

Lessons Learned Applying ATT&CK- Based SOC Assessments

Andy Applebaum
@andyplayse4

SANS Security Operations Summit
June 24th, 2019



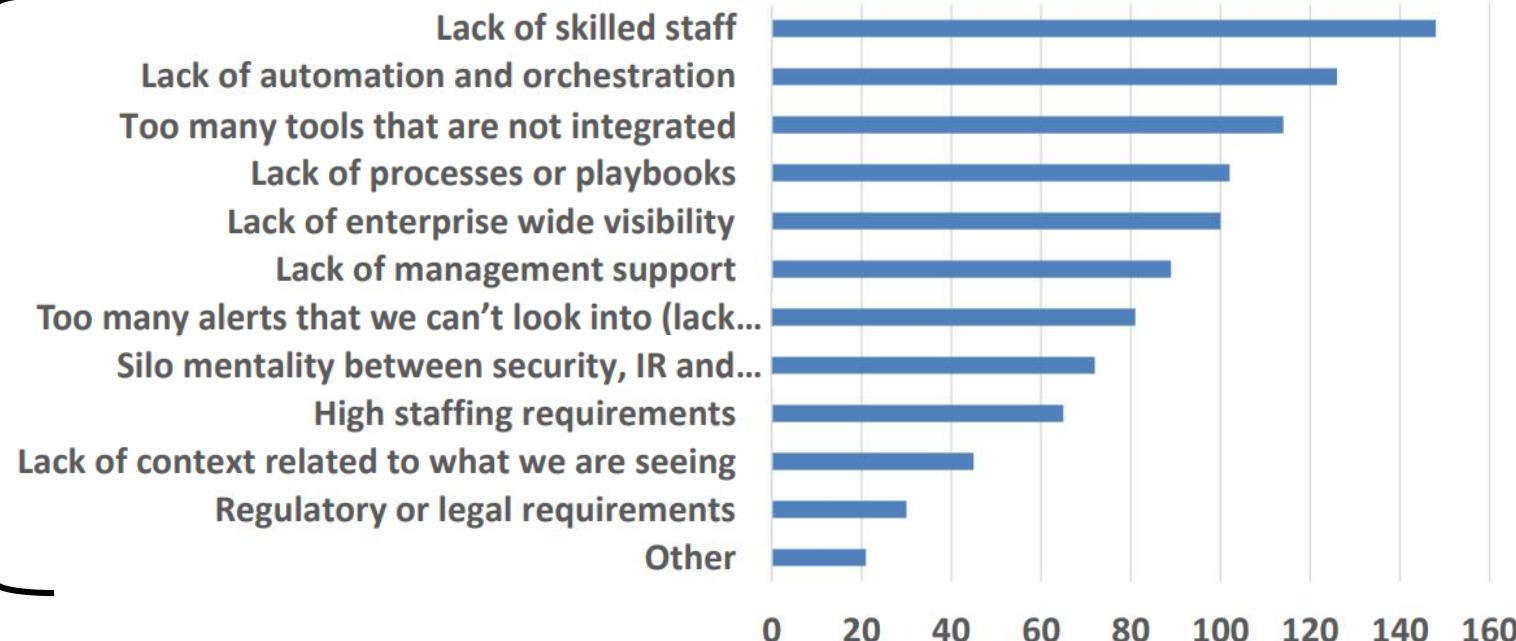
Challenges in the SOC



Challenges, n=239



SANS Analyst Program



©2018 SANS™ Institute | www.sans.org

20

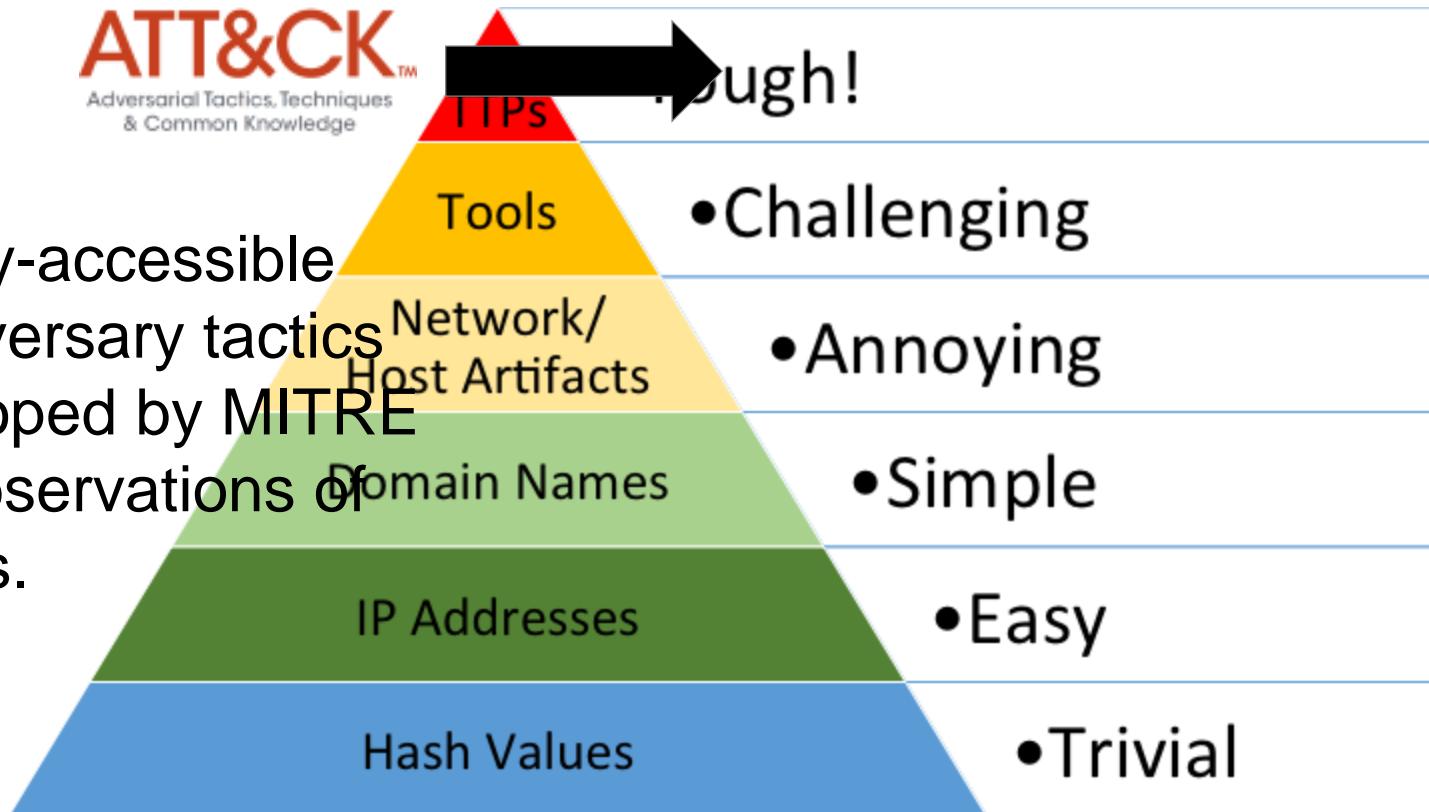
SOC Survey Summary, SANS Security Operations Summit 2018

<https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1532969860.pdf>

Background: What is ATT&CK?

The Pyramid of Pain

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



Source: David Bianco

<https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html>

TTPs = Tactics, Techniques, and Procedures

The ATT&CK Matrix

Publicly Available
attack.mitre.org

Tactics – Adversary's technical goal											
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise		Scheduled Task		Binary Padding		Network Sniffing					Data Destruction
Exploit Public-Facing Application		Launchctl		Access Token Manipulation		Account Manipulation					Automated Exfiltration
External Remote Services		Local Job Scheduling		Bypass User Account Control		Bash History					Data Encrypted for Impact
Hardware Addition		LSASS Driver				Application Window					Defacement
Replication Through Removable Media		Trap									
Spearphishing Attachment	Command-Line Interface										
Spearphishing Link	Compiled HTML File										
Spearphishing via Service	Control Panel Items		Accessibility								
Supply Chain Compromise	Dynamic Data Exchange		AppCenter								
Trusted Relationship	Execution through API		AppInit								
Valid Accounts											
	Execution through Module Load		Application								
			Dylib Hijack								
	Exploitation for Client Execution		File System Permissions								
	Graphical User Interface		Hook								
	InstallUtil		Launch Daemon								
	Mshta		New Session								
	PowerShell		Port Mapper								
	Regsvcs/Regasm		Service Registry Provider								
	Regsvr32		Setupapi								
	Rundll32		Startup								
	Scripting		Web Server								
	Service Execution		.bash_profile and .bashrc								
			Account Manipulation								
	Signed Binary		Authentication Package								
	Proxy Execution		BITS Jobs								
			Bootkit								
	Source		Browser Extensions								
			Change Default File Association								
	Space after Filename		Component Firmware								
	Third-party Software		Component Object Model Hijacking								
	Trusted Developer Utilities		Create Account								
	User Execution		External Remote Services								
	Windows Management Instrumentation		Hidden Files and Directories								
	Windows Remote Management		Hypervisor								
	XSL Script Processing		Kernel Modules and Extensions								
			Launch Agent								
			LC_LOAD_DYLIB Addition								
			Login Item								
			Logon Scripts								
			Modify Existing Service								
			Netsh Helper DLL								
			Office Application Startup								
			Port Knocking								
			Rc.common								
			Redundant Access								

Techniques – How goal is achieved

Grounded in real data from cyber incidents

Focuses on describing adversary TTPs, not IoCs

Decouples the problem from the solution

(also has information on groups and software)

