SANS

Leveraging MITRE ATT&CK

Using ATT&CK (Navigator) in the enterprise

#SEC599 – Defeating Advanced Adversaries

Your hosts for the webcast

Stephen Sims @Steph3nSims
Erik Van Buggenhout @ErikVaBu

Your Hosts for Today

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

Stephen Sims
SANS Fellow
@Steph3nSims

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

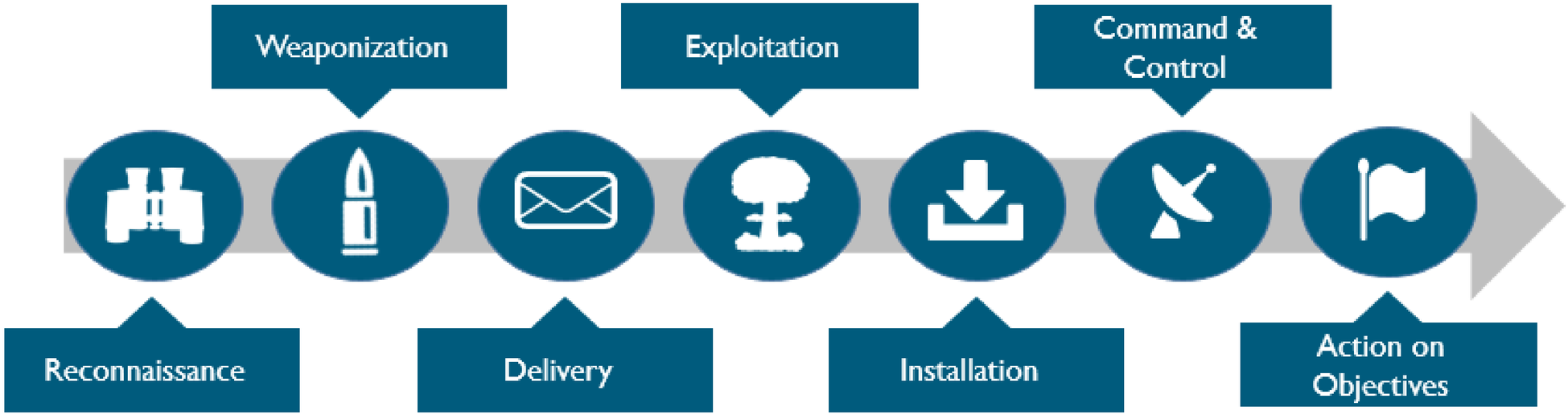
Ask us your questions!

