Security Software Discovery	Shared Webroot	Regsvr32			Remote File Copy
Bootkit	Bypass User Account Control	DLL Injection		System Information Discovery	Taint Shared Content	Rundll32			Standard Application Layer Protocol
Component Object Model Hijacking	DLL Injection	Component Object Model Hijacking		System Owner/User Discovery	Windows Admin Shares	Scheduled Task			Standard Cryptographic Protocol
Basic Input/Output System		Indicator Removal from Tools		System Service Discovery		Scripting			Standard Non-Application Layer Protocol
Change Default File Association		Indicator Removal on Host		System Time Discovery		Service Execution			Uncommonly Used Port
Component Firmware		Install Root Certificate				Windows Management Instrumentation			Web Service
External Remote Services		InstallUtil							
Hypervisor		Masquerading							
Logon Scripts		Modify Registry							
Modify Existing Service		MSBuild							
Netsh Helper DLL		Network Share Removal							
Redundant Access		NTFS Extended Attributes							
Registry Run Keys / Start Folder		Obfuscated Files or Information							
Security Support Provider		Process Hollowing							
Shortcut Modification		Redundant Access							
Windows Management Instrumentation Event Subscription		Regsvcs/Regasm							
Winlogon Helper DLL		Regsvr32							
		Rootkit							
		Rundll32							
		Scripting							
		Software Packing							
		Timestamp							

Example: Bypass User Account Control (T1088)

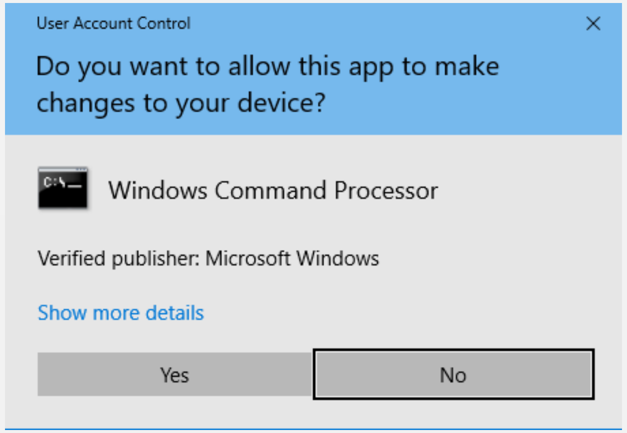


Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
DLL Search Order Hijacking			Brute Force	Account Discovery	Windows Remote Management		Audio Capture	Automated Exfiltration	Commonly Used Port
Legitimate Credentials			Credential Dumping	Application Window Discovery	Third-party Software		Automated Collection	Data Compressed	Communication Through Removable Media
Accessibility Features		Binary Padding			Application Deployment Software	Command-Line	Clipboard Data	Data Encrypted	
AppInit DLLs		Code Signing	Credential Manipulation	File and Directory Discovery		Execution through API	Data Staged	Data Transfer Size Limits	Connection Proxy
Local Port Monitor		Component Firmware			Exploitation of Vulnerability	Execution through Module Load	Data from Local System	Exfiltration Over Alternative Protocol	Custom Command and Control Protocol
New Service		DLL Side-Loading	Credentials in Files	Local Network Configuration Discovery			Data from Network Shared Drive		
Path Interception		Disabling Security Tools	Input Capture		Logon Scripts	Graphical User Interface		Exfiltration Over Command and Control Channel	Custom Cryptographic Protocol
Scheduled Task		File Deletion	Network Sniffing	Local Network Connections Discovery	Pass the Hash	InstallUtil	Data from Removable Media		
File System Permissions Weakness		File System Logical Offsets	Two-Factor Authentication Interception		Pass the Ticket	MSBuild			Data Encoding
Service Registry Permissions Weakness				Network Service Scanning	Remote Desktop Protocol	PowerShell	Email Collection	Exfiltration Over Other Network Medium	Data Obfuscation
Web Shell		Indicator Blocking		Peripheral Device Discovery	Remote File Copy	Process Hollowing	Input Capture		Fallback Channels
Authentication Package	ulnerability				Remote Services	Regsvcs/Regasm	Screen Capture	Exfiltration Over Physical Medium	Multi-Stage Channels
	Bypass User Account Control			Permission Groups Discovery	Replication Through Removable Media	Regsvr32	Video Capture		Multiband Communication
Bootkit	DLL Injection					Rundll32		Scheduled Transfer	
Component Object Model Hijacking		Component Object Model Hijacking		Process Discovery	Shared Webroot	Scheduled Task			Multilayer Encryption
Basic Input/ Output System		Indicator Removal from Tools		Query Registry	Taint Shared Content	Scripting			Remote File Copy
				Remote System Discovery	Windows Admin Shares	Service Execution			Standard Application Layer Protocol
Change Default File Association		Indicator Removal on Host		Security Software Discovery		Windows Management Instrumentation			Standard Cryptographic Protocol
Component Firmware		Install Root Certificate		System Information Discovery					Standard Non-Application Layer Protocol
External Remote Services		InstallUtil							
Hypervisor		Masquerading							
Logon Scripts		Modify Registry		System Owner/User Discovery					
Modify Existing Service		MSBuild							Uncommonly Used Port
Netsh Helper DLL		Network Share Removal		System Service Discovery					Web Service
Redundant Access		NTFS Extended Attributes		System Time Discovery					
Registry Run Keys / Start Folder		Obfuscated Files or Information							
Security Support Provider		Process Hollowing							
Shortcut Modification		Redundant Access							
Windows Management Instrumentation Event Subscription		Regsvcs/Regasm							
		Regsvr32							
		Rootkit							
Winlogon Helper DLL		Rundll32							
		Scripting							
		Software Packing							
		Timestomp							