Core ATT&CK Use Cases

Detection

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

Assessment and Engineering

Procedure	Primary Location	Defined By	Credential Access	Discovery	Uptime Monitoring	Events	Logs	Exfiltration	Command and Control
File System Shadow Copy	Windows Management	File Copy	Account Discovery	Windows File Monitors	Filebeat Collection	Autonomous Collection	Autonomous Exfiltration	CloudWatch Metrics	CloudWatch Metrics
Legitimate Credentials	Windows Management	Binary Padding	Credential Dumping	Application Window Discovery	Third-party Software	Clipboard Data	Data Compressed	Communication Through Network Drives	Communication Through Network Drives
Accessibility Feature	Windows Management	Component Framework	Credential Manipulation	File and Directory Discovery	Application Deployment	Command-Line	Data Staged	Data Transferred	File Transferred
Local Port Monitor	Windows Management	Component Framework	Credential Manipulation	Local Network Configuration	Configuration of Vulnerabilities	Graphical User Interface	Data from Network Share	Data Exfiltration	Data Exfiltration
New Service	Windows Management	DLL Side-Loading	Credential Manipulation	Local Network Connections	Logon Scripts	Installing	Drive	Exfiltration Over Alternative Protocol	Control Protocol
Network Scan	Windows Management	DLL Side-Loading	Input Capture	Network Service Scanning	Pass the Hash	Process in Hollowing	Data Collection	Custom Cryptographic	Data Decryption
Scheduled Task	Windows Management	File Injection	Input Capture	Network Service Scanning	Pass the Ticket	Regoons/Regmons	Email Collections	Exfiltration Over Command and Control Channel	Data Obfuscation
File System Permissions Weakness	File System Logon Offsets	File System Permissions Weakness	File System Permissions Weakness	Network Service Scanning	Port Knocking	Regmon	Import/Export	Exfiltration Over Other Network Services	File-Based Channels
Service Registry Permissions Weakness	File System Logon Offsets	File System Permissions Weakness	File System Permissions Weakness	Network Service Scanning	Port Knocking	Regmon	Import/Export	Exfiltration Over Other Network Services	File-Based Channels
Weak Shell	File System Logon Offsets	File System Permissions Weakness	File System Permissions Weakness	Network Service Scanning	Port Knocking	Regmon	Import/Export	Exfiltration Over Other Network Services	File-Based Channels
File Path Traversal	File System Logon Offsets	File System Permissions Weakness	File System Permissions Weakness	Network Service Scanning	Port Knocking	Regmon	Import/Export	Exfiltration Over Other Network Services	File-Based Channels
Weak Hash	File System Logon Offsets	File System Permissions Weakness	File System Permissions Weakness	Network Service Scanning	Port Knocking	Regmon	Import/Export	Exfiltration Over Other Network Services	File-Based Channels
Evaluation of Vulnerability	File System Logon Offsets	File System Permissions Weakness	File System Permissions Weakness	Network Service Scanning	Port Knocking	Regmon	Import/Export	Exfiltration Over Other Network Services	File-Based Channels
Weak Hash	File System Logon Offsets	File System Permissions Weakness	File System Permissions Weakness	Network Service Scanning	Port Knocking	Regmon	Import/Export	Exfiltration Over Other Network Services	File-Based Channels
Weak Hash	File System Logon Offsets	File System Permissions Weakness	File System Permissions Weakness	Network Service Scanning	Port Knocking	Regmon	Import/Export	Exfiltration Over Other Network Services	File-Based Channels
Change Default File Association	Component Object Model Hijacking	Component Object Model Hijacking	Component Object Model Hijacking	Peripherals Device Discovery	Remote Services	Scheduled Task	Audio Capture	Exfiltration Over Other Network Services	File-Based Channels
Component Hijacking	Component Object Model Hijacking	Indicator Removal from Tools	Indicator Removal from Tools	Peripherals Device Discovery	Remote Services	Scripting	Video Capture	Exfiltration Over Other Network Services	File-Based Channels
Logon Scripts	Component Object Model Hijacking	Indicator Removal from Tools	Indicator Removal from Tools	Peripherals Device Discovery	Remote Services	Scripting	Video Capture	Exfiltration Over Other Network Services	File-Based Channels
Modify Existing Service	Component Object Model Hijacking	Indicator Removal from Tools	Indicator Removal from Tools	Peripherals Device Discovery	Remote Services	Scripting	Video Capture	Exfiltration Over Other Network Services	File-Based Channels
Redundant Access	Component Object Model Hijacking	Indicator Removal from Tools	Indicator Removal from Tools	Peripherals Device Discovery	Remote Services	Scripting	Video Capture	Exfiltration Over Other Network Services	File-Based Channels
Registry Run Keys / Start Entries	Component Object Model Hijacking	Indicator Removal from Tools	Indicator Removal from Tools	Peripherals Device Discovery	Remote Services	Scripting	Video Capture	Exfiltration Over Other Network Services	File-Based Channels
Security Support Provider	Component Object Model Hijacking	Indicator Removal from Tools	Indicator Removal from Tools	Peripherals Device Discovery	Remote Services	Scripting	Video Capture	Exfiltration Over Other Network Services	File-Based Channels
Shortcuts Modification	Component Object Model Hijacking	Indicator Removal from Tools	Indicator Removal from Tools	Peripherals Device Discovery	Remote Services	Scripting	Video Capture	Exfiltration Over Other Network Services	File-Based Channels
Windows Management Instrumentation Event Subscription	Component Object Model Hijacking	Indicator Removal from Tools	Indicator Removal from Tools	Peripherals Device Discovery	Remote Services	Scripting	Video Capture	Exfiltration Over Other Network Services	File-Based Channels
Windows Management API	Component Object Model Hijacking	Indicator Removal from Tools	Indicator Removal from Tools	Peripherals Device Discovery	Remote Services	Scripting	Video Capture	Exfiltration Over Other Network Services	File-Based Channels
NtAuth Helper DLL	Component Object Model Hijacking	Indicator Removal from Tools	Indicator Removal from Tools	Peripherals Device Discovery	Remote Services	Scripting	Video Capture	Exfiltration Over Other Network Services	File-Based Channels
Authentication Package	Component Object Model Hijacking	Indicator Removal from Tools	Indicator Removal from Tools	Peripherals Device Discovery	Remote Services	Scripting	Video Capture	Exfiltration Over Other Network Services	File-Based Channels
External Remote Services	Component Object Model Hijacking	Indicator Removal from Tools	Indicator Removal from Tools	Peripherals Device Discovery	Remote Services	Scripting	Video Capture	Exfiltration Over Other Network Services	File-Based Channels

Threat Intelligence

Adversary Emulation

Persistence	PrivilegeEscalation	DefenseEvasion	CredentialAccess	Discovery	LateralMovement	Execution	Collection	Exfiltration	CommandAndControl
AccessibilityFeatures	AccessibilityFeatures	BinaryPadding	BruteForce	AccountDiscovery	ApplicationDeployment	Command-Line	AutomatedCollection	AutomatedExfiltration	CommonlyUsedPort
AppInitDLLs	AppInitDLLs	BypassUserAccountControl	CredentialDumping	ApplicationWindowsDiscovery	ExploitatioNf0f	ExecutionThroughAPI	ClipboardData	DataCompressed	CommunicationThroughRemovableMedia
BasicInput/OutputSystemControl	CodeSignin	CredentialManipulation	FileAndDirectoryDiscovery	LogonScripts	GraphicalUserInterface	DataStaged	DataEncrypted	CustomCommandsAndControlProtocol	CustomCryptographicProtocol
Bootkit	DLLInjection	ComponentFirmware	CredentialsInFiles	LocalNetworkDiscovery	PassTheHash	PowerShell	DataFromLocalSystem	DataTransferSizeLimits	DataExfiltrationOverProtocol
ChangeDefaultFile2Handlers	DLLSearchOrderHijacking	DLLInjection	ExploitatioNf0f	LocalNetworkConnectionsDiscovery	PassTheTicket	ProcessHollowing	DataFromNetworkSharedDrive	AlternativeProtocol	DataRebifusion
ComponentFirmwareVulnerability	DLLSearchOrderUnpacking	InputCapture	NetworkServicesScanning	RemoteDesktopProtocol	Rundll32	DataFromRemovableMedia	DataExfiltrationOverCommandAndControlChannel	FallbackChannels	Multi-StageChannels
DLLSearchOrderHijacking	LegitimateCredentials	On-Side-Loading	NetworkSniffing	PeripheralDeviceDiscovery	RemoteFileCopy	ScheduledTask	EmailCollection	DataExfiltrationOverOtherNetworkMedium	Multi-HandCommunication
Hypervisor	LocalPortMonitor	DisablingSecurityTools	Two-FactorAuthenticationInterception	PermissionGroupsDiscovery	RemoteServices	ServiceExecution	InputCapture	ExtremelyHighPriority	MultihandCommunication
LegitimateCredentials	NewService	Vulnerability	ProcessDiscovery	ReplicationThroughRemovableMedia	Third-partySoftware	ScreenCapture	ScheduledTransfer	ScheduledEncryption	TwoFactorManagement

Starting with ATT&CK: Understanding Detection Gaps

We have some confidence we would detect
Automated Exfiltration if ex...

Removable Media	CMSTP	Image File Execution
Spearphishing Attachment	Command-Line Interface	Plist Modification
Spearphishing Link	Compiled HTML File	Valid Accounts
Spearphishing via Service	Control Panel Items	Accessibility Features
Supply Chain Compromise	Dynamic Data Exchange	AppCert DLLs
Trusted Relationship	Execution through API	AppInit DLLs
Valid Accounts	Execution through Module Load	Application Shimming
	Exploitation for	Dylib Hijacking
		File System Permissions Weakness

Communicate capabilities with a common reference

Knowledge of my detection gaps allows me to...

should de...
ited

Inform tooling purchases for biggest ROI

History Injection	File Permissions Modification
Sudo	File System Permissions
Sudo Caching	File System Permissions
	File System Permissions

and Control Channel

Exfiltration: Other Alternatives

Layer Protocol
Uncommonly Used Port
Web Service

Identify data sources needed for detection

We have high confidence we would detect
Scheduled Transfer if executed

User Execution	Component Object Model Hijacking
Windows Management Instrumentation	Create Account
	File System Permissions
	File System Permissions
	File System Permissions

Scheduled Transfer

Develop analytics targeting high-impact threats

Login Item
Logon Scripts
Modify Existing Service
Netsh Helper DLL
Office Application Startup
Port Knocking
Rc.common
Redundant Access
Registry Run Keys / Startup Folder
Re-opened Applications
Screensaver

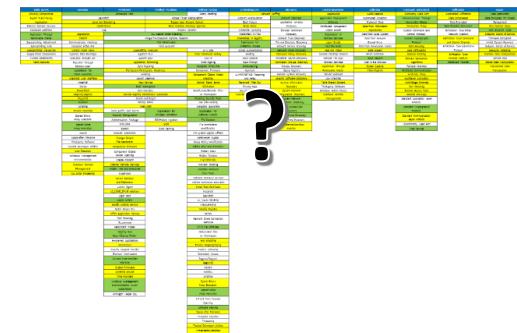
This Talk: Getting Towards Detection Gaps

- Our experiences are from running *ATT&CK-based SOC assessments*
 - Short, rapid-fire methodology to approximate detection gaps in a SOC
- Lessons learned from running these assessments, applicable to:
 - Third-party or in-house assessment
 - “Paper” assessments or hands-on ones
 - General ATT&CK integration
- Why you should care
 - ATT&CK can help solve some of the hard problems – but there are tips, tricks, and pitfalls in trying to use it to do so

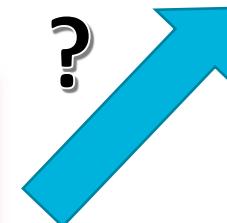
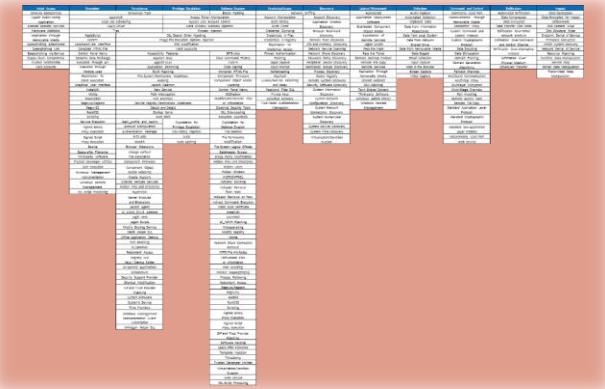
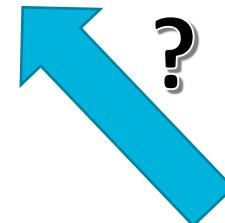
Getting Started: Using ATT&CK for Assessments

