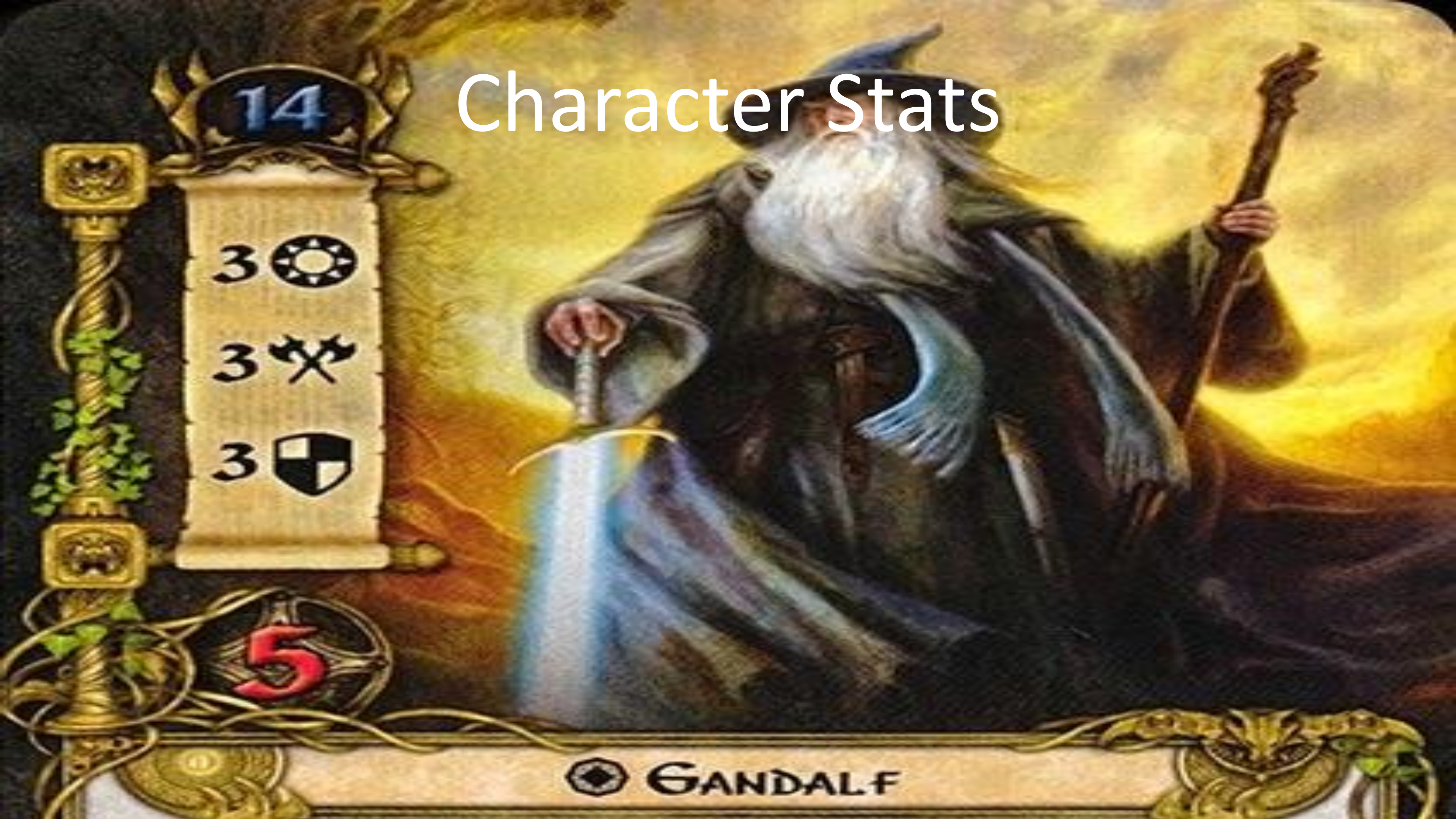
Our Journey into ATT&CK

Christian Kopacsi
Consumers Energy

Character Stats



- Director – Cyber Threat, Response & Adversary Operations
  - Security Monitoring
  - Incident Response
  - Adversary Operations
  - Penetration Testing
  - Vulnerability Management
- Blue + Red = Purple

Special Thanks

- MITRE
- SpecterOps
    - Roberto Rodriguez @Cyb3rWard0g
- Red Canary
    - Casey Smith @subTee
- Consumers Energy CSIRT & Leadership