Example: Bypass User Account Control (T1088)

A Windows security feature that limits application software to standard user privileges until an administrator authorizes an increase or elevation

- Seen used by APT29, Patchwork, BlackEnergy, and others
- Some issues are patched by Microsoft, some are not



User Account Control

Do you want to allow this app to make changes to your device?

Windows Command Processor

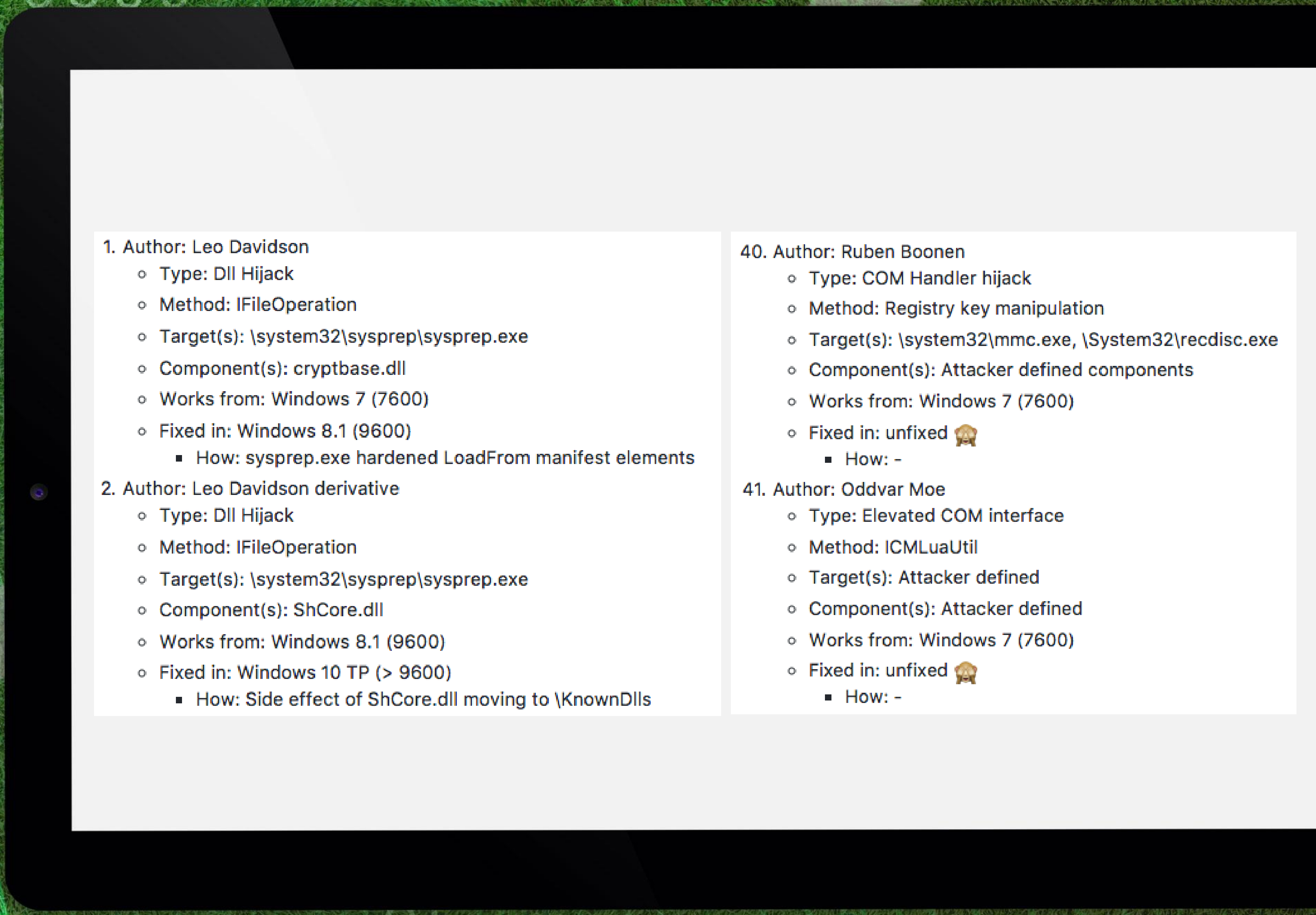
Verified publisher: Microsoft Windows

Show more details

Example: Bypass User Account Control (T1088)

UACME - List of specific procedures to carry out this technique
https://github.com/hfiref0x/UACME

There are… 41!



1. Author: Leo Davidson
   - Type: Dll Hijack
   - Method: IFileOperation
   - Target(s): \system32\sysprep\sysprep.exe
   - Component(s): cryptbase.dll
   - Works from: Windows 7 (7600)
   - Fixed in: Windows 8.1 (9600)
     - How: sysprep.exe hardened LoadFrom manifest elements
2. Author: Leo Davidson derivative
   - Type: Dll Hijack
   - Method: IFileOperation
   - Target(s): \system32\sysprep\sysprep.exe
   - Component(s): ShCore.dll
   - Works from: Windows 8.1 (9600)
   - Fixed in: Windows 10 TP (> 9600)
     - How: Side effect of ShCore.dll moving to \KnownDlls

40. Author: Ruben Boonen
    - Type: COM Handler hijack
    - Method: Registry key manipulation
    - Target(s): \system32\mmc.exe, \System32\recdisc.exe
    - Component(s): Attacker defined components
    - Works from: Windows 7 (7600)
    - Fixed in: unfixed 🙈
      - How: -
41. Author: Oddvar Moe
    - Type: Elevated COM interface
    - Method: ICMLuaUtil
    - Target(s): Attacker defined
    - Component(s): Attacker defined
    - Works from: Windows 7 (7600)
    - Fixed in: unfixed 🙈
      - How: -

Filling the gaps is hard, time-consuming, and expensive.

- There are a lot of prevalent techniques
- Adversary practices are always evolving
- Techniques have a wide set of procedures
- We all have limited resources
- Requires in-depth expertise of system internals

We're making this a team sport.

Tackling the problem together is the only way we can keep up

- More brainpower = faster progress
- A broader array of expertise = broader coverage

But there are some sensitivities you should be aware of…

- The analytics you write and share can have operational security impacts

Multi-faceted approach

- Start out in small working groups
- Not everyone is a producer, feedback is just as important
- Combined with public, open-source, sharing

NH-ISAC Working Group:

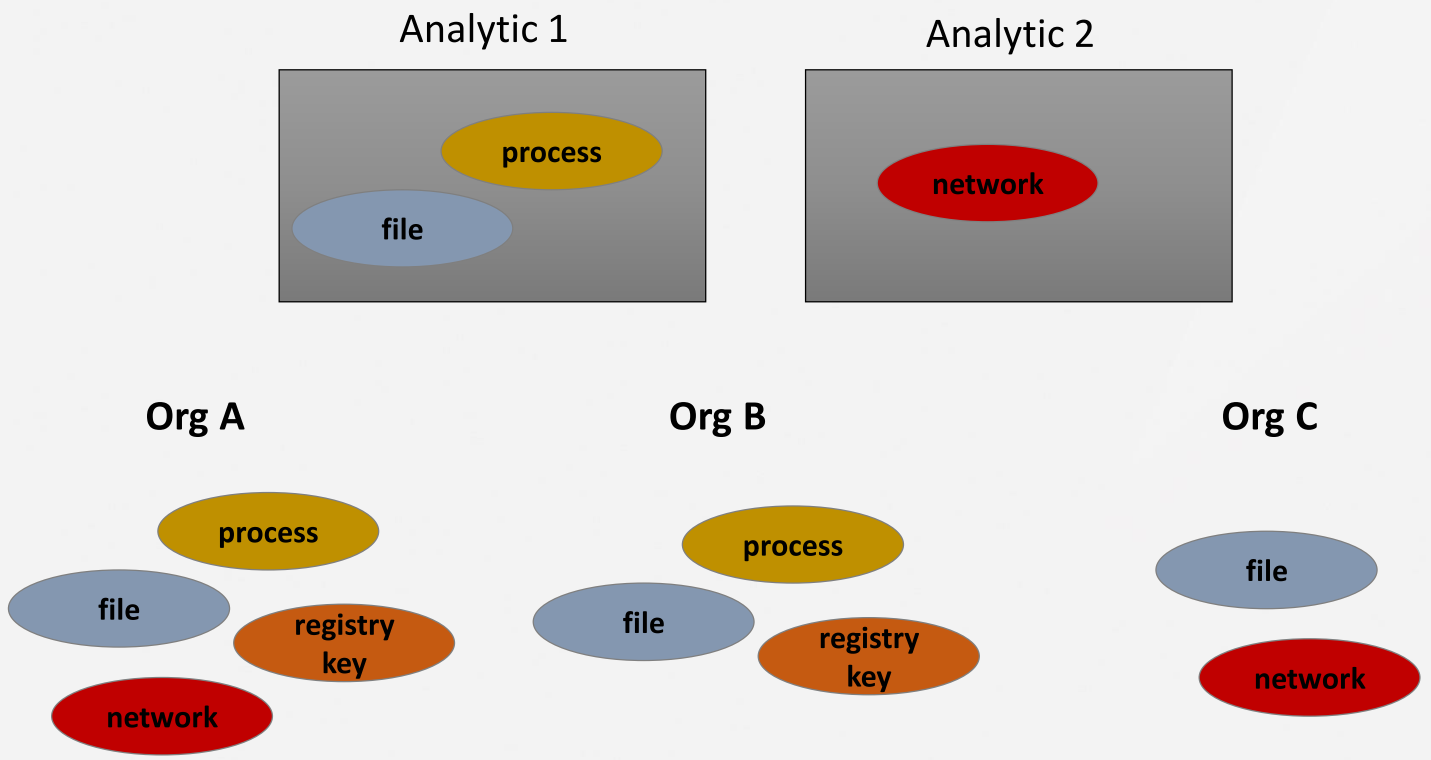
Building out and sharing analytics to cover techniques in the ATT&CK matrix

NH-ISAC
NATIONAL HEALTH - ISAC

- **NH-ISAC Working group, led by Pfizer**
  Particular thanks to Bill Barnes
- **Healthcare companies**
- **Security vendors**
- **HHS**
- **MITRE**