Bringing ATT&CK into the SOC

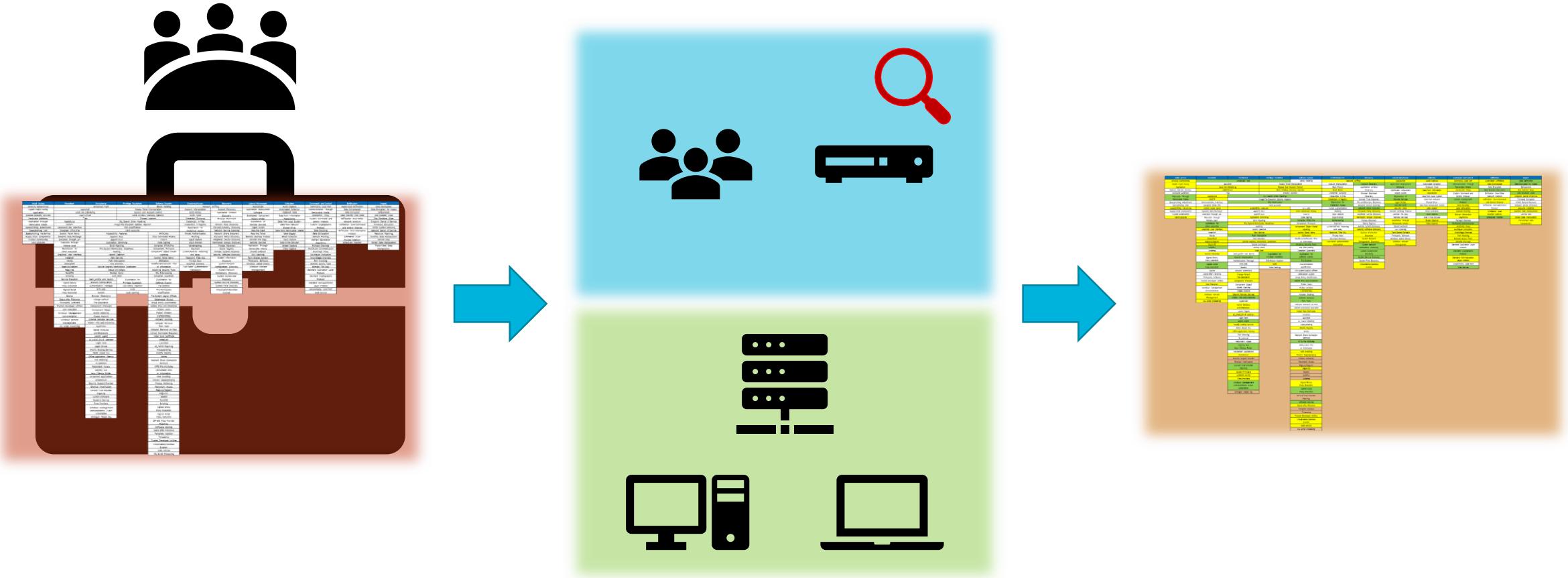
Security Operations Center:
Protecting Network



Defended: Network:
Performing Operational Need



Solution: ATT&CK-based SOC Assessments

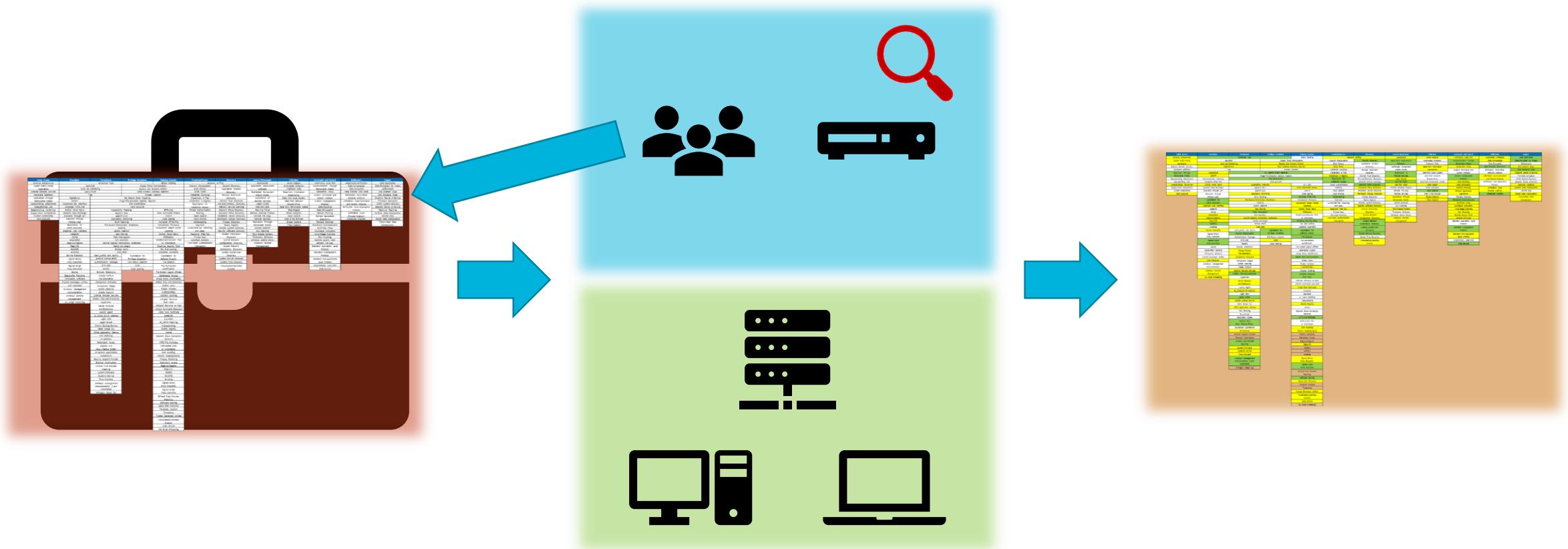


Third-party Assessment Team

Target SOC Environment

Detection Heatmap

Solution: ATT&CK-based SOC Assessments



Internal Assessment Team

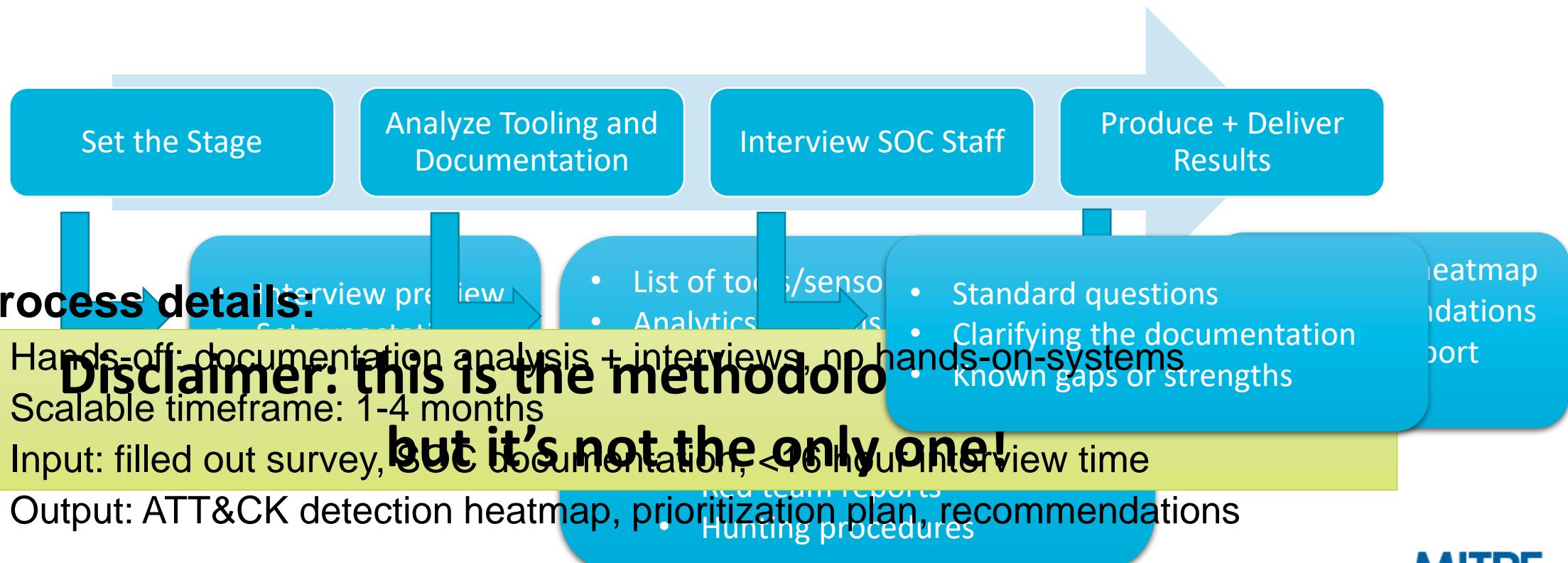
Target SOC Environment

Detection Heatmap

Enter: ATT&CK-based SOC Assessments

■ Methodology to map the SOC's detection abilities to ATT&CK

- Paint broad strokes of detection capabilities
- Provides a rapid, first-look view into SOC's current state
- Useful for SOCs wanting to integrate ATT&CK into day-to-day operations



Experiences with ATT&CK-Based SOC Assessments

- First run in 2017

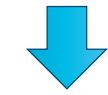
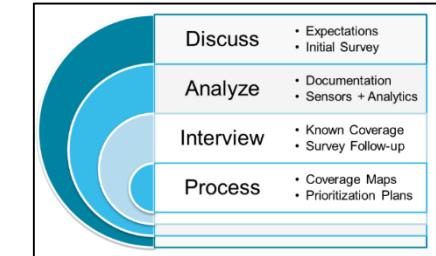
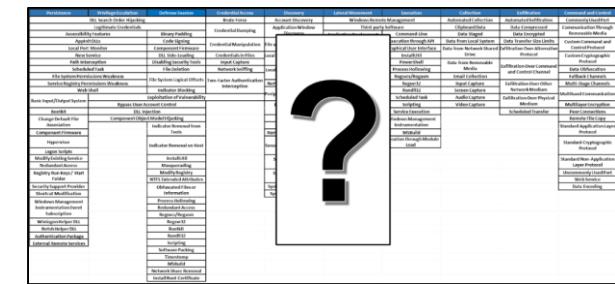
- Since then:

We've learned a lot along the way...

- Lessons for third-party assessors
- Lessons for in-house assessors
- General lessons on using ATT&CK

- What outcomes have we had?