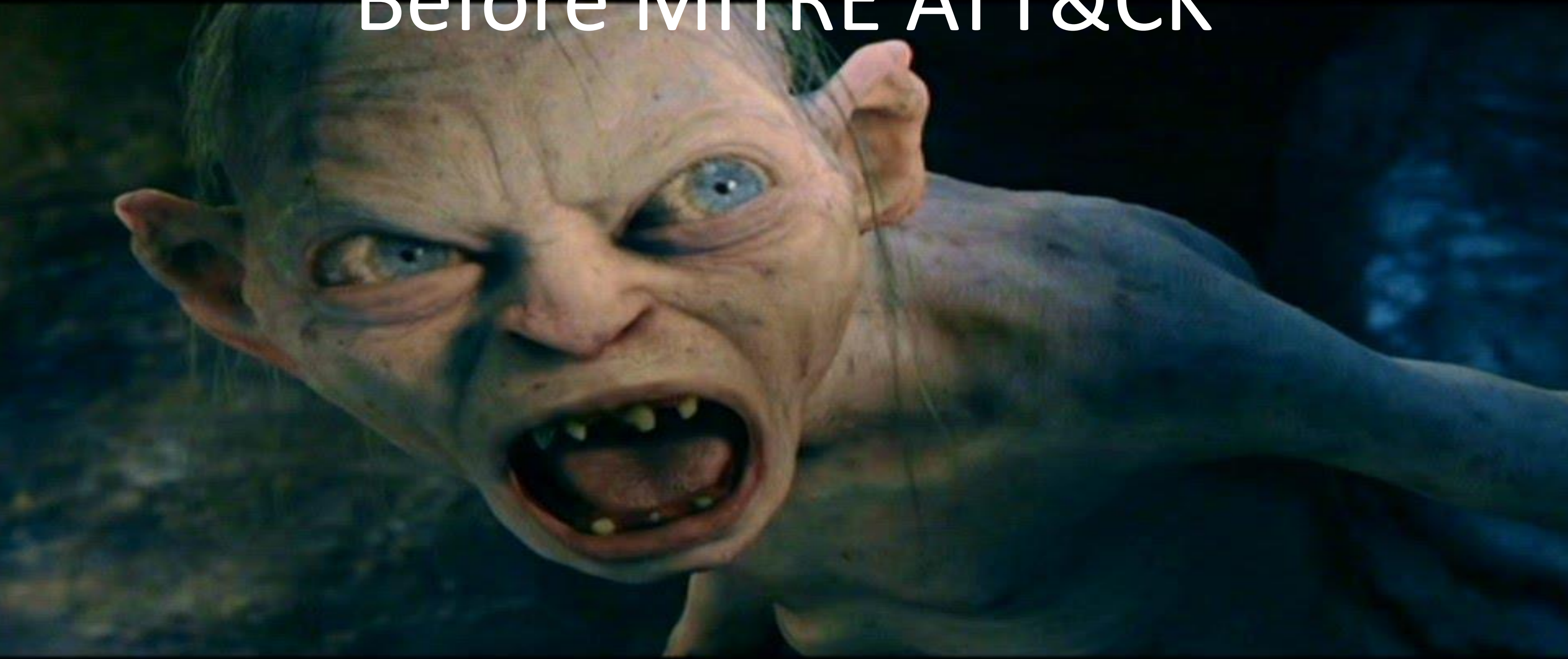
Our Journey Begins

- Alert Fatigue
- Detections created for very specific IOC’s
- Love/Hate relationship between Red/Blue team
- AD Hoc Documentation & Processes
- Do More with Less

My Fellowship

- 4 Analysts responsible for Security Monitoring and Incident Response
- 3 Analysts responsible for Adversary Operations & Vulnerability Management
- 14K Endpoints
- Responsible for Corporate and ICS Environment

Before MITRE ATT&CK



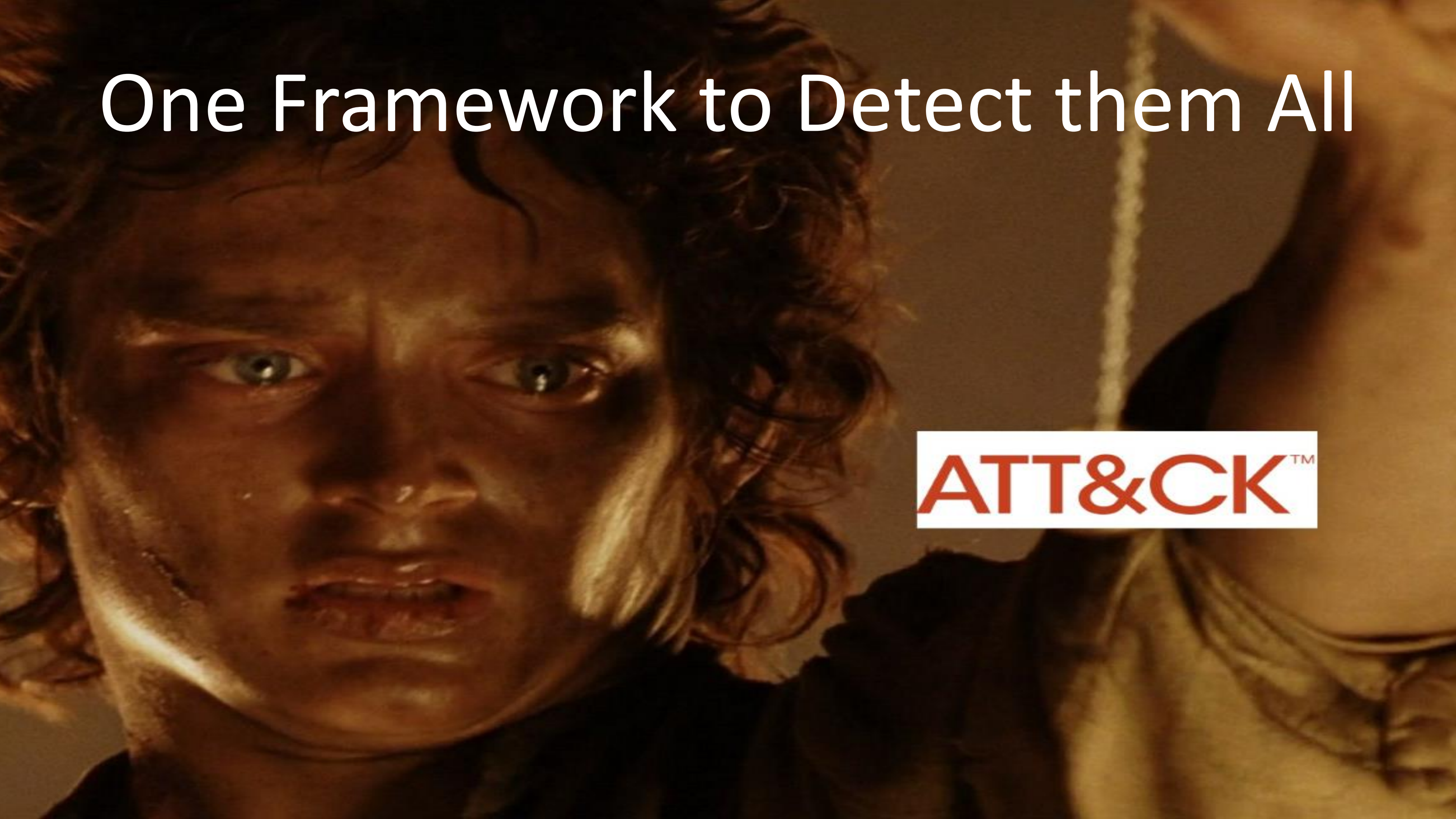
- Blue Team vs Red Team
  - Red Team performs campaign blue team doesn't detect
    - Red Team says Blue Teams sucks
    - Mgmt. then questions effectiveness of Blue Team
    - Human sacrifice, dogs and cats living together... mass hysteria ensues!

- Detections, Detections and More Detections
  - Analysts creating very specific detections for very specific IOC’s.
  - Works great if you are attacked using the exact same IOC’s

After MITRE ATT&CK

- Consistent terminology between Red and Blue Team
- Ability to measure effectiveness of detections/toolset
- Better detection in depth

