

Quantify Your Hunt:

Not Your Parent's Red Teaming Redux



E.



Agenda for this talk

- Who we are
- Why we're giving this talk with these updates
- Understanding effectiveness
- Things you might be already measuring
- Enterprise ATT&CK, the practitioner's choice of knowledge bases
- Measuring, data quality and ATT&CK
- Statistics, Data science and how they help





Introductions

Honestly, we're not as interesting as this topic



E.



Devon Kerr @_devonkerr_



Principal Threat Researcher for R&D @endgameinc, I do these things:

- Detection and response capability development
- Endgame SOC lead
- RTA contributor and simulation advocate
- Hunt desk reference co-author

Former Incident Response lead at Mandiant with more than 6 years of IR, forensics, analyst training and security program development.

Knowledge areas include Incident management and response, living off the land using native features, adversary tradecraft, simulation and threat detection.





Roberto Rodriguez @Cyb3rWard0g

- Adversary Detection Analyst @**SpecterOps**
- <https://github.com/Cyb3rWard0g>
 - ThreatHunter-Playbook
 - Hunting ELK (HELK)
 - ATTACK-Python-Client
 - Open Source Security Event Metadata (OSSEM)
- Former:
 - Capital One, Senior Threat Hunter





Why this talk?

Why again?



E.



Hunt teams still struggle with ...

- Aligning hunting campaigns & business priorities
- Providing transparency to senior leadership
- Showing progress over time
- Mapping gaps to data sources and security controls
 - Coverage of adversary techniques is much more than a green check or red “x”
- Assessing the effectiveness of the program and any tools used during engagements
- Developing and implementing parity with ATT&CK
- Just getting started, candidly





Effective Hunting

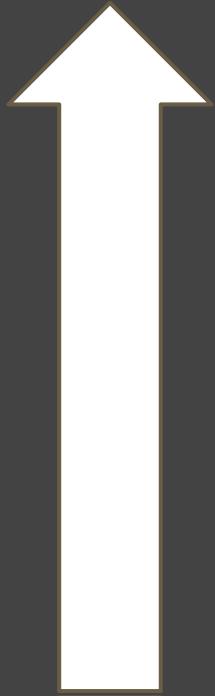
How are you effective? What does being effective even mean?



E.



for effective threat hunting



E.



Efficiency

Efficacy



Effectiveness



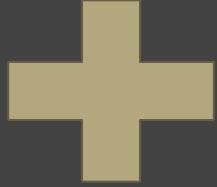
<https://twitter.com/Cyb3rPandaH>

E.



Efficiency

The way resources are used (or wasted),
How much I make the most of the
resources I have



Effectiveness

Accomplishes the goals (to be efficacious)
employing the best and most economic
methodology (to be efficient).

Efficacy

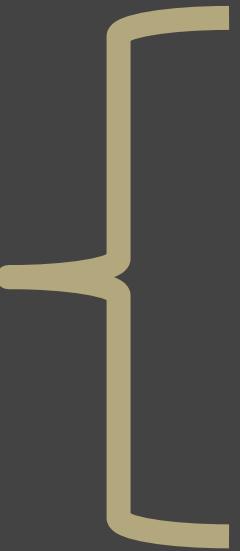
It doesn't matter how we do it, but
only on what we accomplish



E.

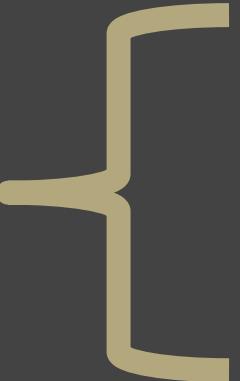


Efficiency



- Choosing an adversary model
- Assessing quality of data
 - Do we even have the data?
- Utilizing the right technology
- Applying the right personnel skills
- Prioritizing adversary techniques
- Enhancing data security analytics

Efficacy



- Let's find evil! Can we detect it? Yes or No?
 - Signatures vs security analytics
 - Are you considering attack variations?
- Uncovering Incidents vs Validating Detection of adversaries



E.



Where do I start?

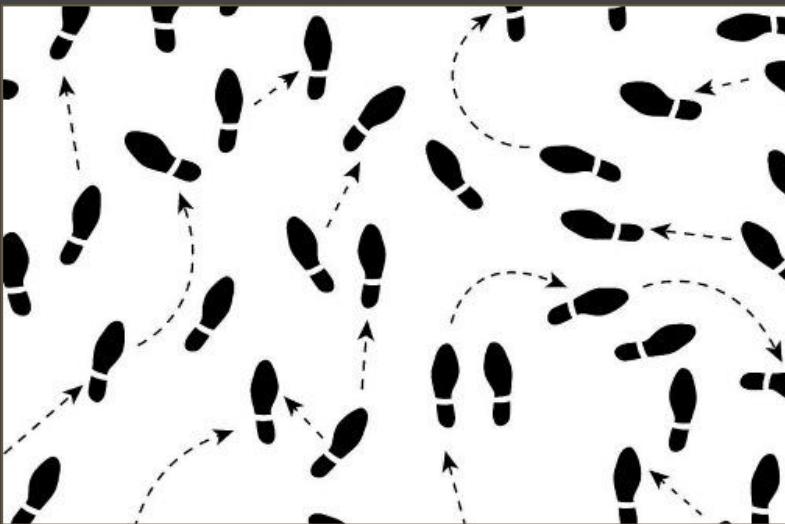
How are we going to start approaching this?



E.



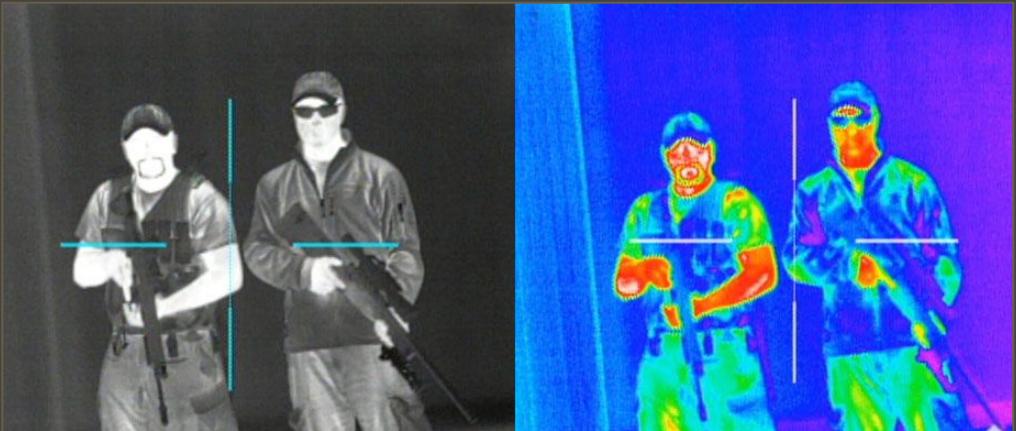
Two steps back, one step forward: or history repeats itself



E.



The Evolution of the Hunt HeatMap



How Hot Is Your Hunt Team?

<https://cyberwardog.blogspot.com/2017/07/how-hot-is-your-hunt-team.html>



Ready to hunt? First, Show me
your data!

<https://cyberwardog.blogspot.com/2017/12/ready-to-hunt-first-show-me-your-data.html>





What are you potentially measuring already?



E.



Risk Forecasting

Choose a risk to measure

Decompose the scenario

Gather supporting data

Make forecasts

Mitigate the potential risk

Measure again

Scenario: "An attacker can access destructive AWS IAM permissions in the next 365 days."

2016 - Q3: **25%**

First forecast. We haven't fixed anything yet.

2016 - Q4: **23%**

We have limited the destructive capability of keys in production.

2017 - Q1: **16%**

We added multifactor protection to keys used by engineers.

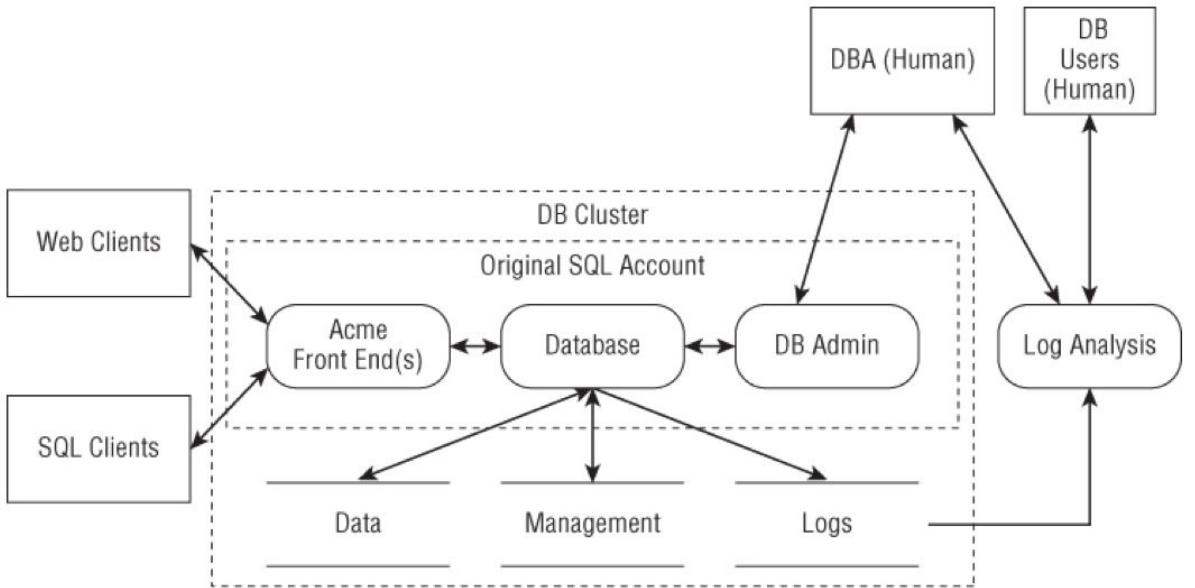
2017 - Q2: **10%**

We took keys out of source code and use roles now.

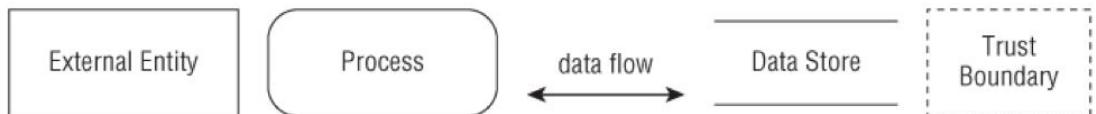
An increase in confidence against this risk of 15%.



Threat Modeling



Key:



Model the system

Identify Threats

Define how threat occurs

Address threats

Validate

Measure again





Where do you fit “hunt”?



E.



Threat Hunting

Identify a technique

Develop a hypothesis

Identify scope and
resources

Develop Analytics

Validate & Report

Automate? & Repeat



E.

Risk Forecasting

Choose a risk to measure

Decompose the scenario

Gather supporting data

Make forecasts

Mitigate the potential risk

Measure again

Threat Hunting

Identify a technique

Develop a hypothesis

Identify scope and resources

Develop Analytics

Validate & Report

Automate? & Repeat

Threat Modeling

Model the system

Identify Threats

Define how threat occurs

Address threats

Validate

Measure again



Risk Forecasting

Choose a risk to measure

Decompose the scenario

Gather supporting data

Make forecasts

Mitigate the potential risk

Measure again

Threat Hunting

Identify a technique

Develop a hypothesis

Identify scope and resources

Develop Analytics

Validate & Report

Automate? & Repeat

Threat Modeling

Model the system

Identify Threats

Define how threat occurs

Address threats

Validate

Measure again



Risk Forecasting

Choose a risk to measure

Decompose the scenario

Gather supporting data

Make forecasts

Mitigate the potential risk

Measure again

Threat Hunting

ATT&CK™

Adversarial Tactics, Techniques
& Common Knowledge

Identify scope and resources

Develop Analytics

Validate & Report

Automate? & Repeat

Threat Modeling

Model the system

Identify Threats

Define how threat occurs

Address threats

Validate

Measure again





What can we measure from a hunt detection?



E.



We need to understand what we are trying to measure from a detection perspective

- Do we have the right resources to validate the detection of identified threats?
 - What percentage of my tools help the most during a hunt?
 - What percentage of data is utilized the most during a hunt?
- How much can we cover with the current resources we have?
 - Percentage of data in relation to detected techniques
 - Percentage of successful analytics for hunt engagements
- Are we reducing the probability of attackers achieving their objective?
 - Percentage reduced each quarter after a hunting engagement. forecasting?



E.



ENTERPRISE ATT&CK

The practitioner's choice of knowledge base



E.