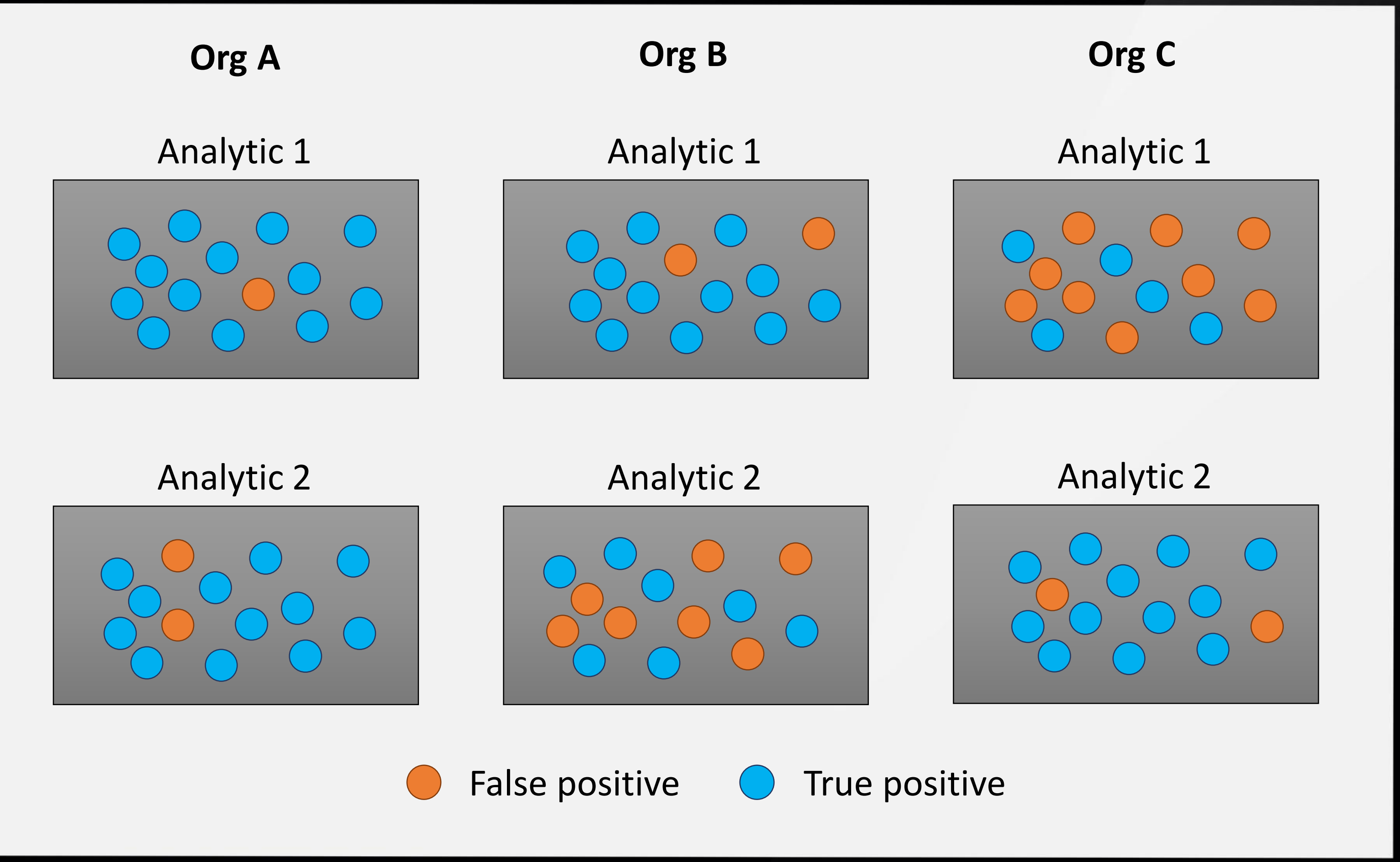
Challenge: Sensor coverage varies.

- Organizations have different types of sensors
- Organizations have different sensors even for the same data
- Sensors are not enough, you need to be able to collect data from your sensors



	Org A	Org B	Org C
Analytic 1	✓	✓	✗
Analytic 2	✓	✗	✓

Challenge: Operational environments vary.



Each environment is unique and will have unique false positives

- **Lots of developers vs. few**
- **Use of Tool A vs. Tool B**

Configurations of OS or other tools differ and cause analytics targeting them to differ

Challenge: There is no common language or taxonomy.