One Framework to Detect them All

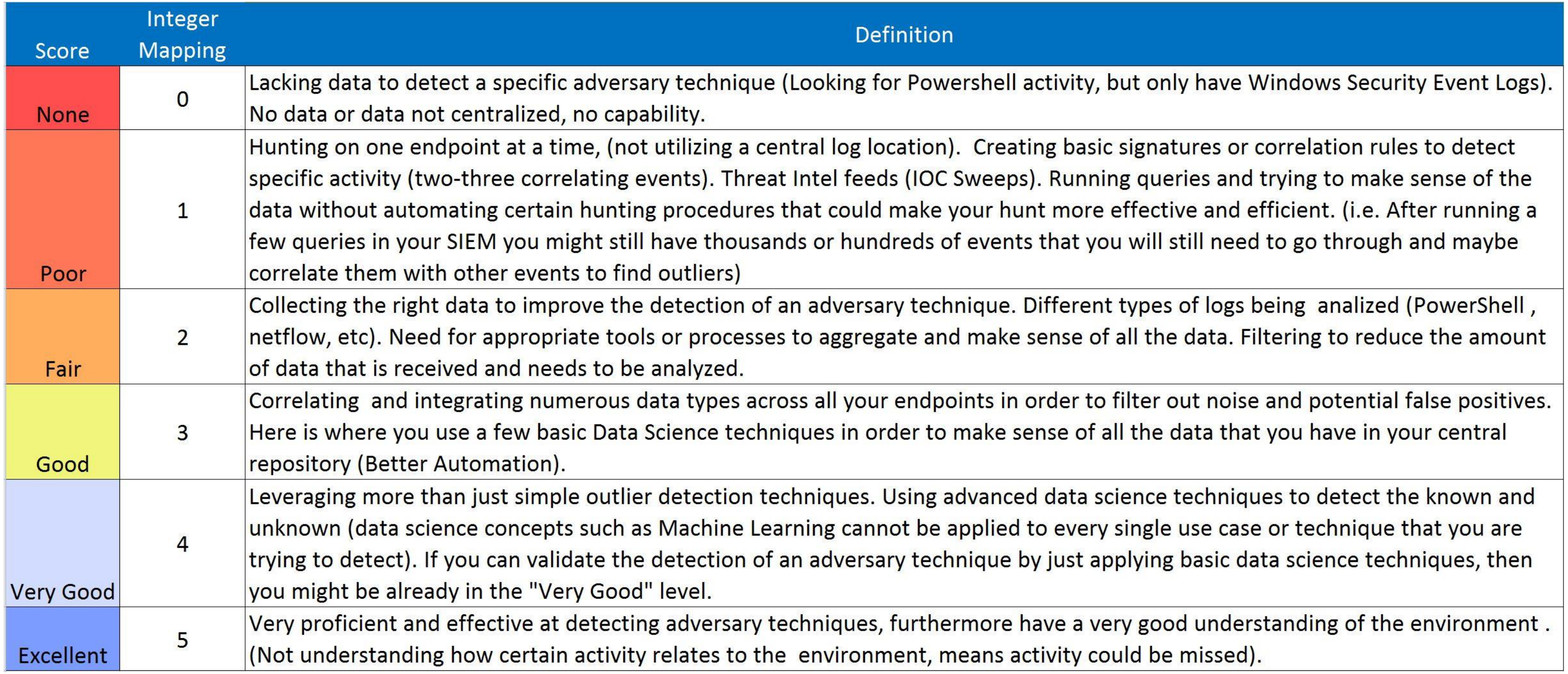


- MITRE ATT&CK isn't a Silver Bullet
  - Requires Effort
    - Lot’s of tuning depending on your organizations infrastructure/environment and habits
    - What's normal in my environment may not be in yours
- It’s a starting point
  - Provides good cross sectional coverage of adversarial techniques
  - Focuses on detecting behavior, not a specific tool

The Journey Begins

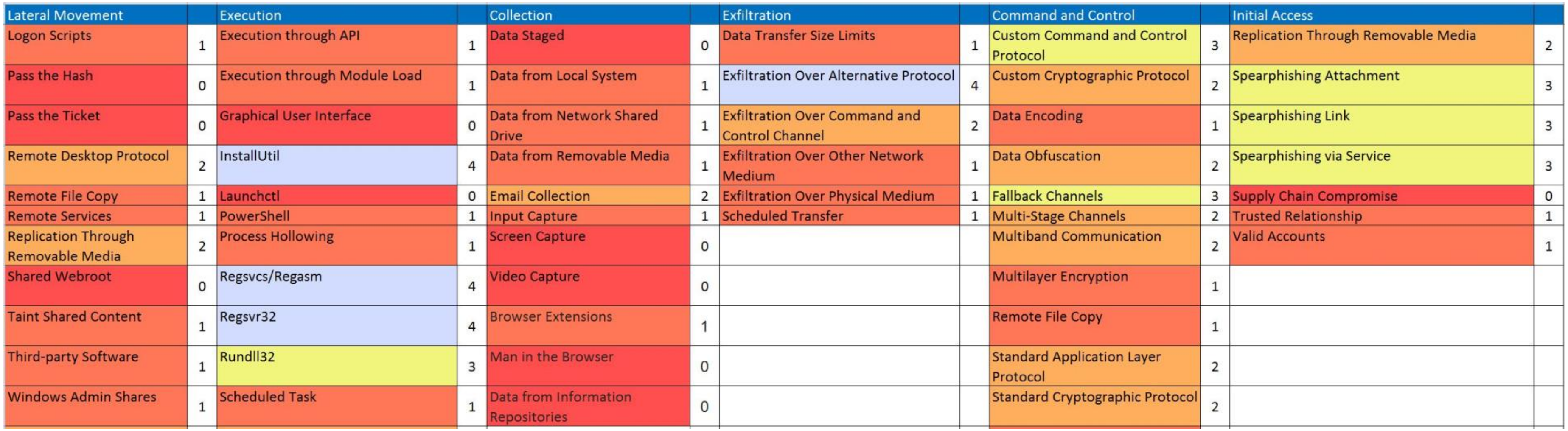
- Develop a Plan of ATT&CK
- Follow a Process/Methodology
- Meet with Team and Discuss
- Make Changes based on Feedback

