Leveraging MITRE ATT&CK ™

The Common Language

SANSFIRE 18 June 2019

Your Host for Today

Erik Van Buggenhout
SANS Certified Instructor
Co-Founder NVISO
@ErikVaBu

At SANS:
2009 -> 2012: Local Mentor (SEC560)
2012 -> 2016: Community Instructor (SEC560)
2016 -> Now: Certified Instructor & Author (SEC599)

Other:
2008 -> 2012: Penetration Testing & Big 4
2012 -> Now: NVISO (Adversary Emulation)

The Agenda for Today

WHAT WE’D LIKE TO DISCUSS

1. What is MITRE ATT&CK

Introduction

2. ATT&CK use cases

How can MITRE ATT&CK be used?

3. ATT&CK initiatives

Some interesting references

4. Demo - CALDERA

Demonstration of a tool

5. Q&A

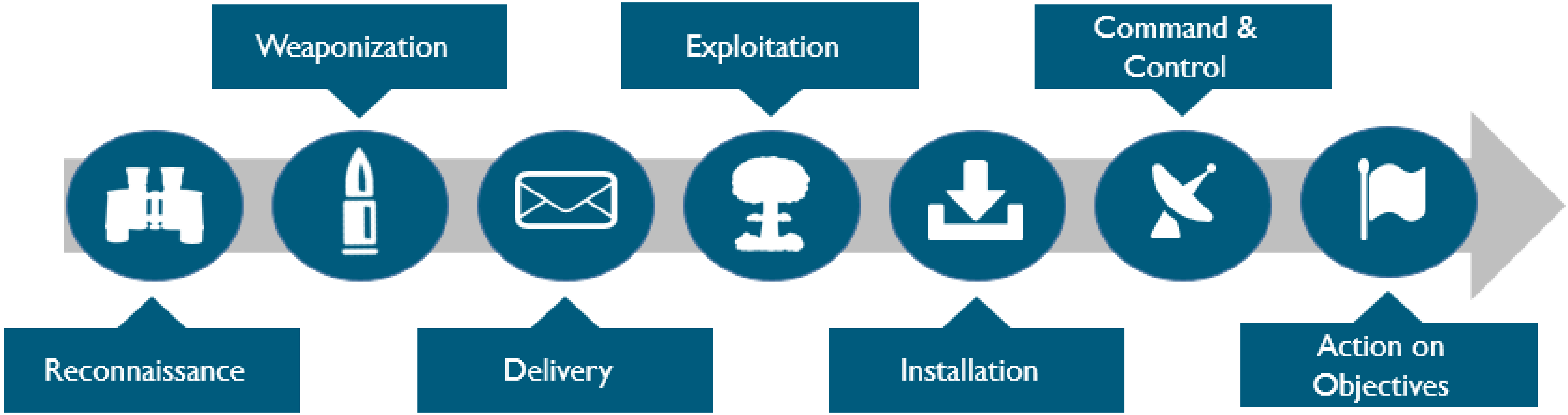
Ask us your questions!

What is MITRE ATT&CK

Introduction

Kill Chain vs ATT&CK

Where does ATT&CK come from?



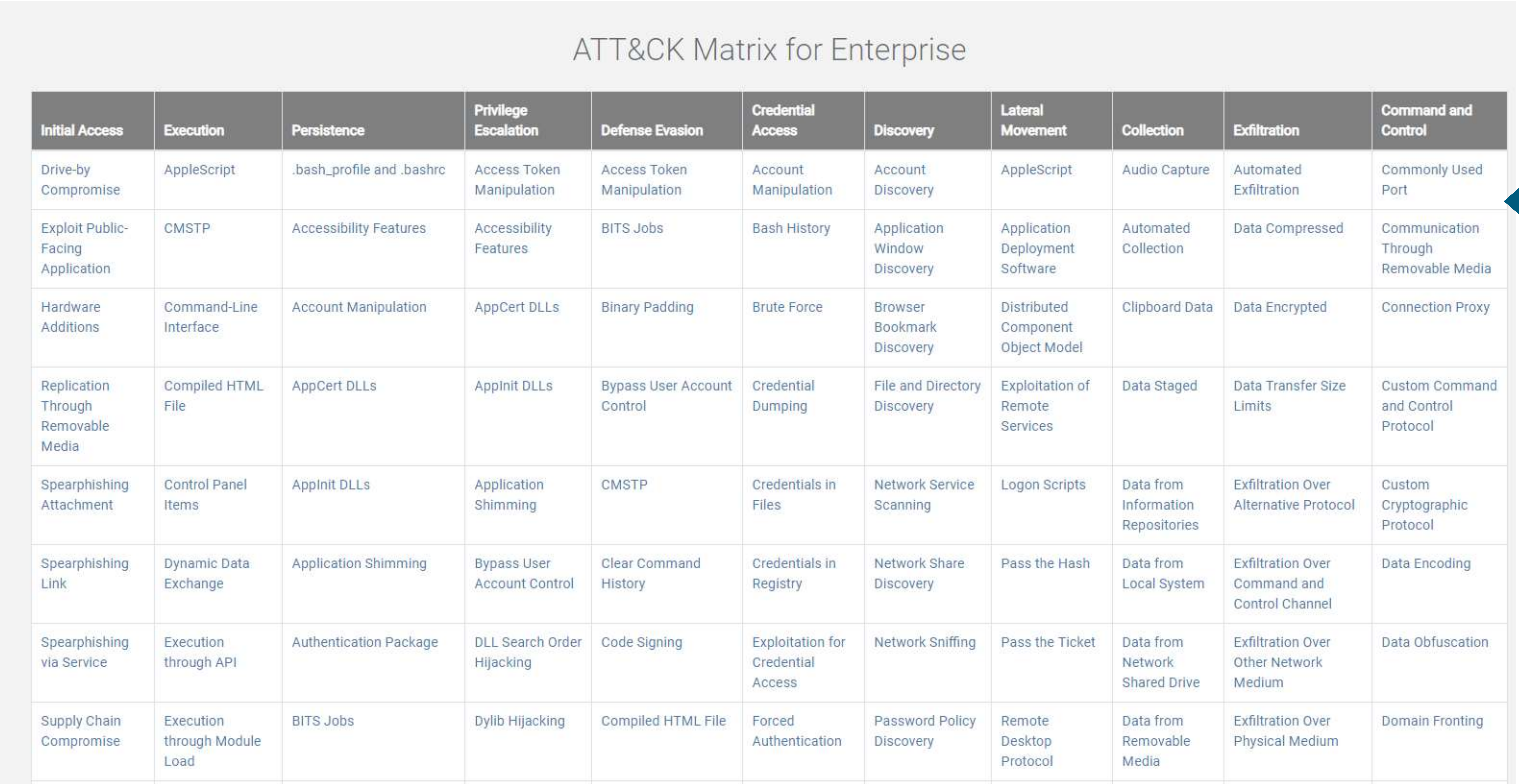
The Cyber Kill Chain provides a 30.000ft view of an attack

“Action on Objectives” covers a lot of stuff…
Good for a general overview, but how do you make this actionable?

MITRE ATT&CK?

What is MITRE ATT&CK

ATT&CK™
Adversarial Tactics, Techniques
& Common Knowledge



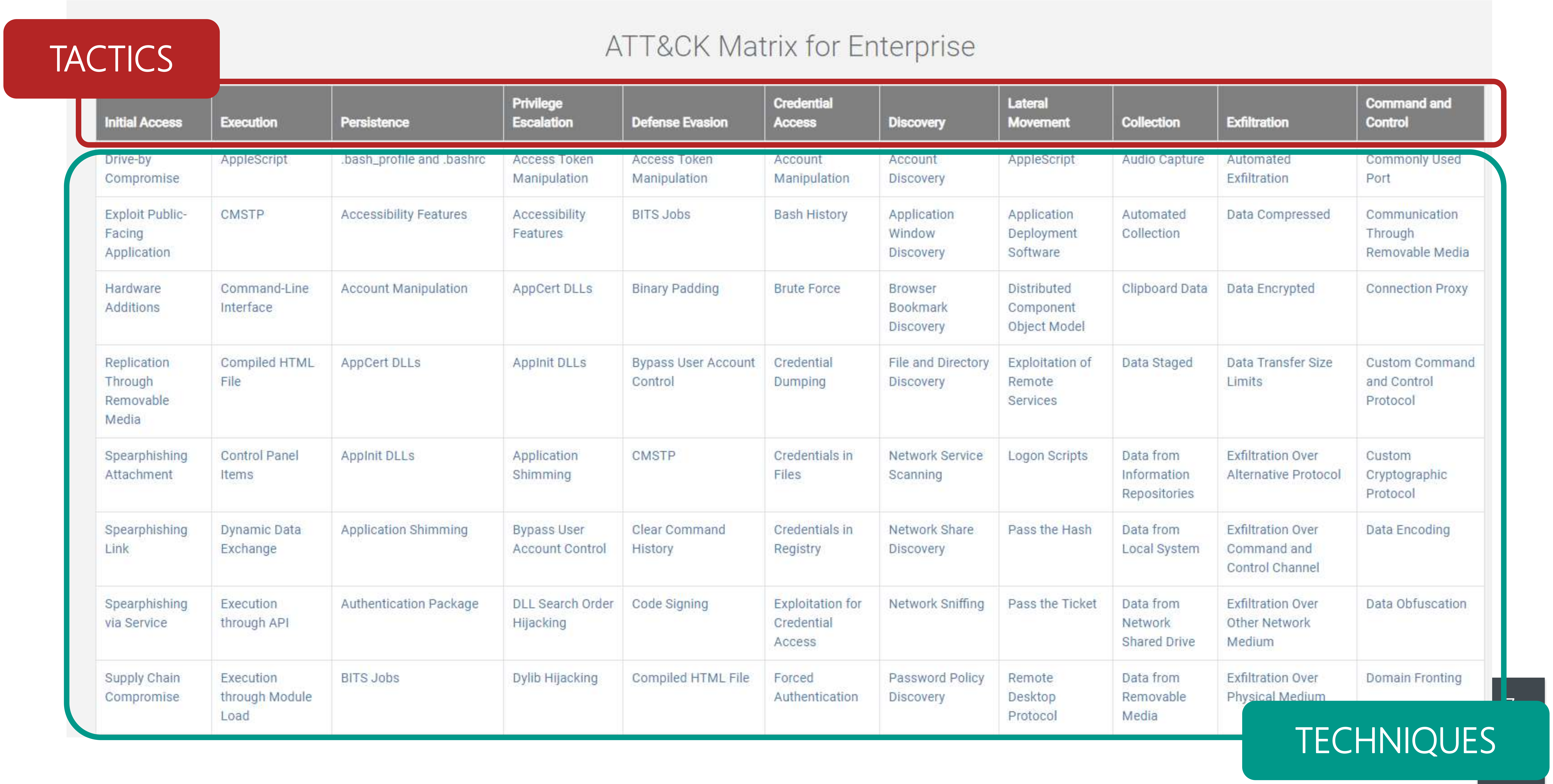
ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.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	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting

MITRE has developed the ATT&CK Matrix as a central repository for adversary TTP's. It is used by red teams and blue teams alike. It is rapidly gaining traction as a de facto standard!

MITRE ATT&CK?

Tactics vs Techniques



ATT&CK Matrix for Enterprise

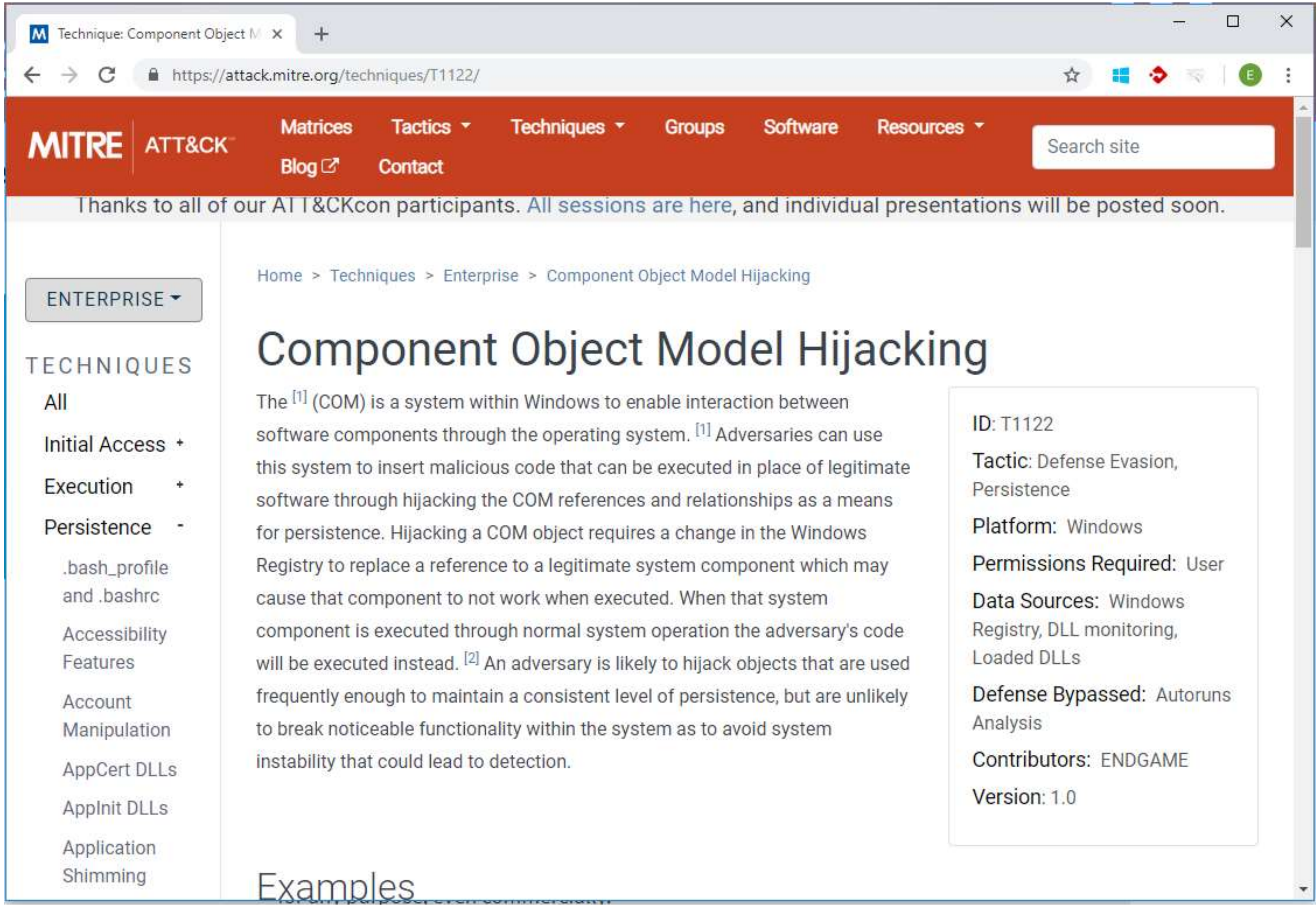
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting

TACTICS

TECHNIQUES

MITRE ATT&CK?

Zooming in on a technique



Thanks to all of our ATT&CKcon participants. All sessions are here, and individual presentations will be posted soon.

Home > Techniques > Enterprise > Component Object Model Hijacking

Component Object Model Hijacking

The [1] (COM) is a system within Windows to enable interaction between software components through the operating system. [1] Adversaries can use this system to insert malicious code that can be executed in place of legitimate software through hijacking the COM references and relationships as a means for persistence. Hijacking a COM object requires a change in the Windows Registry to replace a reference to a legitimate system component which may cause that component to not work when executed. When that system component is executed through normal system operation the adversary's code will be executed instead. [2] An adversary is likely to hijack objects that are used frequently enough to maintain a consistent level of persistence, but are unlikely to break noticeable functionality within the system as to avoid system instability that could lead to detection.

ID: T1122

Tactic: Defense Evasion, Persistence

Platform: Windows

Permissions Required: User

Data Sources: Windows Registry, DLL monitoring, Loaded DLLs

Defense Bypassed: Autoruns Analysis

Contributors: ENDGAME

Version: 1.0

Examples

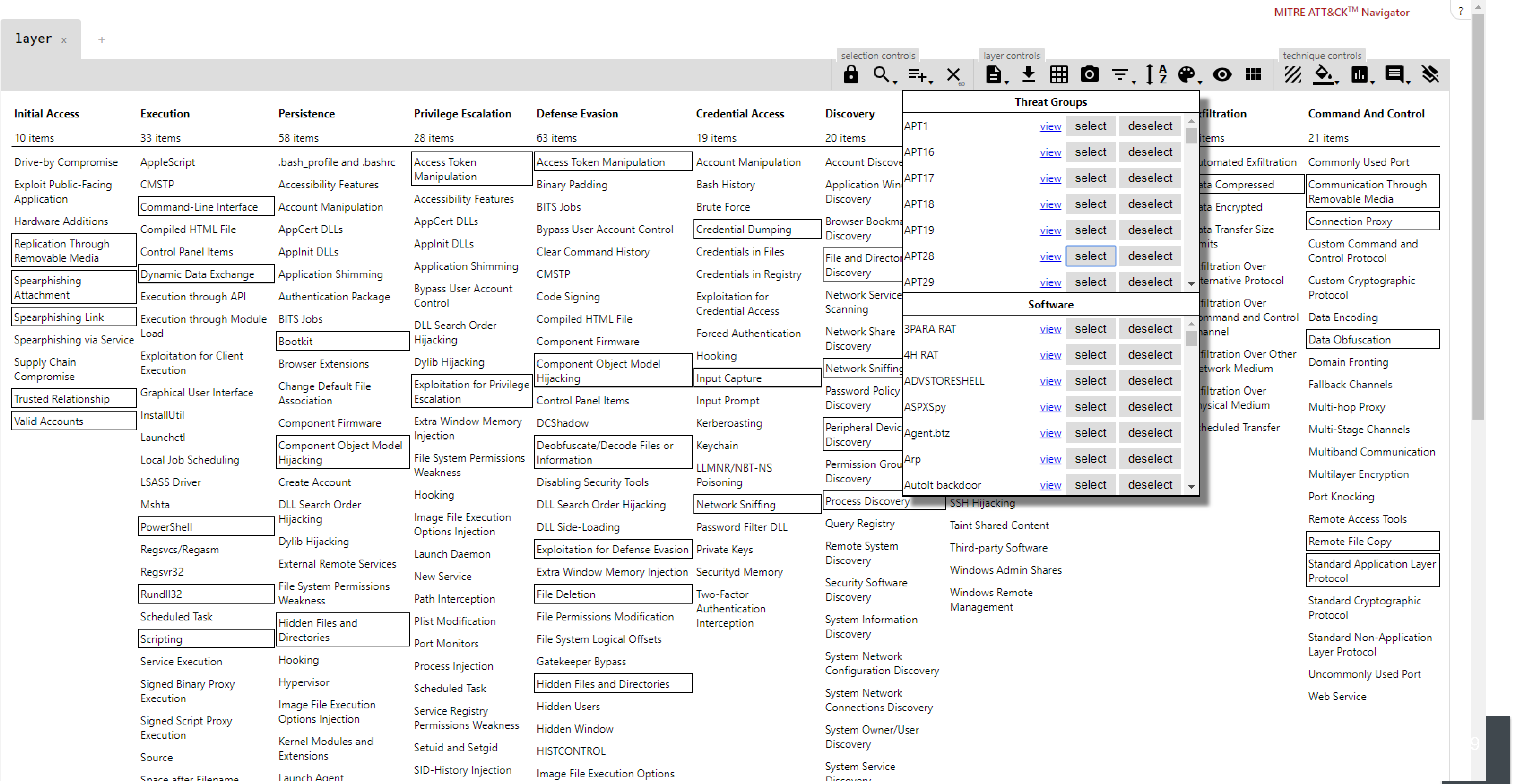
As an example, let's have a look at one of Turla's favorite techniques: COM object hijacking. In MITRE's ATT&CK framework, this technique is known as T1122, and it's part of the "Defense Evasion" and "Persistence" tactics for Windows.