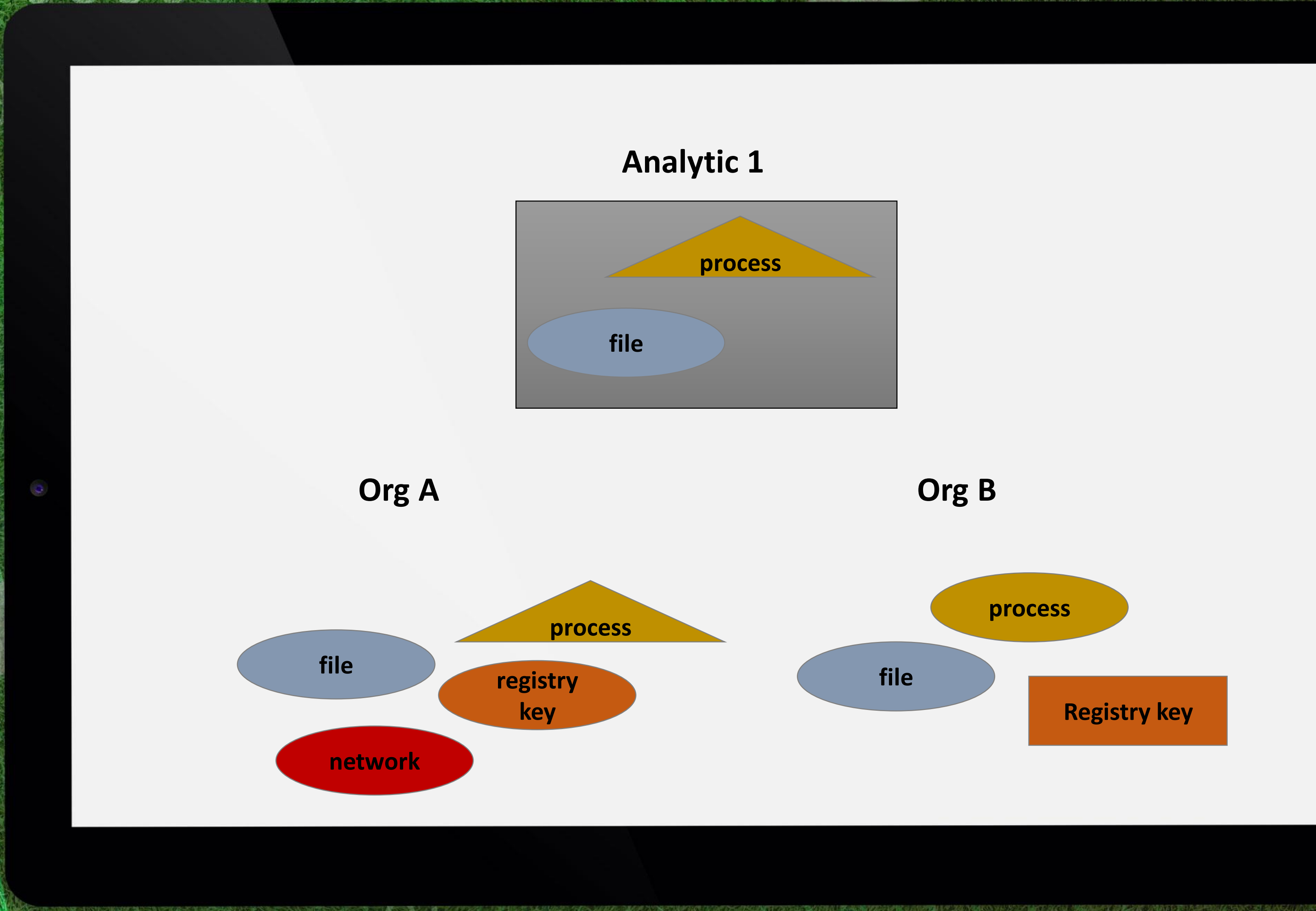
No common

- Query language
- Data taxonomy

Manual conversions are tractable, for now

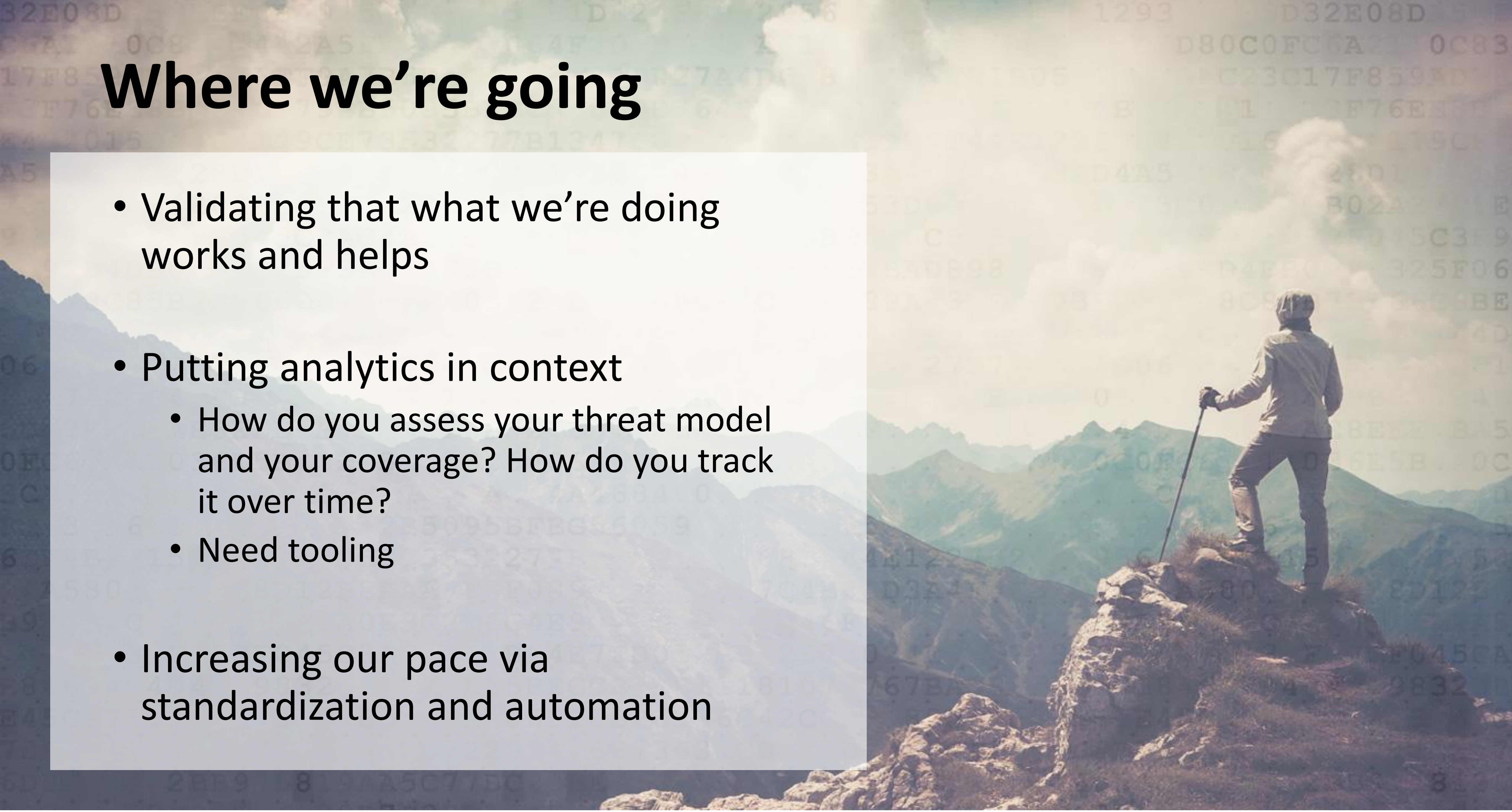
- Simpler analytics
- Lower volume

Need to look to the future



Where we’re going

- Validating that what we’re doing works and helps
- Putting analytics in context
  - How do you assess your threat model and your coverage? How do you track it over time?
  - Need tooling
- Increasing our pace via standardization and automation