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

TACTICS

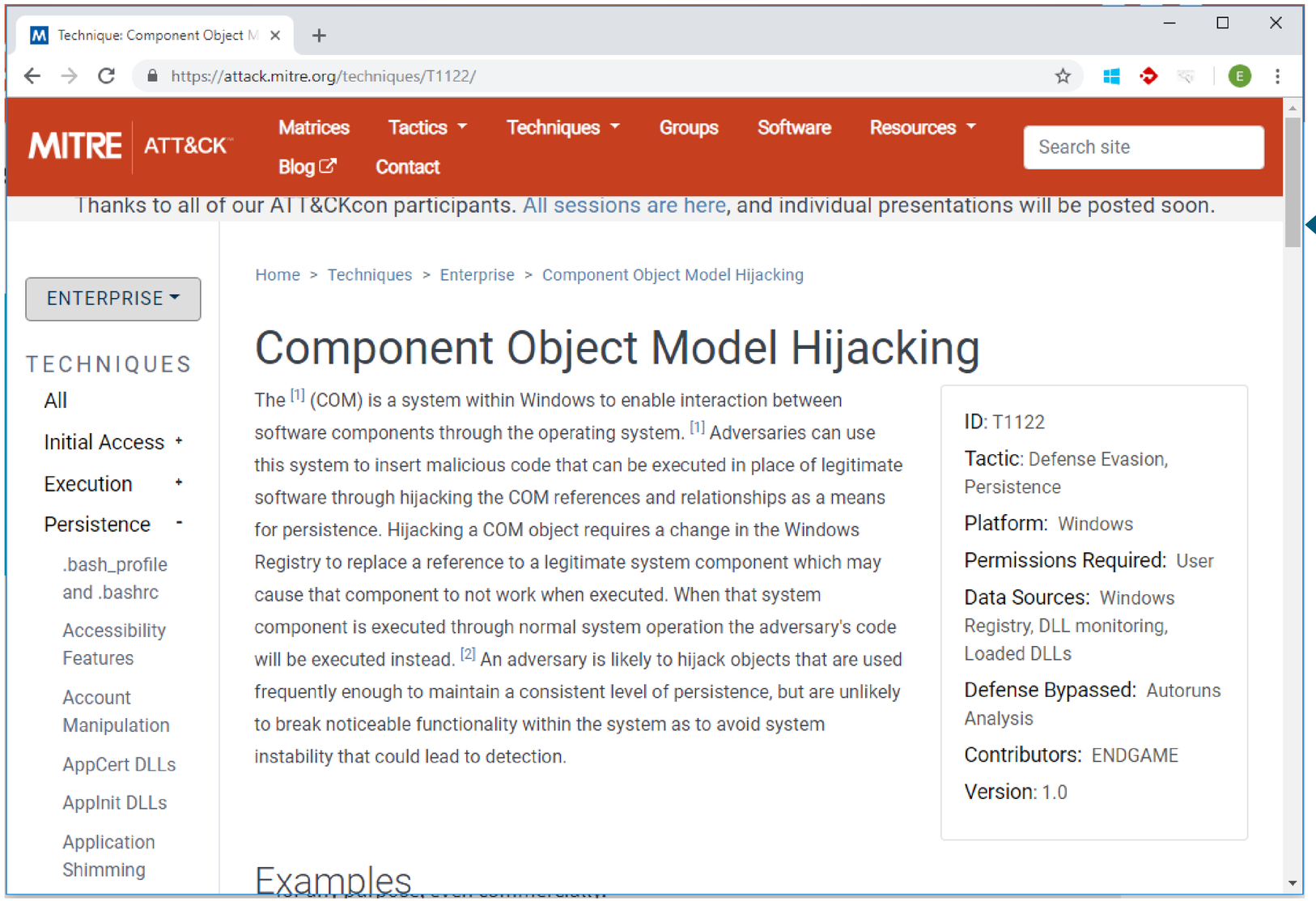
ATT&CK Matrix for Enterprise

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

TECHNIQUES

MITRE ATT&CK?

Zooming in on a technique



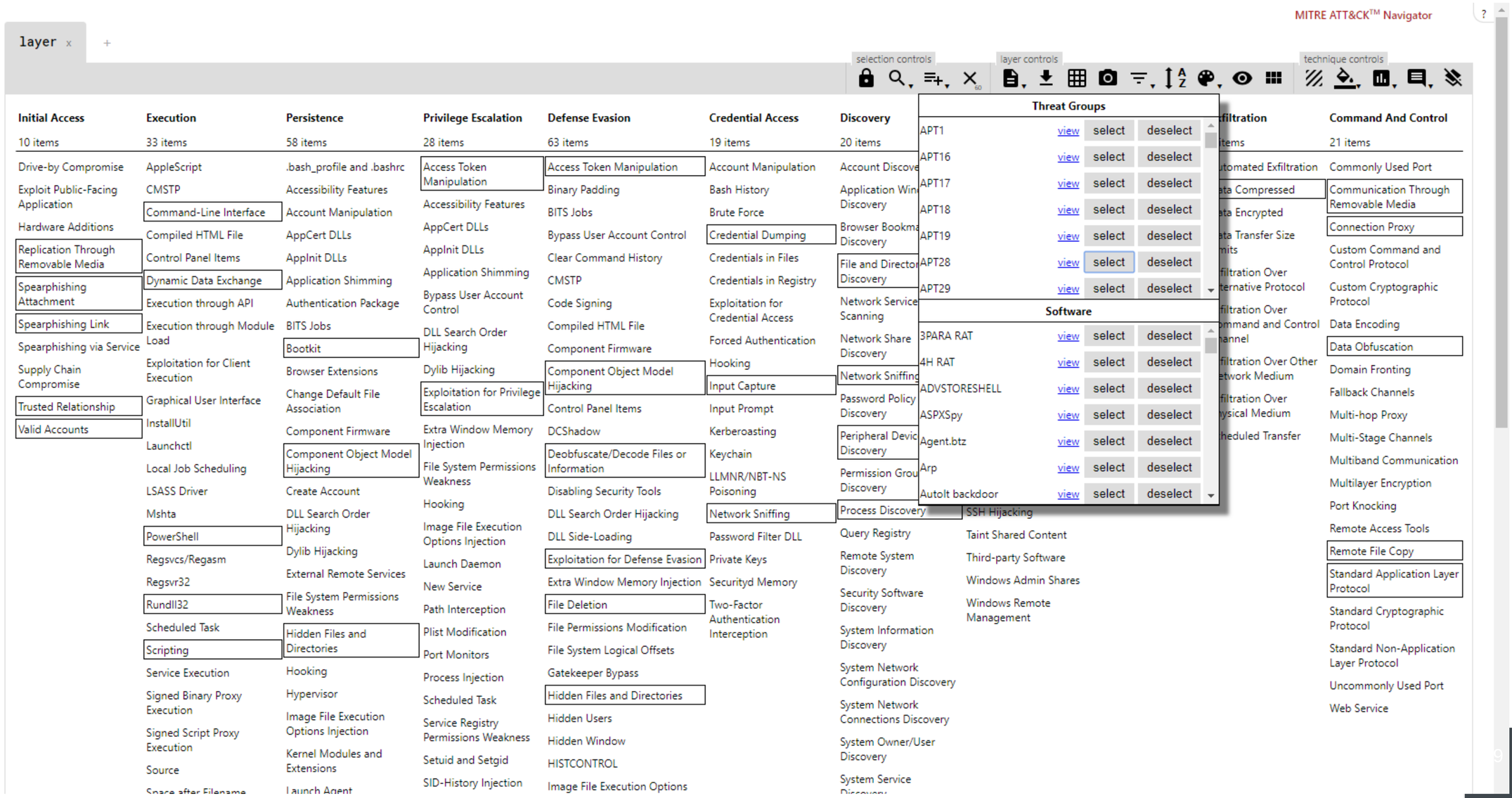
As an example, let's have a look at one of Turla's favorite techniques: COM object hijacking. In MITRE's ATT&CK framework, this technique is known as T1122, and it's part of the "Defense Evasion" and "Persistence" tactics for Windows.