Develop Scoring



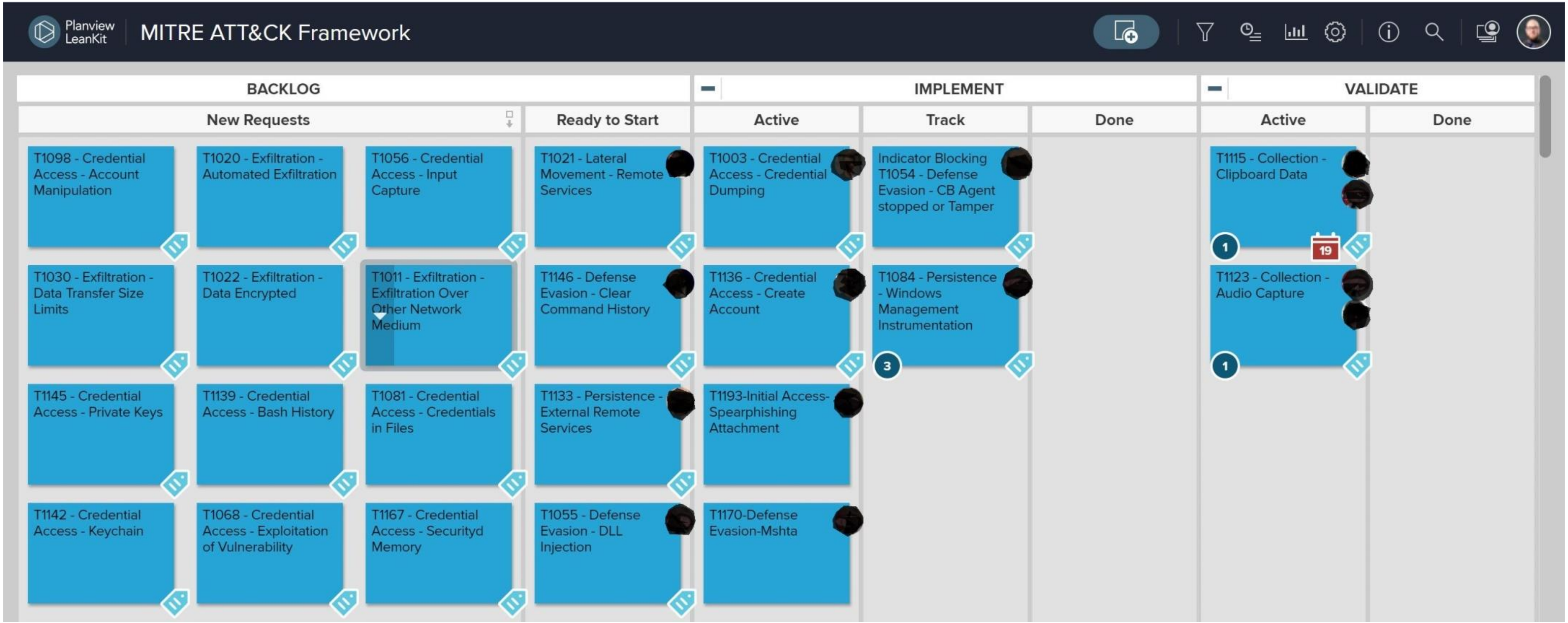
Score	Integer Mapping	Definition
None	0	Lacking data to detect a specific adversary technique (Looking for Powershell activity, but only have Windows Security Event Logs). No data or data not centralized, no capability.
Poor	1	Hunting on one endpoint at a time, (not utilizing a central log location). Creating basic signatures or correlation rules to detect specific activity (two-three correlating events). Threat Intel feeds (IOC Sweeps). Running queries and trying to make sense of the data without automating certain hunting procedures that could make your hunt more effective and efficient. (i.e. After running a few queries in your SIEM you might still have thousands or hundreds of events that you will still need to go through and maybe correlate them with other events to find outliers)
Fair	2	Collecting the right data to improve the detection of an adversary technique. Different types of logs being analized (PowerShell , netflow, etc). Need for appropriate tools or processes to aggregate and make sense of all the data. Filtering to reduce the amount of data that is received and needs to be analyzed.
Good	3	Correlating and integrating numerous data types across all your endpoints in order to filter out noise and potential false positives. Here is where you use a few basic Data Science techniques in order to make sense of all the data that you have in your central repository (Better Automation).
Very Good	4	Leveraging more than just simple outlier detection techniques. Using advanced data science techniques to detect the known and unknown (data science concepts such as Machine Learning cannot be applied to every single use case or technique that you are trying to detect). If you can validate the detection of an adversary technique by just applying basic data science techniques, then you might be already in the "Very Good" level.
Excellent	5	Very proficient and effective at detecting adversary techniques, furthermore have a very good understanding of the environment . (Not understanding how certain activity relates to the environment, means activity could be missed).

Assess Current Process/Toolset



Lateral Movement		Execution		Collection		Exfiltration		Command and Control		Initial Access	
Logon Scripts	1	Execution through API	1	Data Staged	0	Data Transfer Size Limits	1	Custom Command and Control Protocol	3	Replication Through Removable Media	2
Pass the Hash	0	Execution through Module Load	1	Data from Local System	1	Exfiltration Over Alternative Protocol	4	Custom Cryptographic Protocol	2	Spearphishing Attachment	3
Pass the Ticket	0	Graphical User Interface	0	Data from Network Shared Drive	1	Exfiltration Over Command and Control Channel	2	Data Encoding	1	Spearphishing Link	3
Remote Desktop Protocol	2	InstallUtil	4	Data from Removable Media	1	Exfiltration Over Other Network Medium	1	Data Obfuscation	2	Spearphishing via Service	3
Remote File Copy	1	Launchctl	0	Email Collection	2	Exfiltration Over Physical Medium	1	Fallback Channels	3	Supply Chain Compromise	0
Remote Services	1	PowerShell	1	Input Capture	1	Scheduled Transfer	1	Multi-Stage Channels	2	Trusted Relationship	1
Replication Through Removable Media	2	Process Hollowing	1	Screen Capture	0			Multiband Communication	2	Valid Accounts	1
Shared Webroot	0	Regsvcs/Regasm	4	Video Capture	0			Multilayer Encryption	1		
Taint Shared Content	1	Regsvr32	4	Browser Extensions	1			Remote File Copy	1		
Third-party Software	1	Rundll32	3	Man in the Browser	0			Standard Application Layer Protocol	2		
Windows Admin Shares	1	Scheduled Task	1	Data from Information Repositories	0			Standard Cryptographic Protocol	2		