Take action

Figure out where you are

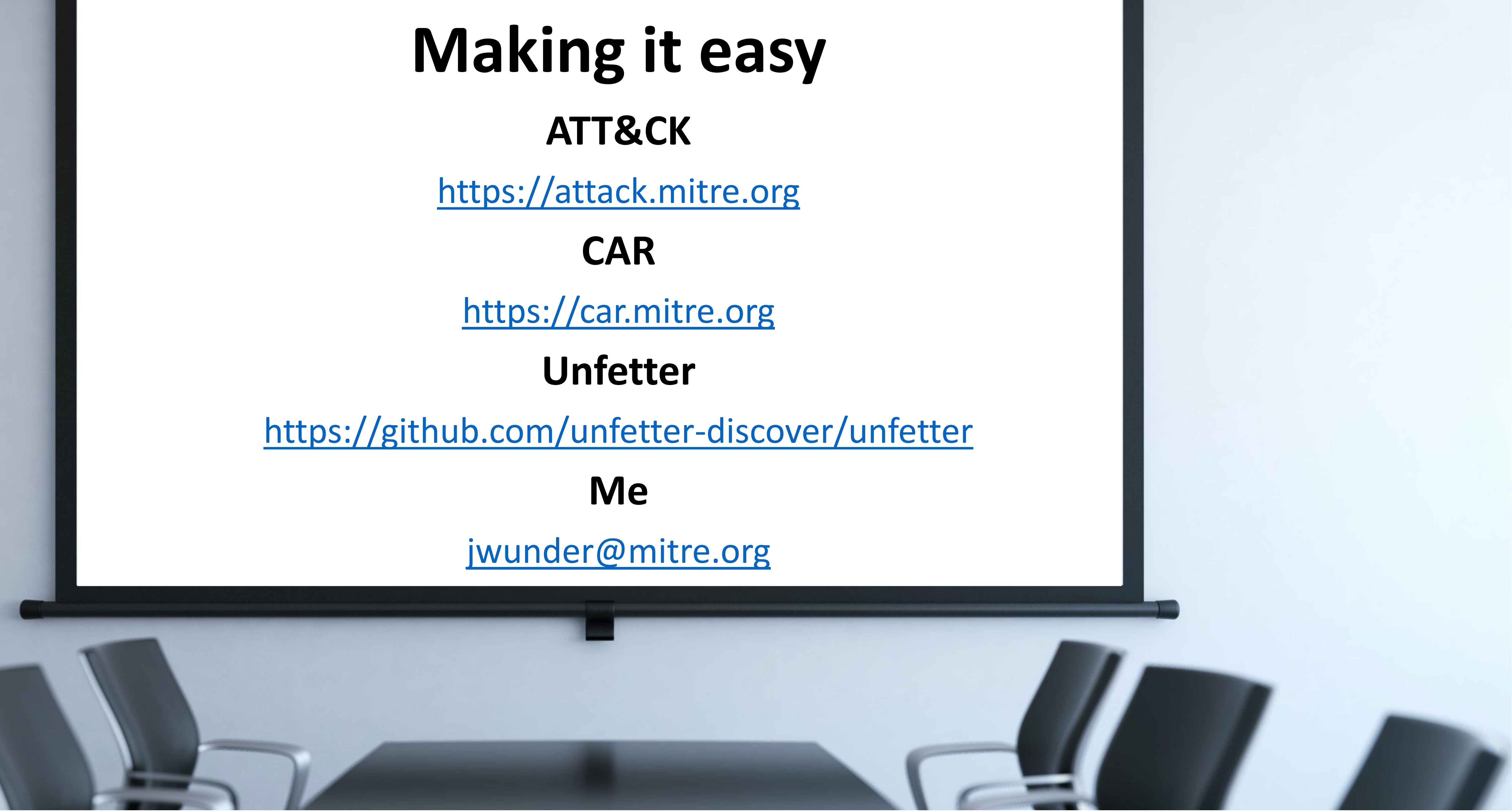
- Define your threat model in ATT&CK.
- Assess your gaps. Ask your vendors.
- Are you where you want to be?

Figure out where to go and how to participate

- Can you use analytics now?
- Can you create analytics yourself?

Find a community to join

- Talk to your ISAO/ISAC, vendors, partners, friends
- Talk to me
- Find open source analytics (look at CAR!)



Making it easy

ATT&CK

https://attack.mitre.org

CAR

https://car.mitre.org

Unfetter

https://github.com/unfetter-discover/unfetter

Me

jwunder@mitre.org