- More structured analytic development programs
- General growth: tooling, data collection, processes



Conducting an ATT&CK-based SOC Assessment

1. Setting the Stage

Setting Expectations

- **ATT&CK's popularity has led some to treat it as a silver bullet**
 - People often have skewed expectations of what performing an ATT&CK assessment provides
 - Applies to assessments done by third parties, as well as those conducted in-house

- **Bottom line: if you're bringing ATT&CK into a SOC, make sure you set the right expectations, particularly if you're doing an assessment**

Messaging ATT&CK-Based SOC Assessments

- **The word “assessment” can sometimes have a negative connotation**
 - Assessments are often used as ways to gauge your skills/progress
 - Cyber mentality is often that assessments are antagonistic
 - The assessor is painting a picture of fault for the assessee
- **Risks of running an “assessment”:**

Staff might not comply with the process



Effort requires more effort/time

Staff might worry about how results will be used



Nitpicks details, wordsmiths report

Personnel might misrepresent/exaggerate current capabilities



Yields inaccurate results

Leadership may overreact to results



End up causing damage, not good

Tips for Staging ATT&CK-Based SOC Assessments

- 1. Consider using a phrase other than assessment**
- 2. Make sure leadership understands the point of the assessment, and that the assessment aligns with their goals**
- 3. Position the assessment as a stepping-stone to improvement; not as a way to gauge performance**
- 4. Ensure SOC staff know they're not being evaluated, rather the SOC's policies, procedures, tooling, etc. are.**
- 5. Prepare to follow-up after running an assessment**

Conducting an ATT&CK-based SOC Assessment

2. Getting Data: Tools, Documentation, and Interviews

Analyzing Tools + Documentation

- 1. Map each tool to the data sources they may detect, and the data sources to the techniques in ATT&CK**
 - Can be useful approximating coverage when documentation is sparse
- 2. Analyze each analytic – will it detect a behavior or is it a static signature? What techniques can it detect?**
- 3. Looking at documentation – find standard processes and procedures, mapping them to ATT&CK whenever possible**
 1. Example: account lockout policy? This can impact Brute Force
 - **For each component: create a coverage heatmap to track your work**

Past Documentation: The Importance of Interviews

Documentation is good, but conducting interviews can give us more *complete* knowledge

Documentation is often stale

- Many SOCs are using tools that they haven't documented (yet)
- Some tools may be used differently in practice than in theory

Tools are only as effective as their deployments

- Most people configure tools and develop pipelines specific to their usage
- Tools can be modified with vendor modules/add-ons, or by the end-user

Personnel can speak more concretely about coverage

- Documentation often lacks direct ATT&CK mapping which can be hard to infer
- Documentation can be ambiguous; interviews tend to provide more specifics

Tips for Conducting Interviews

1. Break questions down by team

2. Walk through examples: how would you detect lateral movement?

- If these questions go well, start scoping to tactics and techniques
- If they don't, try asking general questions

3. Ask each team what their favorite tool is, and why

- How often do they use it? What do they look for?

4. Come prepared – but be prepared to change your script

Conducting an ATT&CK-based SOC Assessment

3. Producing the Heatmap

Pick a Good Scoring Scheme For Your Heatmap

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	CredentialAccess	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise		Scheduled Task		Binary Padding	Network Sniffing		AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	Launchcti	Local Job Scheduling	Access Token Manipulation	Account Manipulation	Account Discovery		Application Deployment	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	LSASS Driver		Bypass User Account Control	Bash History	Application Window Discovery		Software	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Trap		Extra Window Memory Injection	Brute Force			Distributed Component Object Model	Data from Information Repositories	Data Transfer Size Limits	Disk Content Wipe	Disk Structure Wipe
Replication Through Removable Media	AppleScript	CMSTP	DLL Search Order Hijacking	Credential Dumping	Browser Bookmark Discovery		Exploitation of Remote Services	Data from Local System	Custom Command and Control Protocol	Exfiltration Over Network Medium	Endpoint Denial of Service
Spearphishing Attachment	Command-Line Interface		Image File Execution Options Injection	Credentials in Registry	Domain Trust Discovery		Logon Scripts	Data from Network Shared Drive	Custom Cryptographic Protocol	Exfiltration Over Command and Control Channel	Firmware corruption
Spearphishing Link	Compiled HTML File		List Modification	Credential Access	File and Directory Discovery		Network Service Scanning	Pass the Hash	Data from Removable Media	Data Encoding	Inhibit System Recovery
Spearphishing via Service	Control Panel Items		Valid Accounts	Forced Authentication	Network Share Discovery		Pass the Ticket	Data Staged	Data Obfuscation	Exfiltration Over Alternative Protocol	Network Denial of Service
Supply Chain Compromise	Dynamic Data Exchange		Accessibility Features	BITS Jobs	Network Share Discovery		Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Fronting	Runtime Data Manipulation
Trusted Relationship	Execution through API		AppCert DLLs	Clear Command History	Hooking		Peripheral Device Discovery	Remote File Copy	Input Capture	Domain Generation Algorithms	Service Stop
	Execution through Module Load		AppInit DLLs	CMSTP	Input Capture		Permission Groups Discovery	Remote Services	Man in the Browser	Exfiltration Over Physical Medium	Scheduled Transfer
	Exploitation for Client Execution		Application Shimming	Code Signing	Input Prompt		Kerberoasting	Replication Through Removable Media	Screen Capture	Fallback Channels	Stored Data Manipulation
			Dylib Hijacking	Compiled HTML File	Process Discovery		Keychain	Shared Webroot	Video Capture	Multiband Communication	Transmitted Data Manipulation
			File System Permissions Weakness	Component Firmware	Query Registry		LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	Multi-hop Proxy		
	Graphical User Interface		Hooking	Component Object Model Hijacking	System Information Discovery		Deobfuscate/Decode Files or Information	SSH Hijacking	Multi-layer Encryption		
	Installutil		Launch Daemon	Control Panel Items	Taint Shared Content		DCShadow	System Configuration Discovery	Multi-Stage Channels		
	Mshta		New Service	Deobfuscate/Decode Files or Information	Third-party Software		Disabling Security Tools	System Network Configuration Discovery	Port Knocking		
	PowerShell		Path Interception	Two-Factor Authentication Interception	Windows Admin Shares		DLL Side-loading	System Network Management	Remote Access Tools		
	Regsvcs/Regasm		Port Monitors	System Network Configuration Discovery	Windows Remote Management		Setuid and Setgid	Virtualization/Sandbox Evasion	Remote File Copy		
Valid Accounts	Regsvr32		Service Registry Permissions Weakness	System Owner/User Discovery			Startup Items	System Service Discovery	Standard Application Layer Protocol		
	Rundll32		Setuid and Setgid	System Time Discovery			Startup Items	System Time Discovery	Standard Cryptographic Protocol		
	Scripting		Startup Items	Virtualization/Sandbox Evasion			Web Shell	System Owner/User Discovery	Standard Non-Application Layer Protocol		
	Service Execution		Web Shell	System Service Discovery			.bash_profile and .bashrc	System Service Discovery	Uncommonly Used Port		
	Signed Binary		Execution Guardrails	System Time Discovery			Account Manipulation	System Time Discovery	Web Service		
	Proxy Execution		File Deletion	Virtualization/Sandbox Evasion			Authentication Package	Virtualization/Sandbox Evasion			
	Signed Script		File Permissions Modification				SID-History Injection				
	Proxy Execution		File System Logical Offsets				Sudo				
	Source		Gatekeeper Bypass				Bootkit				
	Space after Filename		Group Policy Modification				Browser Extensions				
User Execution	Third-party Software		Hidden Files and Directories				Change Default File Association				
	Trusted Developer Utilities		Hidden Users				Component Firmware				
	User Execution		Hidden Window				Create Account				
	Windows Management Instrumentation		HISTCONTROL				External Remote Services				
			Indicator Blocking				Hidden Files and Directories				
			Indicator Removal from Tools				Indicator Removal on Host				
			Indirect Command Execution				Install Root Certificate				
			Installutil				Indirect Command Execution				
			Launch Agent				Installutil				
	XSL Script Processing		LC_LOAD_DYLIB Addition				Launchcti				
Windows Remote Management			Login Item				LC_MAIN Hijacking				
			Logon Scripts				Masquerading				
			Modify Existing Service				Modify Registry				
			Netsh Helper DLL				Mshta				
			Office Application Startup				Network Share Connection Removal				
			Port Knocking				NTFS File Attributes				
			Rc.common				Obfuscated Files or Information				
			Redundant Access				Port Knocking				
			Registry Run				Process Doppelgänging				
			Keys / Startup Folder				Screensaver				
Windows Persistence			Re-opened Applications								
			Screensaver								

Legend

- High Confidence of Detection
- Some Confidence of Detection
- Low Confidence of Detection
- No Confidence of Detection
- Static Detection Possible

Legend

- High Confidence of Detection
- Some Confidence of Detection
- Low Confidence of Detection
- No Confidence of Detection
- Static Detection Possible

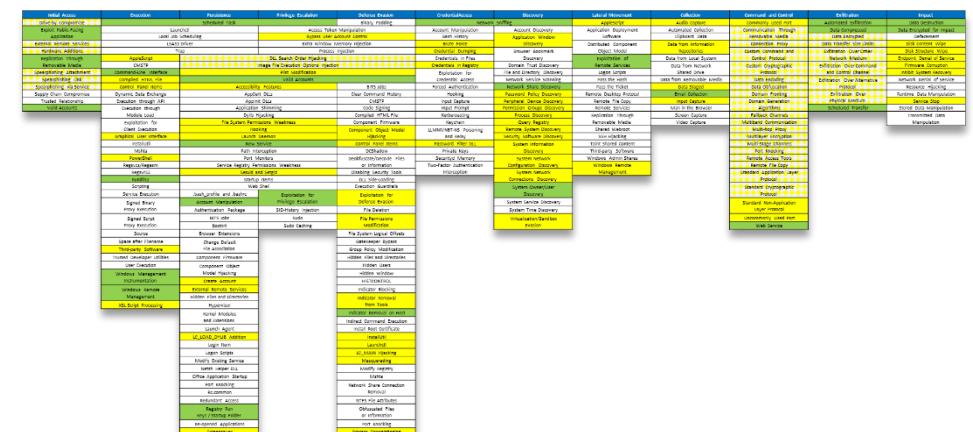
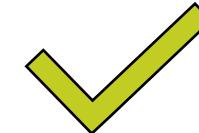
Pick a Good Scoring Scheme For Your Heatmap

~~Regardless of attack type or use case, have a good scoring scheme!~~

- Define categories that are relevant to your audience
- Easy to get lost in labels
- Avoid mixing category types (confidence + likelihood) (too noisy)
- Remember: your goal is to paint a picture
- Know your audience: leadership wants big picture, stakeholders need details
- Choose good color schemes (gradient, discrete, etc.)

