Lessons Learned Applying ATT&CK-Based SOC Assessments

Andy Applebaum

@andyplayse4

SANS Security Operations Summit

June 24th, 2019

MITRE

© 2019 The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited 18-3288-11.

Challenges in the SOC

ATT&CK™
Adversarial Tactics, Techniques & Common Knowledge

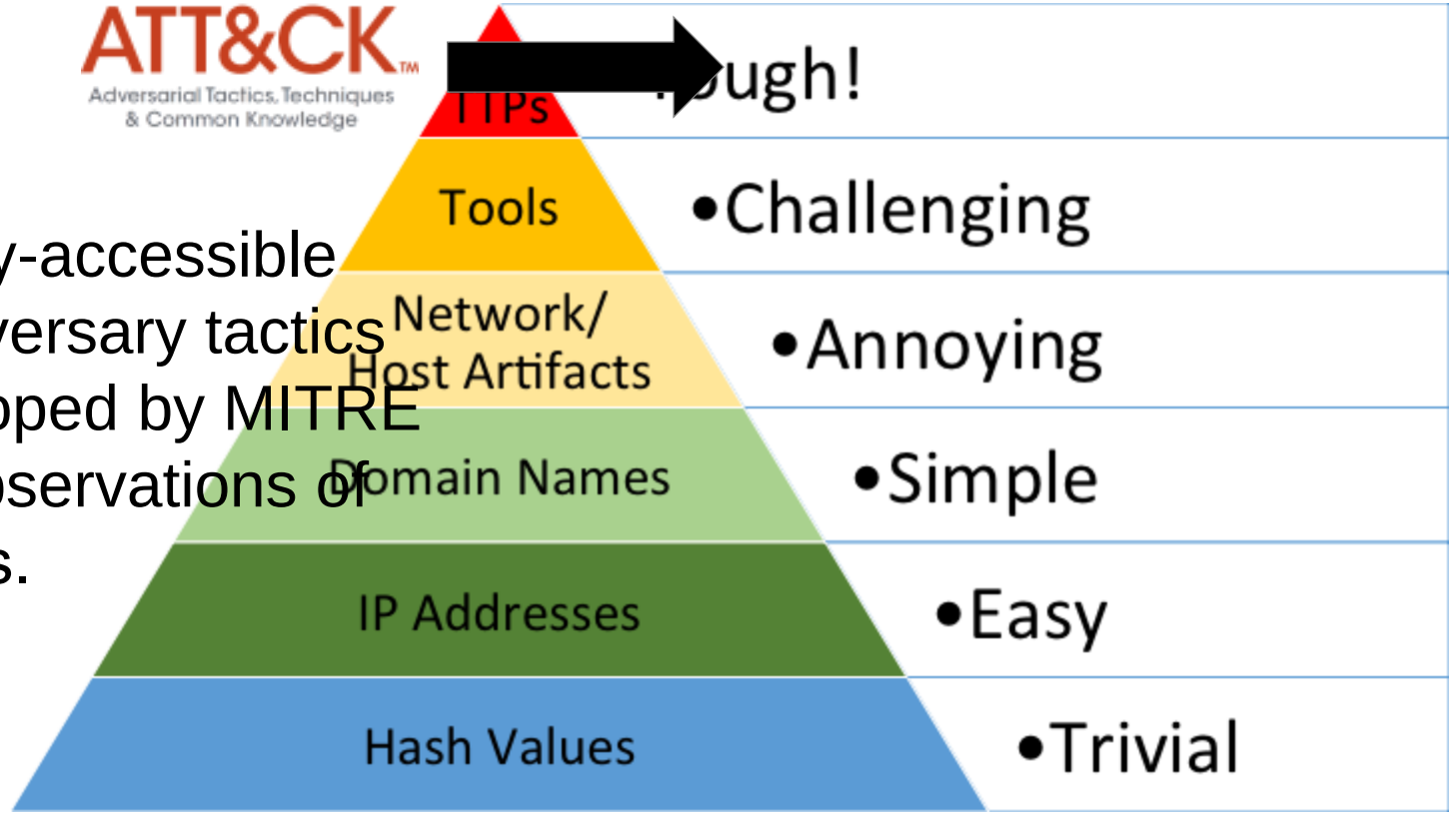
SOC Survey Summary, SANS Security Operations Summit 2018
https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1532969860.pdf

© 2019 The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited 18-3288-11.