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



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

See Evaluations » | Get Evaluated » | Read Methodology »

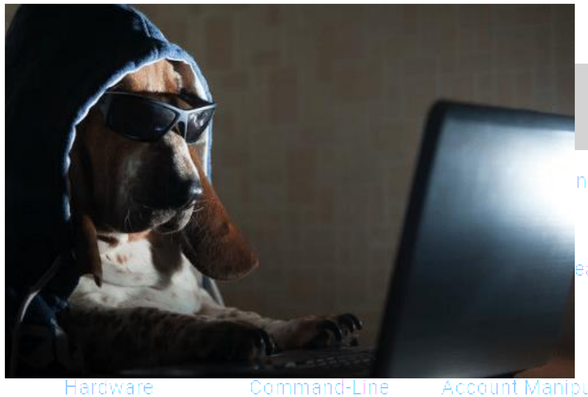
Carbon Black. FIREEYE™ CROWDSTRIKE

ATT&CK Use Cases

How can MITRE ATT&CK be used?

Key use cases for ATT&CK

ATT&CK as a common language!



Adversary emulation

Prioritize defenses

Detection capability

Threat Intelligence

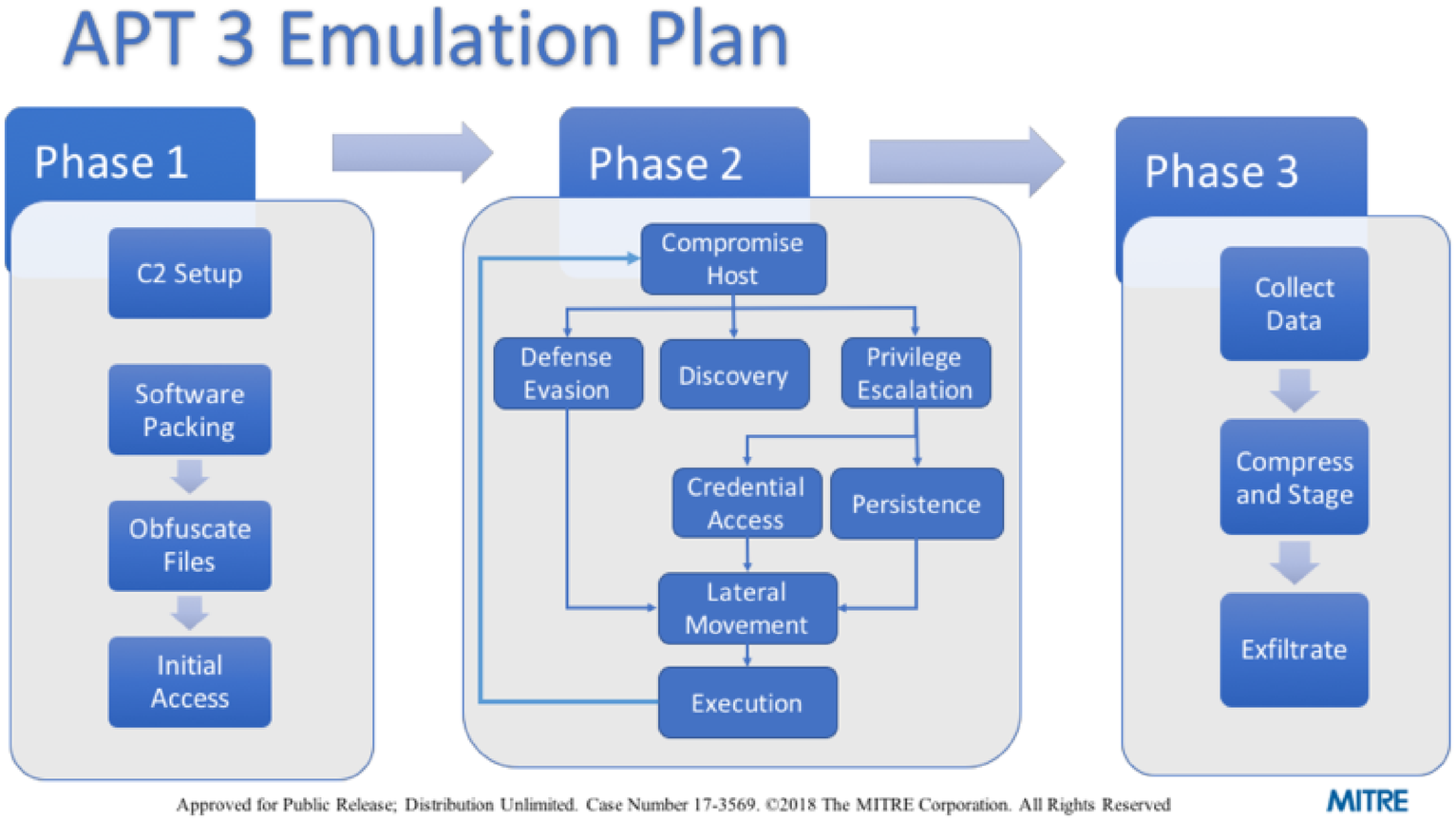
ATT&CK Matrix for Enterprise

	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection		Command and Co
nc .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 Software	Automated Collection		Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCer		Distributed Component Object Model			
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit		Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
			Applica Shimmi		Logon Scripts	Data from Inform Repo		
imming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data Loca		
Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Netw Shared		
Supply Chain Compromise	Execution Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Media

ATT&CK™

Adversarial Tactics, Techniques & Common Knowledge

ATT&CK for adversary emulation



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.

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

APT15 was also observed using Mimikatz to dump credentials and generate Kerberos golden tickets. This allowed the group to persist in th ent of

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

Scripting (T1064)

Registry Run Keys / Startup Folder (T1060)

Command-Line Interface (T1059)

Discovery - T1057, T1018, T1049, T1082, T1016

Cred Dumping (T1003)

Input Capture (T1056)

Pass the Ticket (T1097)

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.

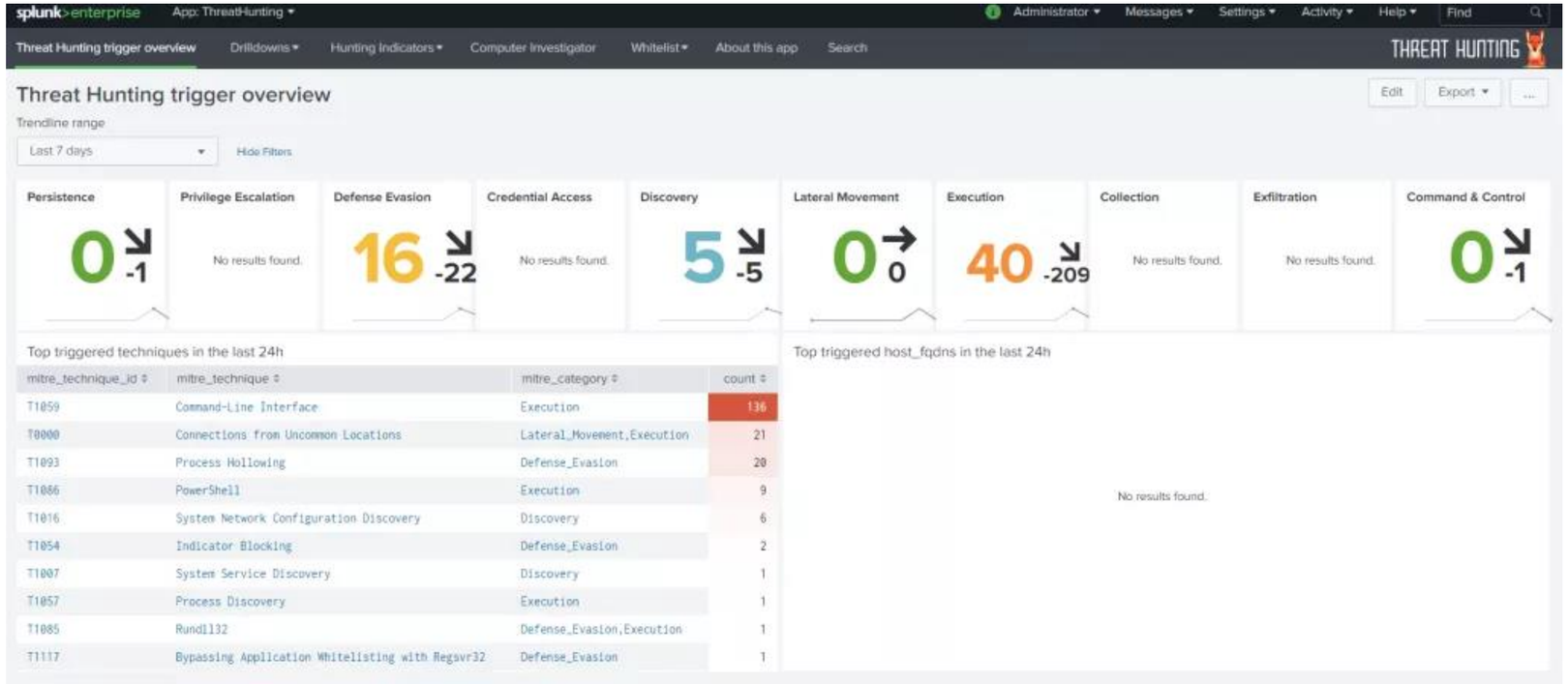
https://www.tripwire.com/state-of-security/security-data-protection/security-controls/mapping-the-attck-framework-to-cis-controls/

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**?