Develop Process

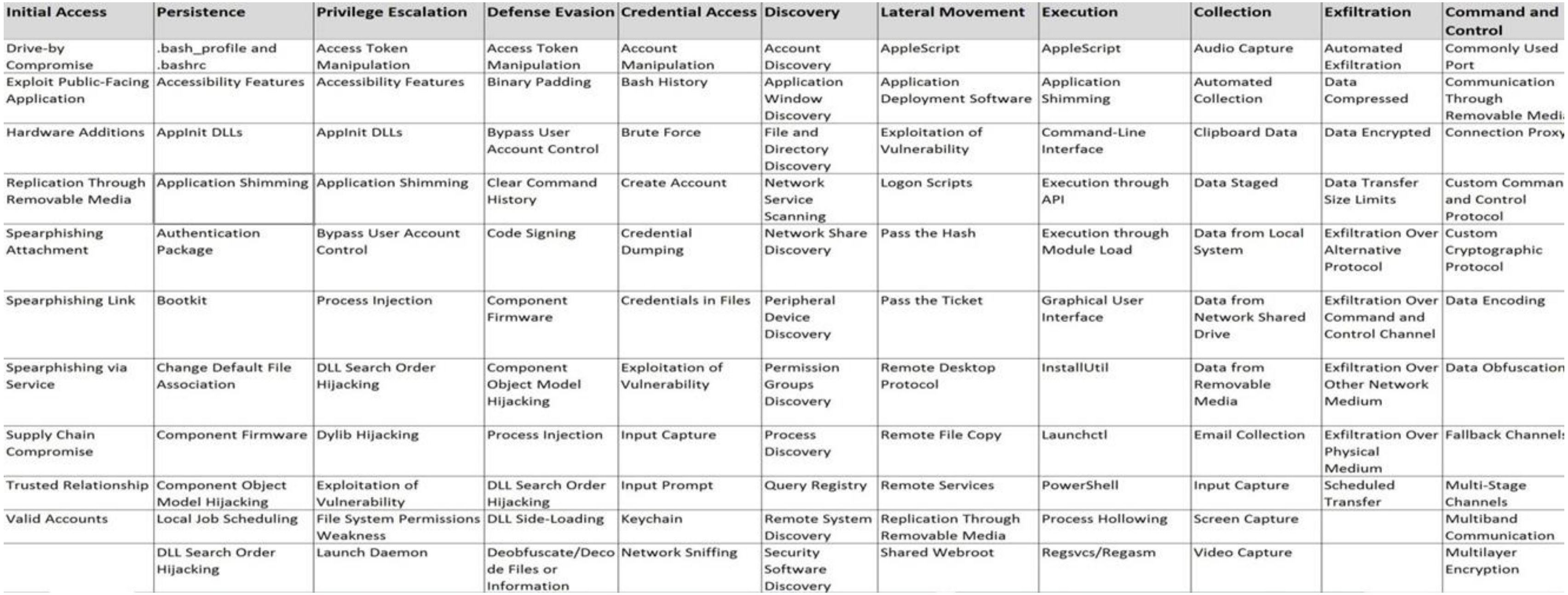


Planview LeanKit

MITRE ATT&CK Framework

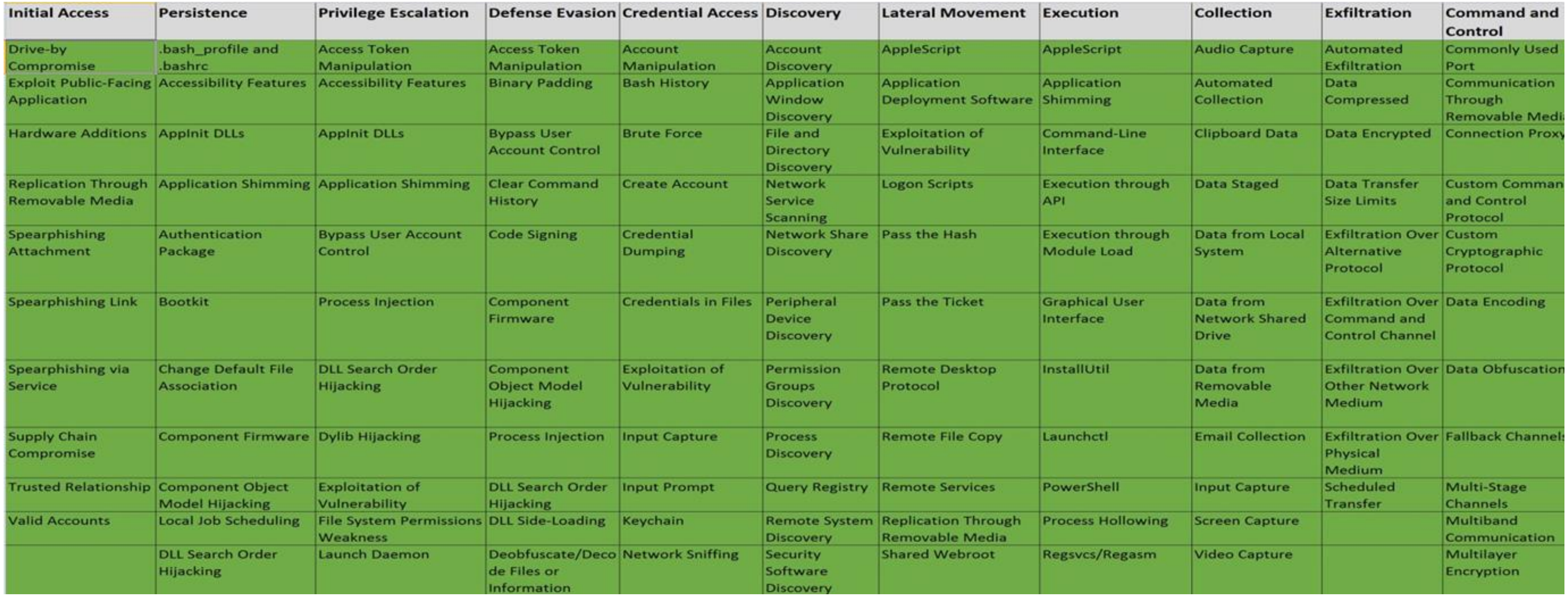
BACKLOG				IMPLEMENT			VALIDATE	
New Requests			Ready to Start	Active	Track	Done	Active	Done
T1098 - Credential Access - Account Manipulation	T1020 - Exfiltration - Automated Exfiltration	T1056 - Credential Access - Input Capture	T1021 - Lateral Movement - Remote Services [redacted]	T1003 - Credential Access - Credential Dumping [redacted]	Indicator Blocking T1054 - Defense Evasion - CB Agent stopped or Tamper [redacted]		T1115 - Collection - Clipboard Data [redacted] [redacted] 1 19	
T1030 - Exfiltration - Data Transfer Size Limits	T1022 - Exfiltration - Data Encrypted	T1011 - Exfiltration - Exfiltration Over Other Network Medium	T1146 - Defense Evasion - Clear Command History [redacted]	T1136 - Credential Access - Create Account [redacted]	T1084 - Persistence - Windows Management Instrumentation [redacted] 3		T1123 - Collection - Audio Capture [redacted] [redacted] 1	
T1145 - Credential Access - Private Keys	T1139 - Credential Access - Bash History	T1081 - Credential Access - Credentials in Files	T1133 - Persistence - External Remote Services [redacted]	T1193-Initial Access-Spearphishing Attachment [redacted]				
T1142 - Credential Access - Keychain	T1068 - Credential Access - Exploitation of Vulnerability	T1167 - Credential Access - Securityd Memory	T1055 - Defense Evasion - DLL Injection [redacted]	T1170-Defense Evasion-Mshta [redacted]				