For every one of these techniques, MITRE includes a dedicated entry with amongst others:

- Technique information
- Known adversaries that use it
- Detection opportunities
- Prevention opportunities

ATT&CK Navigator

Operationalizing ATT&CK



Initial Access
10 items
Drive-by Compromise
Exploit Public-Facing Application
Hardware Additions
Replication Through Removable Media
Spearphishing Attachment
Spearphishing Link
Spearphishing via Service
Supply Chain Compromise
Trusted Relationship
Valid Accounts

Execution
33 items
AppleScript
CMSTP
Command-Line Interface
Compiled HTML File
Control Panel Items
Dynamic Data Exchange
Execution through API
Execution through Module Load
Exploitation for Client Execution
Graphical User Interface
InstallUtil
Launchctl
Local Job Scheduling
LSASS Driver
Mshta
PowerShell
Regsvcs/Regasm
Regsvr32
Rundll32
Scheduled Task
Scripting
Service Execution
Signed Binary Proxy Execution
Signed Script Proxy Execution
Source
Space after Filename

Persistence
58 items
.bash_profile and .bashrc
Accessibility Features
Account Manipulation
AppCert DLLs
AppInit DLLs
Application Shimming
Authentication Package
BITS Jobs
Bootkit
Browser Extensions
Change Default File Association
Component Firmware
Component Object Model Hijacking
Create Account
DLL Search Order Hijacking
Dylib Hijacking
External Remote Services
File System Permissions Weakness
Hidden Files and Directories
Hooking
Hypervisor
Image File Execution Options Injection
Kernel Modules and Extensions
Launch Agent

Privilege Escalation
28 items
Access Token Manipulation
Accessibility Features
AppCert DLLs
AppInit DLLs
Application Shimming
Bypass User Account Control
DLL Search Order Hijacking
Dylib Hijacking
Exploitation for Privilege Escalation
Extra Window Memory Injection
File System Permissions Weakness
Hooking
Image File Execution Options Injection
Launch Daemon
New Service
Path Interception
Plist Modification
Port Monitors
Process Injection
Scheduled Task
Service Registry Permissions Weakness
Setuid and Setgid
SID-History Injection

Defense Evasion
63 items
Access Token Manipulation
Binary Padding
BITS Jobs
Bypass User Account Control
Clear Command History
CMSTP
Code Signing
Compiled HTML File
Component Firmware
Component Object Model Hijacking
Control Panel Items
DCShadow
Deobfuscate/Decode Files or Information
Disabling Security Tools
DLL Search Order Hijacking
DLL Side-Loading
Exploitation for Defense Evasion
Extra Window Memory Injection
File Deletion
File Permissions Modification
File System Logical Offsets
Gatekeeper Bypass
Hidden Files and Directories
Hidden Users
Hidden Window
HISTCONTROL
Image File Execution Options

Credential Access
19 items
Account Manipulation
Bash History
Brute Force
Credential Dumping
Credentials in Files
Credentials in Registry
Exploitation for Credential Access
Forced Authentication
Hooking
Input Capture
Input Prompt
Kerberoasting
Keychain
LLMNR/NBT-NS Poisoning
Network Sniffing
Password Filter DLL
Private Keys
Securityd Memory
Two-Factor Authentication Interception

Discovery
20 items
Account Discove
Application Win Discovery
Browser Bookma Discovery
File and Director Discovery
Network Service Scanning
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Devic Discovery
Permission Grou Discovery
Process Discovery
Query Registry
Remote System Discovery
Security Software Discovery
System Information Discovery
System Network Configuration Discovery
System Network Connections Discovery
System Owner/User Discovery
System Service Discovery

SSH Hijacking
Taint Shared Content
Third-party Software
Windows Admin Shares
Windows Remote Management

filtration
items
tomated Exfiltration
ta Compressed
ta Encrypted
ta Transfer Size mits
filtration Over ternative Protocol
filtration Over mmand and Control annel
filtration Over Other twork Medium
filtration Over ysical Medium
heduled Transfer

Command And Control
21 items
Commonly Used Port
Communication Through Removable Media
Connection Proxy
Custom Command and Control Protocol
Custom Cryptographic Protocol
Data Encoding
Data Obfuscation
Domain Fronting
Fallback Channels
Multi-hop Proxy
Multi-Stage Channels
Multiband Communication
Multilayer Encryption
Port Knocking
Remote Access Tools
Remote File Copy
Standard Application Layer Protocol
Standard Cryptographic Protocol
Standard Non-Application Layer Protocol
Uncommonly Used Port
Web Service

Threat Groups

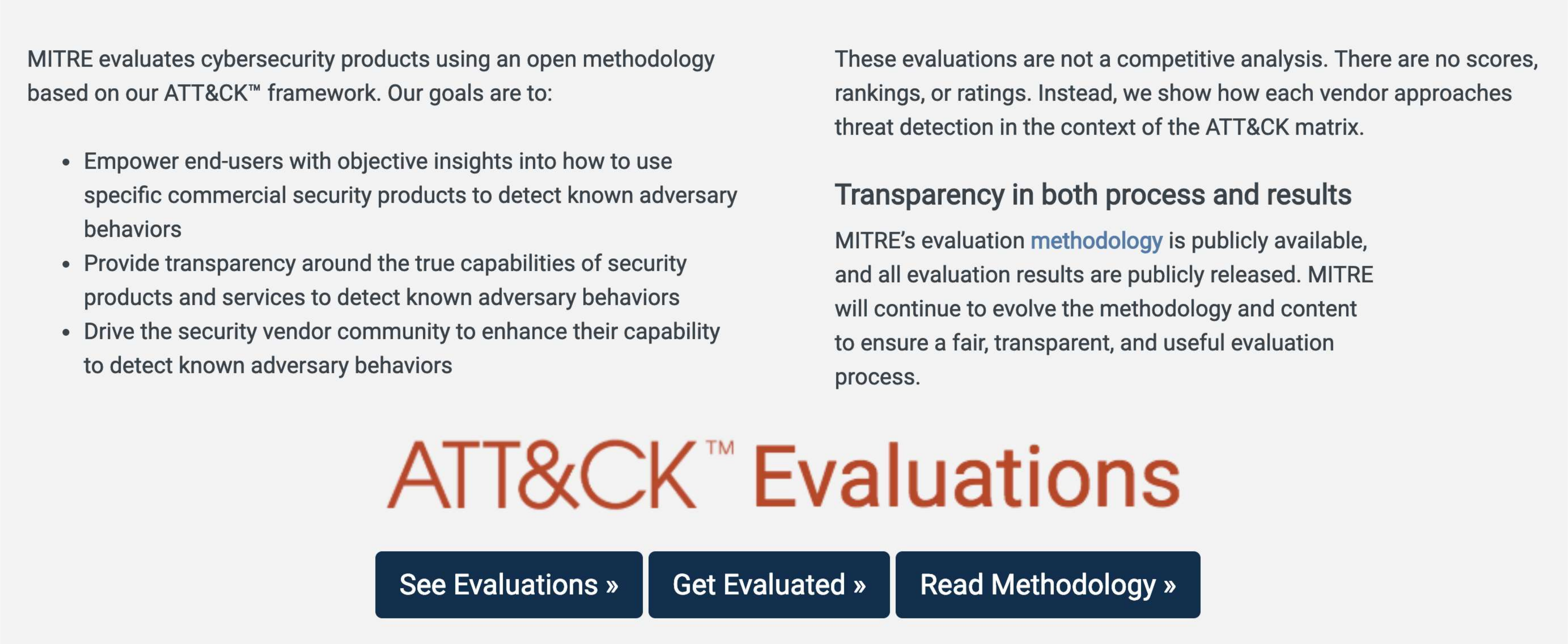
APT1	view	select	deselect
APT16	view	select	deselect
APT17	view	select	deselect
APT18	view	select	deselect
APT19	view	select	deselect
APT28	view	select	deselect
APT29	view	select	deselect

Software

3PARA RAT	view	select	deselect
4H RAT	view	select	deselect
ADVSTORESHELL	view	select	deselect
ASPXSpy	view	select	deselect
Agent.btz	view	select	deselect
Arp	view	select	deselect
Autolt backdoor	view	select	deselect

ATT&CK Evaluations

Using ATT&CK as a framework to evaluate products



MITRE evaluates cybersecurity products using an open methodology based on our ATT&CK™ framework. Our goals are to:

- Empower end-users with objective insights into how to use specific commercial security products to detect known adversary behaviors
- Provide transparency around the true capabilities of security products and services to detect known adversary behaviors
- Drive the security vendor community to enhance their capability to detect known adversary behaviors

These evaluations are not a competitive analysis. There are no scores, rankings, or ratings. Instead, we show how each vendor approaches threat detection in the context of the ATT&CK matrix.

Transparency in both process and results

MITRE's evaluation methodology is publicly available, and all evaluation results are publicly released. MITRE will continue to evolve the methodology and content to ensure a fair, transparent, and useful evaluation process.

ATT&CK™ Evaluations

Carbon Black.

FIREEYE™

CROWDSTRIKE

ATT&CK Use Cases

How can MITRE ATT&CK be used?

Key use cases for ATT&CK

ATT&CK as a common language!

ATT&CK Matrix for Enterprise

			Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection		Command and Co l
		nd .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Captu		mmonly Used Port
		eatures	Accessibility Features	BITS Jobs	Bash History	Application Window	Application Deployment oftware	Automated Collection		Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCer				istributed omponent bject Model			
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit				xploitation of emote ervices	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
			Applica Shimmi				Logon Scripts	Data fro Infor Rep		
		imming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data Loc		
		Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Netw Shared		
Supply Chain	Execution Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data from R Media	Exfiltration Over	Domain Fronting

Adversary emulation

Detection capability

ATT&CK™

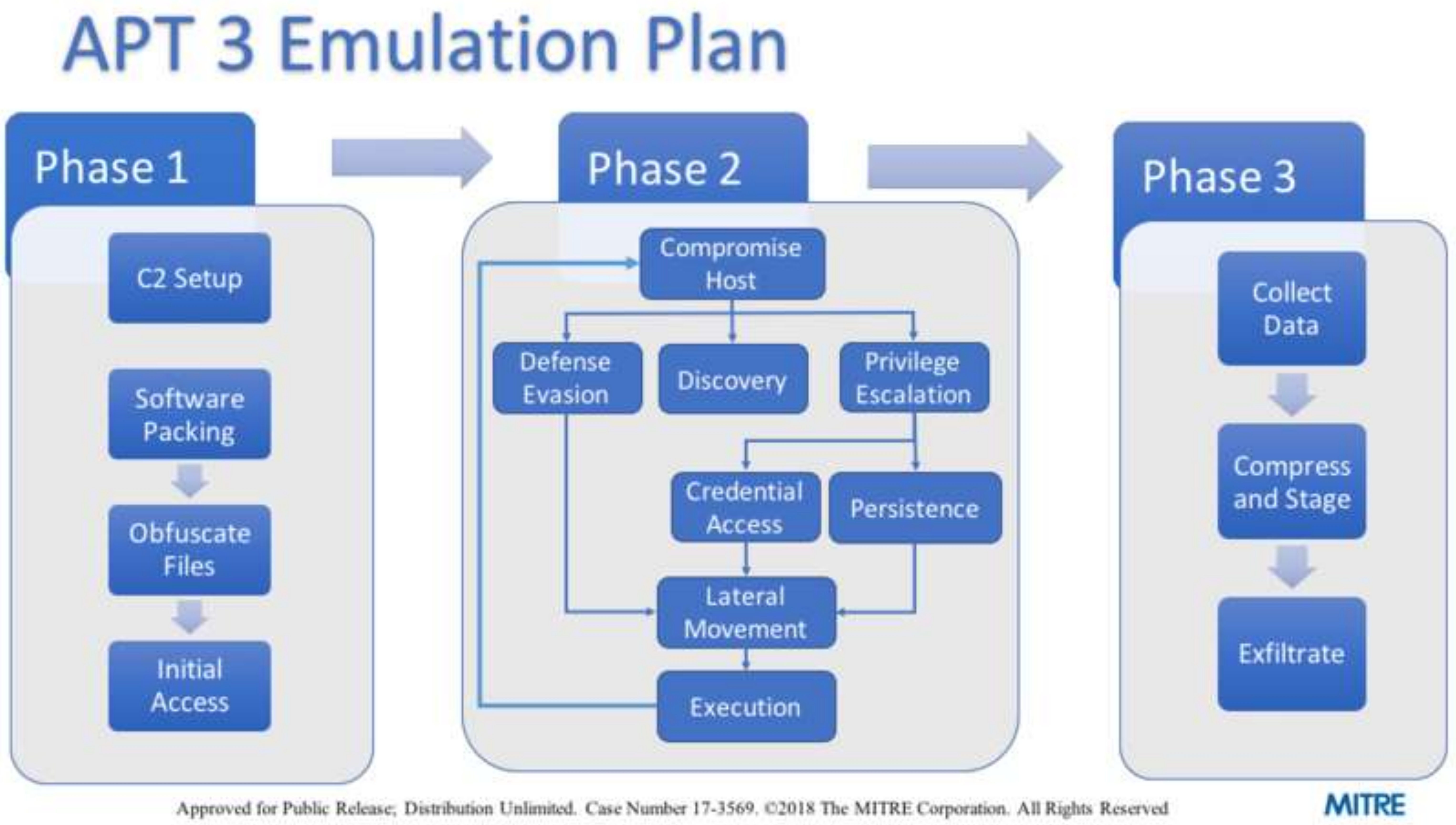
Adversarial Tactics, Techniques & Common Knowledge

Prioritize defenses

Threat Intelligence

SANS

ATT&CK for adversary emulation



APT 3 Emulation Plan

Phase 1

C2 Setup

Software Packing

Obfuscate Files

Initial Access

Phase 2

Compromise Host

Defense Evasion

Discovery

Privilege Escalation

Credential Access

Persistence

Lateral Movement

Execution

Phase 3

Collect Data

Compress and Stage

Exfiltrate

Approved for Public Release; Distribution Unlimited. Case Number 17-3569. ©2018 The MITRE Corporation. All Rights Reserved

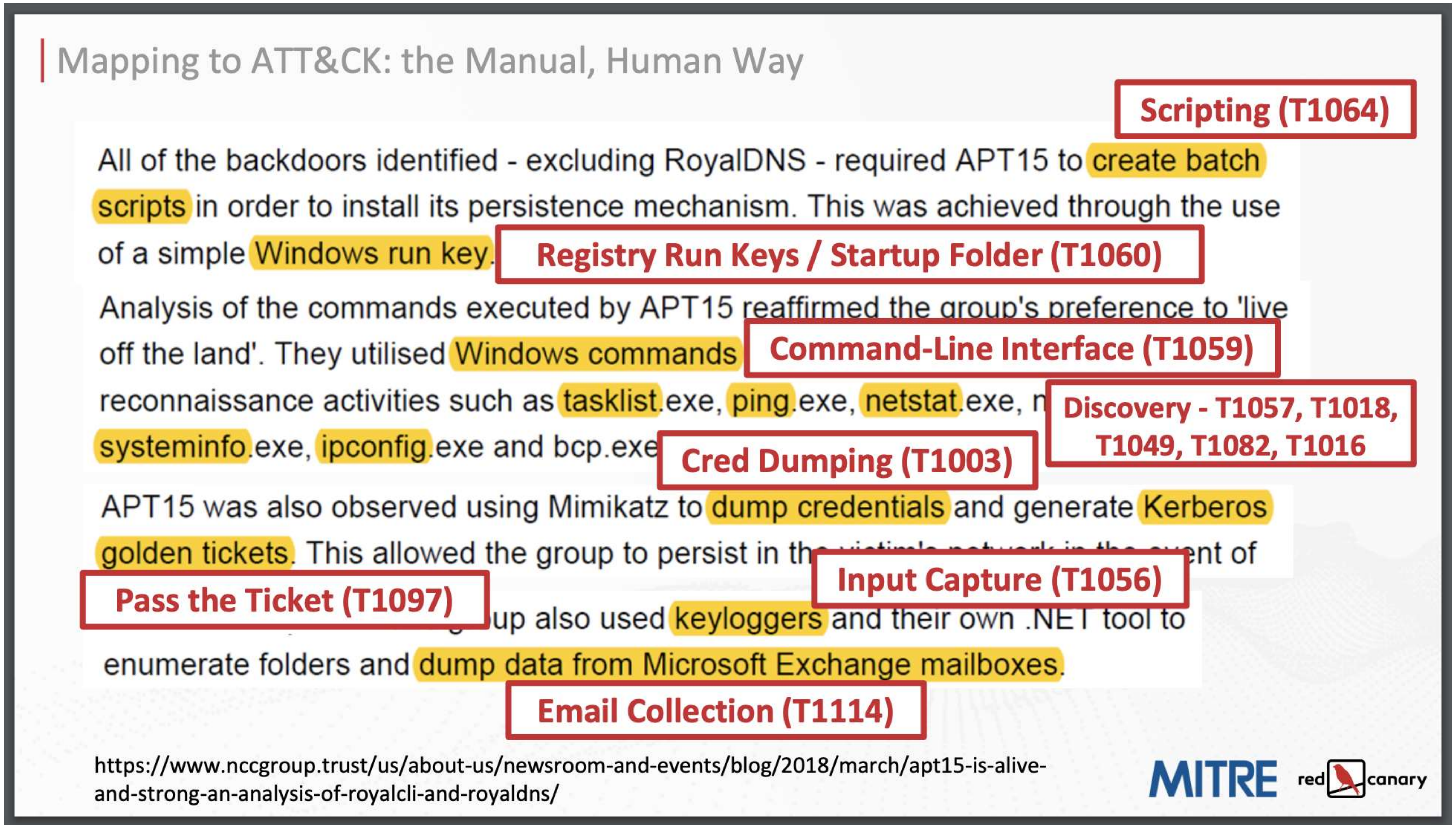
MITRE

When developing scenarios for red teaming / adversary emulation, red teams should use ATT&CK tactics and techniques to describe how the engagement will be delivered.