MITRE said it best

“

MITRE’s Adversarial Tactics, Techniques and Common Knowledge (ATT&CK™) is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary’s lifecycle and the platforms they are known to target. ATT&CK is useful for understanding security risk against known adversary behavior, for planning security improvements, and verifying defenses work as expected.

”

- MITRE ATT&CK -





We *really* like Enterprise ATT&CK

What's not to like:

- it is threat-agnostic, describing the purpose and effect of many techniques
- contains more than 200 categorized and curated entries
- includes forensic artifacts and references to educate analysts and decrease barrier-to-entry
- techniques are cross-referenced by threat group, *if that's important to your business (it might not be, no judgement)*





ATT&CK STATISTICS (As of April 27, 2018)

- 219 techniques
 - 187 - Windows
 - 130 - MacOS
 - 108 - Linux
- 11 Tactics
- 68 groups
- 187 Tools
- 48 Data Sources
- 39 Contributors
- 21 Bypasses





How can I measure against ATT&CK?



E.



Explore ATT&CK

Access Token Manipulation

Technique

ID	T1134
Tactic	Defense Evasion, Privilege Escalation
Platform	Windows
Permissions	User, Administrator
Required	
Effective	SYSTEM
Permissions	
Data	API monitoring, Access Tokens
Sources	

PowerShell

Technique

ID	T1086
Tactic	Execution
Platform	Windows
Permissions	User, Administrator
Required	
Data	Windows Registry, File monitoring,
Sources	Process command-line parameters, Process monitoring
Supports	Yes
Remote	





Explore ATT&CK

Access Token Manipulation

Technique

ID T1134

Tactic Defense Evasion, Privilege Escalation

Platform Windows

Permissions User, Administrator

Required

Effective Permissions SYSTEM

Data Sources API monitoring, Access Tokens

The lowest level of permissions the adversary is required

PowerShell

Technique

ID T1086

Tactic Execution

Platform Windows

Permissions Required User, Administrator

Data Sources Windows Registry, File monitoring, Process command-line parameters, Process monitoring

Supports Remote Yes





Explore ATT&CK

Access Token Manipulation

Technique

ID T1134

Tactic Defense Evasion, Privilege Escalation

Platform Windows

Permissions Required User, Administrator

Effective Permissions

System

Data Sources API monitoring, Access Tokens

The lowest level of permissions the adversary is required

Permissions an adversary will attain by performing the technique

PowerShell

Technique

ID T1086

Tactic Execution

Platform Windows

Permissions Required User, Administrator

Data Sources Windows Registry, File monitoring, Process command-line parameters, Process monitoring

Supports Remote Yes





Explore ATT&CK

Access Token Manipulation

Technique

ID T1134

Tactic Defense Evasion, Privilege Escalation

Platform Windows

Permissions Required User, Administrator

Effective Permissions SYSTEM

Data Sources API monitoring, Access Tokens

The lowest level of permissions the adversary is required

Permissions an adversary will attain by performing the technique

Data recommended to be collected for the detection of an action

PowerShell

Technique

ID T1086

Tactic Execution

Platform Windows

Permissions Required User, Administrator

Data Sources Windows Registry, File monitoring, Process command-line parameters, Process monitoring

Supports Remote Yes





Explore ATT&CK

Access Token Manipulation

Technique

ID T1134

Tactic Defense Evasion, Privilege Escalation

Platform Windows

Permissions Required User, Administrator

Effective Permissions SYSTEM

Data Sources API monitoring, Access Tokens

The lowest level of permissions the adversary is required

Permissions an adversary will attain by performing the technique

Data recommended to be collected for the detection of an action

If the technique can be used to execute something on a remote system

PowerShell

Technique

ID T1086

Tactic Execution

Platform Windows

Permissions Required User, Administrator

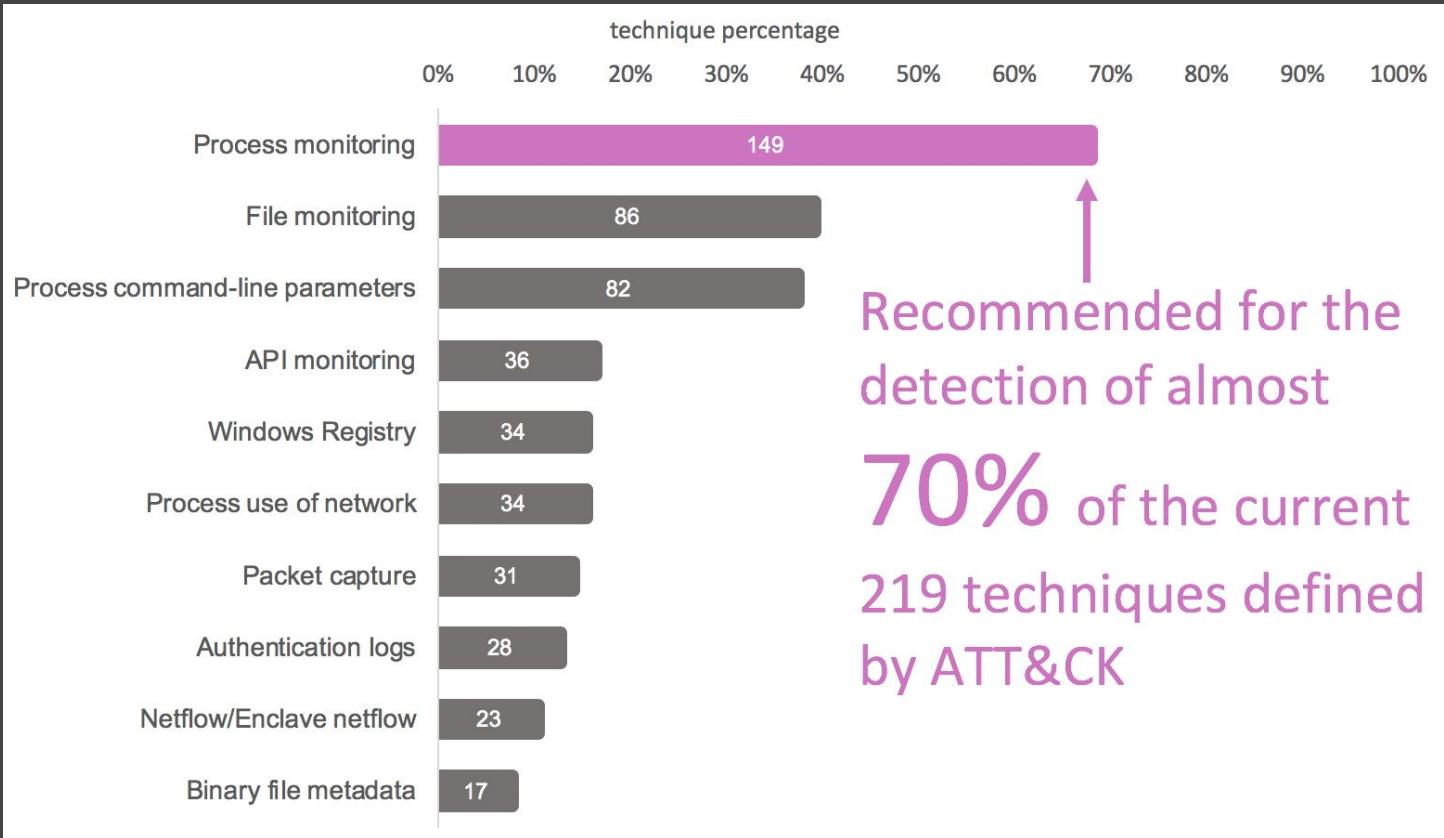
Data Sources Windows Registry, File monitoring, Process command-line parameters, Process monitoring