Diversity of Detection



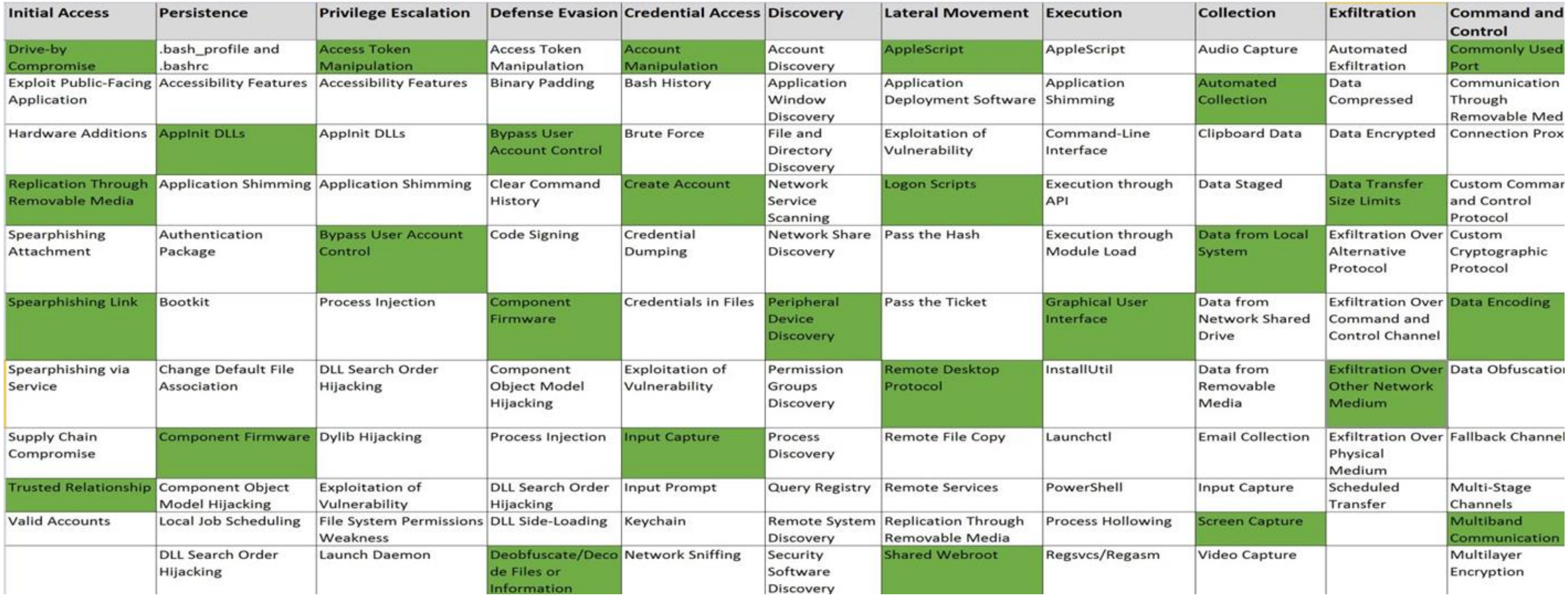
Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Drive-by Compromise	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Application Shimming	Automated Collection	Data Compressed	Communication Through Removable Medi
Hardware Additions	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Brute Force	File and Directory Discovery	Exploitation of Vulnerability	Command-Line Interface	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Application Shimming	Application Shimming	Clear Command History	Create Account	Network Service Scanning	Logon Scripts	Execution through API	Data Staged	Data Transfer Size Limits	Custom Comman and Control Protocol
Spearphishing Attachment	Authentication Package	Bypass User Account Control	Code Signing	Credential Dumping	Network Share Discovery	Pass the Hash	Execution through Module Load	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Bootkit	Process Injection	Component Firmware	Credentials in Files	Peripheral Device Discovery	Pass the Ticket	Graphical User Interface	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Change Default File Association	DLL Search Order Hijacking	Component Object Model Hijacking	Exploitation of Vulnerability	Permission Groups Discovery	Remote Desktop Protocol	InstallUtil	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Component Firmware	Dylib Hijacking	Process Injection	Input Capture	Process Discovery	Remote File Copy	Launchctl	Email Collection	Exfiltration Over Physical Medium	Fallback Channel
Trusted Relationship	Component Object Model Hijacking	Exploitation of Vulnerability	DLL Search Order Hijacking	Input Prompt	Query Registry	Remote Services	PowerShell	Input Capture	Scheduled Transfer	Multi-Stage Channels
Valid Accounts	Local Job Scheduling	File System Permissions Weakness	DLL Side-Loading	Keychain	Remote System Discovery	Replication Through Removable Media	Process Hollowing	Screen Capture		Multiband Communication
	DLL Search Order Hijacking	Launch Daemon	Deobfuscate/Decode Files or Information	Network Sniffing	Security Software Discovery	Shared Webroot	Regsvcs/Regasm	Video Capture		Multilayer Encryption

Diversity of Detection



Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Drive-by Compromise	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Application Shimming	Automated Collection	Data Compressed	Communication Through Removable Medi
Hardware Additions	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Brute Force	File and Directory Discovery	Exploitation of Vulnerability	Command-Line Interface	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Application Shimming	Application Shimming	Clear Command History	Create Account	Network Service Scanning	Logon Scripts	Execution through API	Data Staged	Data Transfer Size Limits	Custom Comman and Control Protocol
Spearphishing Attachment	Authentication Package	Bypass User Account Control	Code Signing	Credential Dumping	Network Share Discovery	Pass the Hash	Execution through Module Load	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Bootkit	Process Injection	Component Firmware	Credentials in Files	Peripheral Device Discovery	Pass the Ticket	Graphical User Interface	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Change Default File Association	DLL Search Order Hijacking	Component Object Model Hijacking	Exploitation of Vulnerability	Permission Groups Discovery	Remote Desktop Protocol	InstallUtil	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Component Firmware	Dylib Hijacking	Process Injection	Input Capture	Process Discovery	Remote File Copy	Launchctl	Email Collection	Exfiltration Over Physical Medium	Fallback Channels
Trusted Relationship	Component Object Model Hijacking	Exploitation of Vulnerability	DLL Search Order Hijacking	Input Prompt	Query Registry	Remote Services	PowerShell	Input Capture	Scheduled Transfer	Multi-Stage Channels
Valid Accounts	Local Job Scheduling	File System Permissions Weakness	DLL Side-Loading	Keychain	Remote System Discovery	Replication Through Removable Media	Process Hollowing	Screen Capture		Multiband Communication
	DLL Search Order Hijacking	Launch Daemon	Deobfuscate/Decode Files or Information	Network Sniffing	Security Software Discovery	Shared Webroot	Regsvcs/Regasm	Video Capture		Multilayer Encryption