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 & Red Canary combined efforts and presented a joint view on ATT&CK at the SANS CTI Summit:

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

All techniques are equal…

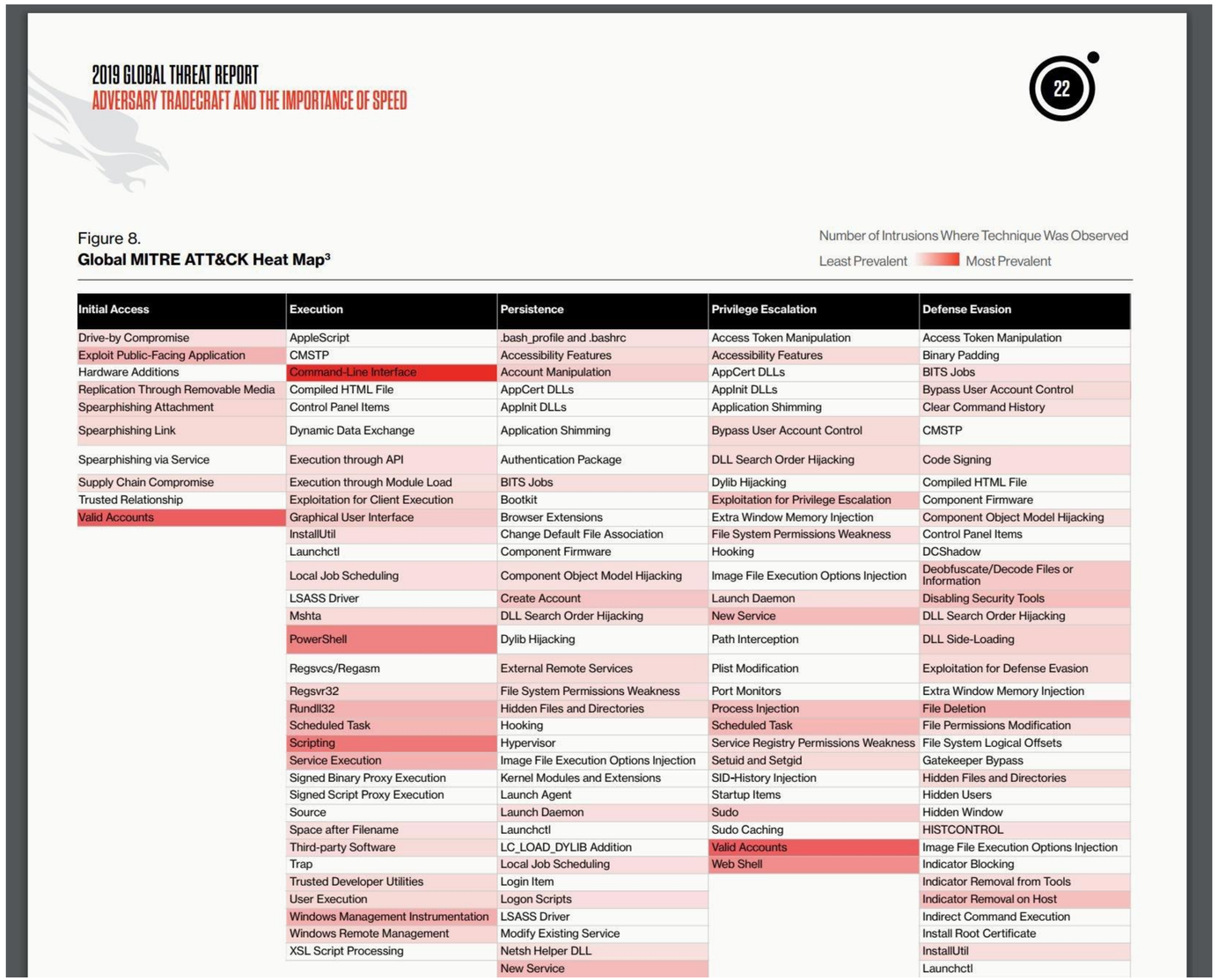
But some techniques are more equal than others

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

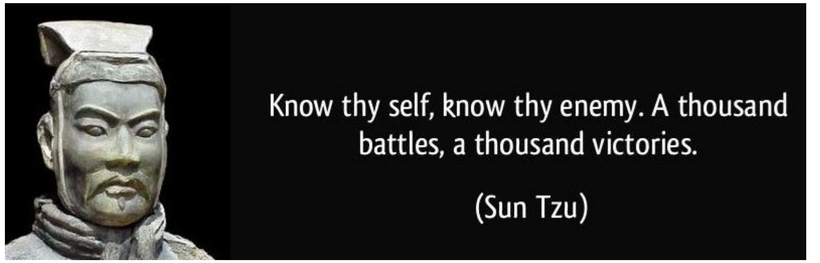
Crowdstrike released the “**Global Threat Report**” in February 2019 and added a “heat map” of MITRE ATT&CK, which can again be used to **prioritize** your efforts and attention!