Supports Remote Yes



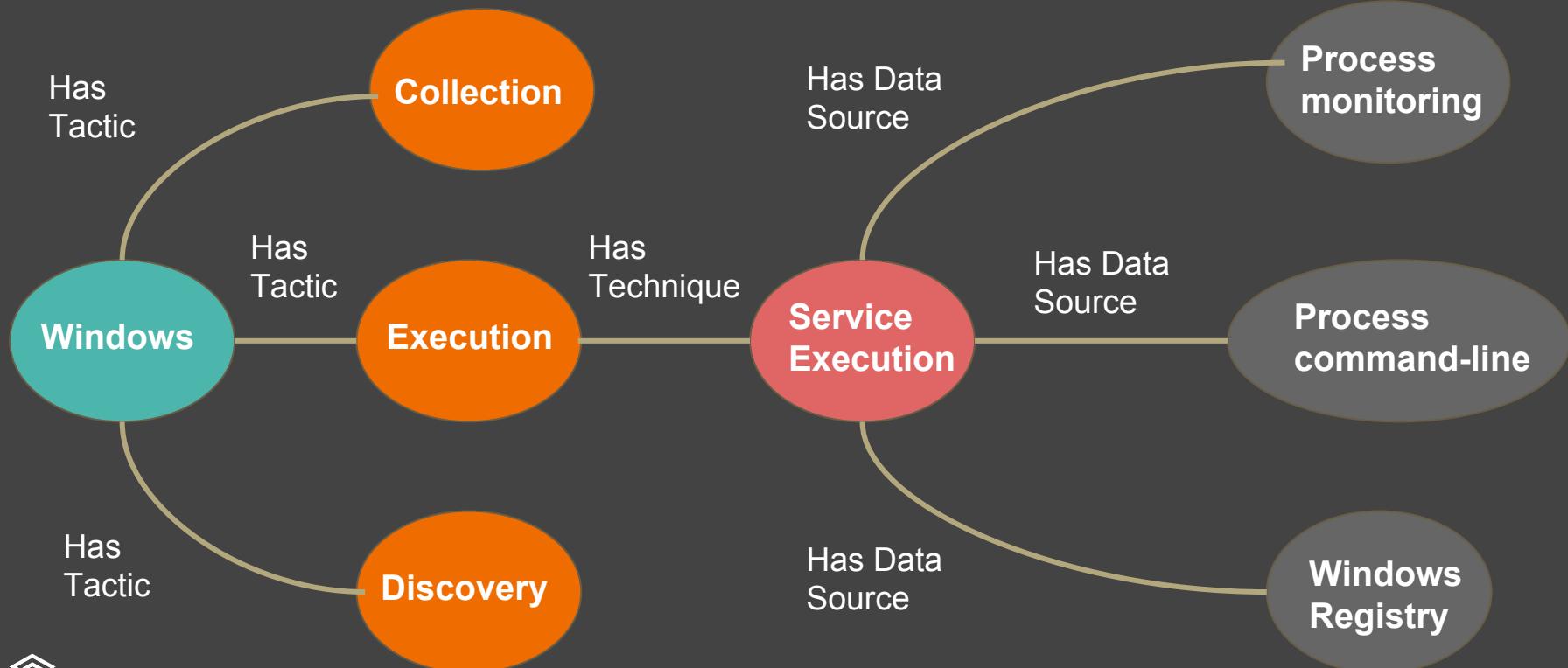


Data Sources -> Adversarial Techniques



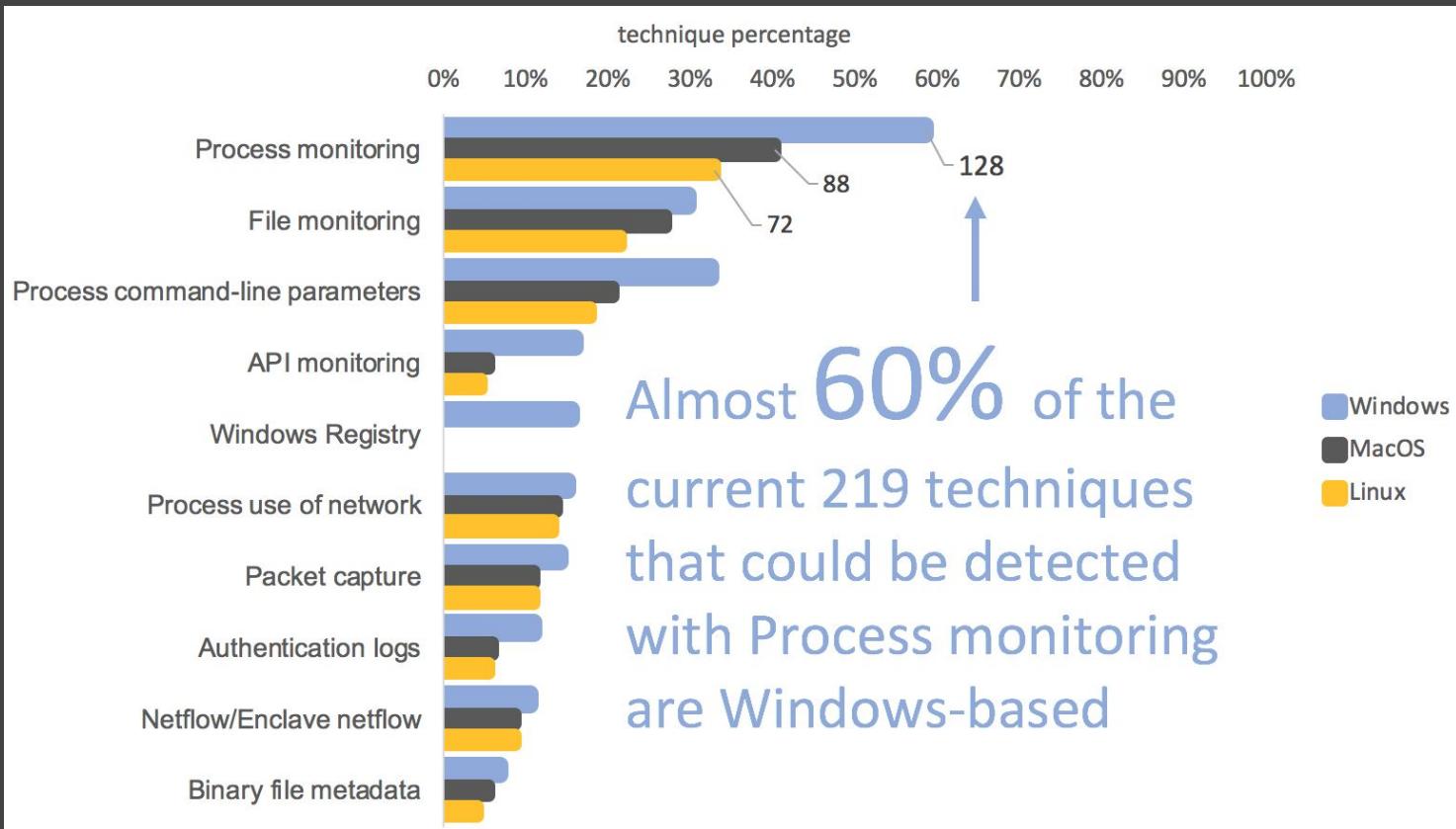


Identify Relationships in ATT&CK



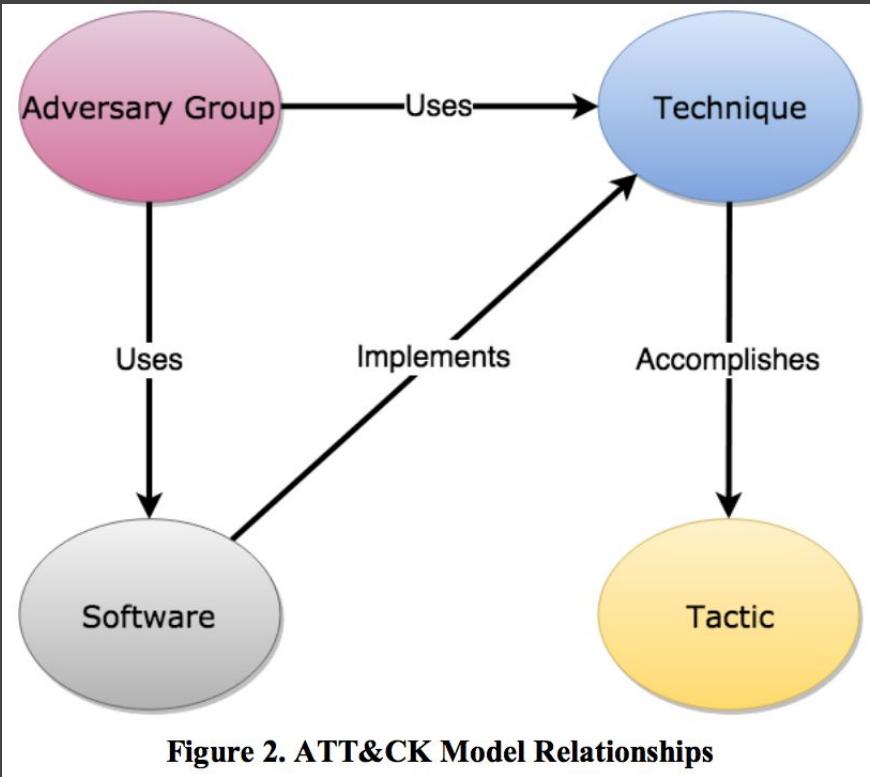


Data Sources -> Adversarial Techniques -> OS

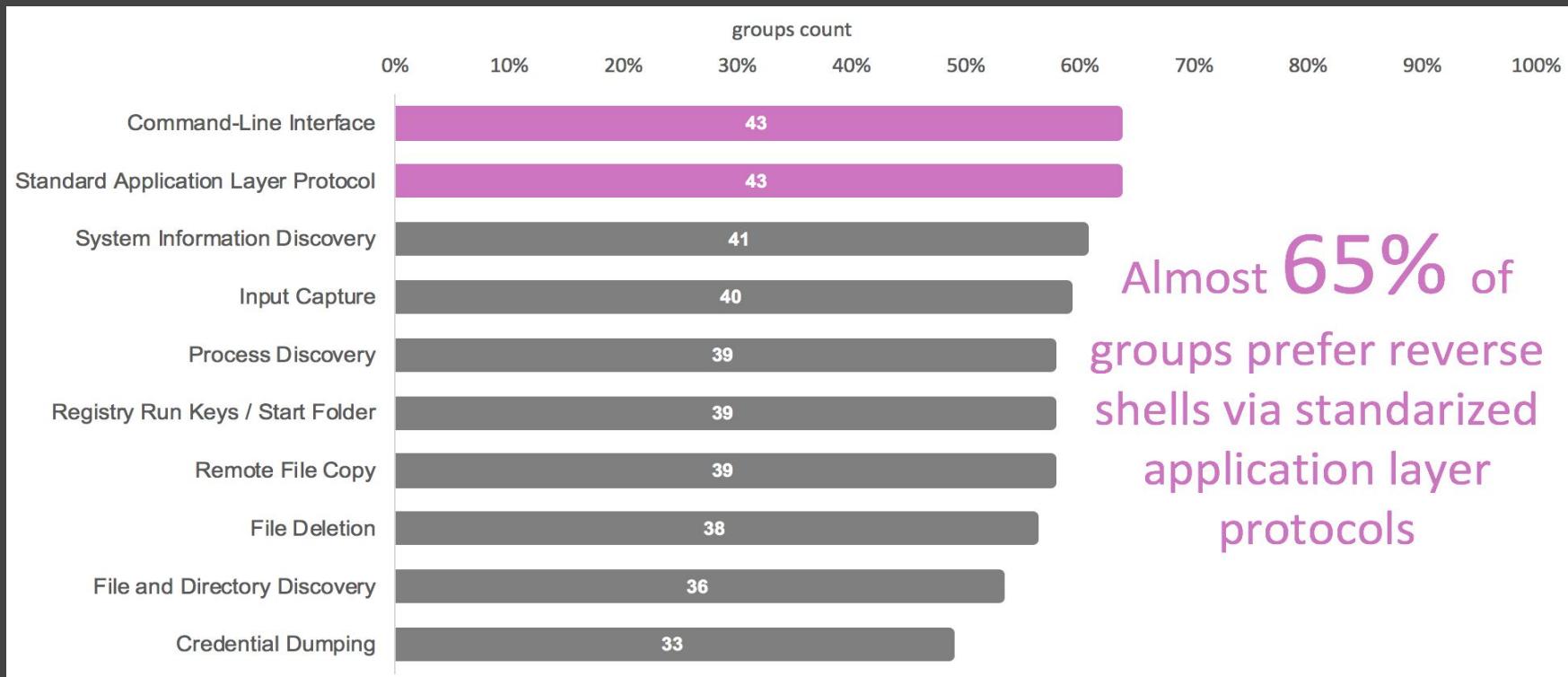




Identify Relationships in ATT&CK



Groups -> Adversarial Techniques





MITRE has already covered this topic, though

Part 1: Using ATT&CK to Advance Cyber Threat Intelligence

This excellent blogpost by Katie Nickels (@likethecoins) covers:

- An overview of traditional CTI
- Challenges
- How ATT&CK can help provide a way of expressing TTPs, exposing a *common language*
- Using ATT&CK to understand blind spots
- Using TTP counts as a metric to justify your CTI program

Part 2: Using ATT&CK to Advance Cyber Threat Intelligence

The second part in this series focuses on knowledge management and adversary behavior curation, which ATT&CK is perfectly designed to assist with.

Two of the major points to take away:

- Get as close to original information as possible to avoid misinterpreting a tactic or event
- Select *appropriate* information to curate





Adversary Techniques->
Data Sources ->
Detection Strategy



E.



What data sources are recommended?

Access Tokens	Detonation chamber	Loaded DLLs
Anti-virus	Digital Certificate Logs	Mail server
API monitoring	DLL monitoring	Malware reverse engineering
Application Logs	DNS records	MBR
Asset Management	EFI	Named Pipes
Authentication logs	Email gateway	Netflow/Enclave netflow
Binary file metadata	Environment variable	Network device logs
BIOS	File monitoring	Network intrusion detection system
Browser extensions	Host network interface	Network protocol analysis
Data loss prevention	Kernel drivers	Packet capture





What data sources are recommended?

PowerShell logs	VBR
Process command-line parameters	Web application firewall logs
Process monitoring	Web logs
Process use of network	Web proxy
Sensor health and status	Windows Error Reporting
Services	Windows event logs
SSL/TLS inspection	Windows Registry
System calls	WMI Objects
Third-party application logs	
User interface	





Let's take a look at data sources again:

- PowerShell logs
- Process command-line parameters
- Process monitoring
- Process use of network
- Sensor health and status
- Services
- SSL/TLS inspection
- System calls
- Third-party application logs
- User interface





Process object attributes...

PowerShell logs
Process command-line parameters
Process monitoring
Process use of network
Sensor health and status
Services
SSL/TLS inspection
System calls
Third-party application logs
User interface

Process
process_name
process_command_line
process_path
process_parent_name
user_name
hash_sha256
host_name





What is a data model?

- A data model basically determines the structure of data and the relationships identified among each other.
- MITRE Data Model:
 - Strongly inspired by CybOX, is an organization of the objects that may be monitored from a host-based or network-based perspective.
 - https://car.mitre.org/wiki/Data_Model
- STIX™ Version 2.0. Part 4: Cyber Observable Objects
 - <http://docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part4-cyber-observable-objects.html>



E.



Data Model (Defining Data Objects)

Ip Object
ip_src
ip_dst
process_name
user_name
host_name

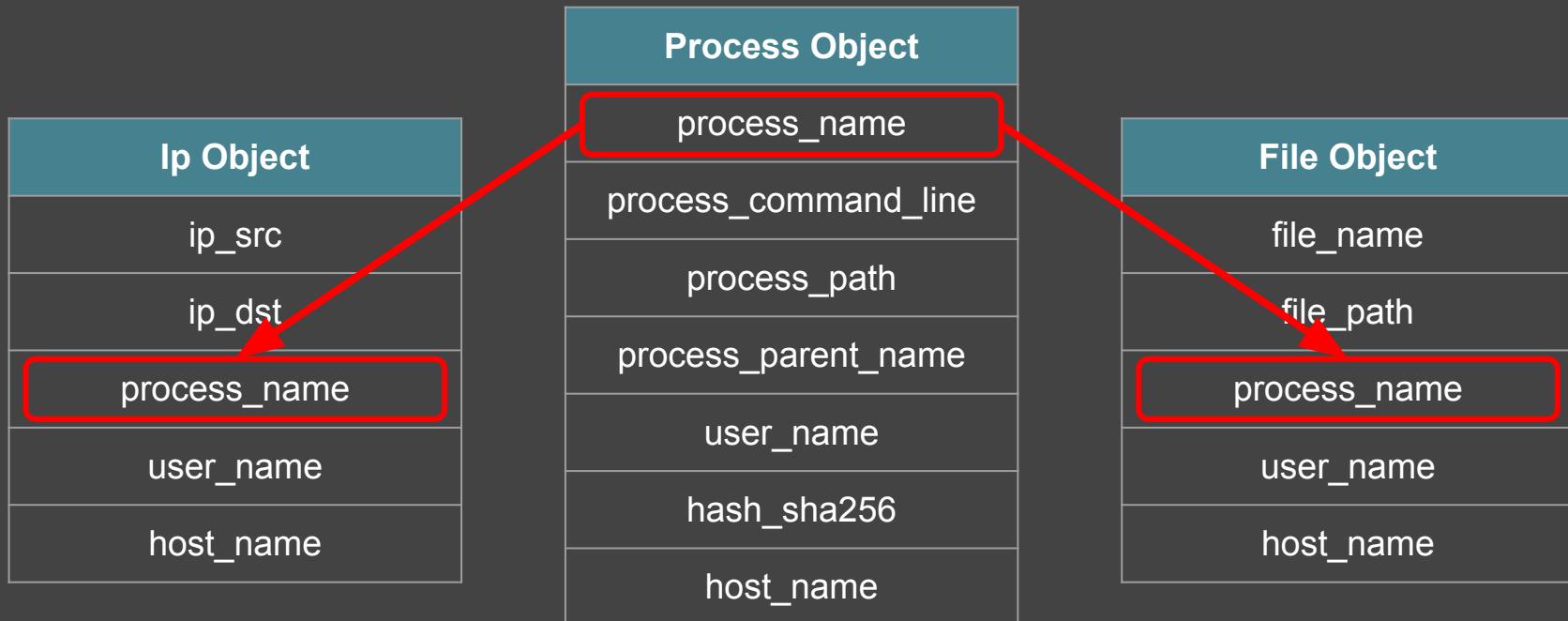
Process Object
process_name
process_command_line
process_path
process_parent_name
user_name
hash_sha256
host_name