This will tremendously increase the value of the engagement, as it helps defenders map issues on a structured framework afterwards!

https://attack.mitre.org/resources/adversary-emulation-plans/

ATT&CK for threat intelligence



Mapping to ATT&CK: the Manual, Human Way

All of the backdoors identified - excluding RoyalDNS - required APT15 to create batch scripts in order to install its persistence mechanism. This was achieved through the use of a simple Windows run key.

Scripting (T1064)

Registry Run Keys / Startup Folder (T1060)

Analysis of the commands executed by APT15 reaffirmed the group's preference to 'live off the land'. They utilised Windows commands reconnaissance activities such as tasklist.exe, ping.exe, netstat.exe, n systeminfo.exe, ipconfig.exe and bcp.exe

Command-Line Interface (T1059)

Discovery - T1057, T1018, T1049, T1082, T1016

Cred Dumping (T1003)

APT15 was also observed using Mimikatz to dump credentials and generate Kerberos golden tickets. This allowed the group to persist in the victim's network in the event of

Pass the Ticket (T1097)

Input Capture (T1056)

up also used keyloggers and their own .NET tool to enumerate folders and dump data from Microsoft Exchange mailboxes.

Email Collection (T1114)

https://www.nccgroup.trust/us/about-us/newsroom-and-events/blog/2018/march/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/

MITRE red canary

ATT&CK techniques can be used to describe adversary activities in an understandable, structured, fashion.

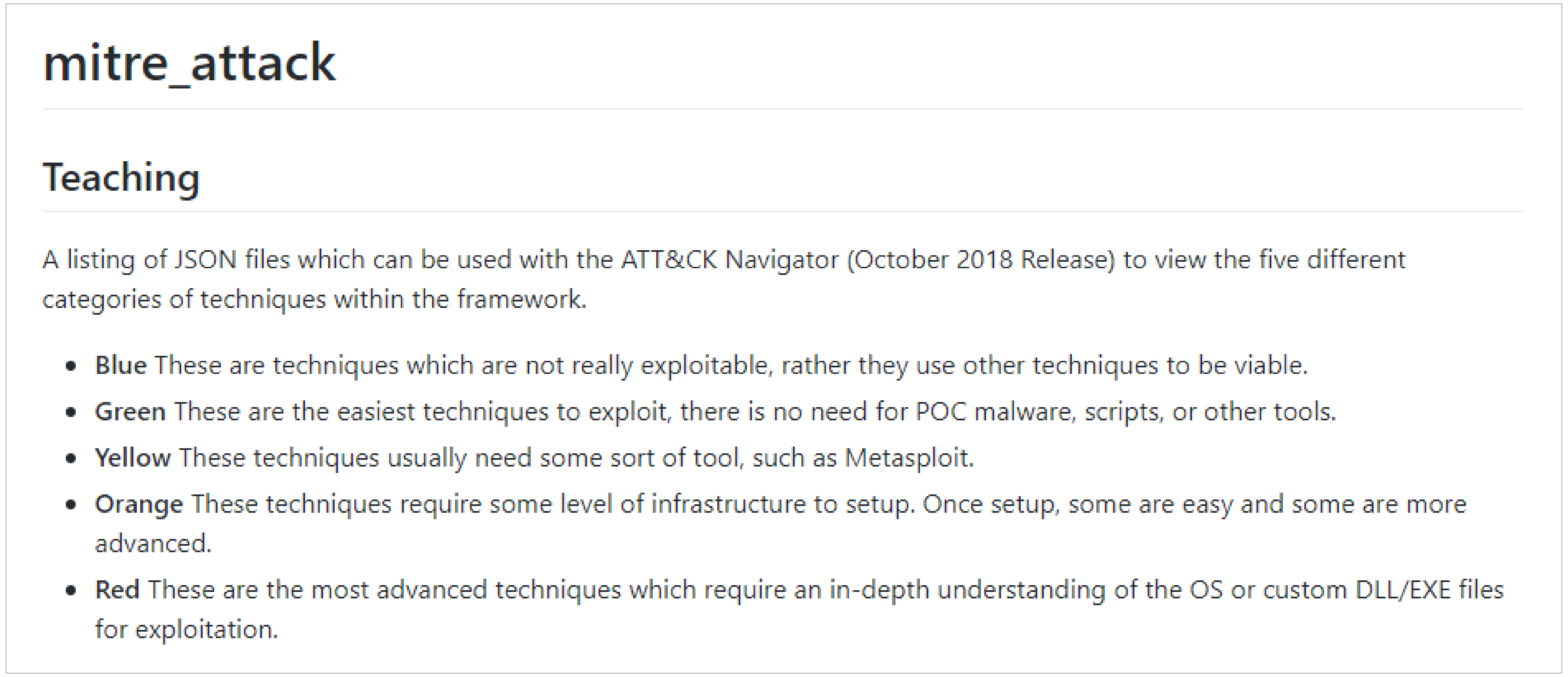
The screenshot on the left provides is an example of an adversary report on APT-15 (by NCC Group), which is annotated by Katie Nickels (MITRE) and Brian Beyer (Red Canary). It was presented at SANS CTI Summit in January 2019!

Source: https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1548090281.pdf

ATT&CK for defense prioritization

“What techniques can you block in your organisation?”

- What ATT&CK techniques are covered by **hardening guidelines** (e.g. group policies or Ansible playbooks)?
- Travis Smith mapped the ATT&CK framework techniques to **CIS Controls**, which provides an interesting insight!



mitre_attack

Teaching

A listing of JSON files which can be used with the ATT&CK Navigator (October 2018 Release) to view the five different categories of techniques within the framework.

- **Blue** These are techniques which are not really exploitable, rather they use other techniques to be viable.
- **Green** These are the easiest techniques to exploit, there is no need for POC malware, scripts, or other tools.
- **Yellow** These techniques usually need some sort of tool, such as Metasploit.
- **Orange** These techniques require some level of infrastructure to setup. Once setup, some are easy and some are more advanced.
- **Red** These are the most advanced techniques which require an in-depth understanding of the OS or custom DLL/EXE files for exploitation.

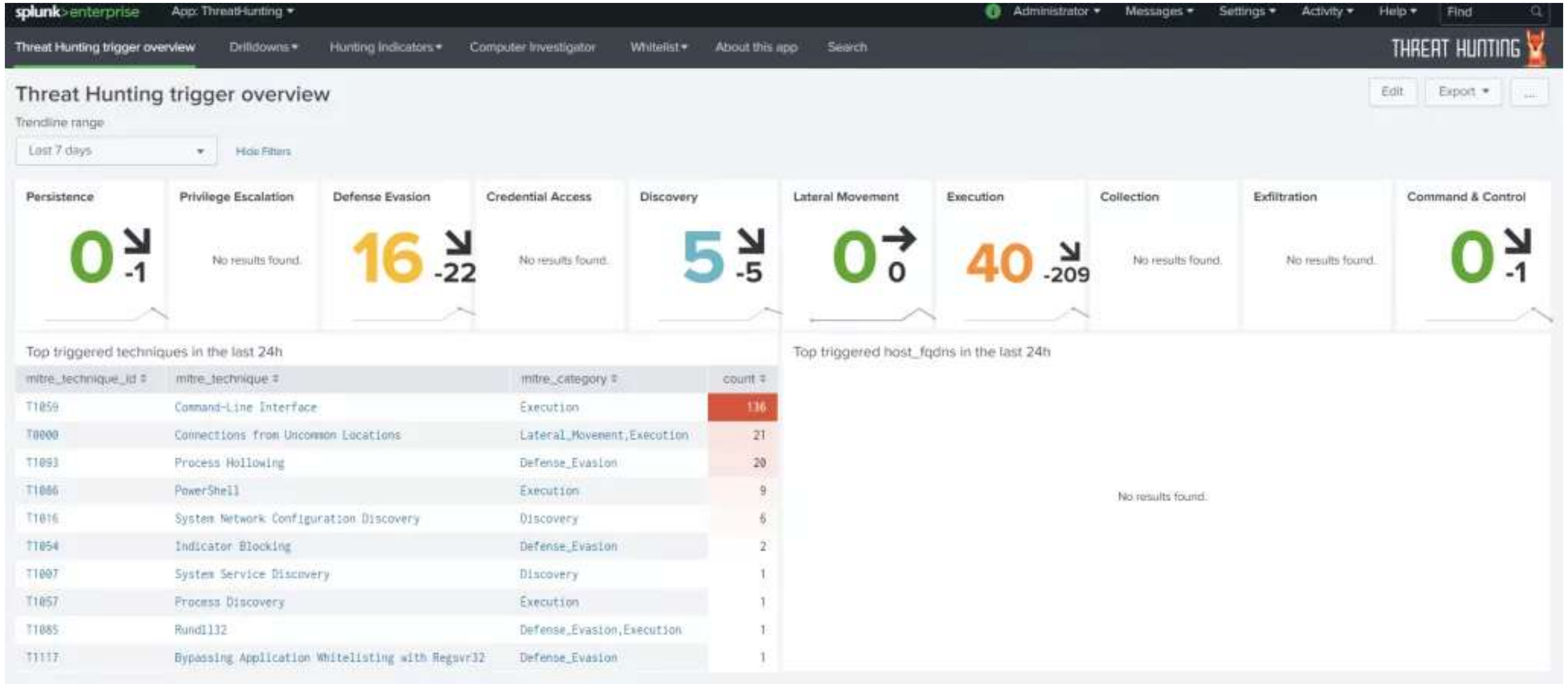
https://www.tripwire.com/state-of-security/security-data-protection/security-controls/mapping-the-attck-framework-to-cis-controls/

https://github.com/TravisFSmith/mitre_attack

ATT&CK for detection coverage

“What techniques can you detect in your organisation?”

- What techniques are covered by use **cases in security monitoring**?
- Do you collect the right **log sources**?
- What techniques can you cover using **threat hunting efforts**?



Threat Hunting trigger overview

Trendline range

Last 7 days ▾

Hide Filters

Persistence: 0 ↘ -1

Privilege Escalation: No results found.

Defense Evasion: 16 ↘ -22

Credential Access: No results found.

Discovery: 5 ↘ -5

Lateral Movement: 0 → 0

Execution: 40 ↘ -209

Collection: No results found.

Exfiltration: No results found.

Command & Control: 0 ↘ -1

Top triggered techniques in the last 24h

mitre_technique_id ⇕	mitre_technique ⇕	mitre_category ⇕	count ⇕
T1059	Command-Line Interface	Execution	136
T0000	Connections from Uncommon Locations	Lateral_Movement,Execution	21
T1093	Process Hollowing	Defense_Evasion	20
T1086	PowerShell	Execution	9
T1016	System Network Configuration Discovery	Discovery	6
T1054	Indicator Blocking	Defense_Evasion	2
T1007	System Service Discovery	Discovery	1
T1057	Process Discovery	Execution	1
T1085	Rundll32	Defense_Evasion,Execution	1
T1117	Bypassing Application Whitelisting with Regsvr32	Defense_Evasion	1

Top triggered host_fqdns in the last 24h

No results found.

https://cyberwardog.blogspot.com/2017/07/how-hot-is-your-hunt-team.html
https://github.com/olafhartong/ThreatHunting

Key use cases for ATT&CK

ATT&CK as a common language!

Adversary emulation

Define **red team scenarios** using ATT&CK

Link **vulnerabilities & findings** to ATT&CK

Detection capability

Assess **detection coverage** using ATT&CK

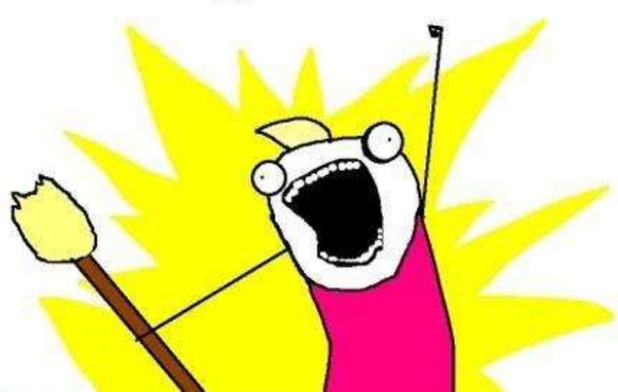
Define **hypotheses** for threat hunting using ATT&CK

Threat Intelligence

Categorize / tag **indicators** & techniques with ATT&CK

Prioritize defenses

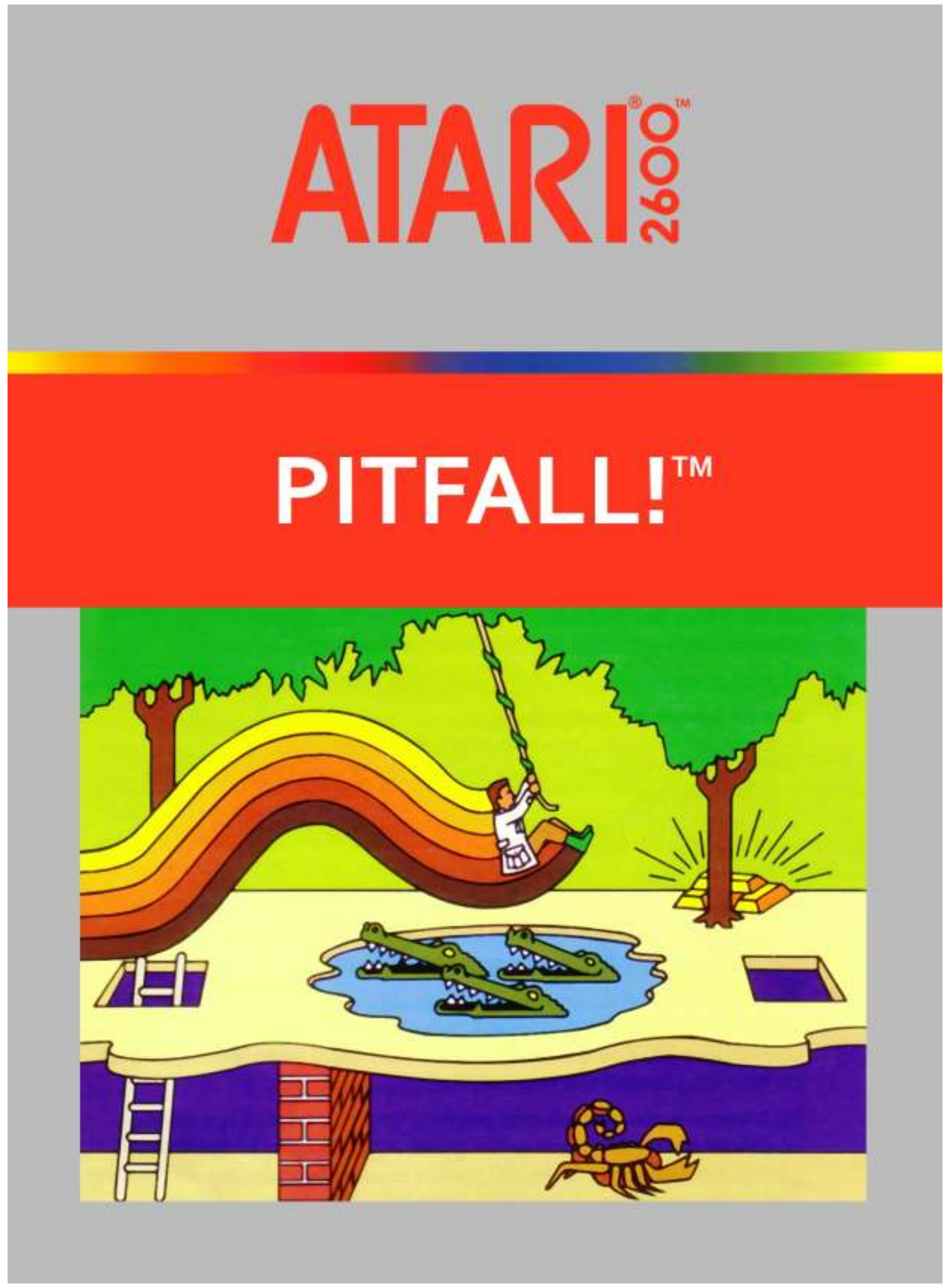
What ATT&CK techniques are you **blocking**?



ATT&CK all the things!

Common pitfalls

How to not use ATT&CK



Pitfall 1
Consider all techniques equal

Pitfall 2
Try to do everything at once

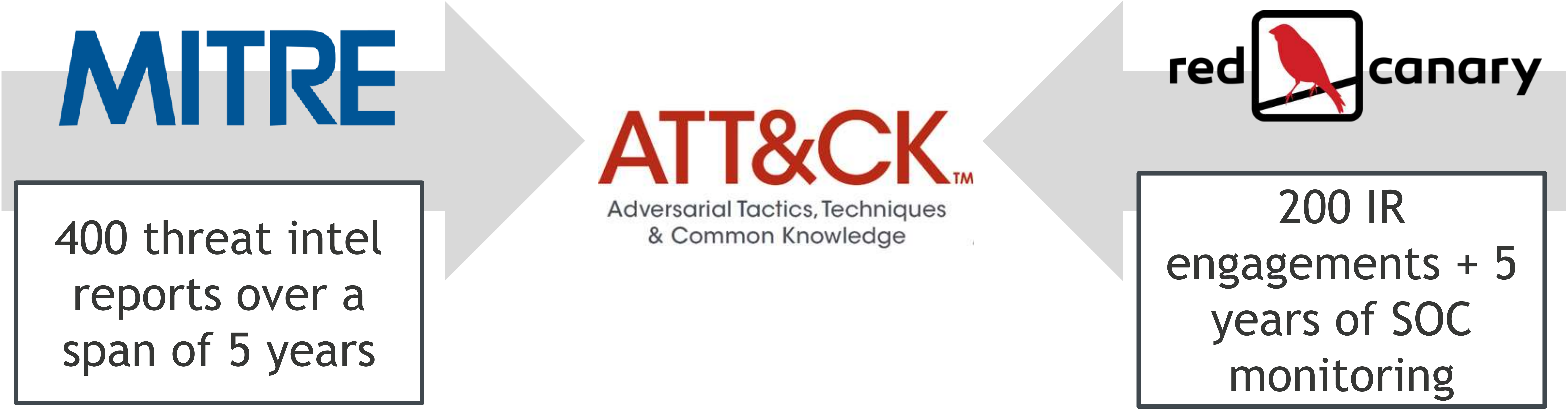
Pitfall 3
Misunderstand your coverage rating *(it's usually not binary)*

Good read: https://www.redcanary.com/blog/avoiding-common-attack-pitfalls/

All techniques are equal…

But some techniques are more equal than others

In January 2019, MITRE (Katie Nickels) & Red Canary (Brian Beyer) combined efforts and presented a joint view on ATT&CK at the SANS CTI Summit:



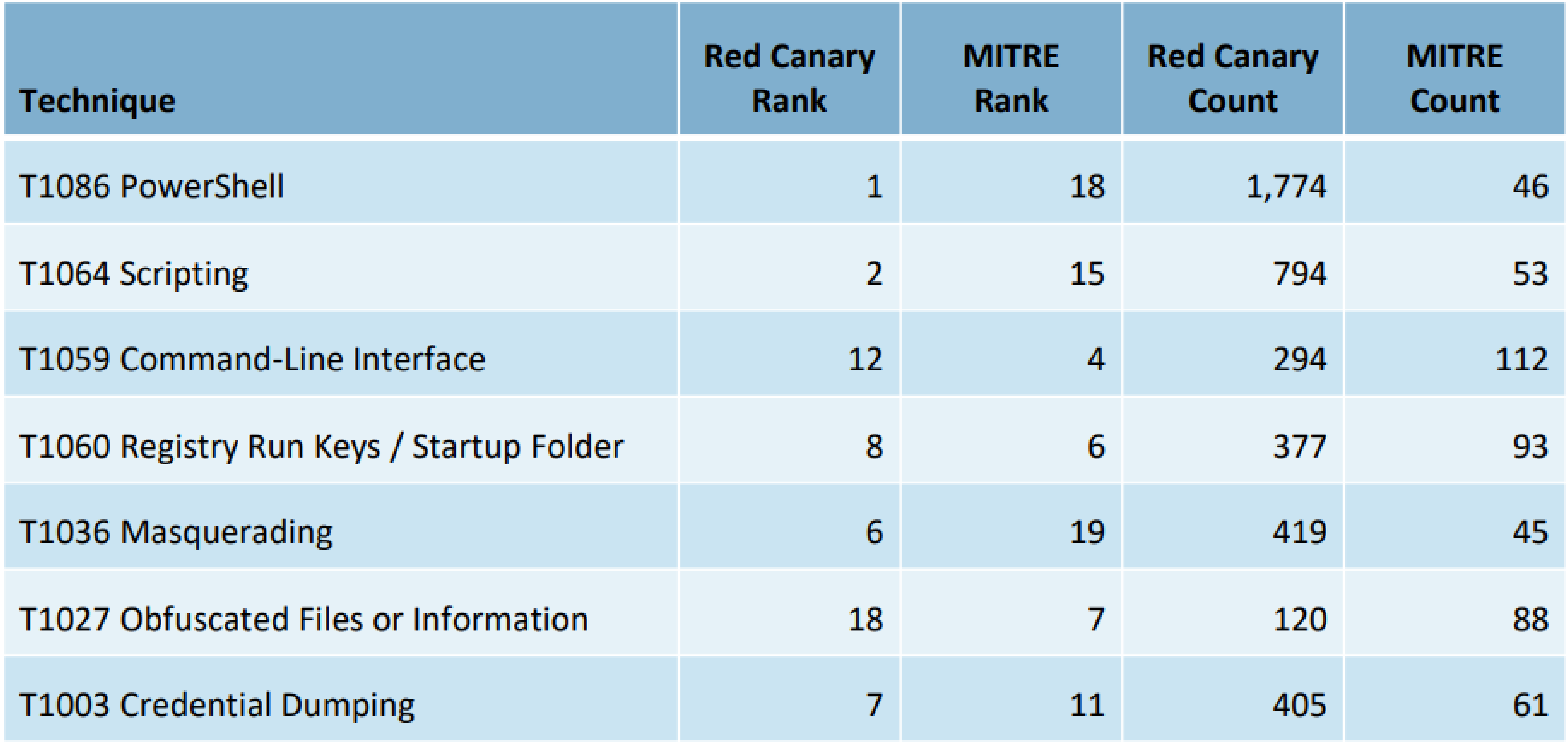
400 threat intel reports over a span of 5 years

200 IR engagements + 5 years of SOC monitoring

Source: https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1548090281.pdf

All techniques are equal…

But some techniques are more equal than others

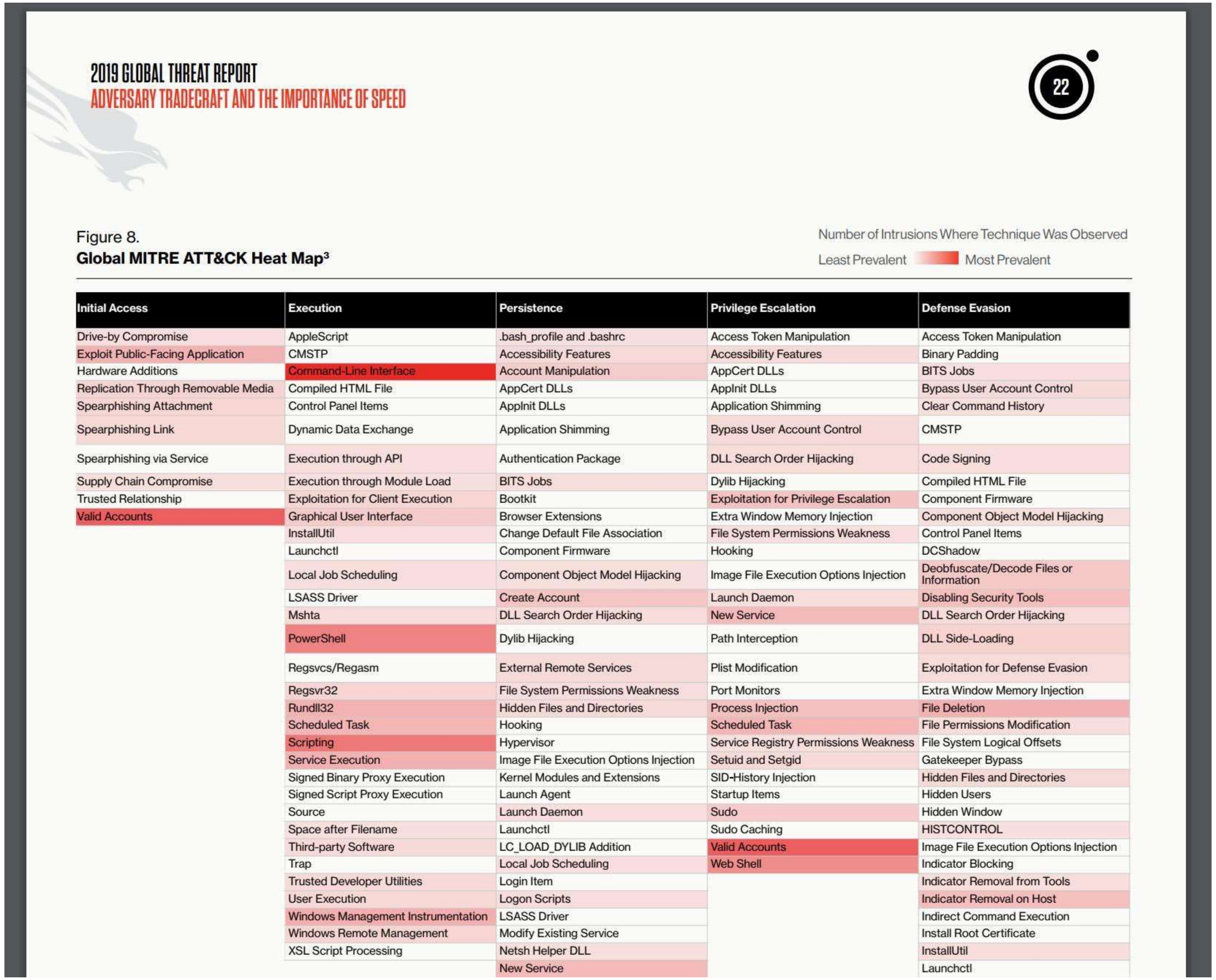


Technique	Red Canary Rank	MITRE Rank	Red Canary Count	MITRE Count
T1086 PowerShell	1	18	1,774	46
T1064 Scripting	2	15	794	53
T1059 Command-Line Interface	12	4	294	112
T1060 Registry Run Keys / Startup Folder	8	6	377	93
T1036 Masquerading	6	19	419	45
T1027 Obfuscated Files or Information	18	7	120	88
T1003 Credential Dumping	7	11	405	61

Source: https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1548090281.pdf

All techniques are equal…

But some techniques are more equal than others



2019 GLOBAL THREAT REPORT
ADVERSARY TRADECRAFT AND THE IMPORTANCE OF SPEED

22

Figure 8.
Global MITRE ATT&CK Heat Map[3]

Number of Intrusions Where Technique Was Observed
Least Prevalent 🟥 Most Prevalent

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking
	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items
	Launchctl	Component Firmware	Hooking	DCShadow
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information
	LSASS Driver	Create Account	Launch Daemon	Disabling Security Tools
	Mshta	DLL Search Order Hijacking	New Service	DLL Search Order Hijacking
	PowerShell	Dylib Hijacking	Path Interception	DLL Side-Loading
	Regsvcs/Regasm	External Remote Services	Plist Modification	Exploitation for Defense Evasion
	Regsvr32	File System Permissions Weakness	Port Monitors	Extra Window Memory Injection
	Rundll32	Hidden Files and Directories	Process Injection	File Deletion
	Scheduled Task	Hooking	Scheduled Task	File Permissions Modification
	Scripting	Hypervisor	Service Registry Permissions Weakness	File System Logical Offsets
	Service Execution	Image File Execution Options Injection	Setuid and Setgid	Gatekeeper Bypass
	Signed Binary Proxy Execution	Kernel Modules and Extensions	SID-History Injection	Hidden Files and Directories
	Signed Script Proxy Execution	Launch Agent	Startup Items	Hidden Users
	Source	Launch Daemon	Sudo	Hidden Window
	Space after Filename	Launchctl	Sudo Caching	HISTCONTROL
	Third-party Software	LC_LOAD_DYLIB Addition	Valid Accounts	Image File Execution Options Injection
	Trap	Local Job Scheduling	Web Shell	Indicator Blocking
	Trusted Developer Utilities	Login Item		Indicator Removal from Tools
	User Execution	Logon Scripts		Indicator Removal on Host
	Windows Management Instrumentation	LSASS Driver		Indirect Command Execution
	Windows Remote Management	Modify Existing Service		Install Root Certificate
	XSL Script Processing	Netsh Helper DLL		InstallUtil
		New Service		Launchctl

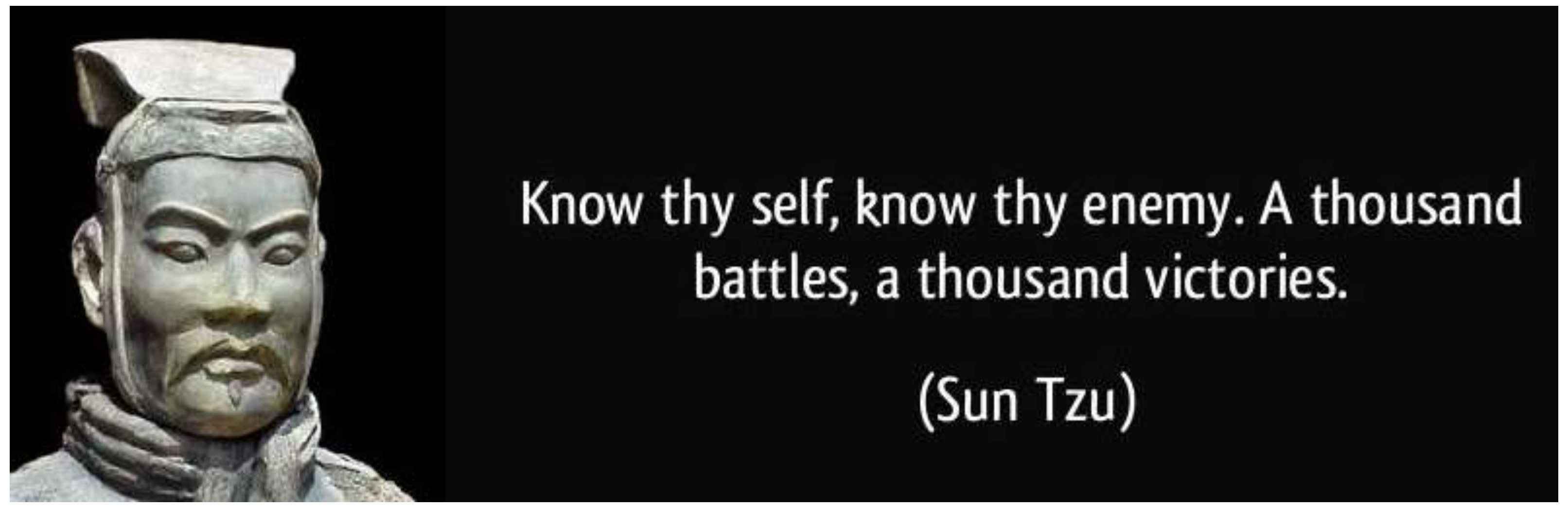
Crowdstrike released the “**Global Threat Report**” in February 2019 and added a “heat map” of MITRE ATT&CK, which can again be used to **prioritize** your efforts and attention!

The results are in line with the MITRE & Red Canary data previously seen!

https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/

All techniques are equal…

But some techniques are more equal than others

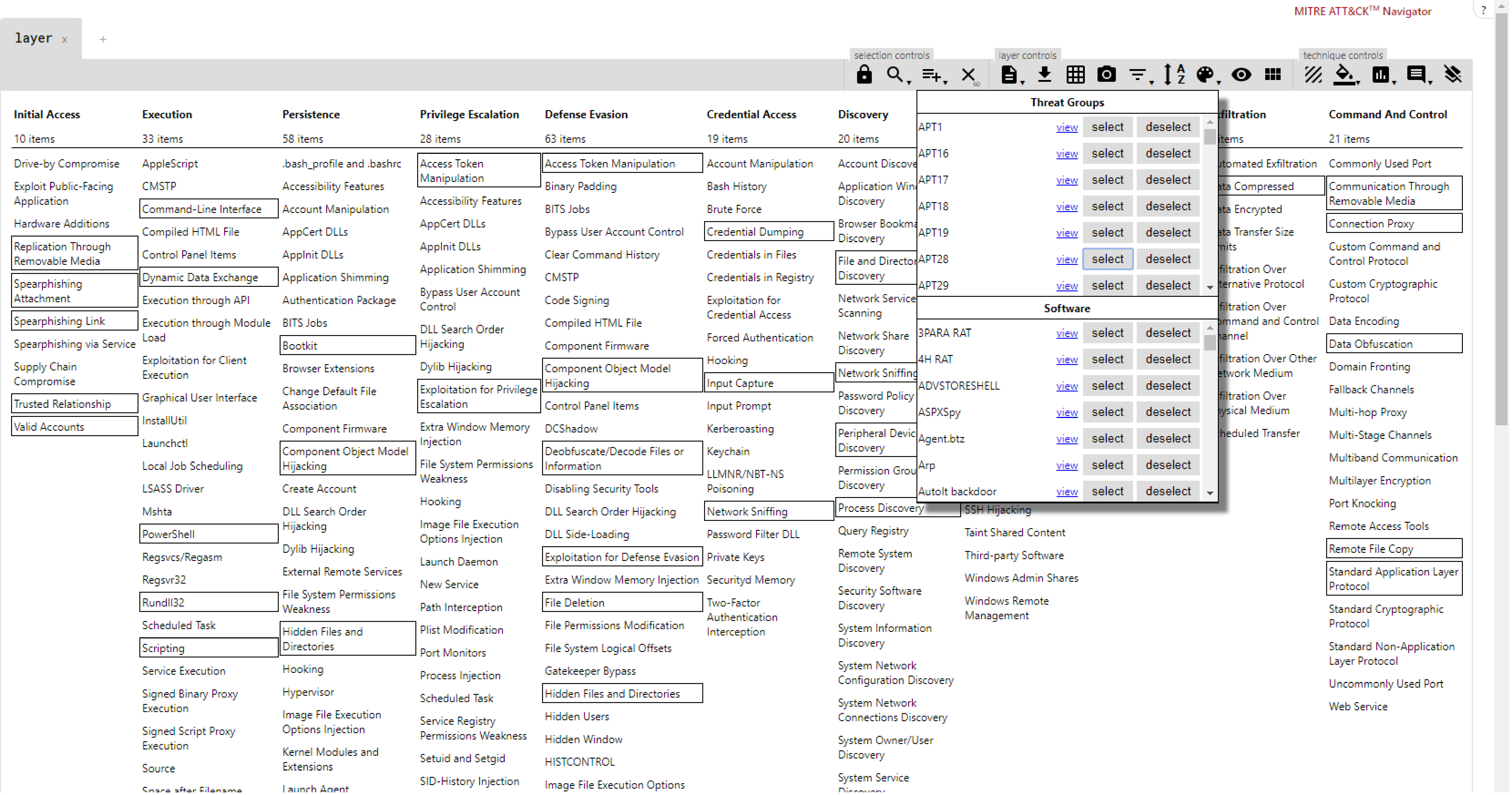


Know thy self, know thy enemy. A thousand battles, a thousand victories.

(Sun Tzu)

Next to the “technique popularity contest”, there is also the question of what techniques are most important TO YOUR ORGANZIATION:

1. Know what threat actors are relevant to you
2. Know what techniques these threat actors are known to use
3. Prioritize accordingly!