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

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

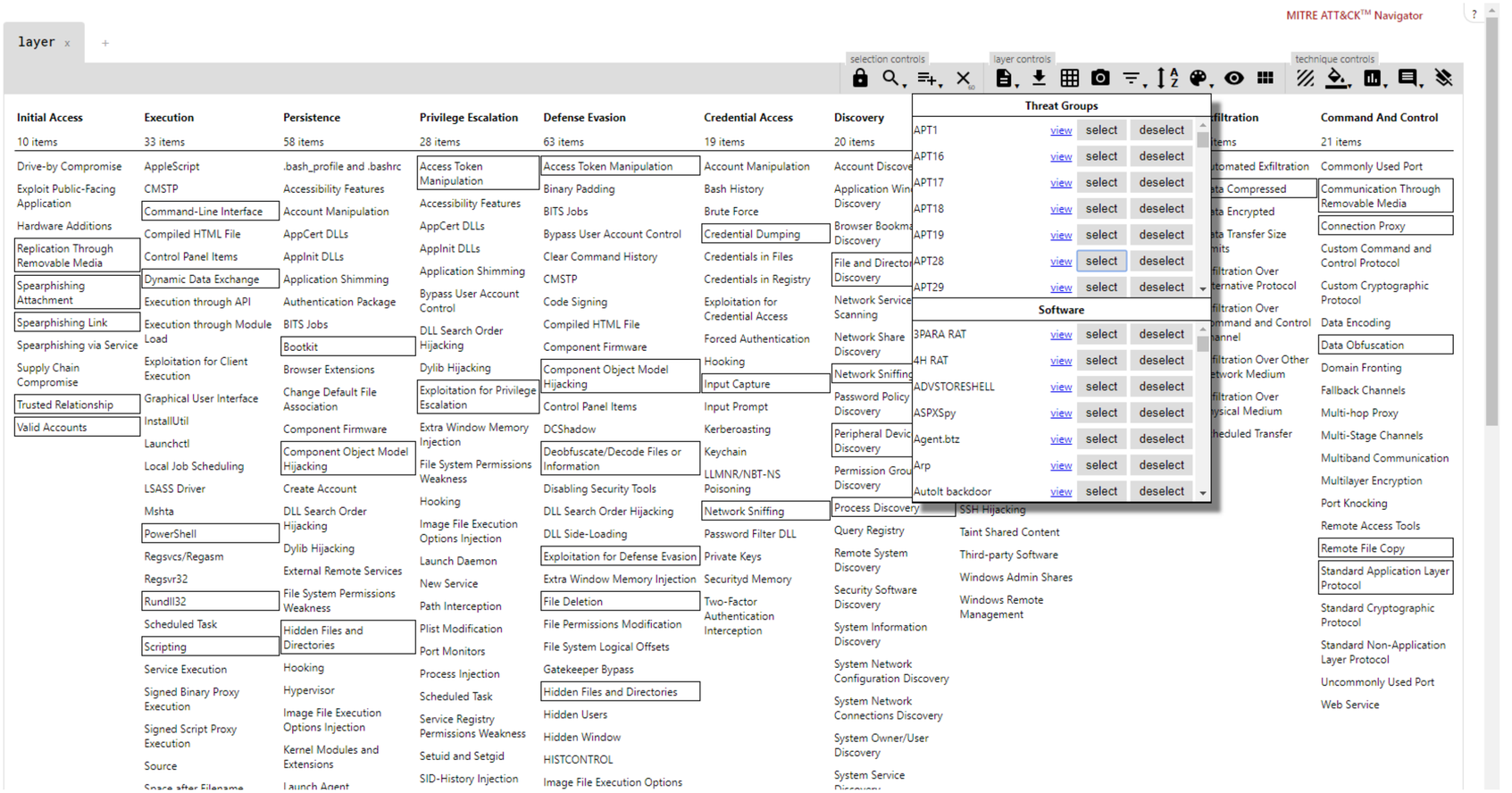
All techniques are equal…

But some techniques are more equal than others



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!



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

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 the work that was already performed by SwiftOnSecurity, as he uses that configuration file as a starting point! He also wrote a blog post series called "Endpoint detection Superpowers on the cheap"!