File Object
file_name
file_path
process_name
user_name
host_name





Data Model (Defining Data Objects)





Data Model (Defining Object Relationships)

Applicable Objects (Source)	Relationship	Applicable Objects (Destination)
Process	Created	File, Process, Win Registry Key, Service
File, Process, Win Registry Key, Service	Created_By	Process
Process	Parent_Of	Process
Process	Modified_Properties_Of	File, Win Registry Key, Service
Process	Renamed	File
File	Renamed_By	Process
Process	Connected_To	IP, Hostname





Example: Process use of network

PowerShell logs	VBR
Process command-line parameters	Web application firewall logs
Process monitoring	Web logs
Process use of network	Web proxy
Sensor health and status	Windows Error Reporting
Services	Windows event logs
SSL/TLS inspection	Windows Registry
System calls	WMI Objects
Third-party application logs	
User interface	





Process use of network: Process & IP Relationship

Applicable Objects (Source)	Relationship	Applicable Objects (Destination)
Process	Created	File, Process, Win Registry Key, Service
Process	Parent_Of	Process
File, Process, Win Registry Key, Service	Created_By	Process
Process	Modified_Properties_Of	File, Win Registry Key, Service
Process	Renamed	File
File	Renamed_By	Process
Process	Connected_To	IP, Hostname





Data Source: Process use of network

Process Object
process_name
process_command_line
process_path
process_parent_name
user_name
hash_sha256
host_name

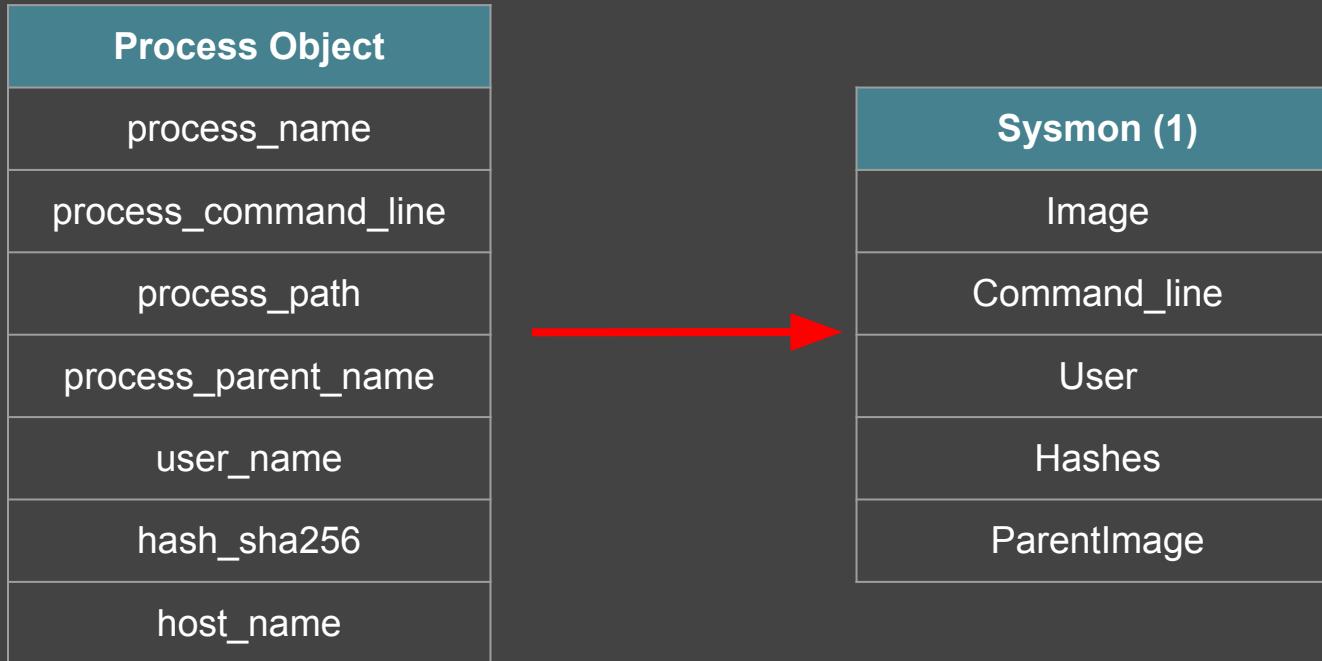
Connected_To


Ip Object
ip_src
ip_dst
process_name
user_name
host_name





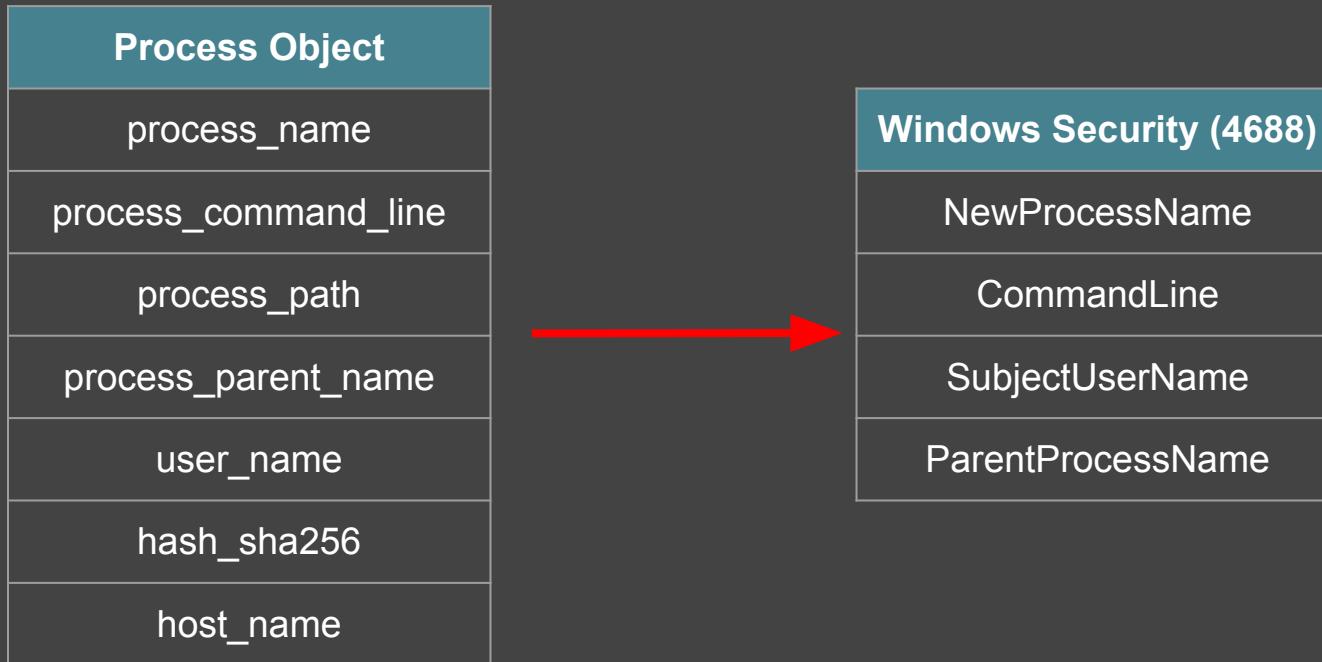
Linking it to data sensors (Sysmon)



E.



Linking it to data sensors (Windows Security)





Do I have what I need?

Process Object
process_name
process_command_line
process_path
process_parent_name
user_name
hash_sha256
host_name

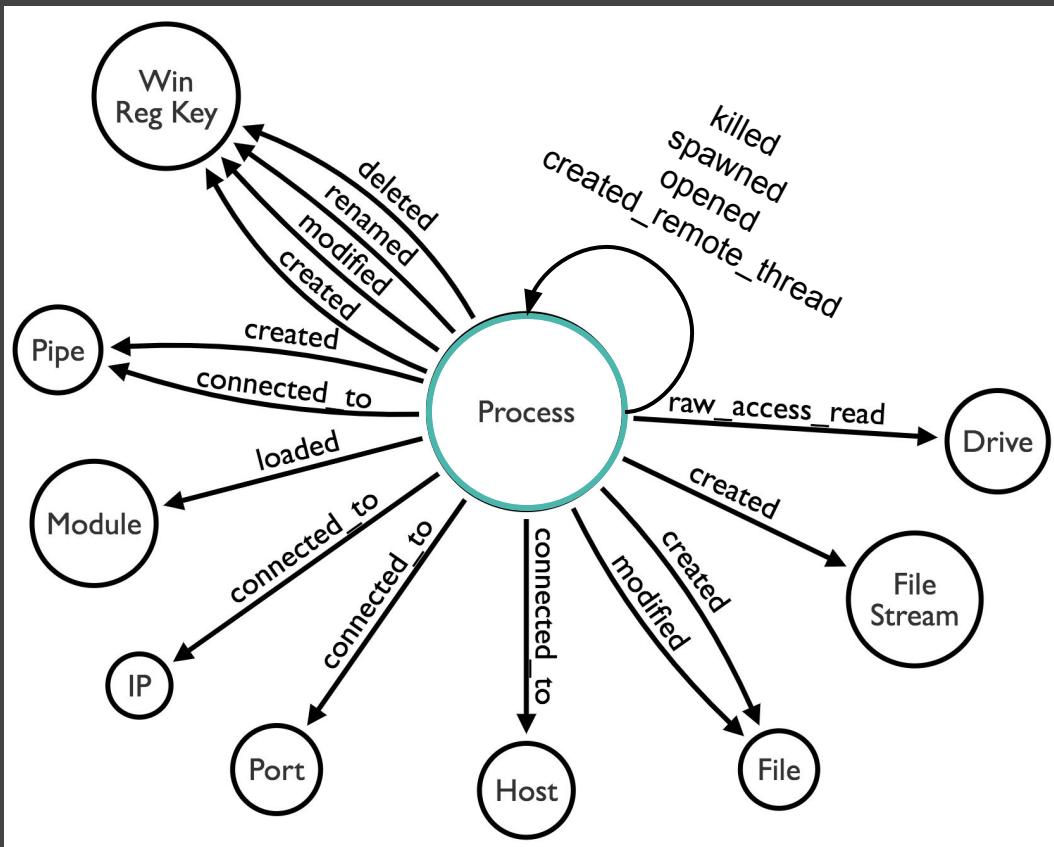
Sysmon
Image
Command_line
User
Hashes
ParentImage

Windows Security (4688)
NewProcessName
CommandLine
SubjectUserName
ParentProcessName





Do I have what I need? (Modeling Sysmon Events)





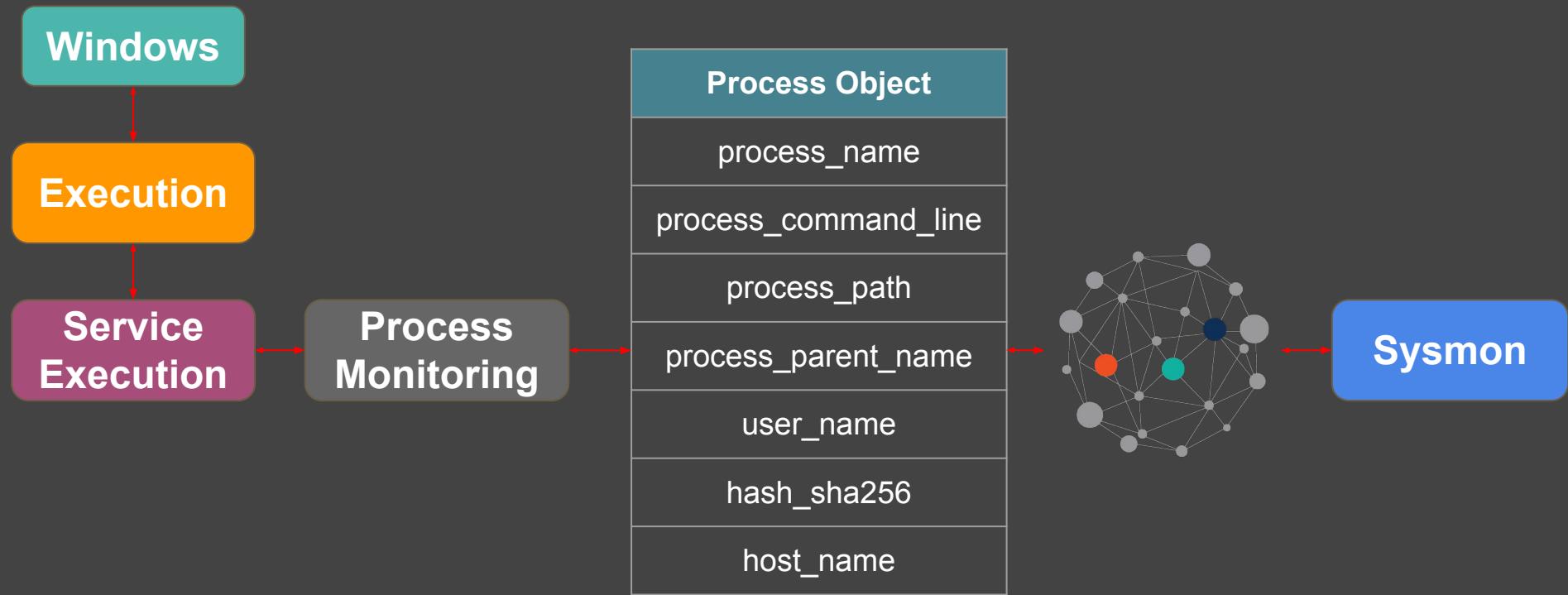
Do I have what I need? (mmm... tell me more)



E.