Initial Access
10 items
Drive-by Compromise
Exploit Public-Facing Application
Hardware Additions
Replication Through Removable Media
Spearphishing Attachment
Spearphishing Link
Spearphishing via Service
Supply Chain Compromise
Trusted Relationship
Valid Accounts

Execution
33 items
AppleScript
CMSTP
Command-Line Interface
Compiled HTML File
Control Panel Items
Dynamic Data Exchange
Execution through API
Execution through Module Load
Exploitation for Client Execution
Graphical User Interface
InstallUtil
Launchctl
Local Job Scheduling
LSASS Driver
Mshta
PowerShell
Regsvcs/Regasm
Regsvr32
Rundll32
Scheduled Task
Scripting
Service Execution
Signed Binary Proxy Execution
Signed Script Proxy Execution
Source
Space after Filename

Persistence
58 items
.bash_profile and .bashrc
Accessibility Features
Account Manipulation
AppCert DLLs
AppInit DLLs
Application Shimming
Authentication Package
BITS Jobs
Bootkit
Browser Extensions
Change Default File Association
Component Firmware
Component Object Model Hijacking
Create Account
DLL Search Order Hijacking
Dylib Hijacking
External Remote Services
File System Permissions Weakness
Hidden Files and Directories
Hooking
Hypervisor
Image File Execution Options Injection
Kernel Modules and Extensions
Launch Agent

Privilege Escalation
28 items
Access Token Manipulation
Accessibility Features
AppCert DLLs
AppInit DLLs
Application Shimming
Bypass User Account Control
DLL Search Order Hijacking
Dylib Hijacking
Exploitation for Privilege Escalation
Extra Window Memory Injection
File System Permissions Weakness
Hooking
Image File Execution Options Injection
Launch Daemon
New Service
Path Interception
Plist Modification
Port Monitors
Process Injection
Scheduled Task
Service Registry Permissions Weakness
Setuid and Setgid
SID-History Injection

Defense Evasion
63 items
Access Token Manipulation
Binary Padding
BITS Jobs
Bypass User Account Control
Clear Command History
CMSTP
Code Signing
Compiled HTML File
Component Firmware
Component Object Model Hijacking
Control Panel Items
DCShadow
Deobfuscate/Decode Files or Information
Disabling Security Tools
DLL Search Order Hijacking
DLL Side-Loading
Exploitation for Defense Evasion
Extra Window Memory Injection
File Deletion
File Permissions Modification
File System Logical Offsets
Gatekeeper Bypass
Hidden Files and Directories
Hidden Users
Hidden Window
HISTCONTROL
Image File Execution Options

Credential Access
19 items
Account Manipulation
Bash History
Brute Force
Credential Dumping
Credentials in Files
Credentials in Registry
Exploitation for Credential Access
Forced Authentication
Hooking
Input Capture
Input Prompt
Kerberoasting
Keychain
LLMNR/NBT-NS Poisoning
Network Sniffing
Password Filter DLL
Private Keys
Securityd Memory
Two-Factor Authentication Interception

Discovery
20 items
Account Discove
Application Win Discovery
Browser Bookma Discovery
File and Director Discovery
Network Service Scanning
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Devic Discovery
Permission Grou Discovery
Process Discovery
Query Registry
Remote System Discovery
Security Software Discovery
System Information Discovery
System Network Configuration Discovery
System Network Connections Discovery
System Owner/User Discovery
System Service Discovery

SSH Hijacking
Taint Shared Content
Third-party Software
Windows Admin Shares
Windows Remote Management

filtration
items
utomated Exfiltration
ata Compressed
ata Encrypted
ata Transfer Size mits
filtration Over ternative Protocol
filtration Over ommand and Control hannel
filtration Over Other etwork Medium
filtration Over ysical Medium
heduled Transfer

Command And Control
21 items
Commonly Used Port
Communication Through Removable Media
Connection Proxy
Custom Command and Control Protocol
Custom Cryptographic Protocol
Data Encoding
Data Obfuscation
Domain Fronting
Fallback Channels
Multi-hop Proxy
Multi-Stage Channels
Multiband Communication
Multilayer Encryption
Port Knocking
Remote Access Tools
Remote File Copy
Standard Application Layer Protocol
Standard Cryptographic Protocol
Standard Non-Application Layer Protocol
Uncommonly Used Port
Web Service

Threat Groups

APT1	view	select	deselect
APT16	view	select	deselect
APT17	view	select	deselect
APT18	view	select	deselect
APT19	view	select	deselect
APT28	view	select	deselect
APT29	view	select	deselect

Software

3PARA RAT	view	select	deselect
4H RAT	view	select	deselect
ADVSTORESHELL	view	select	deselect
ASPXSpy	view	select	deselect
Agent.btz	view	select	deselect
Arp	view	select	deselect
AutoIt backdoor	view	select	deselect

ATT&CK initiatives

Here’s some concrete ideas!

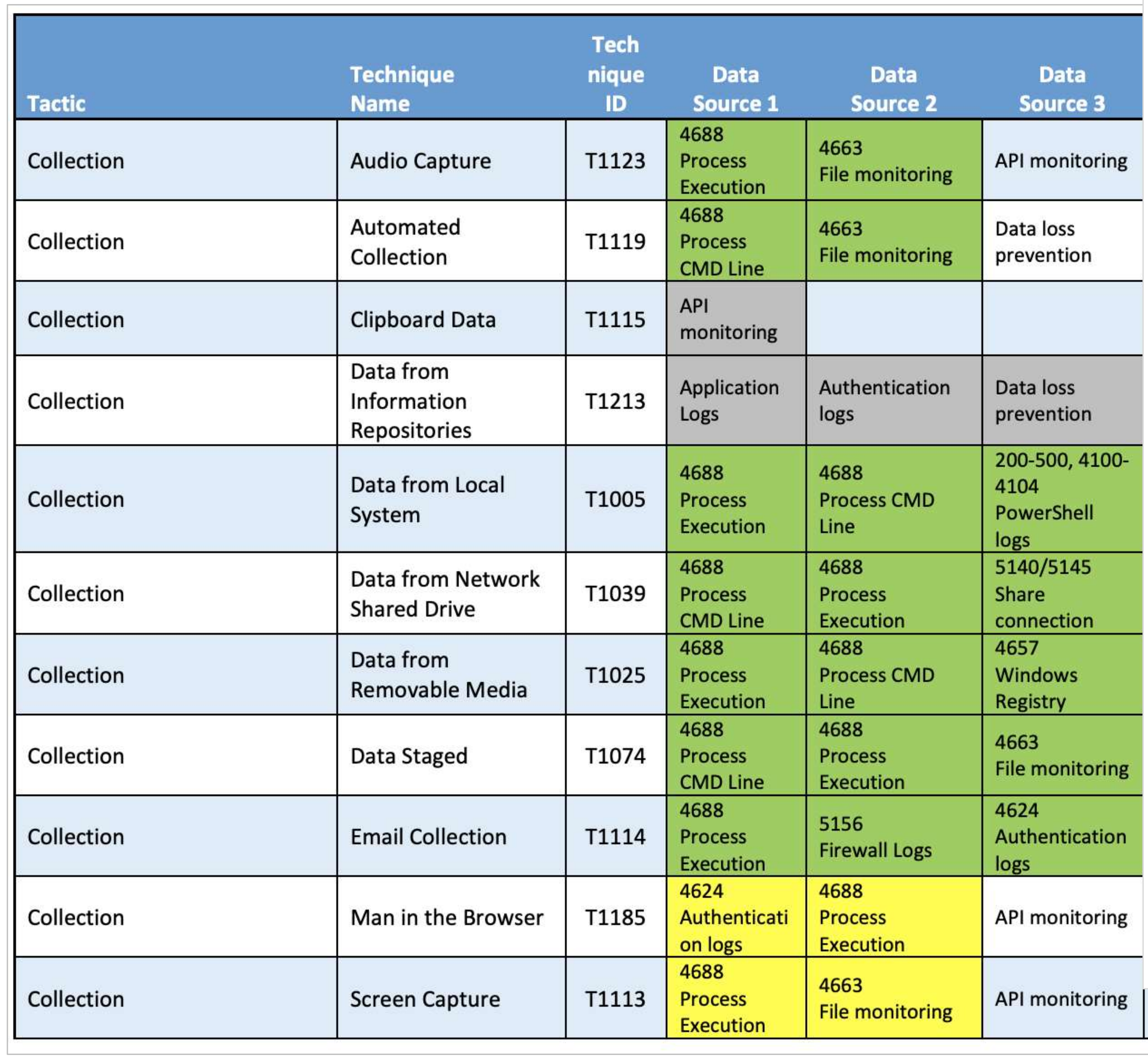
ATT&CK Initiatives - Detection

Many open-source tools align with ATT&CK

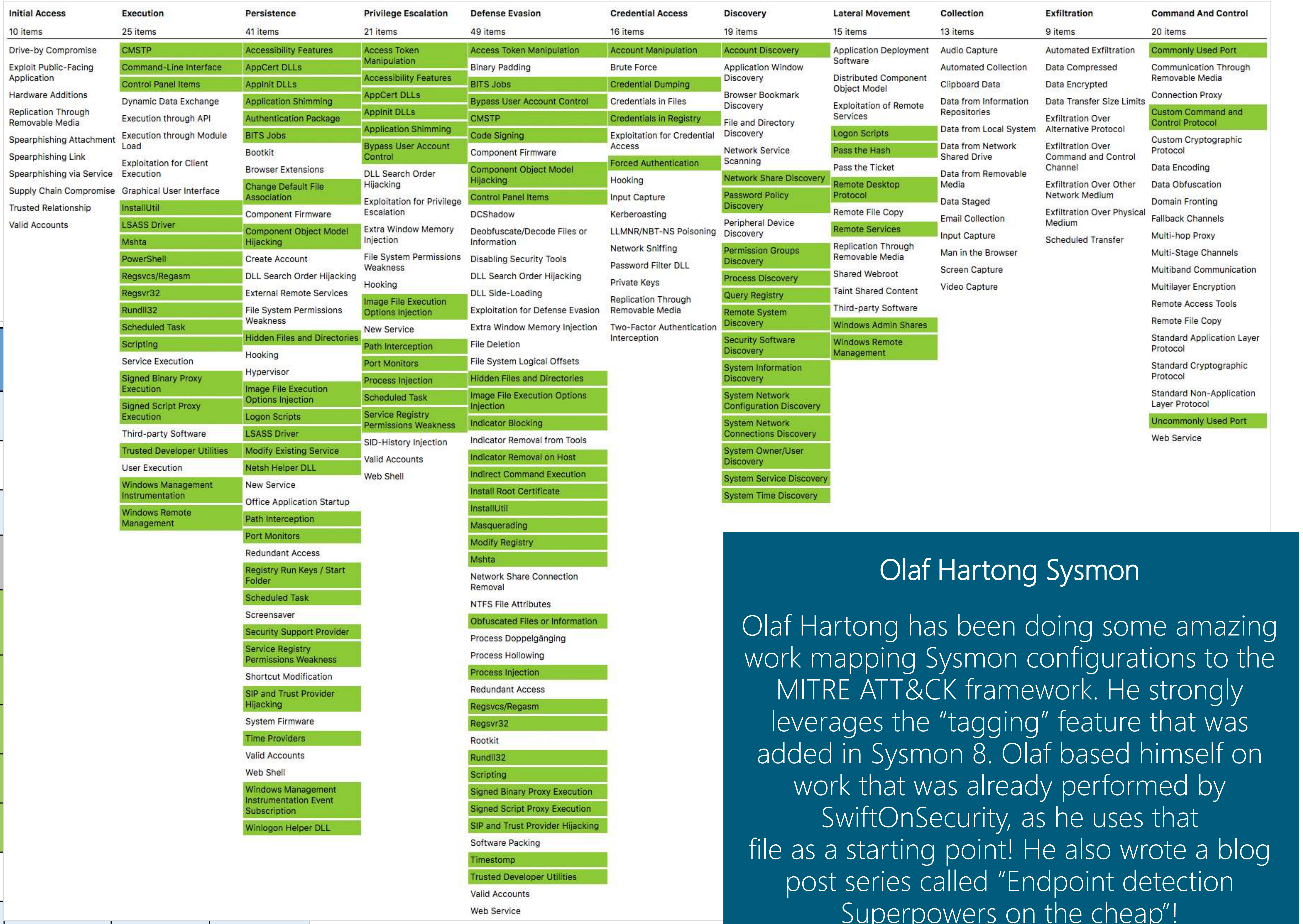
Malware archaeology

The folks over at Malware Archaeology made a mapping of Windows event IDs to the MITRE ATT&CK framework. It includes a coding scheme for most relevant event identifiers as well!

It's updated regularly and can be found at https://www.malwarearchaeology.com/cheat-sheets.



Tactic	Technique Name	Technique ID	Data Source 1	Data Source 2	Data Source 3
Collection	Audio Capture	T1123	4688 Process Execution	4663 File monitoring	API monitoring
Collection	Automated Collection	T1119	4688 Process CMD Line	4663 File monitoring	Data loss prevention
Collection	Clipboard Data	T1115	API monitoring		
Collection	Data from Information Repositories	T1213	Application Logs	Authentication logs	Data loss prevention
Collection	Data from Local System	T1005	4688 Process Execution	4688 Process CMD Line	200-500, 4100-4104 PowerShell logs
Collection	Data from Network Shared Drive	T1039	4688 Process CMD Line	4688 Process Execution	5140/5145 Share connection
Collection	Data from Removable Media	T1025	4688 Process Execution	4688 Process CMD Line	4657 Windows Registry
Collection	Data Staged	T1074	4688 Process CMD Line	4688 Process Execution	4663 File monitoring
Collection	Email Collection	T1114	4688 Process Execution	5156 Firewall Logs	4624 Authentication logs
Collection	Man in the Browser	T1185	4624 Authentication logs	4688 Process Execution	API monitoring
Collection	Screen Capture	T1113	4688 Process Execution	4663 File monitoring	API monitoring



Initial Access 10 items
- Drive-by Compromise
- Exploit Public-Facing Application
- Hardware Additions
- Replication Through Removable Media
- Spearphishing Attachment
- Spearphishing Link
- Spearphishing via Service
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts

Execution 25 items
- CMSTP
- Command-Line Interface
- Control Panel Items
- Dynamic Data Exchange
- Execution through API
- Execution through Module Load
- Exploitation for Client Execution
- Graphical User Interface
- InstallUtil
- LSASS Driver
- Mshta
- PowerShell
- Regsvcs/Regasm
- Regsvr32
- Rundll32
- Scheduled Task
- Scripting
- Service Execution
- Signed Binary Proxy Execution
- Signed Script Proxy Execution
- Third-party Software
- Trusted Developer Utilities
- User Execution
- Windows Management Instrumentation
- Windows Remote Management

Persistence 41 items
- Accessibility Features
- AppCert DLLs
- AppInit DLLs
- Application Shimming
- Authentication Package
- BITS Jobs
- Bootkit
- Browser Extensions
- Change Default File Association
- Component Firmware
- Component Object Model Hijacking
- Create Account
- DLL Search Order Hijacking
- External Remote Services
- File System Permissions Weakness
- Hidden Files and Directories
- Hooking
- Hypervisor
- Image File Execution Options Injection
- Logon Scripts
- LSASS Driver
- Modify Existing Service
- Netsh Helper DLL
- New Service
- Office Application Startup
- Path Interception
- Port Monitors
- Redundant Access
- Registry Run Keys / Start Folder
- Scheduled Task
- Screensaver
- Security Support Provider
- Service Registry Permissions Weakness
- Shortcut Modification
- SIP and Trust Provider Hijacking
- System Firmware
- Time Providers
- Valid Accounts
- Web Shell
- Windows Management Instrumentation Event Subscription
- Winlogon Helper DLL

Privilege Escalation 21 items
- Access Token Manipulation
- Accessibility Features
- AppCert DLLs
- AppInit DLLs
- Application Shimming
- Bypass User Account Control
- DLL Search Order Hijacking
- Exploitation for Privilege Escalation
- Extra Window Memory Injection
- File System Permissions Weakness
- Hooking
- Image File Execution Options Injection
- New Service
- Path Interception
- Port Monitors
- Process Injection
- Scheduled Task
- Service Registry Permissions Weakness
- SID-History Injection
- Valid Accounts
- Web Shell

Defense Evasion 49 items
- Access Token Manipulation
- Binary Padding
- BITS Jobs
- Bypass User Account Control
- CMSTP
- Code Signing
- Component Firmware
- Component Object Model Hijacking
- Control Panel Items
- DCShadow
- Deobfuscate/Decode Files or Information
- Disabling Security Tools
- DLL Search Order Hijacking
- DLL Side-Loading
- Exploitation for Defense Evasion
- Extra Window Memory Injection
- File Deletion
- File System Logical Offsets
- Hidden Files and Directories
- Image File Execution Options Injection
- Indicator Blocking
- Indicator Removal from Tools
- Indicator Removal on Host
- Indirect Command Execution
- Install Root Certificate
- InstallUtil
- Masquerading
- Modify Registry
- Mshta
- Network Share Connection Removal
- NTFS File Attributes
- Obfuscated Files or Information
- Process Doppelgänging
- Process Hollowing
- Process Injection
- Redundant Access
- Regsvcs/Regasm
- Regsvr32
- Rootkit
- Rundll32
- Scripting
- Signed Binary Proxy Execution
- Signed Script Proxy Execution
- SIP and Trust Provider Hijacking
- Software Packing
- Timestomp
- Trusted Developer Utilities
- Valid Accounts
- Web Service

Credential Access 16 items
- Account Manipulation
- Brute Force
- Credential Dumping
- Credentials in Files
- Credentials in Registry
- Exploitation for Credential Access
- Forced Authentication
- Hooking
- Input Capture
- Kerberoasting
- LLMNR/NBT-NS Poisoning
- Network Sniffing
- Password Filter DLL
- Private Keys
- Replication Through Removable Media
- Two-Factor Authentication Interception

Discovery 19 items
- Account Discovery
- Application Window Discovery
- Browser Bookmark Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery
- Process Discovery
- Query Registry
- Remote System Discovery
- Security Software Discovery
- System Information Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery

Lateral Movement 15 items
- Application Deployment Software
- Distributed Component Object Model
- Exploitation of Remote Services
- Logon Scripts
- Pass the Hash
- Pass the Ticket
- Remote Desktop Protocol
- Remote File Copy
- Remote Services
- Replication Through Removable Media
- Shared Webroot
- Taint Shared Content
- Third-party Software
- Windows Admin Shares
- Windows Remote Management

Collection 13 items
- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Information Repositories
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged
- Email Collection
- Input Capture
- Man in the Browser
- Screen Capture
- Video Capture

Exfiltration 9 items
- Automated Exfiltration
- Data Compressed
- Data Encrypted
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol
- Exfiltration Over Command and Control Channel
- Exfiltration Over Other Network Medium
- Exfiltration Over Physical Medium
- Scheduled Transfer

Command And Control 20 items
- Commonly Used Port
- Communication Through Removable Media
- Connection Proxy
- Custom Command and Control Protocol
- Custom Cryptographic Protocol
- Data Encoding
- Data Obfuscation
- Domain Fronting
- Fallback Channels
- Multi-hop Proxy
- Multi-Stage Channels
- Multiband Communication
- Multilayer Encryption
- Remote Access Tools
- Remote File Copy
- Standard Application Layer Protocol
- Standard Cryptographic Protocol
- Standard Non-Application Layer Protocol
- Uncommonly Used Port
- Web Service

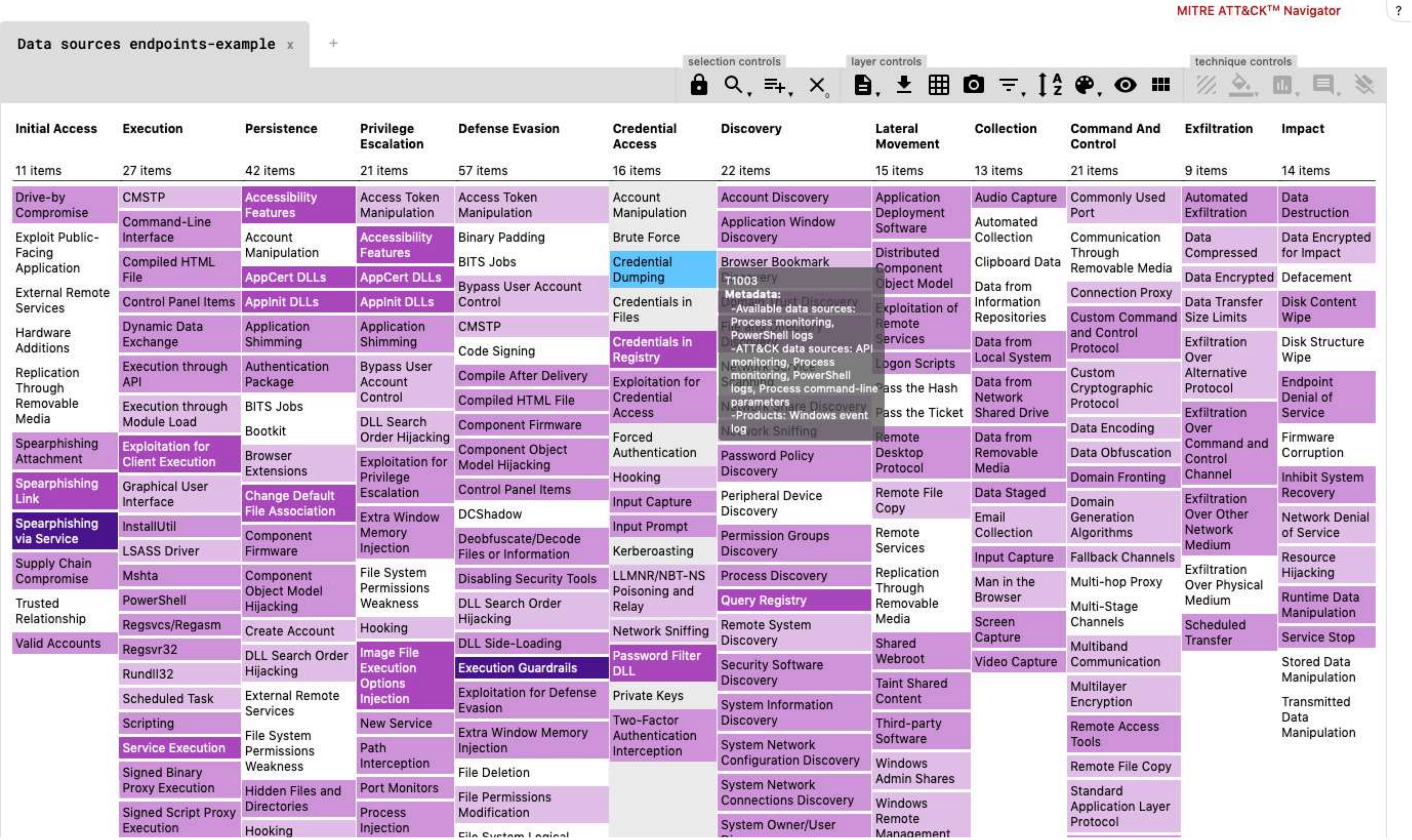
Olaf Hartong Sysmon

Olaf Hartong has been doing some amazing work mapping Sysmon configurations to the MITRE ATT&CK framework. He strongly leverages the "tagging" feature that was added in Sysmon 8. Olaf based himself on work that was already performed by SwiftOnSecurity, as he uses that file as a starting point! He also wrote a blog post series called "Endpoint detection Superpowers on the cheap"!