■ Settle on something that conveys the right information at the right layer

- Removing just one category has significant communication impacts



Heatmaps: Avoiding Red

Legend

High Confidence of Detection
Some Confidence of Detection
Low Confidence of Detection

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise		Scheduled Task		Binary Padding	Network Sniffing		AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	Launchctl		Access Token Manipulation		Account Manipulation	Account Discovery	Application Deployment	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Imp
External Remote Services		Local Job Scheduling	Bypass User Account Control		Bash History	Application Window Discovery	Clipboard Data	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions		LSASS Driver	Extra Window Memory Injection		Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	AppleScript	Trap	Process Injection		Credential Dumping	Credentials in Files	Exploitation of Remote Services	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Network Medium	Disk Structure Wipe
Spearphishing Attachment	Command-Line Interface		DLL Search Order Hijacking		Credentials in Registry	Domain Trust Discovery	File and Directory Discovery	Data from Network Shared Drive	Custom Cryptographic Protocol	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Compiled HTML File		Image File Execution Options injection		Exploitation for Credential Access	Logon Scripts	File or Directory Discovery	Data from Removable Media	Data Encoding	Exfiltration Over Alternative Protocol	Firmware Corruption
Spearphishing via Service	Control Panel Items		Accessibility Features		Forced Authentication	Network Service Scanning	Pass the Hash	Data Staged	Data Obfuscation	Network Denial of Service	Inhibit System Recovery
Supply Chain Compromise	Dynamic Data Exchange		AppCert DLLs		BITS Jobs	Network Share Discovery	Pass the Ticket	Email Collection	Domain Fronting	Resource Hijacking	Runtime Data Manipulation
Trusted Relationship	Execution through API		AppInp DLLs		Clear Command History	Hooking	Remote Desktop Protocol	Domain Generation Algorithms	Exfiltration Over Physical Medium	Service Stop	Scheduled Transfer
Valid Accounts	Execution through Module Load		Application Shimming		CMSTP	Input Capture	Remote Desktop Protocol	Domain Generation Algorithms	Stored Data Manipulation	Transmitted Data Manipulation	
			Dylib Hijacking		Code Signing	Input Prompt	Remote Desktop Protocol	Domain Generation Algorithms			
			File System Permissions Weakness		Compiled HTML File	Permission Groups Discovery	Remote Desktop Protocol	Domain Generation Algorithms			
			Hooking		Kerberoasting	Process Discovery	Remote Desktop Protocol	Domain Generation Algorithms			
			Launch Daemon		Component Firmware	Query Registry	Remote Desktop Protocol	Domain Generation Algorithms			
			New Service		Hijacking	Keychain	Remote System Discovery	Domain Generation Algorithms			
			Path Interception		Control Panel Items	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	Domain Generation Algorithms			
			Port Monitors		DCShadow	>Password Filter DLL	System Information Discovery	Domain Generation Algorithms			
			Regsvcs/Regasm	Service Registry Permissions Weakness	Deobfuscated/Decode Files or Information	Private Keys	Taint Shared Content	Domain Generation Algorithms			
			Regsvr32	Setuid and Setgid	Securityd Memory	Securityd Memory	Third-party Software	Domain Generation Algorithms			
			Rundll32	Startup Items	Disabling Security Tools	Two-Factor Authentication Interception	Windows Admin Shares	Domain Generation Algorithms			
			Scripting		DLL Side-Loading	Configuration Discovery	Windows Remote Management	Domain Generation Algorithms			
			Service Execution	.bash_profile and .bashrc	Execution Guardrails	System Network Connections Discovery	Domain Generation Algorithms				
			Signed Binary Proxy Execution	Account Manipulation	Exploitation for Privilege Escalation	System Owner/User Discovery	Domain Generation Algorithms				
			Signed Script Proxy Execution	Authentication Package	SID-History Injection	System Service Discovery	Domain Generation Algorithms				
			Signed Script Proxy Execution	BITS Jobs	Sudo	System Time Discovery	Domain Generation Algorithms				
			Source	Bootkit	Sudo Caching	Virtualization/Sandbox Evasion	Domain Generation Algorithms				
			Space after filename	Browser Extensions	File Permissions Modification	File System Logical Offsets	Domain Generation Algorithms				
				Changes Default	Gatekeeper Bypass	Gatekeeper Bypass	Domain Generation Algorithms				

Red communicates the wrong message

- People see red and assume it's saying "Look here! This is a really big problem!!!"
- Use it only as needed to call attention to specific areas that should be focused on

Heatmaps: Avoiding Red

Legend

High Confidence of Detection
Some Confidence of Detection
Low Confidence of Detection

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise		Scheduled Task		Binary Padding	Network Sniffing	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	Launchcti		Access Token Manipulation	Account Manipulation	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Local Job Scheduling		Bypass User Account Control	Brute Force	Credential Dumping	Browser Bookmark Discovery	Distributed Component Object Model	Data from Information Repositories	Clipboard Data	Data Encrypted	Defacement
Hardware Additions	LSASS Driver		Extra Window Memory Injection	Credentials in Files	Credentials in Registry	Domain Trust Discovery	Exploitation of Remote Services	Data from Local System	Connection Proxy	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Trap		Process Injection	Exploitation for Credential Access	Exploitation for File and Directory Discovery	File and Directory Discovery	Data from Network Shared Drive	Custom Command and Control Protocol	Custom Cryptographic Protocol	Custom Exfiltration	Disk Structure Wipe
Spearphishing Attachment	AppleScript		DLL Search Order Hijacking	Forced Authentication	Forced Authentication	Logon Scripts	Data from Removable Media	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Endpoint Denial of Service	Endpoint Denial of Service
Spearphishing Link	CMSTP		Image File Execution Options Injection	Hooking	Input Capture	Pass the Hash	Data from Removable Media	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Firmware Corruption	Inhibit System Recovery
Spearphishing via Service	Compiled HTML File		Valid Accounts	Kerberasting	Input Prompt	Pass the Ticket	Data Staged	Data Encoding	Exfiltration Over Alternative Protocol	Network Denial of Service	Network Denial of Service
Supply Chain Compromise	Dynamic Data Exchange		BITS Jobs	Keychain	Permission Groups Discovery	Remote Desktop Protocol	Domain Fronting	Domain Generation Algorithms	Resource Hijacking	Runtime Data Manipulation	Runtime Data Manipulation
Trusted Relationship	Execution through API		Clear Command History	LLMNR/NBT-NS Poisoning and Relay	Process Discovery	Email Collection	Domain Generation Algorithms	Domain Name Resolution	Exfiltration Over Physical Medium	Service Stop	Service Stop
Valid Accounts	Execution through Module Load		CMSTP	Component Object Model Hijacking	Query Registry	File Copy	Domain Name Resolution	Domain Name Resolution	Scheduled Transfer	Stored Data Manipulation	Stored Data Manipulation
	Exploitation for Client Execution		BITS Jobs	Component Firmware	Remote System Discovery	File Obfuscation	Fallback Channels	File Obfuscation	Transmitted Data Manipulation	Transmitted Data Manipulation	Transmitted Data Manipulation
	File System Permissions Weakness		Control Panel Items	Control Panel Items	Security Software Discovery	File Transfer	Multiband Communication	Multiband Communication			
Graphical User Interface	Hooking		DCShadow	DCShadow	System Information Discovery	File Transfer	Multi-hop Proxy	Multi-hop Proxy			
InstallUtil	Launch Daemon		Deobfuscate/Decode Files or Information	Deobfuscate/Decode Files or Information	System Network Configuration Discovery	File Transfer	Multilayer Encryption	Multilayer Encryption			
Mshta	New Service		Securityd Memory	Two-Factor Authentication Interception	Windows Admin Shares Management	File Transfer	Multi-Stage Channels	Multi-Stage Channels			
PowerShell	Path Interception		Service Registry Permissions Weakness	System Network Configuration Discovery	System Network Connections Discovery	File Transfer	Port Knocking	Port Knocking			
Regsvr32	Port Monitors		Setuid and Setgid	System Owner/User Discovery	System Network Connections Discovery	File Transfer	Remote Access Tools	Remote Access Tools			
Rundl32	Service Registry Permissions Weakness		Startup Items	Disabling Security Tools	System Service Discovery	File Transfer	Remote File Copy	Remote File Copy			
Scripting	Setup and Setgid		DLL Side-Loading	DLL Side-Loading	System Time Discovery	File Transfer	Standard Application Layer Protocol	Standard Application Layer Protocol			
Service Execution	.bash_profile and .bashrc		Exploitation for Privilege Escalation	Execution Guardrails	Virtualization/Sandbox Evasion	File Transfer	Standard Cryptographic Protocol	Standard Cryptographic Protocol			
Signed Binary Proxy Execution	Account Manipulation		SID-History Injection	File Deletion		File Transfer	Standard Non-Application Layer Protocol	Standard Non-Application Layer Protocol			
Signed Script Proxy Execution	Authentication Package		Sudo	File Permissions Modification		File Transfer	Uncommonly Used Port	Uncommonly Used Port			
Source	BITS Jobs		Sudo Caching	File System Logical Offsets		File Transfer	Web Service	Web Service			
	Bootkit										
	Browser Extensions										

A softer color palette is more inviting

- Conveys the same message, but easier to digest
- Positions the results as less antagonistic: these are areas of improvement, not failure
- ***Even outside of assessments – be cautious when using red***

Being Realistic: Heatmaps are not Axiomatic

- Coverage heatmaps are great**

- Easy to understand; tangible and straightforward
- Provides “high level” picture; useful to all staff

but...



- Coverage doesn't always align with how attacks are executed in practice**

- Techniques can be executed in many ways, with different detections for each
- Per-technique detection isn't always the right level of abstraction

- Coverage is not static: what's green today could be gone tomorrow!**

- Attacker TTPs and defender practices rotate; don't ignore what you cover today

- Remember: ATT&CK heatmaps are almost always approximations**

- If you're doing this as a third-party, make sure the SOC knows this
- If you're doing this in-house, make sure colleagues and leadership understand

Complement Your Heatmap with Prose

1. If doing an assessment – don't just hand off a heatmap, describe it

2. Write up a short summary:

- What were some notable ATT&CK strengths?
- What were some notable ATT&CK gaps?
- Talk at the tactic level, but refer to relevant and important techniques

3. Don't stop at ATT&CK

- Summaries are great for the heatmap – but include information on general trends observed as well