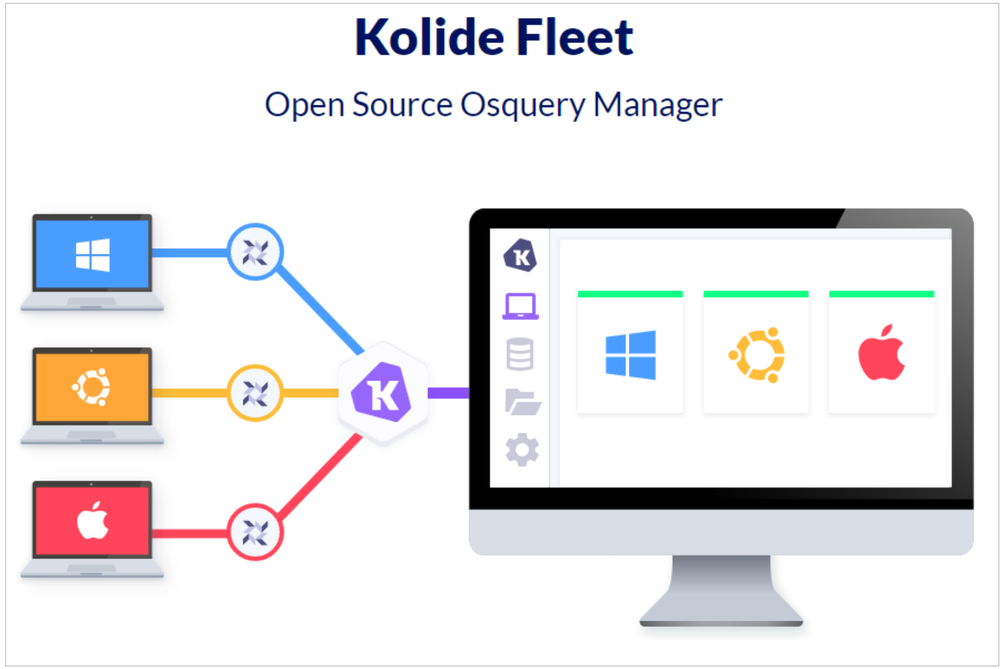
ATT&CK Initiatives - Detection

Many open-source tools align with ATT&CK

73 lines (72 sloc) | 6.34 KB — Raw | Blame | History

```
{
  "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

Branch: master ▾ sigma / rules / windows / builtin / win_alert_mimikatz_keywords.yml Find file | Copy path

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

1 contributor

26 lines (25 sloc) | 677 Bytes Raw | Blame | History

```yaml
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 be used to describe suspicious or malicious behavior. Most SIGMA rules are also mapped to MITRE's ATT&CK framework.