MITRE

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

© 2019 The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited 18-3288-11.

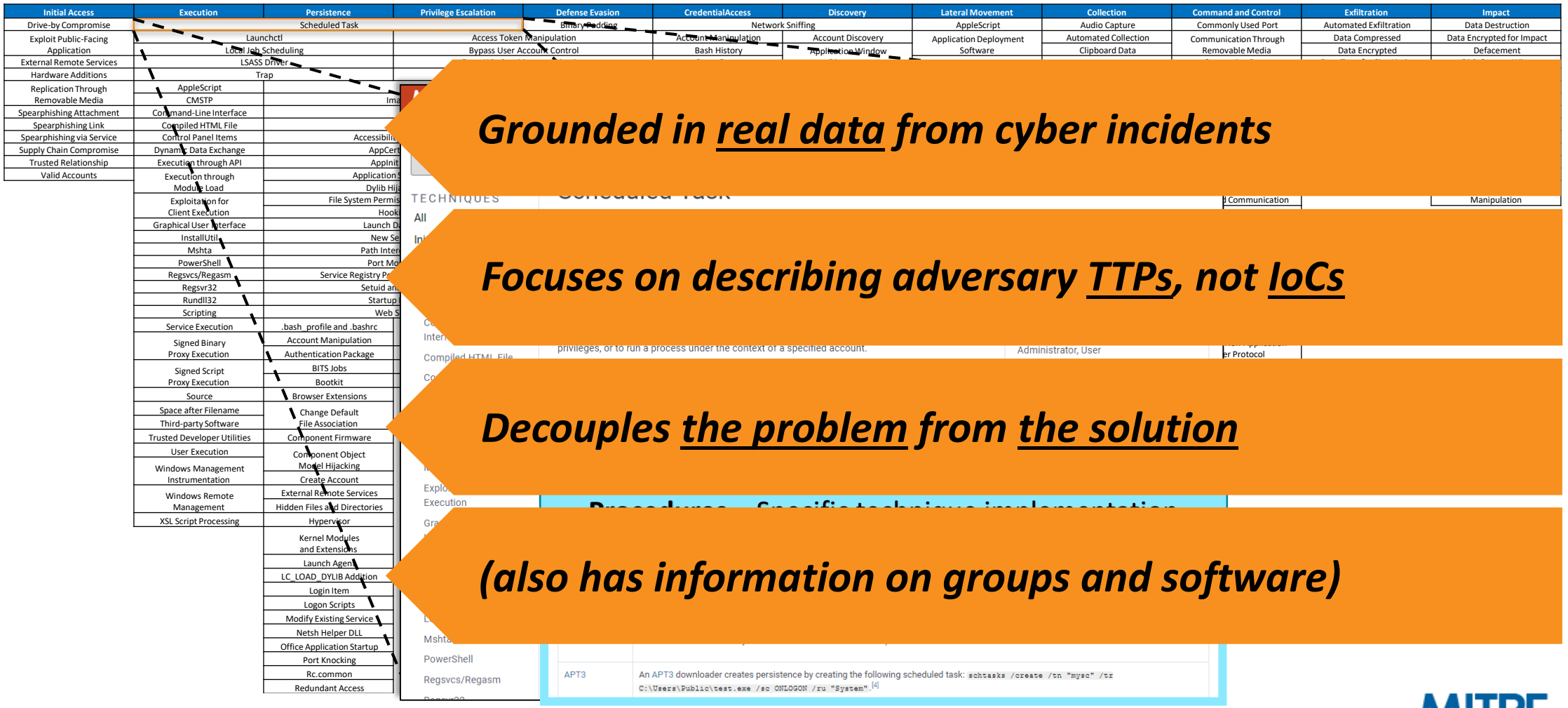
MITRE

The ATT&CK Matrix

Publicly Available
attack.mitre.org

Tactics – Adversary's technical goal

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)

© 2019 The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited 18-3288-11.