Conducting an ATT&CK-based SOC Assessment

4. Delivering Results

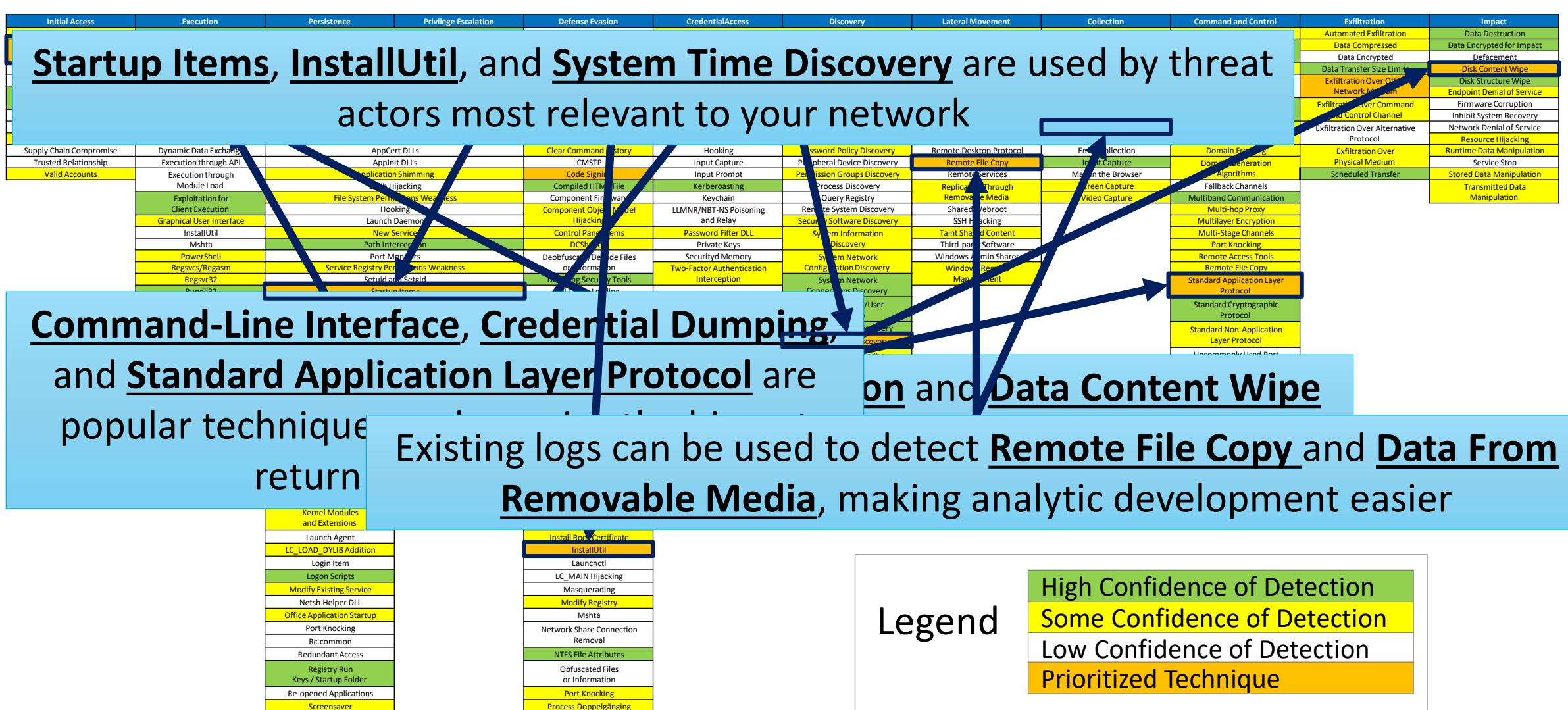
Try to Focus Prioritization

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	CredentialAccess	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise		Scheduled Task		Binary Padding	Network Sniffing		AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	Launchctl		Access Token Manipulation	Account Manipulation	Account Discovery		Automated Collection	Clipboard Data	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Local Job Scheduling	LSASS Driver	Bypass User Account Control	Bash History	Application Window Discovery		Distributed Component Object Model	Data from Information Repositories	Connection Proxy	Data Transfer Size Limits	Disk Content Wipe
Hardware Additions	Trap		Extra Window Memory Injection	Brute Force			Exploitation of Remote Services	Data from Local System	Custom Command and Control Protocol	Exfiltration Over Other Network Medium	Disk Structure Wipe
Replication Through Removable Media	AppleScript	DLL Search Order Hijacking	Process Injection	Credential Dumping	Credentials in Files			Data from Network Shared Drive	Custom Cryptographic Protocol	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Attachment	CMSTP		Image File Execution Options Injection	Credentials in Registry	Domain Trust Discovery		Logon Scripts	Data from Removable Media	Data Encoding	Firmware Corruption	Inhibit System Recovery
Spearphishing Link	Compiled HTML File		Valid Accounts	Exploitation for Credential Access	File and Directory Discovery		Pass the Hash	Data from Removable Media	Exfiltration Over Alternative Protocol	Network Denial of Service	Resource Hijacking
Spearphishing Via Service	Control Panel Items	Accessibility Features	BITS Jobs	Forced Authentication	Network Share Discovery			Data Staged	Data Obfuscation	Exfiltration Over Physical Medium	Runtime Data Manipulation
Supply Chain Compromise	Dynamic Data Exchange	AppCert DLLs	Clear Command History	Hooking	Password Policy Discovery		Remote Desktop Protocol	Email Collection	Domain Fronting	Service Stop	Scheduled Transfer
Trusted Relationship	Execution through API	AppInit DLLs	CMSTP	Input Capture	Peripheral Device Discovery		Remote File Copy	Input Capture	Domain Generation Algorithms	Stored Data Manipulation	Transmitted Data Manipulation
Valid Accounts	Execution through Module Load	Application Shimming	Code Signing	Input Prompt	Permission Groups Discovery		Remote Services	Man in the Browser			
		Dylib Hijacking	Compiled HTML File	Kerberoasting	Process Discovery		Replication Through Removable Media	Screen Capture	Fallback Channels		
Exploitation for Client Execution		File System Permissions Weakness	Component Firmware	Keychain	Query Registry			Video Capture	Multi-hop Communication		
		Hooking	Component Object Model Hijacking	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery				Multi-layer Encryption		
Graphical User Interface		Launch Daemon			Security Software Discovery			Shared Webroot	SSH Hijacking		
InstallUtil		New Service	Control Panel Items	>Password Filter DLL	System Information Discovery				Taint Shared Content		
Mshta		Path Interception	DCShadow	Private Keys					Third-party Software		
PowerShell		Port Monitors	Deobfuscate/Decode Files or Information	SecurityId Memory	System Network Configuration Discovery			Windows Admin Shares	Port Knocking		
Regsvcs/Regasm		Service Registry Permissions Weakness	Setuid and Setgid	Disabling Security Tools	Two-Factor Authentication Interception			Windows Remote Management	Remote Access Tools		
Regsvr32		Startup Items	DLL Side-Loading						Remote File Copy		
Rundll32		Web Shell	Execution Guardrails						Standard Application Layer Protocol		
Scripting									Standard Cryptographic Protocol		
Service Execution	.bash_profile and .bashrc	Exploitation for Privilege Escalation	Exploitation for Defense Evasion						Standard Non-Application Layer Protocol		
Signed Binary Proxy Execution	Account Manipulation	SID-History Injection	File Deletion						Uncommonly Used Port		
Signed Script Proxy Execution	Authentication Package								Web Service		
Source	Browser Extensions										
Space after Filename	Change Default File Association										
Third-party Software											
Trusted Developer Utilities	Component Firmware										
User Execution	Component Object Model Hijacking										
Windows Management Instrumentation	Create Account										
Windows Remote Management	External Remote Services										
XSL Script Processing	Hidden Files and Directories										
	Hypervisor										
	Kernel Modules and Extensions										
	Launch Agent										
	LC_LOAD_DYLIB Addition										
	Login Item										
	Logon Scripts										
	Modify Existing Service										
	Netsh Helper DLL										
	Office Application Startup										
	Port Knocking										
	Rc.common										
	Redundant Access										
	Registry Run Keys / Startup Folder										
	Re-opened Applications										
	Screensaver										

Legend

High Confidence of Detection
Some Confidence of Detection
Low Confidence of Detection

Try to Focus Prioritization



Tips for Prioritization

1. Small lists of techniques are great for short-term wins

2. Follow one of two paradigms:

- A technique or two across tactics, or
- Many techniques in one tactic

3. Focus on techniques that are immediately relevant

- Are they used by relevant threat actors?
- Are they popular or frequently occurring?
- Are they easy to execute and do they enable more techniques?
- Are the necessary logs readily accessible?

Give Tangible Recommendations

It's easy to give recommendations!

...but it's hard to give targeted ones
(and those are the most helpful!)

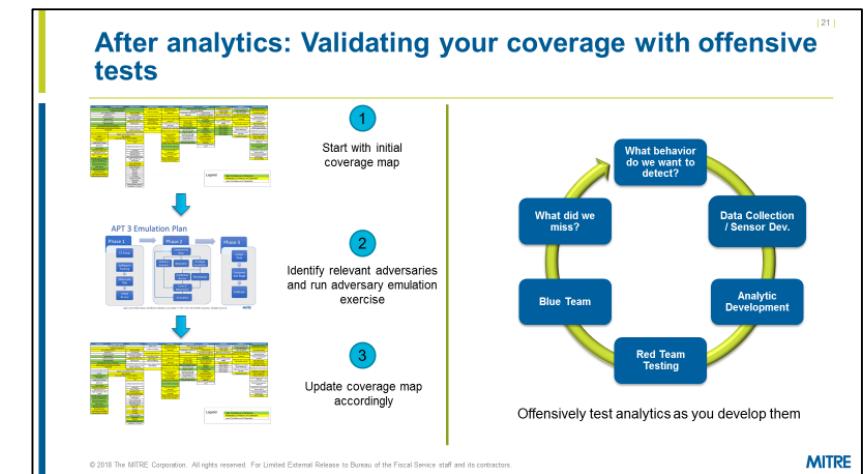
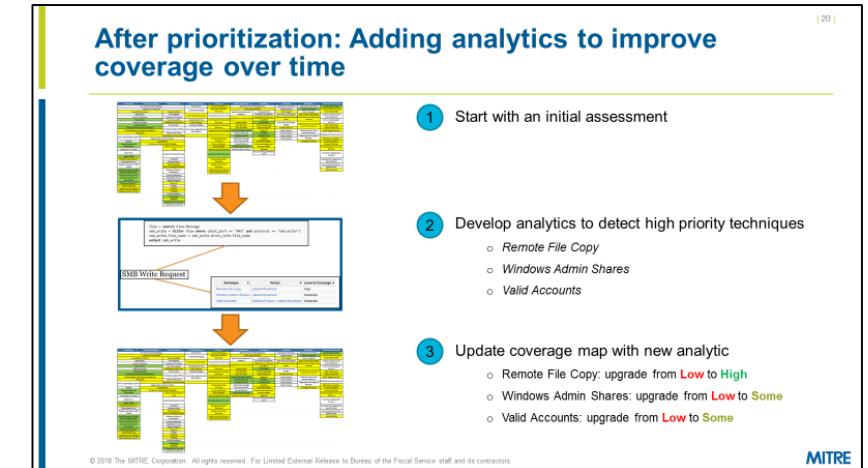
Consider giving:

1. Short- and long-term recommendations

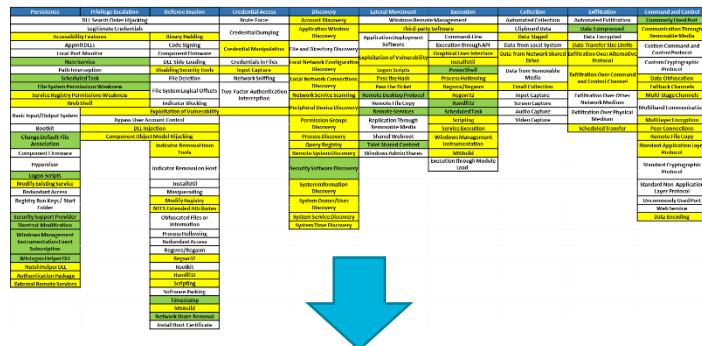
2. Examples and starting points

- Techniques to focus on for analytics
- Threat groups to emulate for adv. emulation
- Reading material to help get started

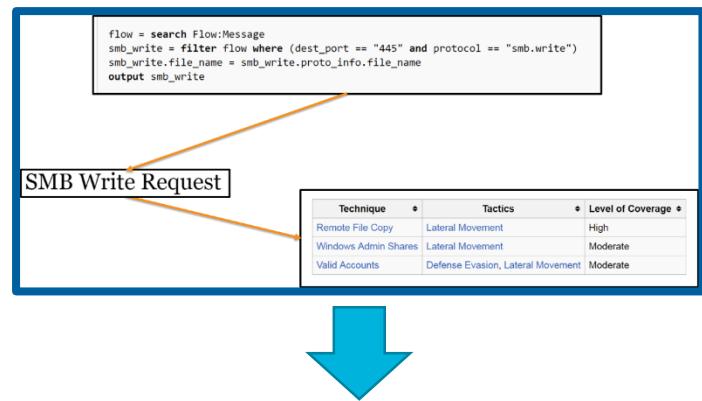
3. Prioritized recommendations for triage



Sample Recommendation: Adding Analytics



1 Start with an initial assessment



2 Focus on high priority techniques

- *Remote File Copy*
- *Windows Admin Shares*
- *Valid Accounts*



3 Update coverage map

- Remote File Copy: **Low to High**
- Windows Admin Shares: **Low to Some**
- Valid Accounts: **Low to Some**