Do I have what I need? (What we propose)





[Remember] Adversaries can influence your data..

```
"UtcTime">2018-04-11 05:25:02.955  
"ProcessGuid">{A98268C1-9C2E-5ACD-0000-0010396CAB00}  
"ProcessId">4756  
"Image">C:\Windows\System32\conhost.exe  
"FileVersion">10.0.16299.15 (WinBuild.160101.0800)  
"Description">Console Window Host  
"Product">Microsoft® Windows® Operating System  
"Company">Microsoft Corporation  
"CommandLine">\??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1  
"CurrentDirectory">C:\WINDOWS  
"User">DESKTOP-WARDOG\wardog  
"LogonGuid">{A98268C1-95F2-5ACD-0000-002019620F00}  
"LogonId">0xf6219  
"TerminalSessionId">1  
"IntegrityLevel">Medium  
"Hashes">SHA1=B0BF5AC2E81BBF597FAD5F349FEEB32CAC449FA2  
"ParentProcessGuid">{A98268C1-9C2E-5ACD-0000-00100266AB00}  
"ParentProcessId">240  
"ParentImage">C:\Windows\System32\cmd.exe  
"ParentCommandLine">"C:\WINDOWS\system32\cmd.exe"
```

High Attacker
Influence Rating!!!





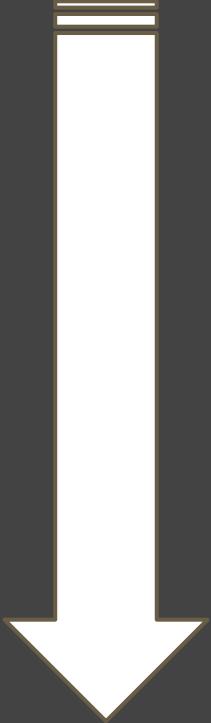
So, what can I
measure *now*?

Do I know what I have?

Is this data
what I need?



E.



Not all data sources are created equal, data quality matters.

E.



If data needed for a hunting engagement does not meet specific requirements defined by the hunt team, then the data is not considered quality data since it is affecting the intended purpose of it.

“

Data are of high quality if they are fit for their intended uses in operations, decision making and planning."

”

- Julian's Quality Handbook -





Data Quality Dimensions

Data Quality	Characteristics Description	Example Metric
Accuracy	A quality of that which is free of error. A qualitative assessment of freedom from error, with a high assessment corresponding to a small error. (FIPS Pub 11-3)	Percent of values that are correct when compared to the actual value. For example, M=Male when the subject is Male.
Completeness	Completeness is the degree to which values are present in the attributes that require them. (Data Quality Foundation)	Percent of data fields having values entered into them.
Consistency	Consistency is a measure of the degree to which a set of data satisfies a set of constraints. (Data Quality Management and Technology)	Percent of matching values across tables/files/records.
Timeliness	As a synonym for currency, timeliness represents the degree to which specified data values are up to date. (Data Quality Management and Technology)	Percent of data available within a specified threshold time frame (e.g., days, hours, minutes).
Uniqueness	The state of being the only one of its kind. Being without an equal or equivalent.	Percent of records having a unique primary key.
Validity	The quality of data that is founded on an adequate system of classification and is rigorous enough to compel acceptance. (DoD 8320.1-M)	Percent of data having values that fall within their respective domain of allowable values.





Data Completeness

- How much data that is required/needed is available in my network?
- Are all required/needed data fields and values recorded?



Data Consistency

- Can we match required/needed fields across data sources?

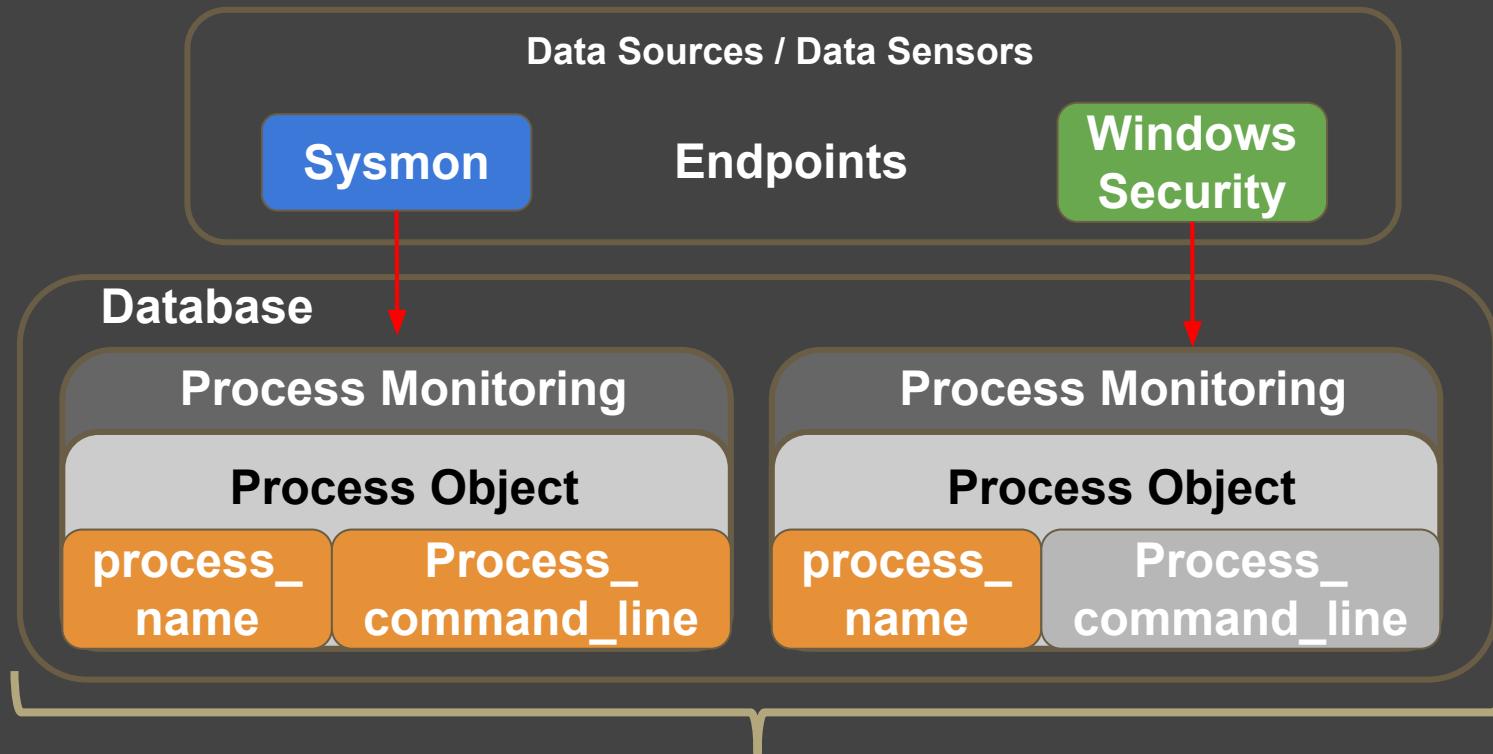
Data Timeliness

- Does my data represent reality?
- How far back in time can I hunt with required/needed data?





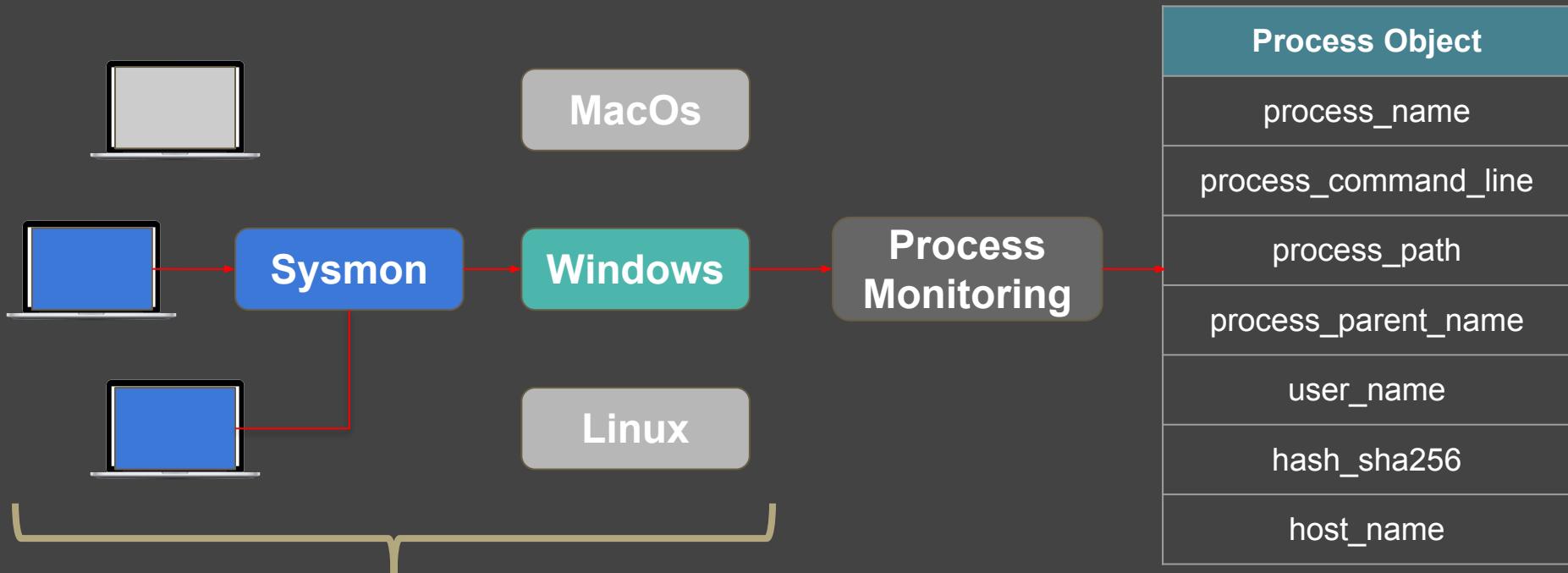
Completeness: Is the expected data complete?



E.



Completeness: Percentage of network covered?