Diversity of Detection



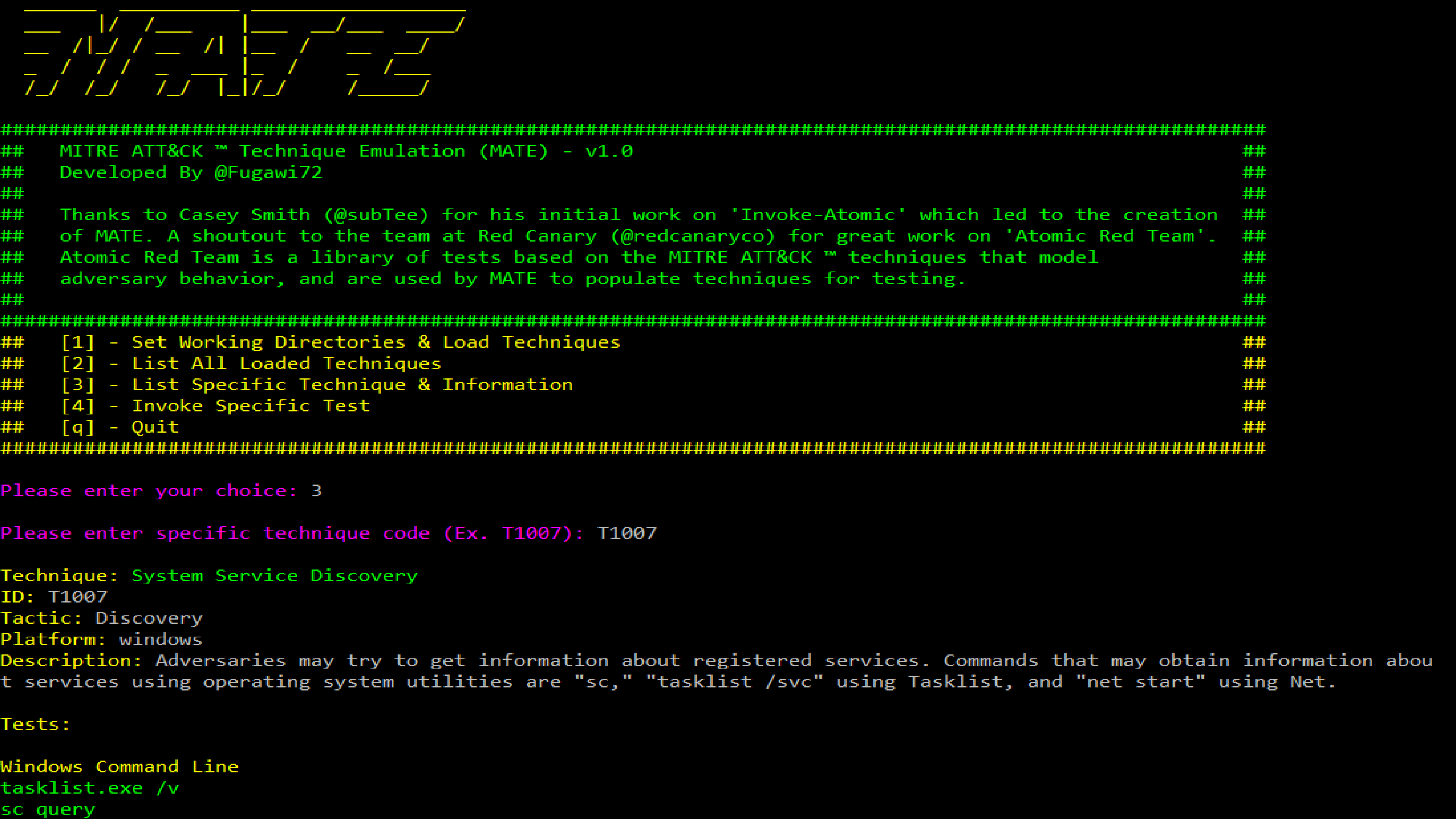
Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Drive-by Compromise	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Application Shimming	Automated Collection	Data Compressed	Communication Through Removable Med
Hardware Additions	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Brute Force	File and Directory Discovery	Exploitation of Vulnerability	Command-Line Interface	Clipboard Data	Data Encrypted	Connection Prox
Replication Through Removable Media	Application Shimming	Application Shimming	Clear Command History	Create Account	Network Service Scanning	Logon Scripts	Execution through API	Data Staged	Data Transfer Size Limits	Custom Commar and Control Protocol
Spearphishing Attachment	Authentication Package	Bypass User Account Control	Code Signing	Credential Dumping	Network Share Discovery	Pass the Hash	Execution through Module Load	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Bootkit	Process Injection	Component Firmware	Credentials in Files	Peripheral Device Discovery	Pass the Ticket	Graphical User Interface	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Change Default File Association	DLL Search Order Hijacking	Component Object Model Hijacking	Exploitation of Vulnerability	Permission Groups Discovery	Remote Desktop Protocol	InstallUtil	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscatio
Supply Chain Compromise	Component Firmware	Dylib Hijacking	Process Injection	Input Capture	Process Discovery	Remote File Copy	Launchctl	Email Collection	Exfiltration Over Physical Medium	Fallback Channel
Trusted Relationship	Component Object Model Hijacking	Exploitation of Vulnerability	DLL Search Order Hijacking	Input Prompt	Query Registry	Remote Services	PowerShell	Input Capture	Scheduled Transfer	Multi-Stage Channels
Valid Accounts	Local Job Scheduling	File System Permissions Weakness	DLL Side-Loading	Keychain	Remote System Discovery	Replication Through Removable Media	Process Hollowing	Screen Capture		Multiband Communication
	DLL Search Order Hijacking	Launch Daemon	Deobfuscate/Decode Files or Information	Network Sniffing	Security Software Discovery	Shared Webroot	Regsvcs/Regasm	Video Capture		Multilayer Encryption