Summary: Addressing Hard Challenges

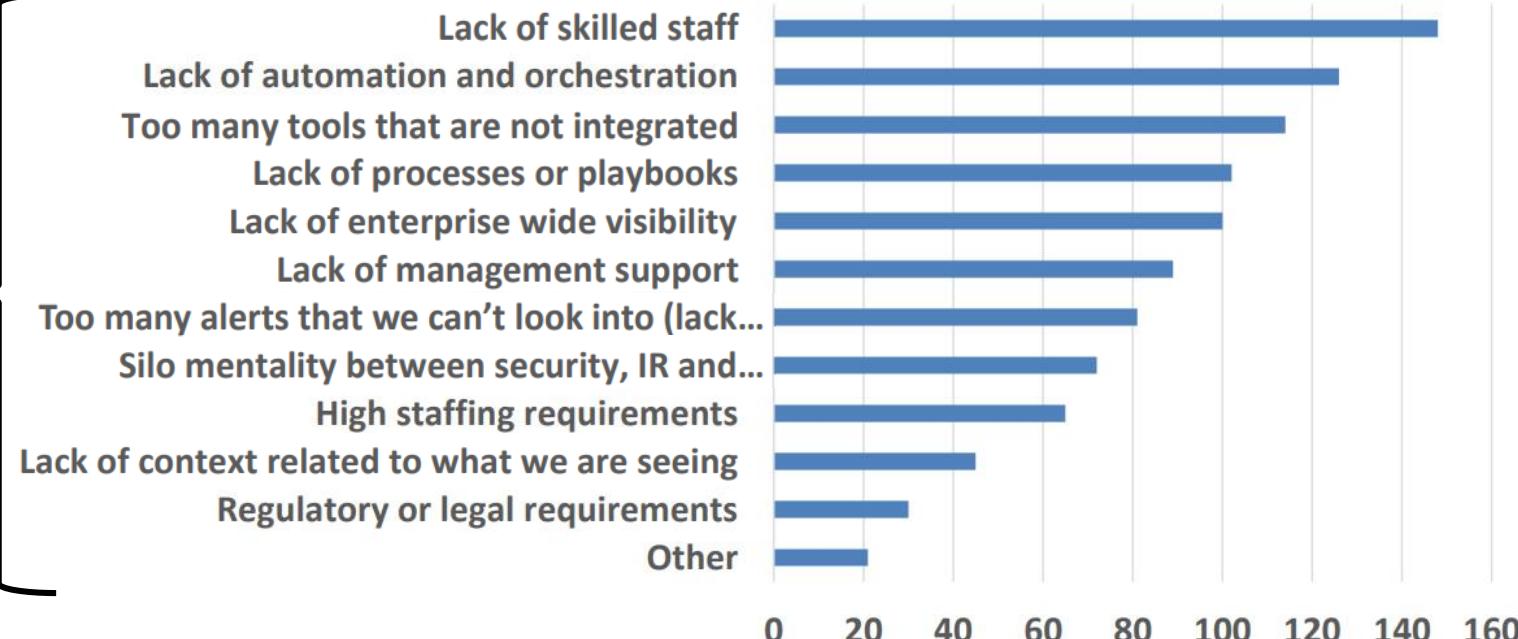
Revisiting the Hard Problems



Challenges, n=239



SANS Analyst Program



©2018 SANS™ Institute | www.sans.org

20

SOC Survey Summary, SANS Security Operations Summit 2018

<https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1532969860.pdf>

With Knowledge of My Detection Gaps, I can...

Too many tools that are not integrated



Map tools to ATT&CK to see overlaps

Lack of management support



Provide big-picture status to initiate efforts

Lack of enterprise wide visibility



Aggregate heatmaps to see enterprise coverage

Too many alerts that we can't look into



Prioritize alerts based on ATT&CK mapping

Silo mentality between security, IR and..



Use ATT&CK as a common language

Lack of context related to what we are seeing



Enrich alerts with relevant TTP info

How an Assessment Helps

Assessment side-effect: producing tool heatmaps

Too many tools that are not integrated

Map tools to ATT&CK to see overlaps

Heatmaps are easily digestible and show progress

Lack of management support

Provide big-picture status to initiate efforts

Assessments provide aggregate coverage charts

Lack of enterprise wide visibility

Aggregate heatmaps to see enterprise coverage

Prioritization can identify high-impact TTPs

Too many alerts that we can't look into

Prioritize alerts based on ATT&CK mapping

Assessments help orient teams to the same page

Silo mentality between security, IR and..

Use ATT&CK as a common language

Side-effect: mapping analytics/alerts to TTPs

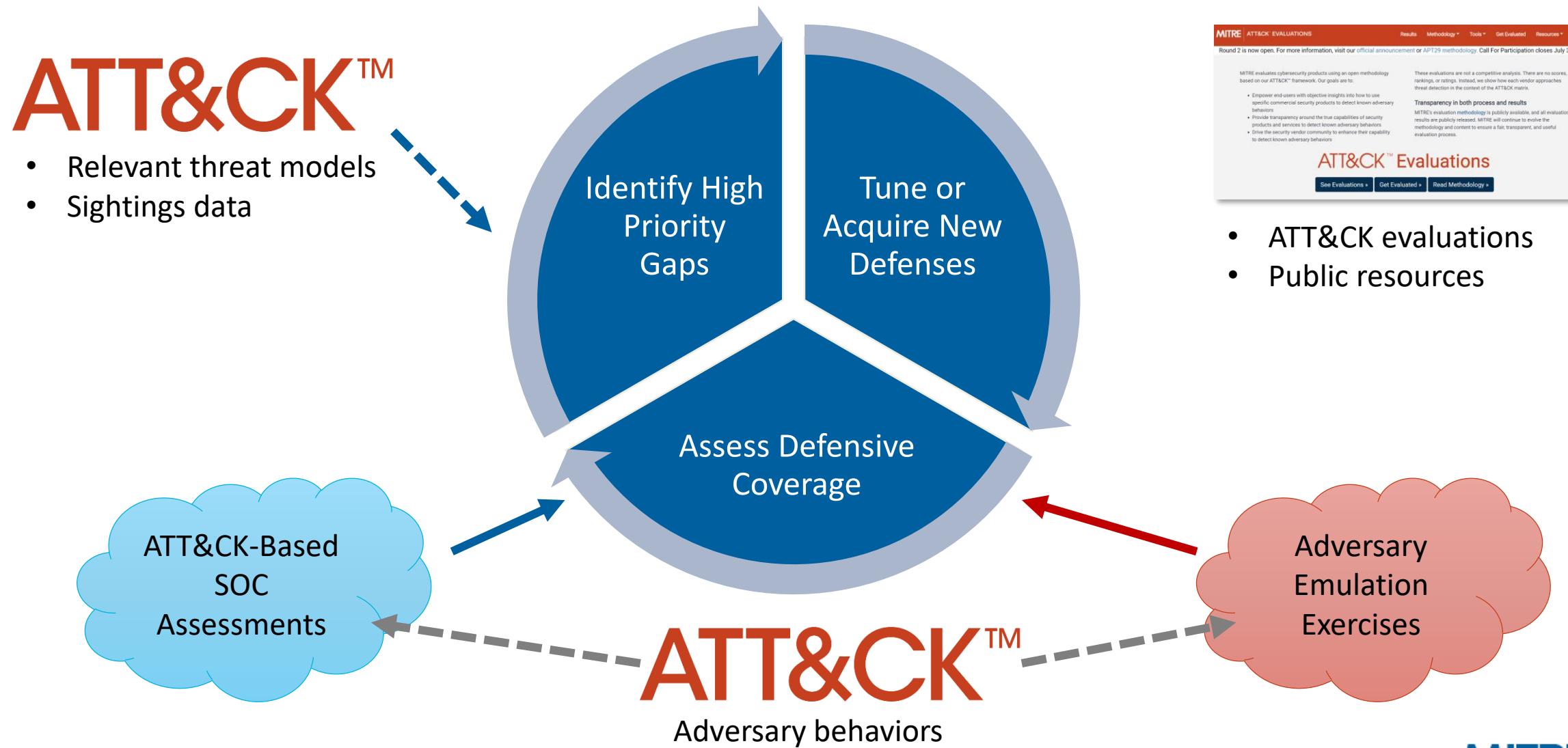
Lack of context related to what we are seeing

Enrich alerts with relevant TTP info

Soundbytes and Takeaways

- **Make sure you're setting the right expectations**
 - ATT&CK – and assessments – are not a silver bullet
- **Your coverage isn't just your tools – it's your people and your processes too**
- **Create heatmaps that convey what you want to convey – and don't use red!**
- **Don't stop with a heatmap**
 - Identify key techniques to prioritize in the short term
 - Have a set plan – or a set of recommendations to follow-up on

Long-term: Following Up After an Assessment



Links and Contact

- **Andy Applebaum**

- aapplebaum@mitre.org
- @andyplayse4

- **ATT&CK**

- <https://attack.mitre.org>
- @MITREattack
- attack@mitre.org

- **Data + Code**

- <https://github.com/mitre/cti> (STIX data)
- <https://github.com/mitre-attack> (code)

- **CALDERA**

- <https://github.com/mitre/caldera>

- **ATT&CK-based Product Evaluations**

- <https://attackevals.mitre.org/>

- **ATT&CKcon**

- <https://www.mitre.org/attackcon>

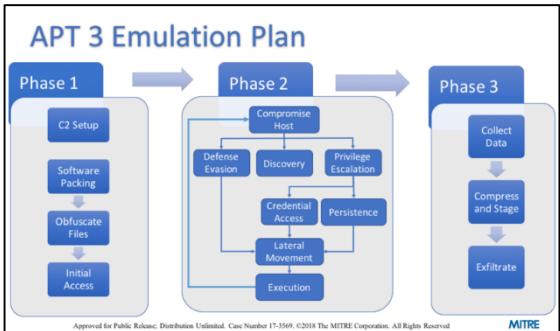
- **Blog**

- <https://medium.com/mitre-attack>

Backup

MITRE's Public ATT&CK Resources

Adversary Emulation Plans



attack.mitre.org/wiki/Adversary_Emulation_Plans

Public ATT&CK Knowledge Base

The screenshot shows the homepage of the Public ATT&CK Knowledge Base. It features a navigation bar with links for ATT&CK, Matrices, Tactics, Techniques, Groups, Software, Resources, Blog, and Contact. Below the navigation is a search bar. A main content area includes a message about the first round of ATT&CK Evaluations, a tweet feed from the @MITREattck account, and a prominent "ATT&CK™" logo with "Get Started", "Contribute", and "Check out our Blog" buttons.