Sigma Format

Generic Signature Description

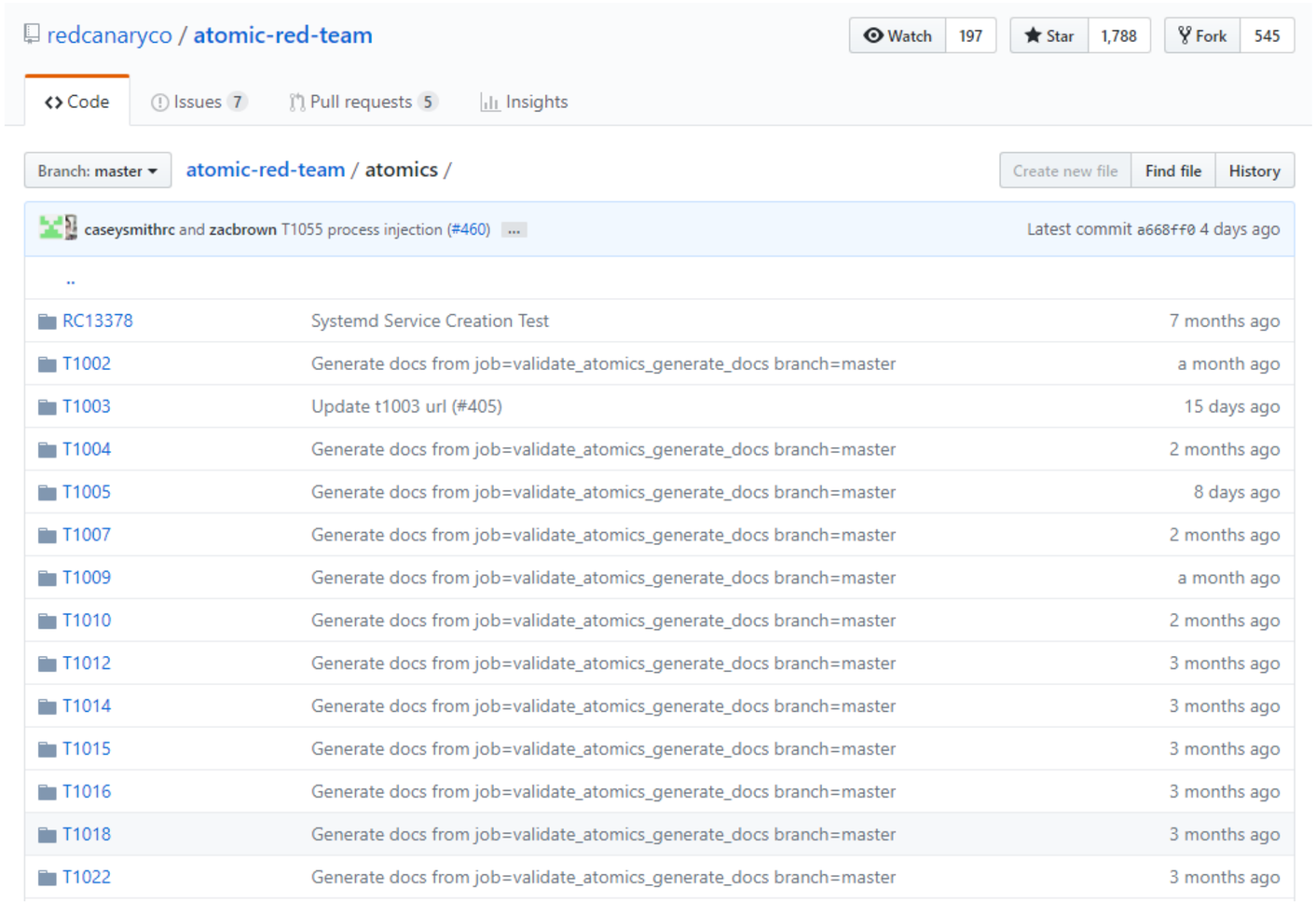
Sigma Converter

Applies Predefined and Custom Field Mapping

- Elastic Search Queries
- Splunk Searches
- ...

ATT&CK Initiatives - 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

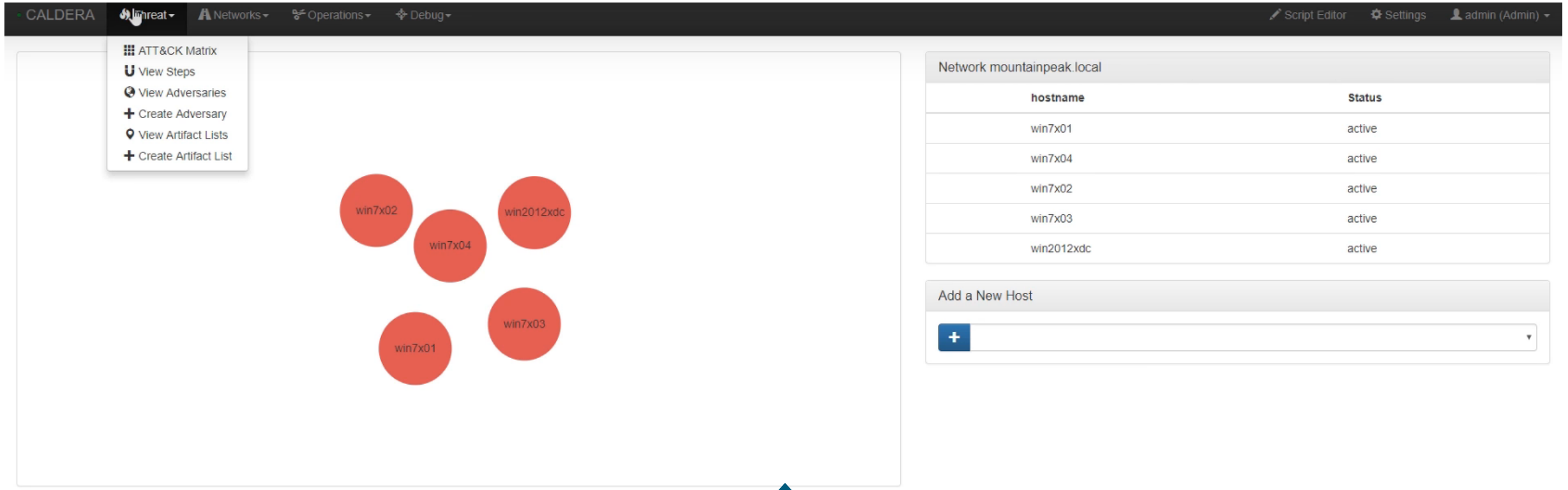
..		
RC13378	Systemd Service Creation Test	7 months ago
T1002	Generate docs from job=validate_atomics_generate_docs branch=master	a month ago
T1003	Update t1003 url (#405)	15 days ago
T1004	Generate docs from job=validate_atomics_generate_docs branch=master	2 months ago
T1005	Generate docs from job=validate_atomics_generate_docs 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



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 - Something new…

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

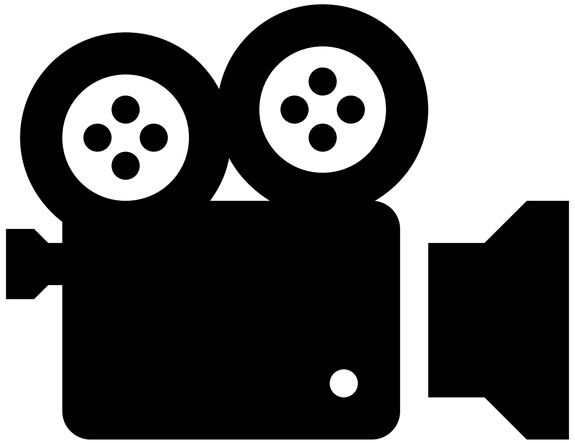
ATT&CK all the things!

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?