ATT&CK Initiatives - Detection

Many open-source tools align with ATT&CK

DeTT&CT



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	27 items	42 items	21 items	57 items	16 items	22 items	15 items	13 items	21 items	9 items	14 items
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	Command-Line Interface	Account Manipulation	Accessibility Features	Binary Padding	Brute Force	Application Window Discovery	Distributed Component Object Model	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Compiled HTML File	AppCert DLLs	AppCert DLLs	BITS Jobs	Credential Dumping	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credentials in Files	Domain Trust Discovery	Logon Scripts	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Dynamic Data Exchange	Application Shimming	Application Shimming	CMSTP	Credentials in Registry	File and Directory Discovery	Pass the Hash	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Execution through API	Authentication Package	Bypass User Account Control	Code Signing	Exploitation for Credential Access	Network Service Scanning	Pass the Ticket	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Compile After Delivery	Forced Authentication	Network Share Discovery	Remote Desktop Protocol	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Network Sniffing	Remote File Copy	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Password Policy Discovery	Remote Services	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Peripheral Device Discovery	Replication Through Removable Media	Input Capture	Fallback Channels		Resource Hijacking
Valid Accounts	LSASS Driver	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Permission Groups Discovery	Shared Webroot	Man in the Browser	Multi-hop Proxy		Runtime Data Manipulation
	Mshta	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	LLMNR/NBT-NS Poisoning and Relay	Process Discovery	Taint Shared Content	Screen Capture	Multi-Stage Channels		Service Stop
	PowerShell	Create Account	New Service	Deobfuscate/Decode Files or Information	Network Sniffing	Query Registry	Third-party Software	Video Capture	Multiband Communication		Stored Data Manipulation
	Regsvcs/Regasm	DLL Search Order Hijacking	Path Interception	Disabling Security Tools	Password Filter DLL	Remote System Discovery	Windows Admin Shares		Multilayer Encryption		Transmitted Data Manipulation
	Regsvr32	External Remote Services	Port Monitors	DLL Search Order Hijacking	Private Keys	Security Software Discovery	Windows Remote Management		Remote Access Tools		
	Rundll32	File System Permissions Weakness	Process Injection	DLL Side-Loading	Two-Factor Authentication Interception	System Information Discovery			Remote File Copy		
	Scheduled Task	Hidden Files and Directories		Execution Guardrails		System Network Configuration Discovery			Standard Application Layer Protocol		
	Scripting	Hooking		Exploitation for Defense Evasion		System Network Connections Discovery					
	Service Execution			Extra Window Memory Injection		System Owner/User Di					
	Signed Binary Proxy Execution			File Deletion							
	Signed Script Proxy Execution			File Permissions Modification							
				File System Logical							

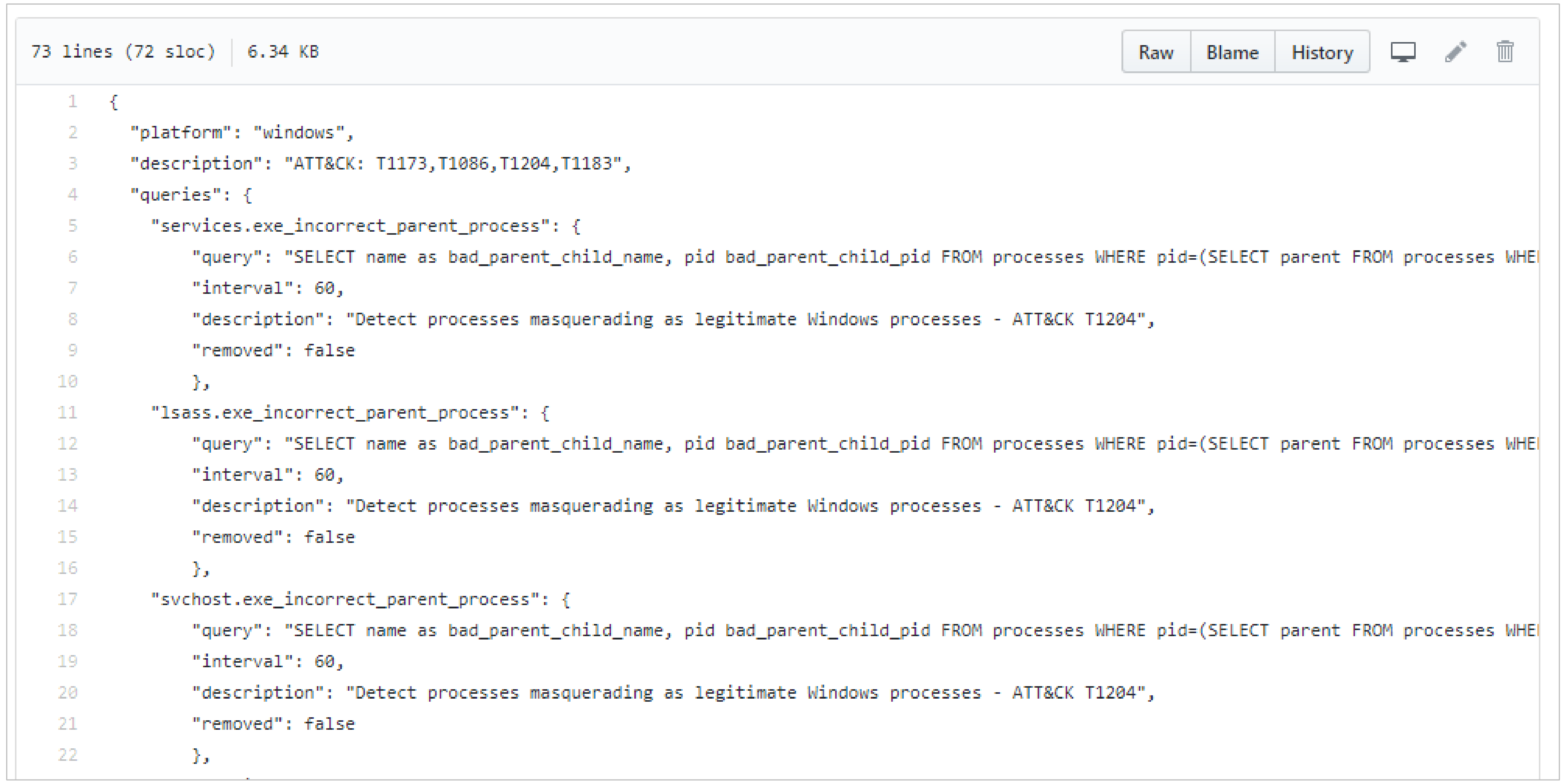
T1003
Metadata:
-Available data sources: Process monitoring, PowerShell logs
-ATT&CK data sources: API monitoring, Process monitoring, PowerShell logs, Process command-line parameters
-Products: Windows event log

DeTT&CT aims to assist blue teams using ATT&CK to score and compare data log source quality, visibility coverage, detection coverage and threat actor behaviours. All of which can help, in different ways, to get more resilient against attacks targeting your organization. The DeTT&CT framework consists of a Python tool, YAML administration files and scoring tables for the different aspects.

https://github.com/rabobank-cdc/DeTTACT

ATT&CK Initiatives - Detection

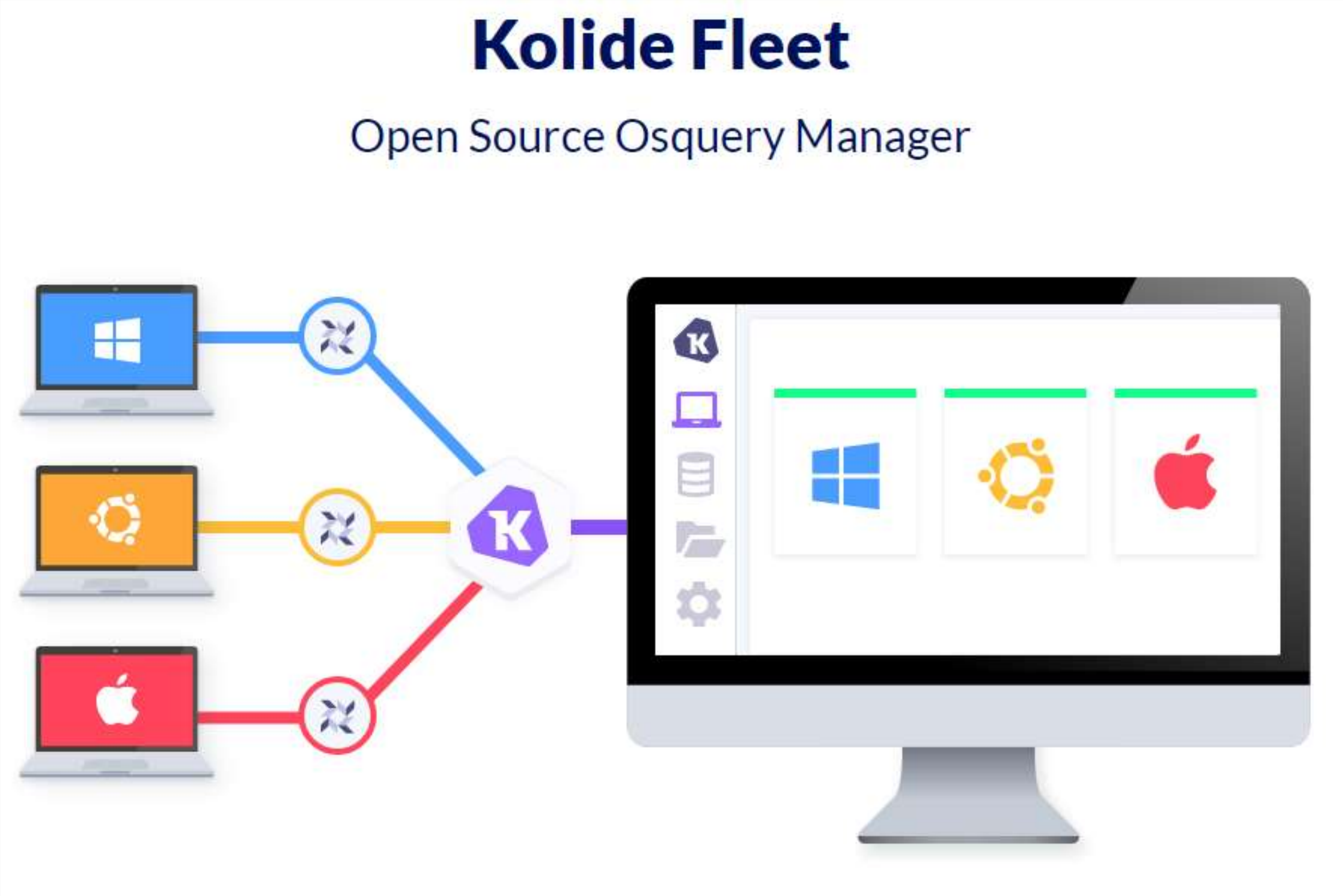
Many open-source tools align with ATT&CK



```
73 lines (72 sloc) | 6.34 KB

{
  "platform": "windows",
  "description": "ATT&CK: T1173,T1086,T1204,T1183",
  "queries": {
    "services.exe_incorrect_parent_process": {
        "query": "SELECT name as bad_parent_child_name, pid bad_parent_child_pid FROM processes WHERE pid=(SELECT parent FROM processes WHE
        "interval": 60,
        "description": "Detect processes masquerading as legitimate Windows processes - ATT&CK T1204",
        "removed": false
        },
    "lsass.exe_incorrect_parent_process": {
        "query": "SELECT name as bad_parent_child_name, pid bad_parent_child_pid FROM processes WHERE pid=(SELECT parent FROM processes WHE
        "interval": 60,
        "description": "Detect processes masquerading as legitimate Windows processes - ATT&CK T1204",
        "removed": false
        },
    "svchost.exe_incorrect_parent_process": {
        "query": "SELECT name as bad_parent_child_name, pid bad_parent_child_pid FROM processes WHERE pid=(SELECT parent FROM processes WHE
        "interval": 60,
        "description": "Detect processes masquerading as legitimate Windows processes - ATT&CK T1204",
        "removed": false
        },
```

https://github.com/teoseller/osquery-attck

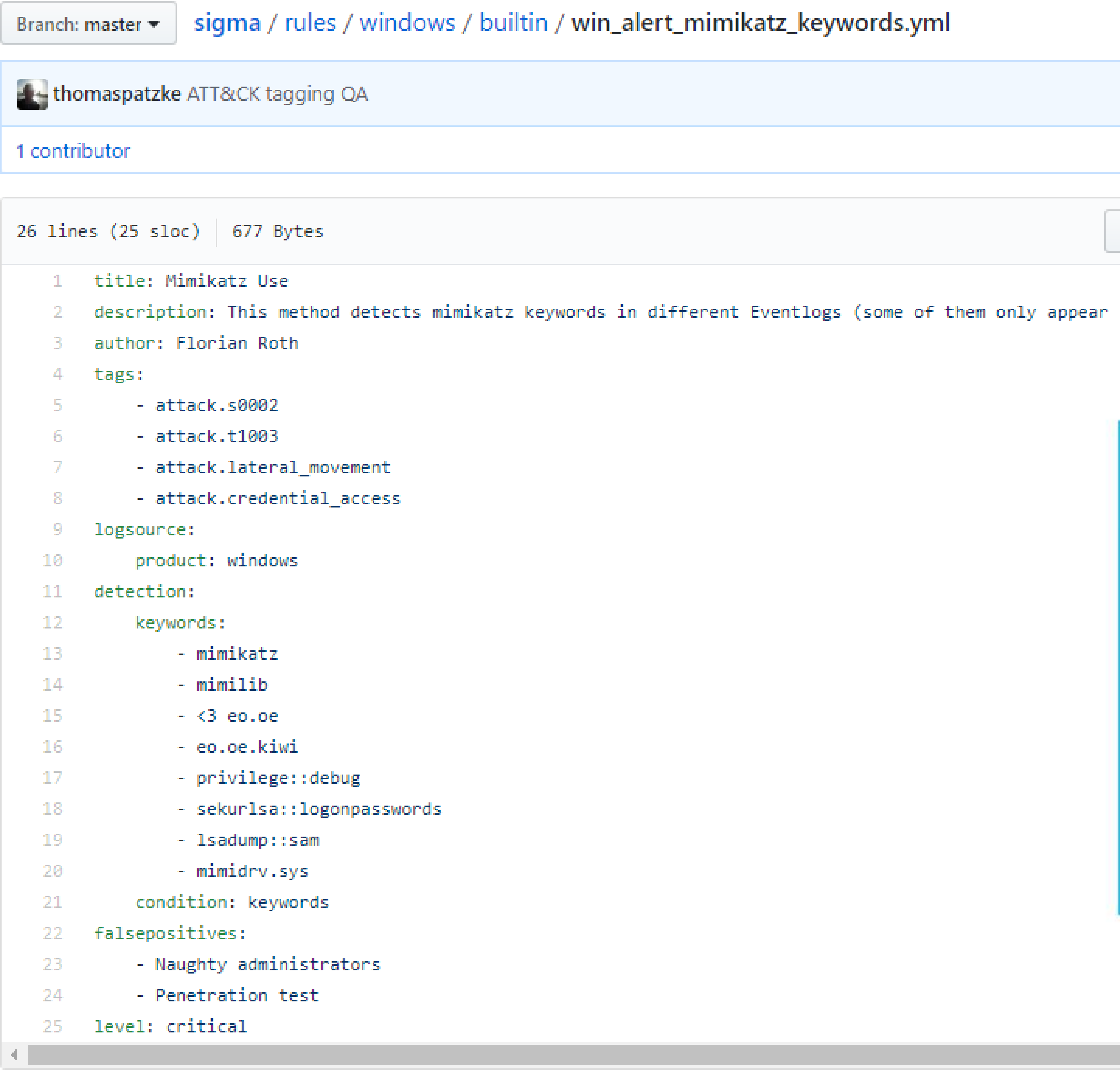


osquery (by Facebook) allows you to easily ask questions about your Linux, Windows, and macOS infrastructure.

A GitHub repository was created by “teoseller” that maps queries to the MITRE ATT&CK framework!