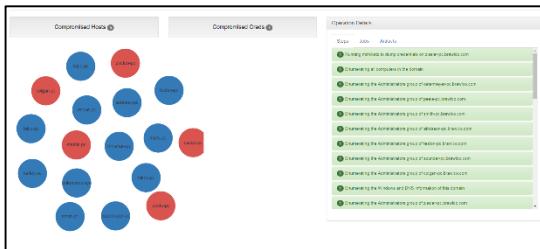
attack.mitre.org

ATT&CK Navigator



mitre.github.io/attack-navigator

CALDERA: Automated Adversary Emulation



<https://github.com/mitre/caldera>

Structured Content



github.com/mitre/cti



cti-taxii.mitre.org



Conference Talks



ATT&CK in the Community

**89 individuals +
orgs contributing
to ATT&CK!**

- Alain Homewood, Insomnia Security
- Alan Neville, @abnev
- Anastasios Pingios
- Andrew Smith, @jakx_
- Barry Shteman, Exabeam
- Bartosz Jerzman
- Bryan Lee
- Carlos Borges, CIP
- Casey Smith
- Christiaan Beek, @ChristiaanBeek
- Cody Thomas, SpecterOps
- Craig Aitchison
- Daniel Oakley
- Darren Spruell
- Dave Westgard
- David Ferguson, CyberSponse
- David Lu, Tripwire
- David Routin
- Ed Williams, Trustwave, SpiderLabs
- Edward Millington
- Elger Vinicius S. Rodrigues, @elgervinicius, CYBINT Centre
- Elia Florio, Microsoft
- Emily Ratliff, IBM
- ENDGAME
- Eric Kuehn, Secure Ideas
- Erye Hernandez, Palo Alto Networks

- Felipe Espósito, @Pr0teus
- FS-ISAC
- Hans Christoffer Gaardløs
- Itamar Mizrahi
- Itzik Kotler, SafeBreach
- Jacob Wilkin, Trustwave, SpiderLabs
- Jan Miller, CrowdStrike
- Jared Atkinson, @jaredcatkinson
- Jeremy Galloway
- John Lambert, Microsoft Threat Intelligence Center
- John Strand
- Josh Abraham
- Justin Warner, ICEBRG
- Leo Loobek, @leoloobek
- Loic Jaquemet
- Marc-Etienne M.Léveillé, ESET
- Mark Wee
- Matt Graeber, @mattifestation, SpecterOps
- Matt Kelly, @breakersall
- Matthew Demaske, Adaptforward
- Matthew Molyett, @s1air
- McAfee
- Michael Cox
- Mike Kemmerer
- Milos Stojadinovic
- Mnemonic
- Nick Carr, FireEye
- Nik Seetharaman, Palantir
- Nishan Maharjan, @loki248
- Oddvar Moe, @oddvarmoe
- Omkar Gudhate
- Patrick Campbell, @pjcampbe11
- Paul Speulstra, AECOM Global Security
- Operations Center**
- Pedro Harrison
- Praetorian
- Rahmat Nurfauzi, @infosecn1nja, PT Xynexis International
- Red Canary
- RedHuntLabs (@redhuntlabs)
- Ricardo Dias
- Richard Gold, Digital Shadows
- Richie Cyrus, SpecterOps
- Robby Winchester, @robwinchester3
- Robert Falcone
- Romain Dumont, ESET
- Ryan Becwar
- Ryan Benson, Exabeam
- Scott Lundgren, @5twenty9, Carbon Black
- Stefan Kanthak
- Sudhanshu Chauhan, @Sudhanshu_C
- Sunny Neo
- Sylvain Gil, Exabeam
- Teodor Cimpoesu
- Tim MalcomVetter
- Tom Ueltschi @c_APT_ure
- Tony Lambert, Red Canary
- Travis Smith, Tripwire
- Tristan Bennett, Seamless Intelligence
- Valerii Marchuk, Cybersecurity Help s.r.o.
- Veeral Patel
- Vincent Le Toux
- Walker Johnson
- Ye Yint Min Thu Htut, Offensive Security Team, DBS Bank
- Yonatan Gotlib, Deep Instinct



ATT&CK
@MITREattack Follows you

MITRE ATT&CK™ - A framework for describing the behavior of cyber adversaries across their intrusive lifecycle. (Replying/Following/Re-tweeting ≠ endorsement)

⌚ McLean, VA ⌚ attack.mitre.org

📅 Joined May 2015

456 Following **23.2K Followers**

GitHub Sign up

Repositories 67
Code
Commits 401
Issues 276

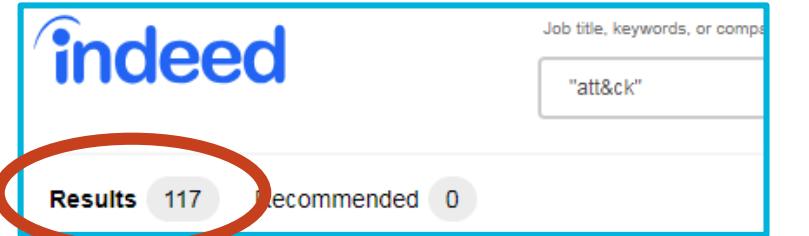
Language Any

Sort Best match

GitHub
67 repository results

Who's using ATT&CK?

Job postings on Indeed as a proxy for usage



The screenshot shows the Indeed search results page for the query "att&ck". The search bar at the top contains the text "att&ck". Below the search bar, there is a red oval highlighting the "Results 117" button. To the right of the results count are two buttons: "Recommended" and "0".

Financial

- SF Fed Reserve
- Bank of America
- JP Morgan
- FS-ISAC
- Experian
- Freddie Mac
- BNY Mellon
- US Bank

Tech

- Microsoft
- Intel
- Airbnb
- Verizon
- Box
- Uber
- CDW

Security

- RevSec
- FireEye
- AppGuard
- CrowdStrike
- CyberSponse
- Verodin

Retail

- Target
- Best Buy
- PepsiCo
- Under Armour

Defense

- Boeing
- Booz Allen
- Leidos

Media

- NBCUniversal
- Nielsen
- Cox
- Comcast

Others

- General Electric
- Deloitte
- Pfizer
- GSK
- Marathon
- UnitedHealth

...and others!

Principal Associate, Red Team Pursuit

Capital One ★★★★ 7,055 reviews
Tysons Corner, VA

Principal Cyber Security Analyst

Federal Reserve Bank of San Francisco ★★★★ 36 reviews
San Francisco, CA 94105 (Financial District area)

BISO Operations Knowledge Manager

Bank of America Corporation ★★★★ 22,914 reviews
Chicago, IL

Senior Cyber Threat Intelligence Analyst

AIG ★★★★ 2,826 reviews
Reston, VA 20191

General Manager, Operations Services

FS-ISAC Inc
Reston, VA

Red Team Manager

EXPERIAN ★★★★ 330 reviews
Costa Mesa, CA

Managing Director - Cyber Resiliency

Charles Schwab ★★★★ 979 reviews
Lone Tree, CO 80124

Global Cybersecurity Operations - Threat Intelligence

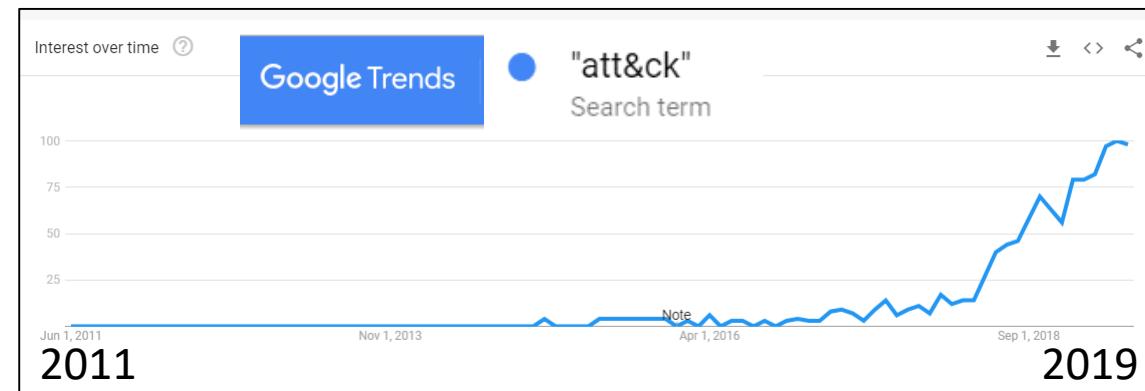
JP Morgan Chase ★★★★ 21,662 reviews
Wilmington, DE 19803

ATT&CK in the Community

**89 individuals +
orgs contributing
to ATT&CK!**

- Alain Homewood, Insomnia Security
- Alan Neville, @abnev
- Anastasios Pingios
- Andrew Smith, @jakx_
- Barry Shteiman, Exabeam
- Bartosz Jerzman
- Bryan Lee
- Carlos Borges, CIP
- Casey Smith
- Christiaan Beek, @ChristiaanBeek
- Cody Thomas, SpecterOps
- Craig Aitchison
- Daniel Oakley
- Darren Spruell
- Dave Westgard

- David Ferguson, CyberSponse
- David Lu, Tripwire
- David Routin
- Ed Williams, Trustwave, SpiderLabs
- Edward Millington
- Elger Vinicius S. Rodrigues, @elgervinicius, CYBINT Centre
- Elia Florio, Microsoft
- Emily Ratliff, IBM
- ENDGAME
- Eric Kuehn, Secure Ideas
- Erye Hernandez, Palo Alto Networks
- Felipe Espósito, @Pr0teus
- FS-ISAC
- Hans Christoffer Gaardløs
- Itamar Mizrahi
- Itzik Kotler, SafeBreach
- Jacob Wilkin, Trustwave, SpiderLabs
- Jan Miller, CrowdStrike
- Jared Atkinson, @jaredcatkinson
- Jeremy Galloway
- John Lambert, Microsoft Threat Intelligence Center
- John Strand
- Josh Abraham
- Justin Warner, ICEBRG
- Leo Loobek, @leoloobek
- Loic Jaquemet
- Marc-Etienne M.Léveillé, ESET
- Mark Wee
- Matt Graeber, @mattifestation, SpecterOps
- Matt Kelly, @breakersall
- Matthew Demaske, Adaptforward
- Matthew Molyett, @s1air
- McAfee
- Michael Cox
- Mike Kemmerer
- Milos Stojadinovic
- Mnemonic
- Nick Carr, FireEye
- Nik Seetharaman, Palantir
- Nishan Maharjan, @loki248
- Oddvar Moe, @oddvarmoe
- Omkar Gudhate
- Patrick Campbell, @pjcampbe11
- Paul Speulstra, AECOM Global Security Operations Center
- Pedro Harrison
- Praetorian
- Rahmat Nurfauzi, @infosecn1nja, PT Xynesis International
- Red Canary
- RedHuntLabs (@redhuntlabs)
- Ricardo Dias
- Richard Gold, Digital Shadows
- Richie Cyrus, SpecterOps
- Robby Winchester, @robwinchester3
- Robert Falcone
- Romain Dumont, ESET
- Ryan Becwar
- Ryan Benson, Exabeam
- Scott Lundgren, @Stwenty9, Carbon Black
- Stefan Kanthak
- Sudhanshu Chauhan, @Sudhanshu_C
- Sunny Neo
- Sylvain Gil, Exabeam
- Teodor Cimpoesu
- Tim MalcomVetter
- Tom Ueltschi @c_APT_ure
- Tony Lambert, Red Canary
- Travis Smith, Tripwire
- Tristan Bennett, Seamless Intelligence
- Valerii Marchuk, Cybersecurity Help s.r.o.
- Veeral Patel
- Vincent Le Toux
- Walker Johnson
- Ye Yint Min Thu Htut, Offensive Security Team, DBS Bank
- Yonatan Gotlib, Deep Instinct



ATT&CK
@MITREattack Follows you

MITRE ATT&CK™ - A framework for describing the behavior of cyber adversaries across their intrusid lifecycle. (Replying/Following/Re-tweeting ≠ endorsement)

⌚ McLean, VA ⌚ attack.mitre.org
📅 Joined May 2015
456 Following 23.2K Followers

MITRE

ATT&CK (and interest in ATT&CK) has grown

Interest over time