Testing Your Detections

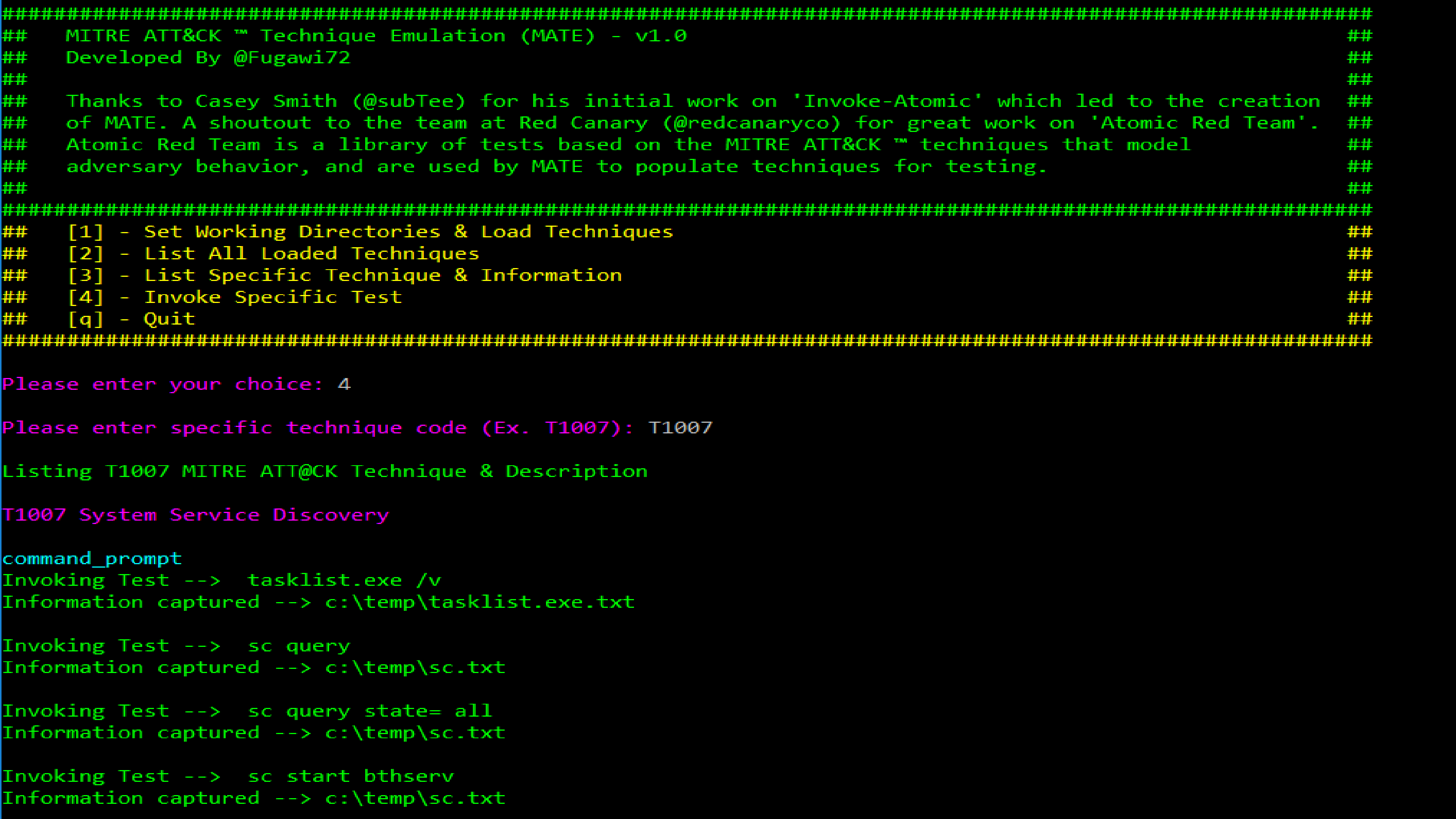
- MITRE Caldera
- Red Canary Atomic Red Team
- Endgame RTA
- Uber Metta

MATE

- MITRE ATT&CK® Technique Emulation
  - https://github.com/fugawi/mate
  - Developed Steve Motts @fugawi72
  - MATE uses modified Red Canary ‘Atomic Red Team’ yaml files
  - Allows for automating execution of MITRE ATT&CK® techniques on Windows OS to test detection



```
   ______  ___________  _______________________
   ___   |/  /___    |___  __/___  ____/
   __  /|_/ / __  /| |__  /   __  __/
   _  /  / /  _  ___ |_  /    _  /___
   /_/  /_/   /_/  |_|/_/     /_____/

######################################################################
##   MITRE ATT&CK ™ Technique Emulation (MATE) - v1.0               ##
##   Developed By @Fugawi72                                          ##
##                                                                   ##
##   Thanks to Casey Smith (@subTee) for his initial work on 'Invoke-Atomic' which led to the creation  ##
##   of MATE. A shoutout to the team at Red Canary (@redcanaryco) for great work on 'Atomic Red Team'.  ##
##   Atomic Red Team is a library of tests based on the MITRE ATT&CK ™ techniques that model        ##
##   adversary behavior, and are used by MATE to populate techniques for testing.                   ##
##                                                                   ##
######################################################################
##   [1] - Set Working Directories & Load Techniques                 ##
##   [2] - List All Loaded Techniques                                ##
##   [3] - List Specific Technique & Information                     ##
##   [4] - Invoke Specific Test                                      ##
##   [q] - Quit                                                      ##
######################################################################

Please enter your choice: 3

Please enter specific technique code (Ex. T1007): T1007

Technique: System Service Discovery
ID: T1007
Tactic: Discovery
Platform: windows
Description: Adversaries may try to get information about registered services. Commands that may obtain information abou
t services using operating system utilities are "sc," "tasklist /svc" using Tasklist, and "net start" using Net.

Tests:

Windows Command Line
tasklist.exe /v
sc query
```



```
###########################################################################################################
##   MITRE ATT&CK ™ Technique Emulation (MATE) - v1.0                                                   ##
##   Developed By @Fugawi72                                                                              ##
##                                                                                                       ##
##   Thanks to Casey Smith (@subTee) for his initial work on 'Invoke-Atomic' which led to the creation   ##
##   of MATE. A shoutout to the team at Red Canary (@redcanaryco) for great work on 'Atomic Red Team'.   ##
##   Atomic Red Team is a library of tests based on the MITRE ATT&CK ™ techniques that model             ##
##   adversary behavior, and are used by MATE to populate techniques for testing.                        ##
##                                                                                                       ##
###########################################################################################################
##   [1] - Set Working Directories & Load Techniques                                                     ##
##   [2] - List All Loaded Techniques                                                                    ##
##   [3] - List Specific Technique & Information                                                         ##
##   [4] - Invoke Specific Test                                                                          ##
##   [q] - Quit                                                                                          ##
###########################################################################################################

Please enter your choice: 4

Please enter specific technique code (Ex. T1007): T1007

Listing T1007 MITRE ATT@CK Technique & Description

T1007 System Service Discovery

command_prompt
Invoking Test -->  tasklist.exe /v
Information captured --> c:\temp\tasklist.exe.txt

Invoking Test -->  sc query
Information captured --> c:\temp\sc.txt

Invoking Test -->  sc query state= all
Information captured --> c:\temp\sc.txt

Invoking Test -->  sc start bthserv
Information captured --> c:\temp\sc.txt
```

Lessons Learned

- Plan!
- Plan!
- Plan!
- **And then Plan some More…**
- Be Consistent and Follow your Plan
- This is a Journey, Celebrate the Small Wins
- Talk to your Vendors

Contact Info

- @1nf0s3cp1mp
- ckopacsi@gmail.com