ATT&CK Initiatives - Detection

Many open-source tools align with ATT&CK



sigma / rules / windows / builtin / win_alert_mimikatz_keywords.yml

thomaspatzke ATT&CK tagging QA — 81515b5 on Sep 20, 2018

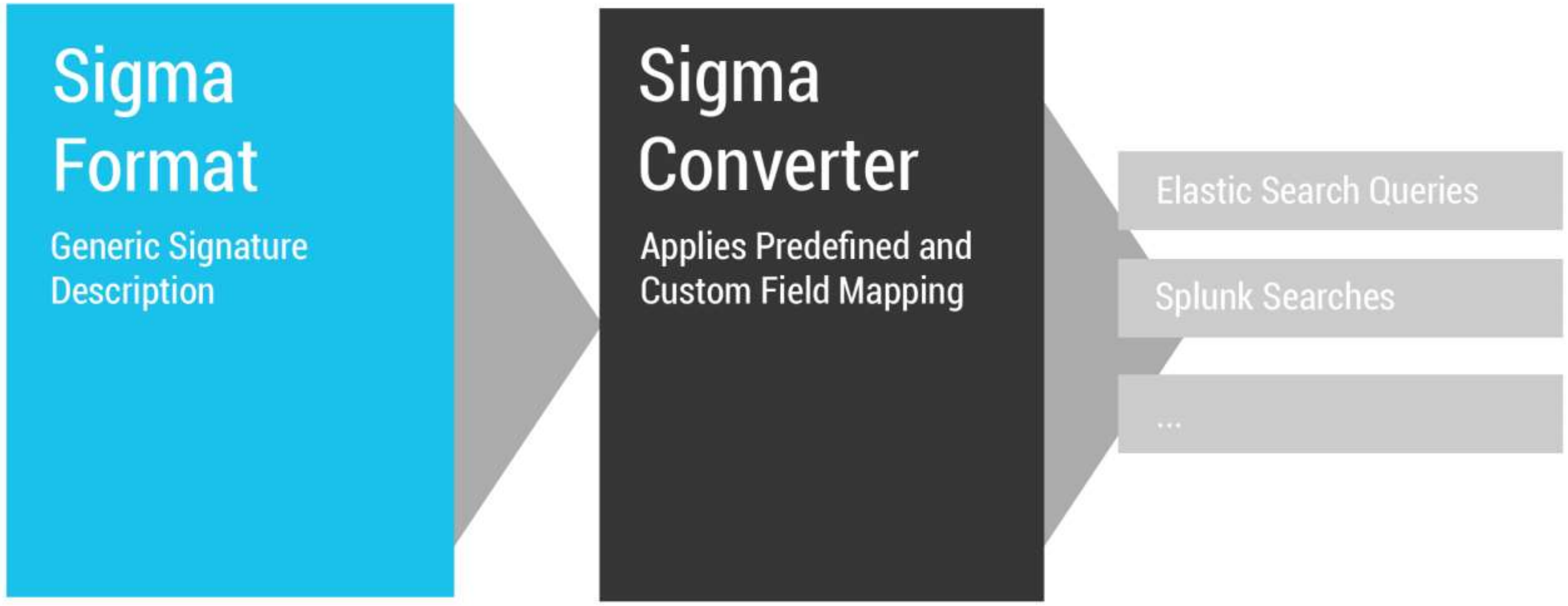
1 contributor

26 lines (25 sloc) | 677 Bytes

```
title: Mimikatz Use
description: This method detects mimikatz keywords in different Eventlogs (some of them only appear in older Mimikatz version that are howe
author: Florian Roth
tags:
    - attack.s0002
    - attack.t1003
    - attack.lateral_movement
    - attack.credential_access
logsource:
    product: windows
detection:
    keywords:
        - mimikatz
        - mimilib
        - <3 eo.oe
        - eo.oe.kiwi
        - privilege::debug
        - sekurlsa::logonpasswords
        - lsadump::sam
        - mimidrv.sys
    condition: keywords
falsepositives:
    - Naughty administrators
    - Penetration test
level: critical
```

SIGMA

Sigma is a project by Florian Roth which tries to provide a generic, vendor-neutral, rule format that can used to describe suspicious or malicious behavior. Most SIGMA rules are also mapped to MITRE's ATT&CK framework.

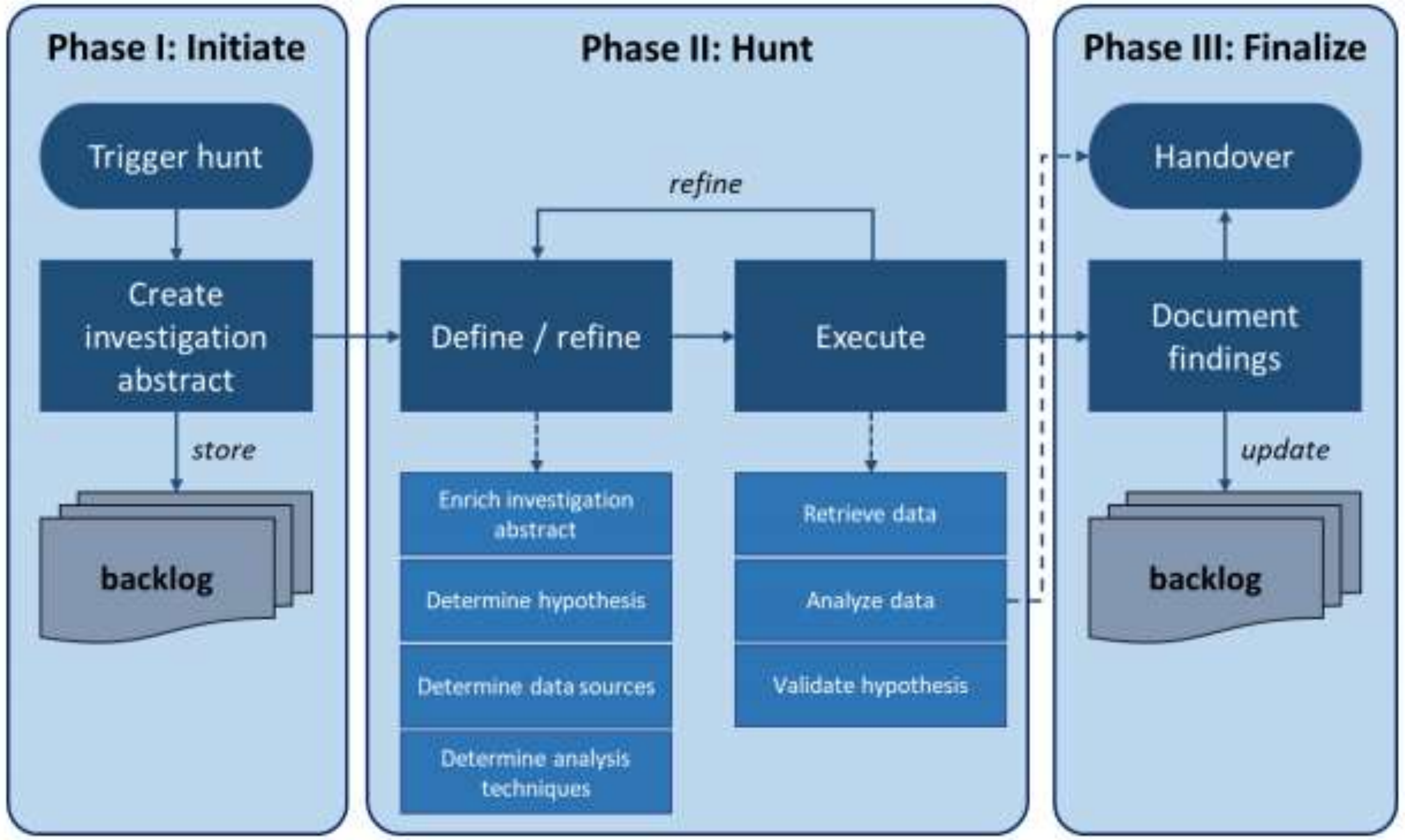

Sigma Format
Generic Signature Description
Sigma Converter
Applies Predefined and Custom Field Mapping
Elastic Search Queries
Splunk Searches
...

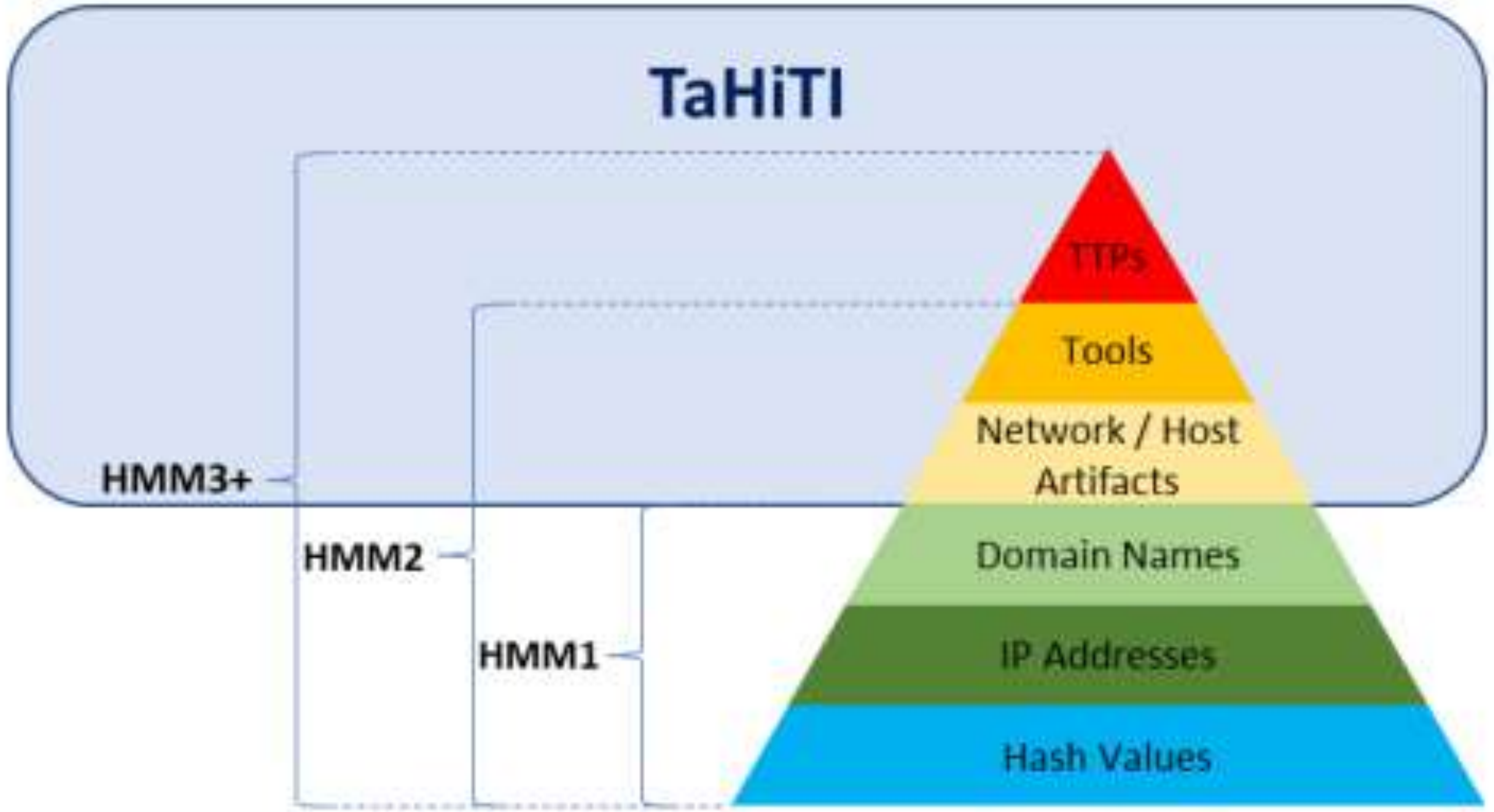
ATT&CK Initiatives - Detection

Many open-source tools align with ATT&CK

TaHiTi Threat Hunting Methodology

Targeted Hunting integrating Threat Intelligence (TaHiTI) methodology was built by the Dutch financial sector and aims to provide a standard methodology for threat hunting.

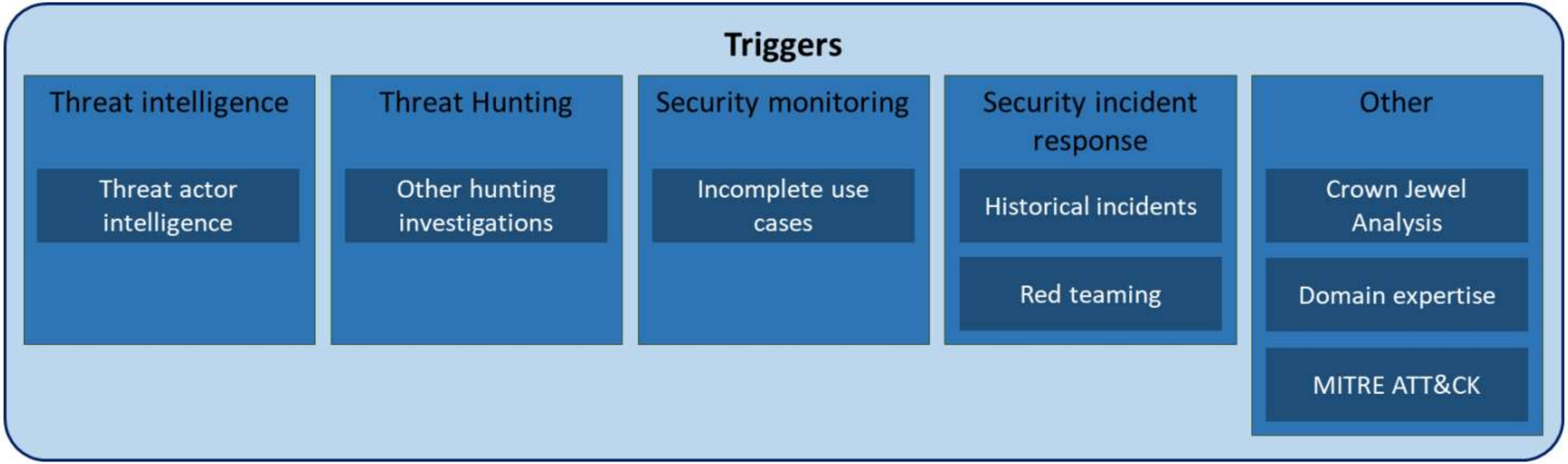




https://www.betaalvereniging.nl/wp-content/uploads/DEF-TaHiTI-Threat-Hunting-Methodology.pdf

ATT&CK Initiatives - Detection

Many open-source tools align with ATT&CK



Triggers

Threat intelligence

- Threat actor intelligence

Threat Hunting

- Other hunting investigations

Security monitoring

- Incomplete use cases

Security incident response

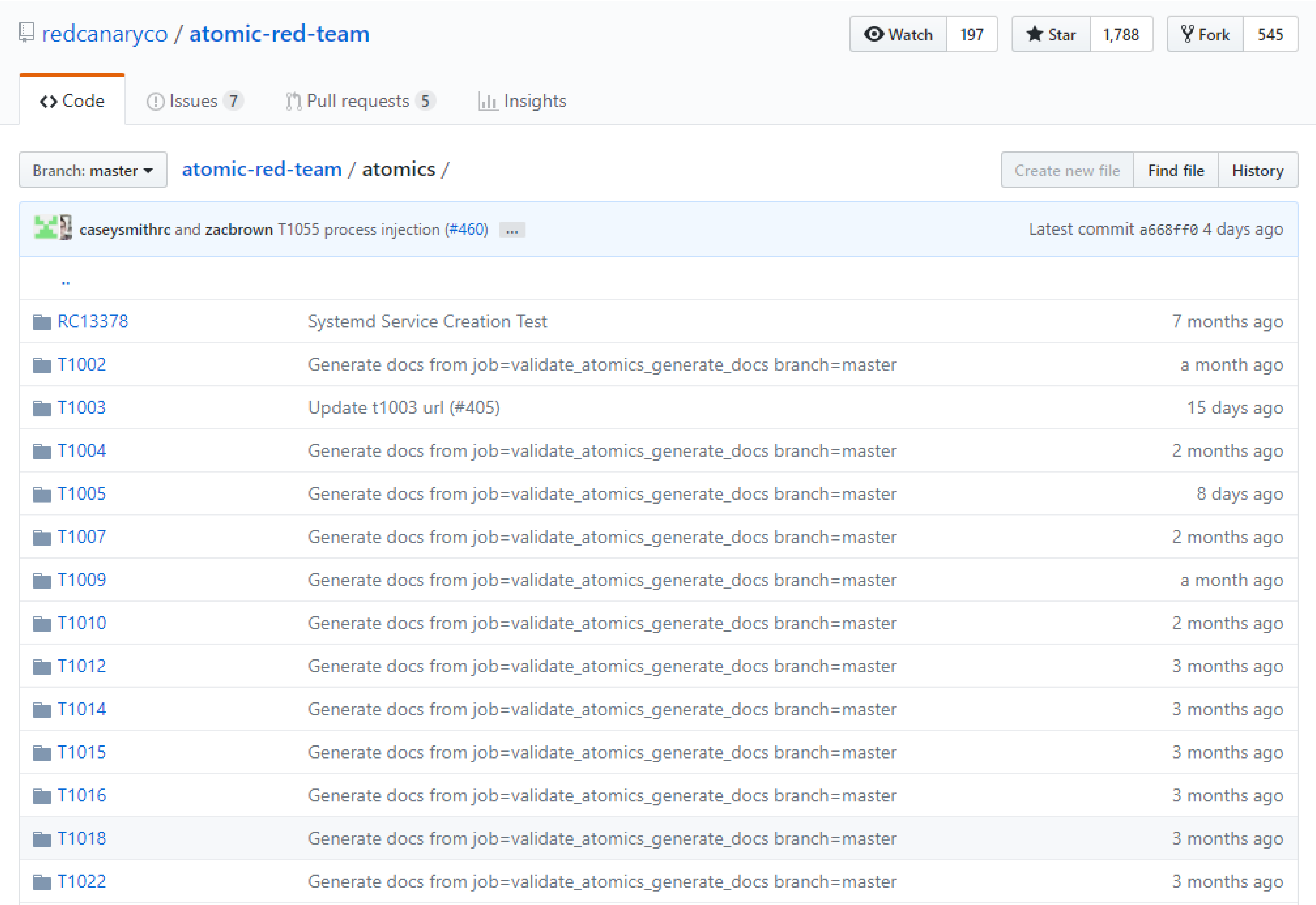
- Historical incidents
- Red teaming

Other

- Crown Jewel Analysis
- Domain expertise
- MITRE ATT&CK

ATT&CK Initiatives - Emulation

Many open-source tools align with ATT&CK



redcanaryco / atomic-red-team

Watch 197 | Star 1,788 | Fork 545

<> Code | Issues 7 | Pull requests 5 | Insights

Branch: master ▾ atomic-red-team / atomics /

Create new file | Find file | History

caseysmithrc and zacbrown T1055 process injection (#460) ... Latest commit a668ff0 4 days ago