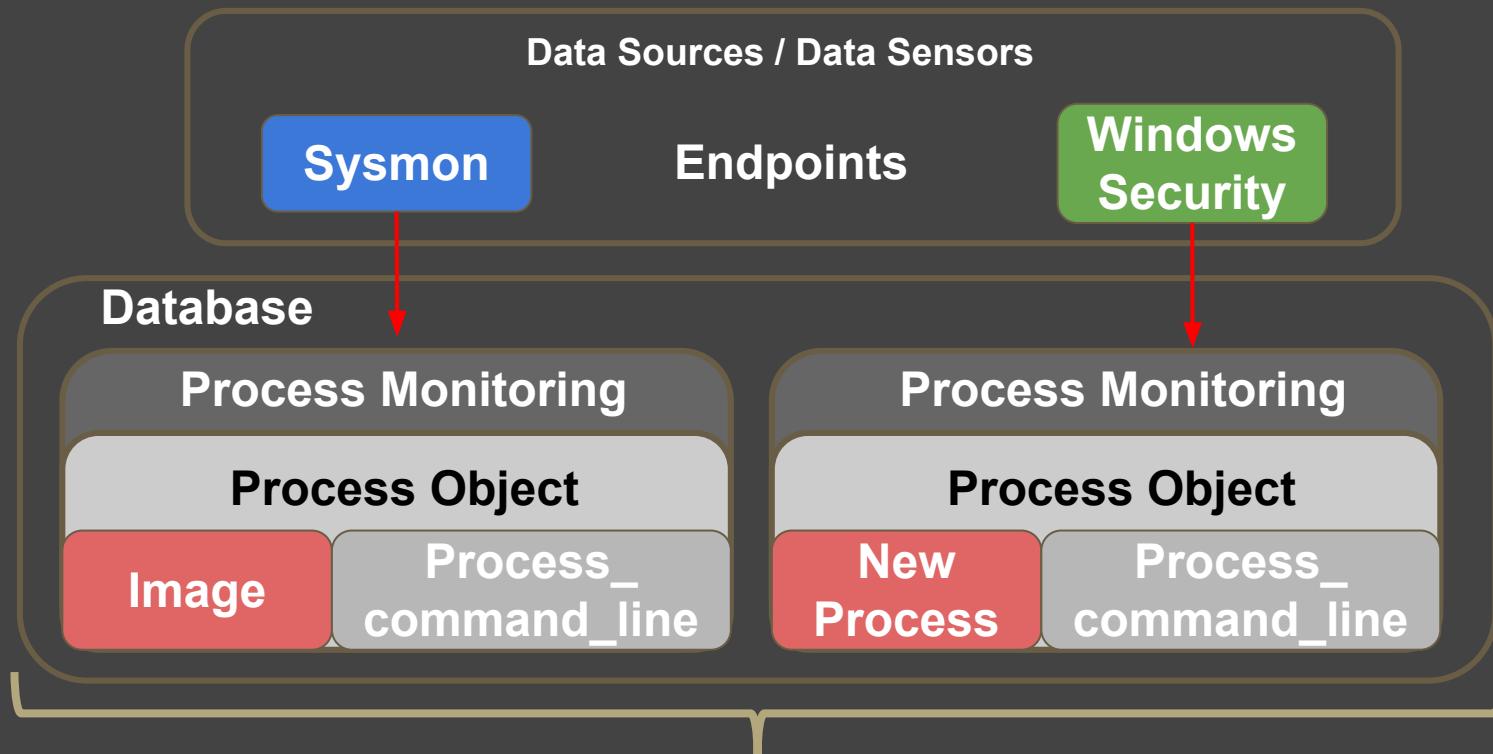


Data Completeness

E.



Consistency: Across all data sources?

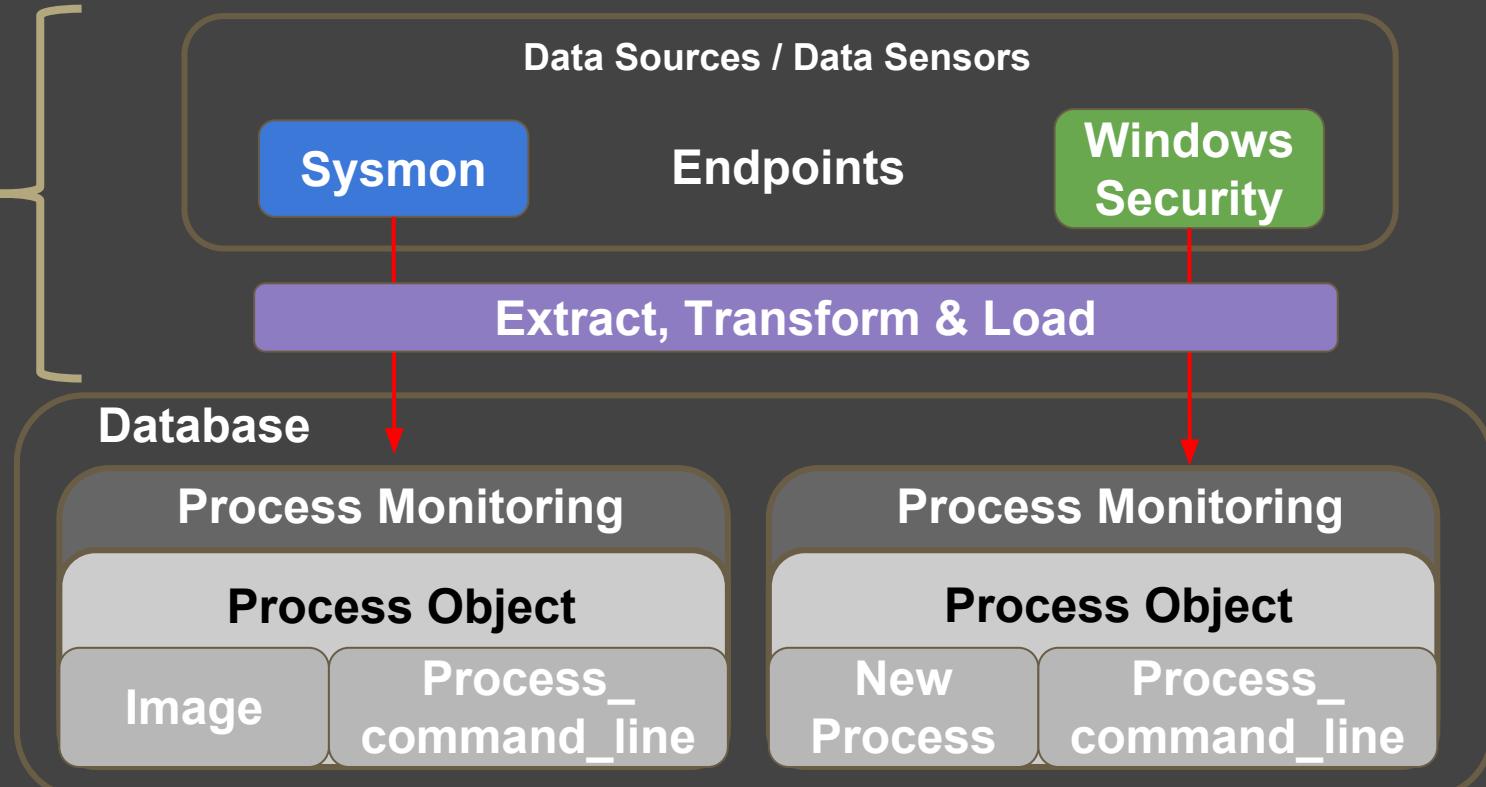


E.



Timeliness: Does my data represent reality?

Data
Timeliness

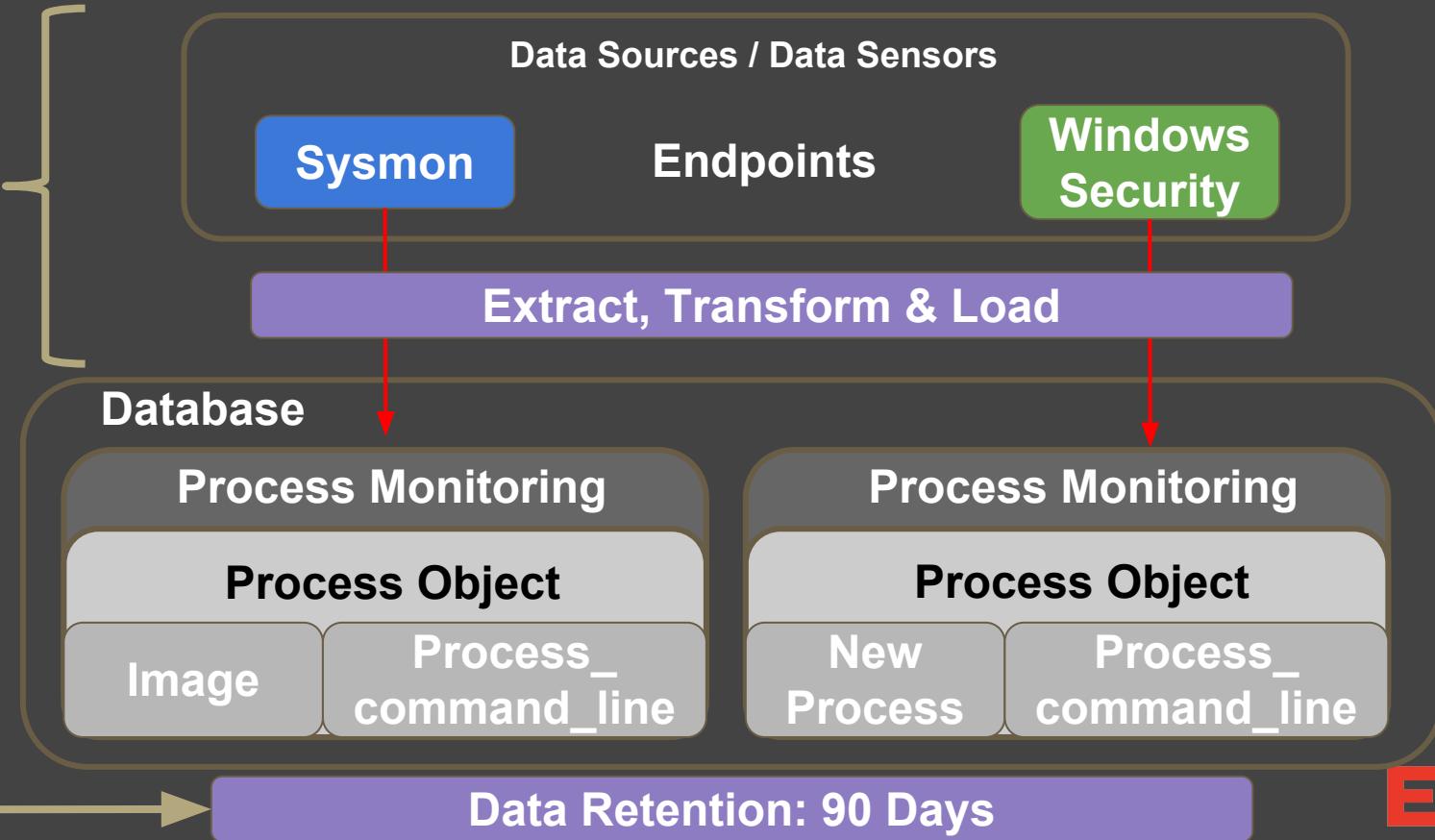


E.



Timeliness: Does my data represent reality?

Data
Timeliness



E.



A few hunt metrics you *could* measure:

- What percentage of recommended data is available for a hunt?
- What percentage of the expected data is complete for a hunt?
- What percentage of my environment could I cover in an hunt based on the available recommend data?
- How far back in time can I hunt with recommended data?
- What percentage of my data sources are consistent across all the data provided by data sensors?
- Do I have the right technology or skills to hunt?





Now, this makes more sense?? A little bit?