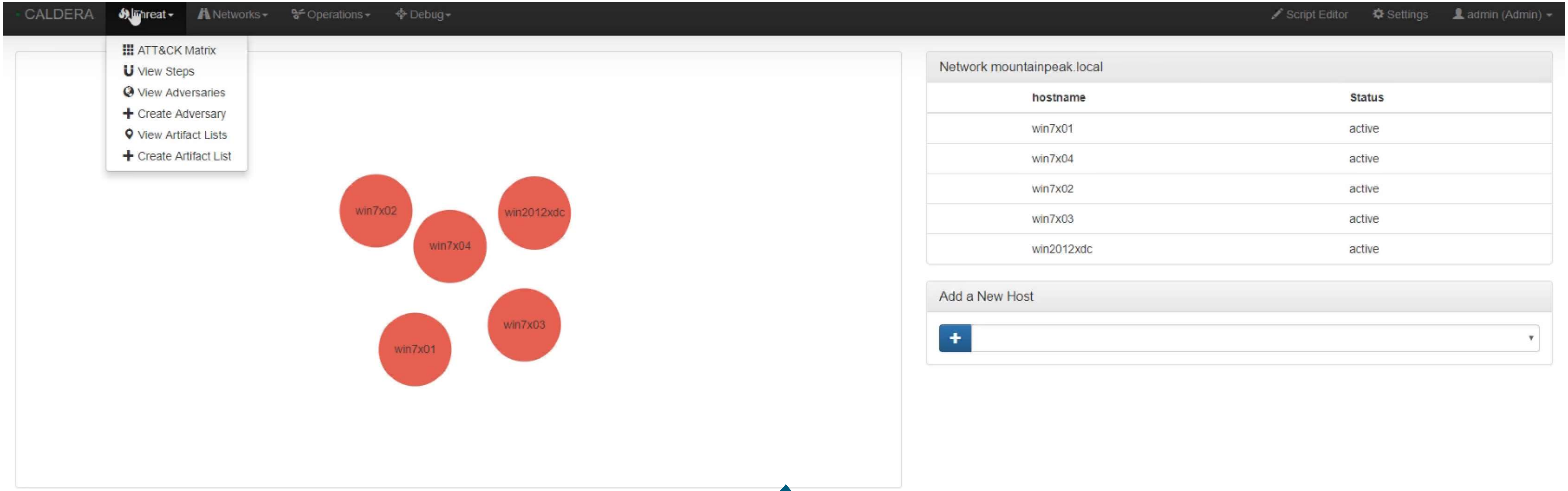
..		
RC13378	Systemd Service Creation Test	7 months ago
T1002	Generate docs from job=validate_atomics_generate_docs branch=master	a month ago
T1003	Update t1003 url (#405)	15 days ago
T1004	Generate docs from job=validate_atomics_generate_docs branch=master	2 months ago
T1005	Generate docs from job=validate_atomics_generate_docs branch=master	8 days ago
T1007	Generate docs from job=validate_atomics_generate_docs branch=master	2 months ago
T1009	Generate docs from job=validate_atomics_generate_docs branch=master	a month ago
T1010	Generate docs from job=validate_atomics_generate_docs branch=master	2 months ago
T1012	Generate docs from job=validate_atomics_generate_docs branch=master	3 months ago
T1014	Generate docs from job=validate_atomics_generate_docs branch=master	3 months ago
T1015	Generate docs from job=validate_atomics_generate_docs branch=master	3 months ago
T1016	Generate docs from job=validate_atomics_generate_docs branch=master	3 months ago
T1018	Generate docs from job=validate_atomics_generate_docs branch=master	3 months ago
T1022	Generate docs from job=validate_atomics_generate_docs branch=master	3 months ago

Red Canary developed "Atomic Red Team", which is a series of "simple" tests that can be used to emulate the behavior of adversaries in the environment.

The tests are linked to MITRE ATT&CK!

ATT&CK Initiatives - Emulation

Many open-source tools align with ATT&CK



Network mountainpeak.local

hostname	Status
win7x01	active
win7x04	active
win7x02	active
win7x03	active
win2012xdc	active

CALDERA is a tool built by MITRE, with the express purpose of doing adversary emulation. It requires a bit of setup (as a server needs to be installed) and it will actively “attack” target systems by deploying custom backdoors. CALDERA’s attack steps are fully linked to the ATT&CK framework techniques!

ATT&CK Initiatives – Atomic Threat Coverage

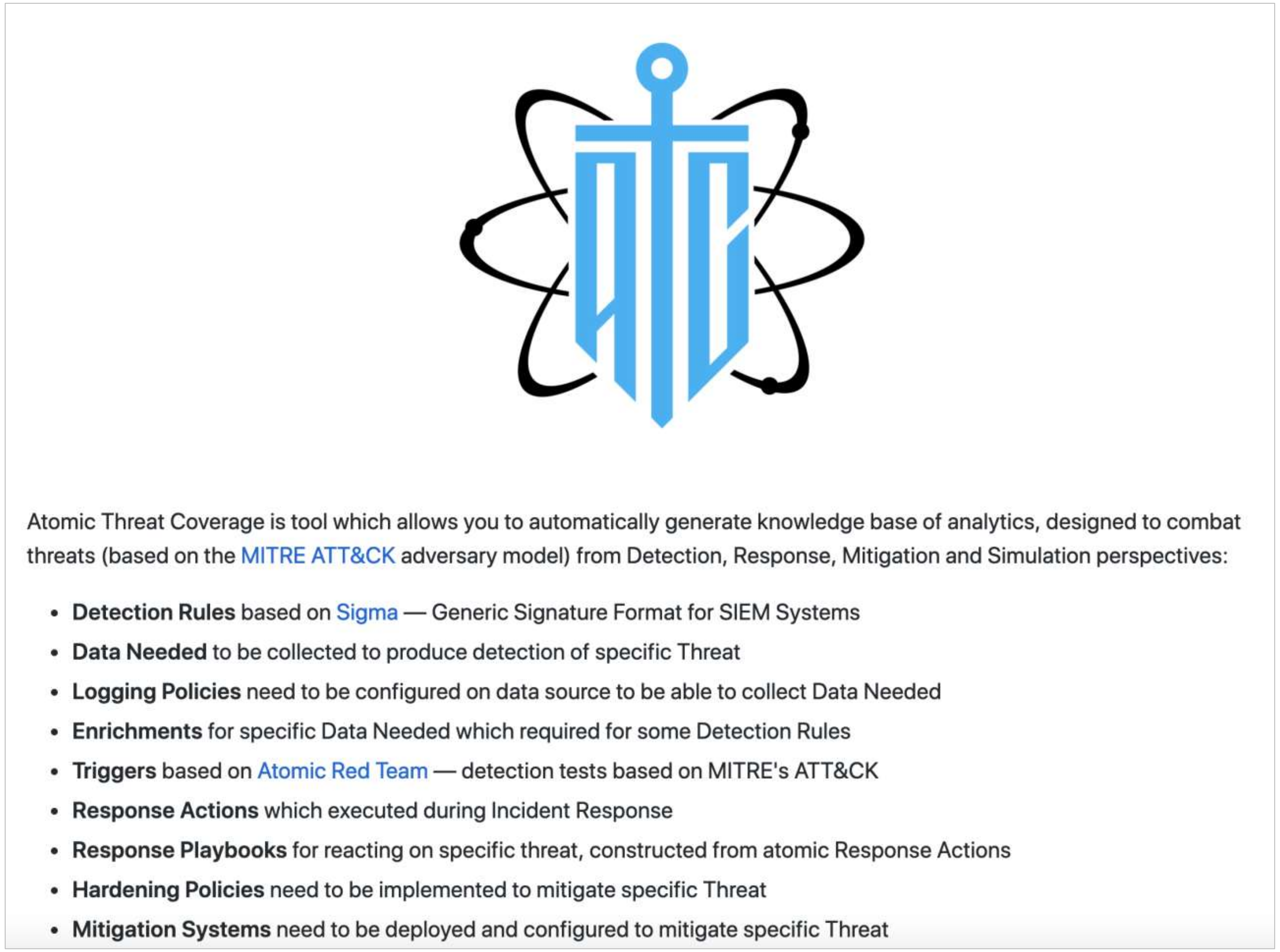
Many open-source tools align with ATT&CK

In February 2019, Atomic Threat Coverage was released by:

- Daniil Yugoslavskiy (@yugoslavskiy)
- Jakob Weinzettl (@mrblacyk)
- Mateusz Wydra (@sn0w0tter)
- Mikhail Aksenov (@AverageS)

Their goal is to have an “all-in-one” solution for detection, response, mitigation and simulation using MITRE ATT&CK!

https://github.com/krakow2600/atomic-threat-coverage



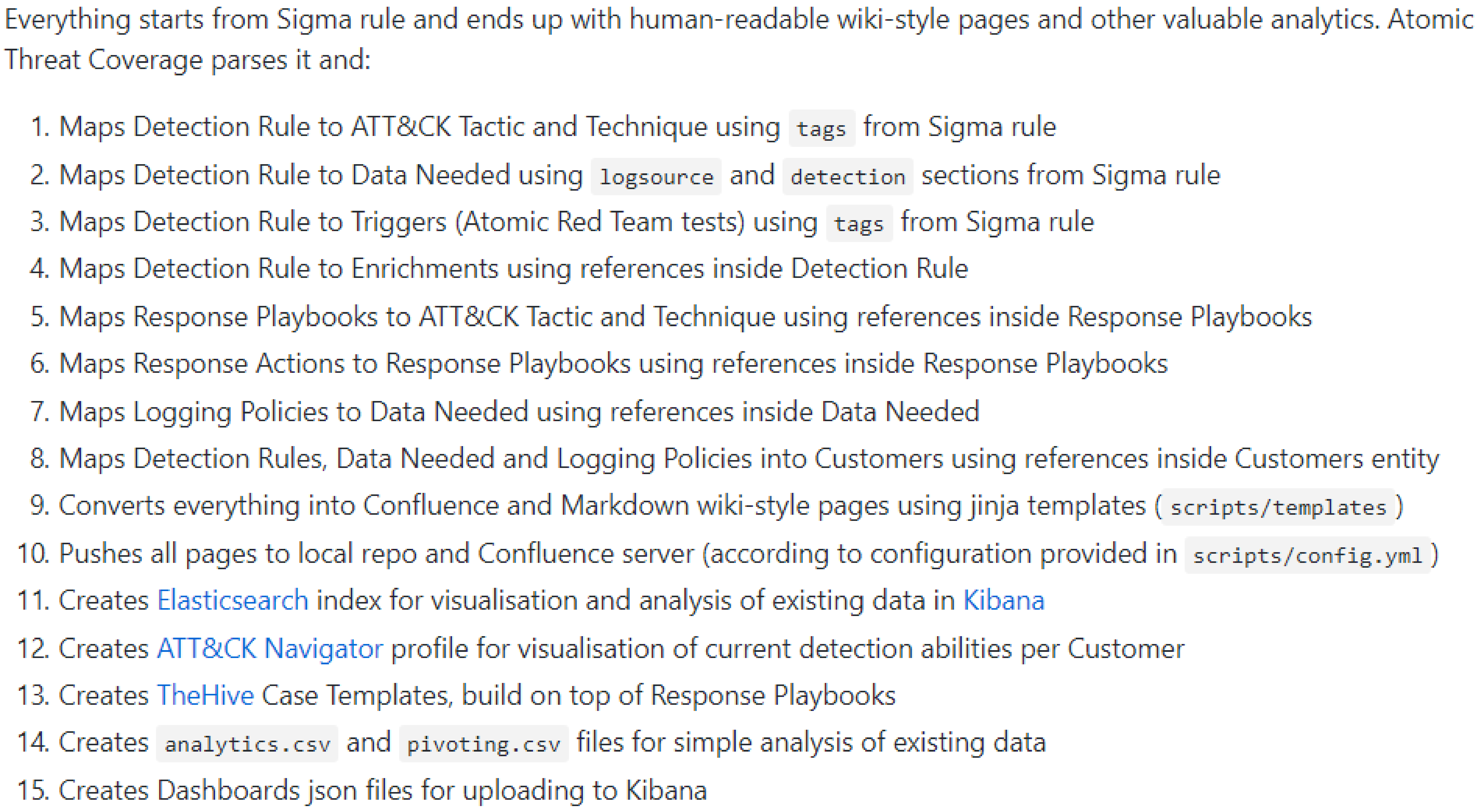
Atomic Threat Coverage is tool which allows you to automatically generate knowledge base of analytics, designed to combat threats (based on the MITRE ATT&CK adversary model) from Detection, Response, Mitigation and Simulation perspectives:

- **Detection Rules** based on Sigma — Generic Signature Format for SIEM Systems
- **Data Needed** to be collected to produce detection of specific Threat
- **Logging Policies** need to be configured on data source to be able to collect Data Needed
- **Enrichments** for specific Data Needed which required for some Detection Rules
- **Triggers** based on Atomic Red Team — detection tests based on MITRE's ATT&CK
- **Response Actions** which executed during Incident Response
- **Response Playbooks** for reacting on specific threat, constructed from atomic Response Actions
- **Hardening Policies** need to be implemented to mitigate specific Threat
- **Mitigation Systems** need to be deployed and configured to mitigate specific Threat

ATT&CK all the things!

ATT&CK Initiatives – Atomic Threat Coverage

Many open-source tools align with ATT&CK



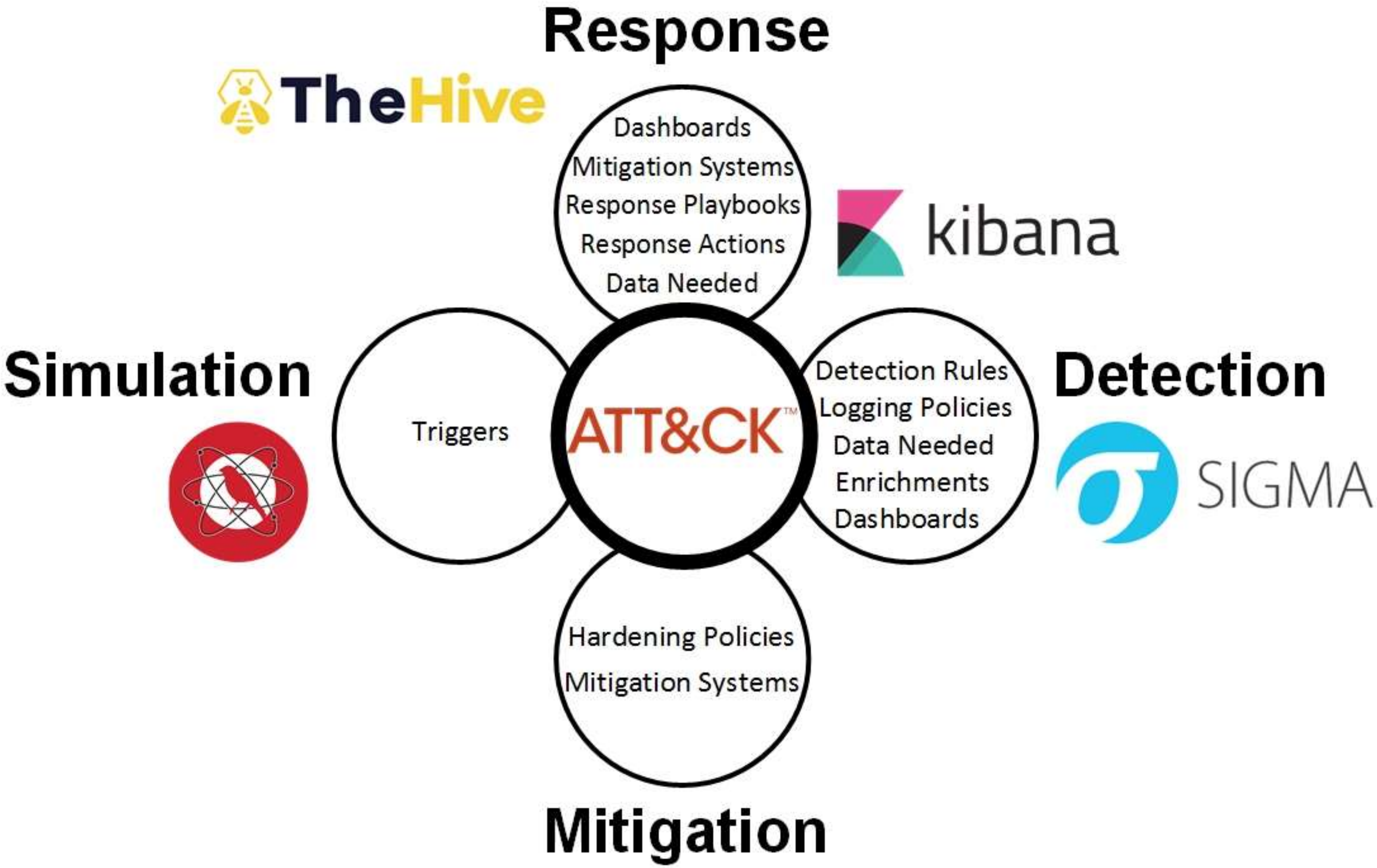
Everything starts from Sigma rule and ends up with human-readable wiki-style pages and other valuable analytics. Atomic Threat Coverage parses it and:

1. Maps Detection Rule to ATT&CK Tactic and Technique using `tags` from Sigma rule
2. Maps Detection Rule to Data Needed using `logsource` and `detection` sections from Sigma rule
3. Maps Detection Rule to Triggers (Atomic Red Team tests) using `tags` from Sigma rule
4. Maps Detection Rule to Enrichments using references inside Detection Rule
5. Maps Response Playbooks to ATT&CK Tactic and Technique using references inside Response Playbooks
6. Maps Response Actions to Response Playbooks using references inside Response Playbooks
7. Maps Logging Policies to Data Needed using references inside Data Needed
8. Maps Detection Rules, Data Needed and Logging Policies into Customers using references inside Customers entity
9. Converts everything into Confluence and Markdown wiki-style pages using jinja templates (`scripts/templates`)
10. Pushes all pages to local repo and Confluence server (according to configuration provided in `scripts/config.yml`)
11. Creates Elasticsearch index for visualisation and analysis of existing data in Kibana
12. Creates ATT&CK Navigator profile for visualisation of current detection abilities per Customer
13. Creates TheHive Case Templates, build on top of Response Playbooks
14. Creates `analytics.csv` and `pivoting.csv` files for simple analysis of existing data
15. Creates Dashboards json files for uploading to Kibana

https://github.com/krakow2600/atomic-threat-coverage

ATT&CK Initiatives – Atomic Threat Coverage

Many open-source tools align with ATT&CK



Demo

Demonstrating Caldera & ATT&CK Navigator

Demo

ATT&CK Navigator and CALDERA in action

Conclusions

- ATT&CK should be used as a “**common language**” by a variety of security functions in the organisation (adversary emulation, security monitoring, threat hunting,…)

- ATT&CK is huge and covering all techniques from the start is not feasible, **prioritize** according to popularity of techniques (general) and your own organization (based on relevant threat actors)!

- Don’t reinvent the wheel: Leverage and contribute to **existing projects** to hit the ground running!

Want more?

Some additional links & references

- **ATT&CKCon 2018 presentations**
  https://www.slideshare.net/attackcon2018/presentations

- **ATT&CK™ Your CTI with Lessons Learned from Four Years in the Trenches - Katie Nickels (MITRE) & Bryan Beyer (Red Canary)**
  https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1548090281.pdf

- **ATT&CK™ Is Only as Good as Its Implementation: Avoiding Five Common Pitfalls (Kyle Rainey - Red Canary)**
  https://www.redcanary.com/blog/avoiding-common-attack-pitfalls/

Q&A

Any questions?