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	31 items	56 items	28 items	59 items	20 items	19 items	17 items	13 items	9 items	21 items
Drive-by Compromise	AppleScript CMSTP	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	Command-Line Interface	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Control Panel Items	AppCert DLLs	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	
Replication Through Removable Media	Dynamical Data Exchange	Appinit DLLs	Appinit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Data from Information Repositories	Data Transfer Size Limits		Connection Proxy
Spearphishing Attachment	Execution through API	Application Shimming	Application Shimming	Clear Command History	Credentials in Files	Exploitation of Registry	Network Service Scanning	Exfiltration Over Alternative Protocol		Custom Command and Control Protocol
Spearphishing Link	Execution through Module Load	Authentication Package	Bypass User Account Control	CMSTP	Code Signing	Exploitation for Credential Access	Network Share Discovery	Data from Local System		Custom Cryptographic Protocol
Spearphishing via Service	Exploitation for Client Execution	BITS Jobs	DLL Search Order Hijacking	Component Firmware	Component Object Model Hijacking	Forced Authentication	Pass the Hash	Data from Network Shared Drive		Data Encoding
Supply Chain Compromise	Graphical User Interface	Bootkit	Dylib Hijacking	Component Object Model Hijacking	Component Object Model Hijacking	Forced Authentication	Pass the Ticket	Exfiltration Over Other Network Medium		Data Obfuscation
Trusted Relationship	InstallUtil	Browser Extensions	Change Default File Association	Control Panel Items	Control Panel Items	Forced Authentication	Remote Desktop Protocol	Data Staged		Domain Fronting
Valid Accounts	Launchctl	Change Default File Association	Component Firmware	DCShadow	DCShadow	Forced Authentication	Remote File Copy	Remote Services		Fallback Channels
	Local Job Scheduling	Component Object Model Hijacking	Component Object Model Hijacking	Deobfuscate/Decode Files or Information	Deobfuscate/Decode Files or Information	Forced Authentication	Replication Through Removable Media	Email Collection		Multi-hop Proxy
	LSASS Driver	Create Account	Component Object Model Hijacking	Extra Window Memory Injection	Extra Window Memory Injection	Forced Authentication	Query Registry	Input Capture		Multi-Stage Channels
	Mshta	DLL Search Order Hijacking	Component Object Model Hijacking	File System Permissions Weakness	File System Permissions Weakness	Forced Authentication	Query Registry	Man in the Browser		
	PowerShell	Dylib Hijacking	Component Object Model Hijacking	DLL Side-Loading	DLL Side-Loading	Forced Authentication	Query Registry	Scheduled Transfer		
	Regsvcs/Regasm	Dylib Hijacking	Component Object Model Hijacking	Disabling Security Tools	Disabling Security Tools	Forced Authentication	Query Registry			Multiband Communication
	Regsvr32	External Remote Services	Component Object Model Hijacking	File System Permissions Weakness	File System Permissions Weakness	Forced Authentication	Query Registry			Multilayer Encryption
	Rundll32	File System Permissions Weakness	Component Object Model Hijacking	File System Weakness	File System Weakness	Forced Authentication	Query Registry			Port Knocking
	Scheduled Task	File System Permissions Weakness	File System Permissions Weakness	File System Weakness	File System Weakness	Forced Authentication	Query Registry			Remote Access Tools
	Scripting	Hidden Files and Directories	File System Permissions Weakness	File System Weakness	File System Weakness	Forced Authentication	Query Registry			Remote File Copy
	Service Execution	Hidden Files and Directories	File System Permissions Weakness	File System Weakness	File System Weakness	Forced Authentication	Query Registry			Standard Application Layer Protocol
	Signed Binary Proxy Execution	Hooking	Hidden Files and Directories	File System Weakness	File System Weakness	Forced Authentication	Query Registry			Standard Cryptographic Protocol
	Signed Script Proxy Execution	Hypervisor	Hidden Files and Directories	File System Weakness	File System Weakness	Forced Authentication	Query Registry			Standard Non-Application Layer Protocol
		Image File Execution Options Injection	Hidden Files and Directories	File System Weakness	File System Weakness	Forced Authentication	Query Registry			
		Scheduled Task	Hidden Files and Directories	File System Weakness	File System Weakness	Forced Authentication	Query Registry			
			Hidden Files and Directories	File System Weakness	File System Weakness	Forced Authentication	Query Registry			
				Hidden Files and Directories	File System Weakness	Forced Authentication	Query Registry			
					Hidden Files and Directories	Forced Authentication	Query Registry			
						Hidden Users	System Owner/User			



A little better..

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	31 items	56 items	28 items	59 items	20 items	19 items	17 items	13 items	9 items	21 items
Drive-by Compromise	AppleScript CMSTP	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port Communication Through Removable Media
Exploit Public-Facing Application	Command-Line Interface	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	
Hardware Additions		AppCert DLLs		BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	ApplnIt DLLs	ApplnIt DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Credentials in Files	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	Clear Command History	Credentials in Registry	Network Service Scanning	Exploitation of Remote Services	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package		CMSTP		Logon Scripts		Data from Network Shared Drive		
Spearphishing via Service	Execution through Module Load	BITS Jobs	Bypass User Account Control	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Hash		Exfiltration Over Command and Control Channel	Data Encoding
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	DLL Search Order Hijacking	Component Firmware		Pass the Ticket		Data from Network Shared Drive		Data Obfuscation
Trusted Relationship	Browser Extensions	Change Default File Association	Dylib Hijacking	Component Object Model Hijacking	Forced Authentication	>Password Policy Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Other Network Medium	Domain Fronting
Valid Accounts	Graphical User Interface			Control Panel Items	Hooking	Peripheral Device Discovery	Remote File Copy	Data Staged		Fallback Channels
	InstallUtil	Component Firmware	Exploitation for Privilege Escalation	DCShadow	Input Capture	Remote Services	Email Collection		Exfiltration Over Physical Medium	Multi-hop Proxy
	Launchctl	Component Object Model Hijacking	Extra Window Memory Injection	Deobfuscate/Decode Files or Information	Input Prompt	Input Capture	Input Capture			Multi-Stage Channels
	Local Job Scheduling	Create Account		Disabling Security Tools	Kerberoasting	Process Discovery	Replication Through Removable Media	Man in the Browser	Scheduled Transfer	Multiband Communication
	LSASS Driver	DLL Search Order Hijacking	File System Permissions Weakness	DLL Side-Loading	Keychain	Query Registry	Query Registry	Shared Webroot	Screen Capture	Multilayer Encryption
	Mshta			Network Sniffing		Remote System Discovery	SSH Hijacking		Video Capture	Port Knocking
	PowerShell	Dylib Hijacking	Hooking	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning	Security Software Discovery	Taint Shared Content			Remote Access Tools
	Regsvcs/Regasm	External Remote Services	Image File Execution Options Injection	Exploitation for Defense Evasion	>Password Filter DLL					Remote File Copy
	Regsvr32				Private Keys	System Information Discovery				
	Rundll32	File System Permissions Weakness	Launch Daemon	Extra Window Memory Injection		Third-party Software				Standard Application Layer Protocol
	Scheduled Task		New Service	File Deletion	Replication Through Removable Media	System Network Configuration Discovery	Windows Admin Shares			Standard Cryptographic Protocol
	Scripting	Hidden Files and Directories	Path Interception	File System Logical Offsets	Securityd Memory	System Network Connections	Windows Remote Management			Standard Non-... ...
	Service Execution				Two-Factor Authentication Interception					
	Signed Binary Privacy	Hooking	Plist Modification	Gatekeeper Bypass						



We visualize each type of thing *separately*

Data Source Availability

filters

stages: act
platforms: windows, linux, mac

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	OS
10 items	31 items	50 items	28 items	50 items	20 items	19
Drive-by Compromise	App/Script	base, profile and basic	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Access
Exploit Public-Facing	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Base64 History	Access
Hardware Address	Command-Line Interface	App/GUI DLLs	App/GUI DLLs	BITS Jobs	Brute Force	Root
HTTP Network	Control Panel Items	App/HLL DLLs	App/HLL DLLs	Bypass User Account Control	Credential Dumping	Root
Speakingn Attachment	DYNAMIC Data Exchange	Application Shimming	Application Shimming	Clear Command History	Credential In Files	Root
Speakingn Link	Execution through API	Authentication Package	Bypass User Account Control	Credentials in Registry	File	Root
Speakingn via Service	Execution Through Module	BITS Jobs	CCU Search Order Hijacking	Component Firmware	Component Firmware	Root
Supply Chain Compromise	Fileless	Clipboard	Code Signing	Component Object Model	Component Object Model	Root
Trusted Relationship	Graphical User Interface	Component Framework	Component Object Model	Container Object Model	Container Object Model	Root
Valid Accounts	Browser Extensions	Component Object Model	Container Object Model	Container Object Model	Container Object Model	Root
Impersonate	Change Default File	Container Object Model	Container Object Model	Container Object Model	Container Object Model	Root
Launchd	Component Framework	Control Panel Items	Container Object Model	Container Object Model	Container Object Model	Root
Local Job Scheduling	Component Object Model	Containers	Container Object Model	Container Object Model	Container Object Model	Root
Power Driver	Create Account	Container Object Model	Container Object Model	Container Object Model	Container Object Model	Root
Metric	DLL Search Order Hijacking	Container Object Model	Container Object Model	Container Object Model	Container Object Model	Root
PowerShell	Clipboard	Container Object Model	Container Object Model	Container Object Model	Container Object Model	Root
RegEx/Regasm	New Service	Container Object Model	Container Object Model	Container Object Model	Container Object Model	Root
Regexec/Regasm	DLL Side-Loading	Container Object Model	Container Object Model	Container Object Model	Container Object Model	Root
Regexec/Regasm	Network Sniffing	Container Object Model	Container Object Model	Container Object Model	Container Object Model	Root
Runfile	Path Interception	Exploitation for Defense	Exploitation for Defense	Exploit Filter DLL	Exploit Filter DLL	Root
Runfile	File System Permissions	Root				
Runfile	File Modification	File System Permissions	File System Permissions	File System Permissions	File System Permissions	Root
Runfile	File Deletion	File System Permissions	File System Permissions	File System Permissions	File System Permissions	Root
Scheduled Task	Hidden Files and Directories	File Deletion	File Deletion	File Deletion	File Deletion	Root
Scripting	Process Injection	File System Logical Objects	Root			
Service Execution	Hypervisor	File System Logical Objects	Root			
Service Execution	Gateway API	File System Logical Objects	Root			
Signed Binary Policy	Service Registry Permissions	File System Logical Objects	Root			
Signed Module and Script	Service Modules and Scripts	File System Logical Objects	Root			
Signed Script Prog. Exec.	Service Modules and Scripts	File System Logical Objects	Root			
Source	Launch Agent	File System Logical Objects	Root			
Space after Filename	Startup Items	HESTCONTROL	HESTCONTROL	HESTCONTROL	HESTCONTROL	Root
Third-party Software	Launchd	GUICONTROL	GUICONTROL	GUICONTROL	GUICONTROL	Root
Thrd	Local Job Scheduling	GUICONTROL	GUICONTROL	GUICONTROL	GUICONTROL	Root
Trusted Developer Utilities	Valid Accounts	Indicator Removal from Tools	Root			
User Execution	Web Shell	Indicator Removal on Host	Root			
User Execution	Login Screen	Indirect Command Execution	Indirect Command Execution	Indirect Command Execution	Indirect Command Execution	Root

Analytics (alert only)

filters

stages: act
platforms: windows, linux, ma

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
10 items	31 items	50 items	28 items	50 items	20 items
Drive-by Compromise	App/Script	base, profile and basic	Access Token Manipulation	Access Token Manipulation	Account Manipulations
Exploit Public-Facing	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Base64 History
Hardware Address	Command-Line Interface	App/GUI DLLs	App/GUI DLLs	BITS Jobs	Brute Force
HTTP Network	Control Panel Items	App/HLL DLLs	App/HLL DLLs	Bypass User Account Control	Credential Dumping
Speakingn Attachment	DYNAMIC Data Exchange	Application Shimming	Application Shimming	Clear Command History	Credential In Files
Speakingn Link	Execution through API	Authentication Package	Bypass User Account Control	CCU Search Order hijacking	Code Signing
Speakingn via Service	Execution Through Module	BITS Jobs	CCU Search Order hijacking	Component Firmware	Component Authentication
Supply Chain Compromise	Fileless	Clipboard	Clipboard	Component Firmware	Component Object Model
Trusted Relationship	Graphical User Interface	Browser Extensions	Container Object Model	Container Object Model	Container Object Model
Valid Accounts	Initial Access	Change Default File	Container Object Model	Container Object Model	Container Object Model
Impersonate	Launchd	Container Object Model	Container Object Model	Container Object Model	Container Object Model
Launchd	Local Job Scheduling	Component Firmware	Component Object Model	Component Object Model	Component Object Model
Local Job Scheduling	Power Driver	Container Object Model	Container Object Model	Container Object Model	Container Object Model
Power Driver	PowerShell	Container Object Model	Container Object Model	Container Object Model	Container Object Model
Metric	Runfile	Container Object Model	Container Object Model	Container Object Model	Container Object Model
Regexec/Regasm	Runfile	Container Object Model	Container Object Model	Container Object Model	Container Object Model
Regexec/Regasm	Runfile	Container Object Model	Container Object Model	Container Object Model	Container Object Model
Runfile	Runfile	Container Object Model	Container Object Model	Container Object Model	Container Object Model
Scheduled Task	Scripting	Container Object Model	Container Object Model	Container Object Model	Container Object Model
Scripting	Service Execution	Container Object Model	Container Object Model	Container Object Model	Container Object Model
Service Execution	Service Registry Permissions	Container Object Model	Container Object Model	Container Object Model	Container Object Model
Signed Binary Policy	Service Modules and Scripts	Container Object Model	Container Object Model	Container Object Model	Container Object Model
Signed Module and Script	Service Modules and Scripts	Container Object Model	Container Object Model	Container Object Model	Container Object Model
Signed Script Prog. Exec.	Service Modules and Scripts	Container Object Model	Container Object Model	Container Object Model	Container Object Model
Source	Launch Agent	File System Logical Objects			
Space after Filename	Startup Items	HESTCONTROL	HESTCONTROL	HESTCONTROL	HESTCONTROL
Third-party Software	Launchd	GUICONTROL	GUICONTROL	GUICONTROL	GUICONTROL
Thrd	Local Job Scheduling	GUICONTROL	GUICONTROL	GUICONTROL	GUICONTROL
Trusted Developer Utilities	Valid Accounts	Indicator Removal from Tools			
User Execution	Web Shell	Indicator Removal on Host			
User Execution	Login Screen	Indirect Command Execution	Indirect Command Execution	Indirect Command Execution	Indirect Command Execution





What about DETECTION of
adversary techniques?

Does measuring the
quality of my data
really help me find
compromise?



E.



Using statistics to universally measure

Credit to the *Towards Data Science* blog and their article “Beyond Accuracy: Precision and Recall”



E.

Threat Hunting vs Detection



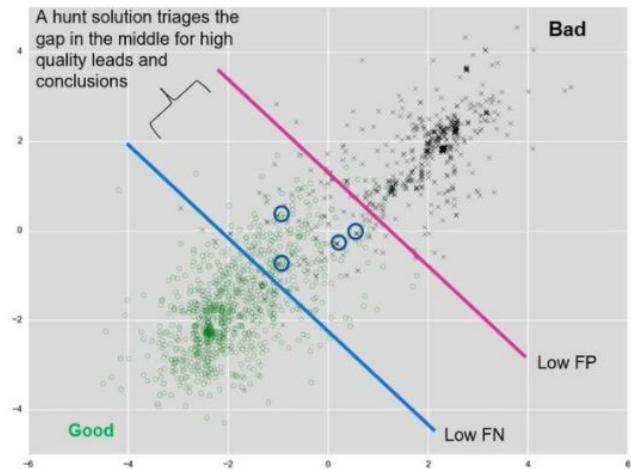
Chris Gerritz @gerritzc · Mar 15

Why most prevention and detection tools make poor #ThreatHunting solutions in one slide. @InfocyteInc

Threat Hunting vs Detection - The Optimization Problem

Why do most defensive tools make poor hunt tools?

- Prevention and real-time detection solutions are **optimized for low False Positive (FP) Alerting**
- Hunt solutions are **optimized for low False Negatives (FN)**
 - For Hunting: Anomalies, Outliers, and Suspicious Activity are leads, not FPs to be tuned out
 - A good hunt solution sorts and scores leads, then enables a quick path to verify and investigate to a conclusion



Original Diagram Source: [CrowdStrike's Blog on Machine Learning](#)





Precision is being tolerant of False Positives

True Positive - a malicious thing
you correctly identify as
malicious

False Positive - a benign thing
you incorrectly identify as
malicious

$\text{Precision} = (\text{True Positives}/(\text{True Positives} + \text{False Positives}))$

Example:

100 events

74 TPs

26 FPs

0.74 precision



E.



Recall is how well you find malicious activity

True Positive - a malicious thing
you correctly identify as
malicious

False Negative - a malicious
thing you incorrectly identify as
benign

Recall = (True Positives/(True
Positives + False Negatives))

Example:

100 events

55 TPs

21 FPs

24 FNs

0.69 recall



E.



But be wary of extremes

Perfect recall finds all the threat activity while also generating tons of false positives.

Perfect precision might find nothing to be malicious, missing all the threat activity without generating any false positives.

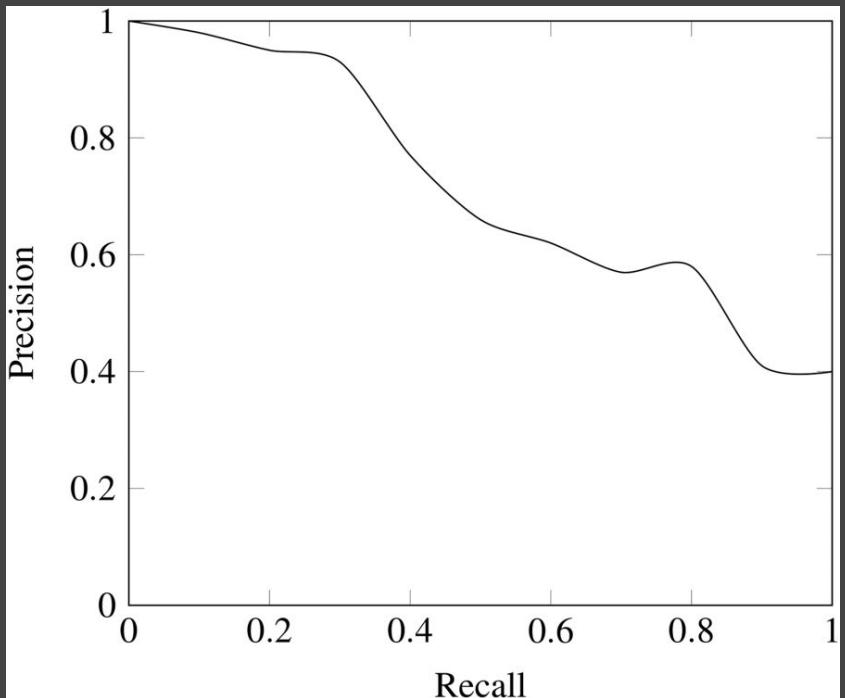


Image credit:

<https://towardsdatascience.com/beyond-accuracy-precision-and-recall-3da06bea9f6c>





Wait a darn minute, you skipped something!

How do you determine False Negatives?

1. Adversary simulation tools will show you
2. Your red team will tell you
3. Third parties doing offensive security work for you will deliver a report on it

Note:

- Many organizations will begin testing in a lab or other contrived environment which need to be representative of your enterprise
- If you're hunting, your environment will absolutely change between measurements
- This is best effort
- Vendors often have helpful telemetry, so they have a leg up on measuring recall
- **Data quality directly influences precision and recall**





Quantifying detections using precision and recall

An F1 Score is a value between 0 and 1 that describes how well you judge something to be malicious using precision and recall:

$$F_1 = 2 * \frac{precision * recall}{precision + recall}$$

Image credit:

<https://towardsdatascience.com/beyond-accuracy-precision-and-recall-3da06bea9f6c>

Those examples from before gave us a precision of 0.74 and a recall of 0.69, let's see our F1 score:

$$F1 = 2 * (0.51/1.43) = 0.71$$

But this value doesn't mean anything to us - at least not yet.





F1 scores are a kind of tolerance for classification

Threshold	TP	FP	TN	FN
0.0	50	50	0	0
0.1	48	47	3	2
0.2	47	40	9	4
0.3	45	31	16	8
0.4	44	23	22	11
0.5	42	16	29	13
0.6	36	12	34	18
0.7	30	11	38	21
0.8	20	4	43	33
0.9	12	3	45	40
1.0	0	0	50	50

What does a 0.71 mean? It means we're capable of finding 60% of malicious things.

Image credit:

<https://towardsdatascience.com/beyond-accuracy-precision-and-recall-3da06bea9f6c>





F1 scores are a kind of tolerance for classification

Threshold	TP	FP	TN	FN
0.0	50	50	0	0
0.1	48	47	3	2
0.2	47	40	9	4
0.3	45	31	16	8
0.4	44	23	22	11
0.5	42	16	29	13
0.6	36	12	34	18
0.7	30	11	38	21
0.8	20	4	43	33
0.9	12	3	45	40
1.0	0	0	50	50

Image credit:

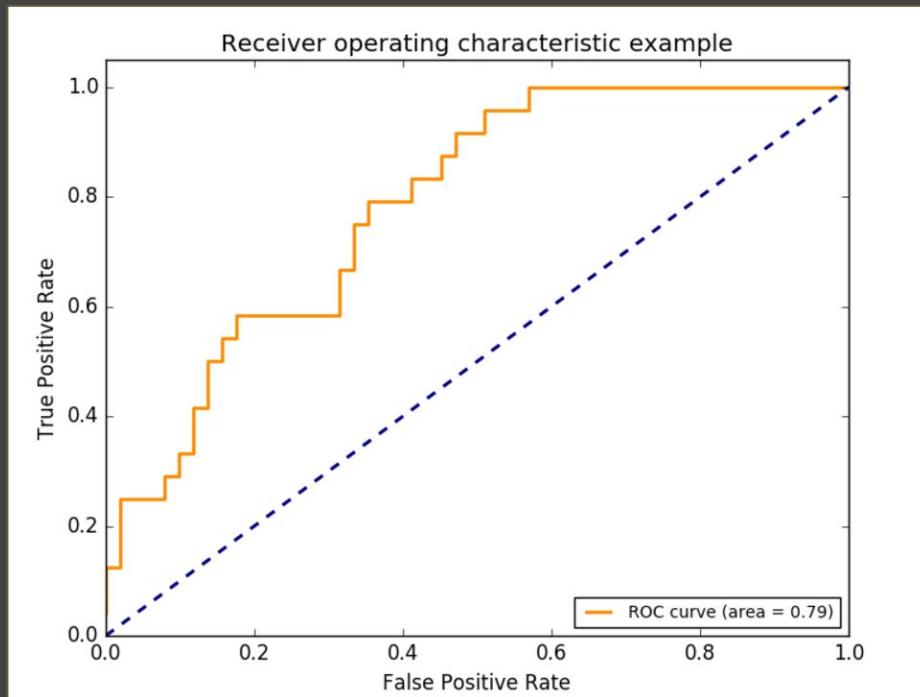
<https://towardsdatascience.com/beyond-accuracy-precision-and-recall-3da06bea9f6c>

Do you have a requirement to find 80% of malicious things? Try a threshold of 0.4.

Work backwards to figure out acceptable precision and recall values for this goal.



We can even try to find ideal thresholds!



Data science gives us tools for judging how well a classifier works, like how well we judge something to be malicious - this is what many machine learning malware classifiers do.

First, a Receiver Operator Characteristic (ROC) curve looks at TP and FP rates on X and Y axes to help display how well our chosen threshold (F1 score) works.

Measuring the area under the curve (AUC) for ROC values is the *quantification* of how well our classification works given our tolerance for TP and FP values.

Plot these on a regular basis to determine if your detection improves or not.



Image credit: qiita.com





Closing thoughts

We could keep going with this topic



E.

Links and things (if we talked about it, here it is):

Thing	Link
MITRE ATT&CK	https://attack.mitre.org
MITRE CAR	https://car.mitre.org/wiki/Main_Page
MITRE common data model	https://car.mitre.org/wiki/Data_Model
Roberto's Github (Sysmon configs, hunter's playbook, HELK, OSSEM, Invoke-AttackAPI)	https://github.com/Cyb3rWard0g
Endgame Github (RTA, other things)	https://github.com/endgameinc/



Thank you

If you didn't get a chance to ask a question, come chat with us in person or reach out via social media!

Also we are thankful to the Beyond Data Science blog, MITRE, the ATT&CK team, authors of simulation tools and everyone out there helping change the landscape for defenders.



This is an appendix

All this is stuff we wanted you to have



E.



Quick wins

Count	Technique
92	Remote File Copy
92	Standard Application Layer Protocol
91	Command-Line Interface
85	System Information Discovery
75	File and Directory Discovery
70	Credential Dumping
68	Process Discovery
67	Registry Run Keys /Start Folder
62	File Deletion
57	Input Capture

# Techniques	Data Source
149	Process monitoring
86	File monitoring
82	Process command-line parameters
36	API monitoring
34	Windows Registry
34	Process use of network
31	Packet capture
28	Authentication logs
23	Netflow/Enclave netflow
17	Binary File Metadata





Data Sources -> Adversary Techniques

# Techniques	Name
149	Process monitoring
86	File monitoring
82	Process command-line parameters
36	API monitoring
34	Windows Registry
34	Process use of network
31	Packet capture
28	Authentication logs
23	Netflow/Enclave netflow

# Techniques	Name
17	Binary file metadata
16	DLL monitoring
16	Network protocol analysis
14	Windows event logs
12	Loaded DLLs
9	System calls
8	SSL/TLS inspection
8	Malware reverse engineering
6	Anti-virus





Data Sources -> Adversary Techniques

# Techniques	Name
6	Data loss prevention
5	Application Logs
4	Network device logs
4	Windows Error Reporting
4	Network intrusion detection system
4	User interface
4	Web proxy
3	Kernel drivers
3	Services

# Techniques	Name
3	Email gateway
3	Third-party application logs
2	Mail server
2	Detonation chamber
2	MBR
2	Environment variable
2	BIOS
2	Host network interface
1	Web logs





Data Sources -> Adversary Techniques

# Techniques	Name
1	Asset Management
1	Web application firewall logs
1	EFI
1	DNS records
1	Browser extensions
1	Sensor health and status
1	Named Pipes
1	VBR
1	PowerShell logs

# Techniques	Name
1	Access Tokens
1	Digital Certificate Logs
1	WMI Objects