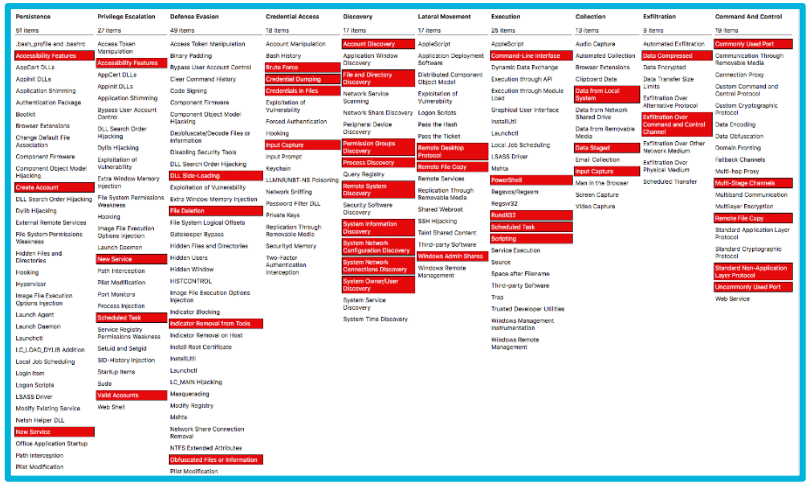
MITRE

Core ATT&CK Use Cases

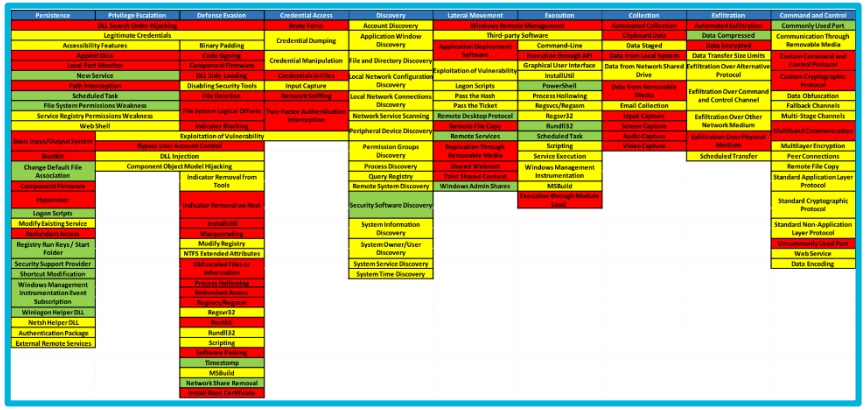
Detection

```
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
```

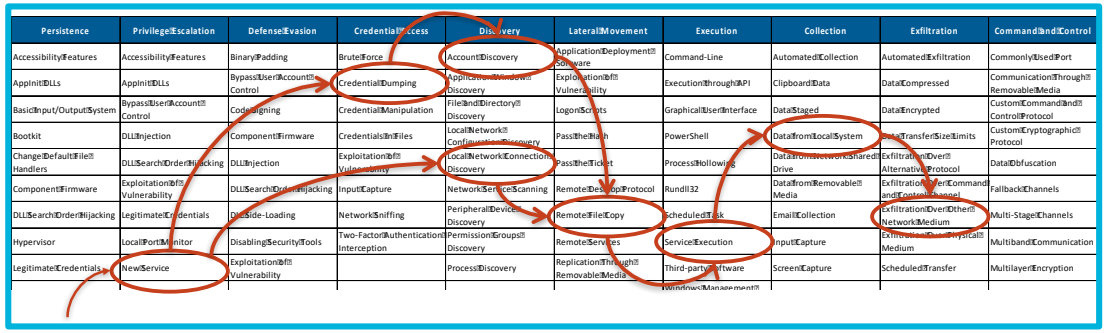
Threat Intelligence



Assessment and Engineering



Adversary Emulation



© 2019 The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited 18-3288-11.

MITRE

Starting with ATT&CK: Understanding Detection Gaps

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

Knowledge of my detection gaps allows me to…

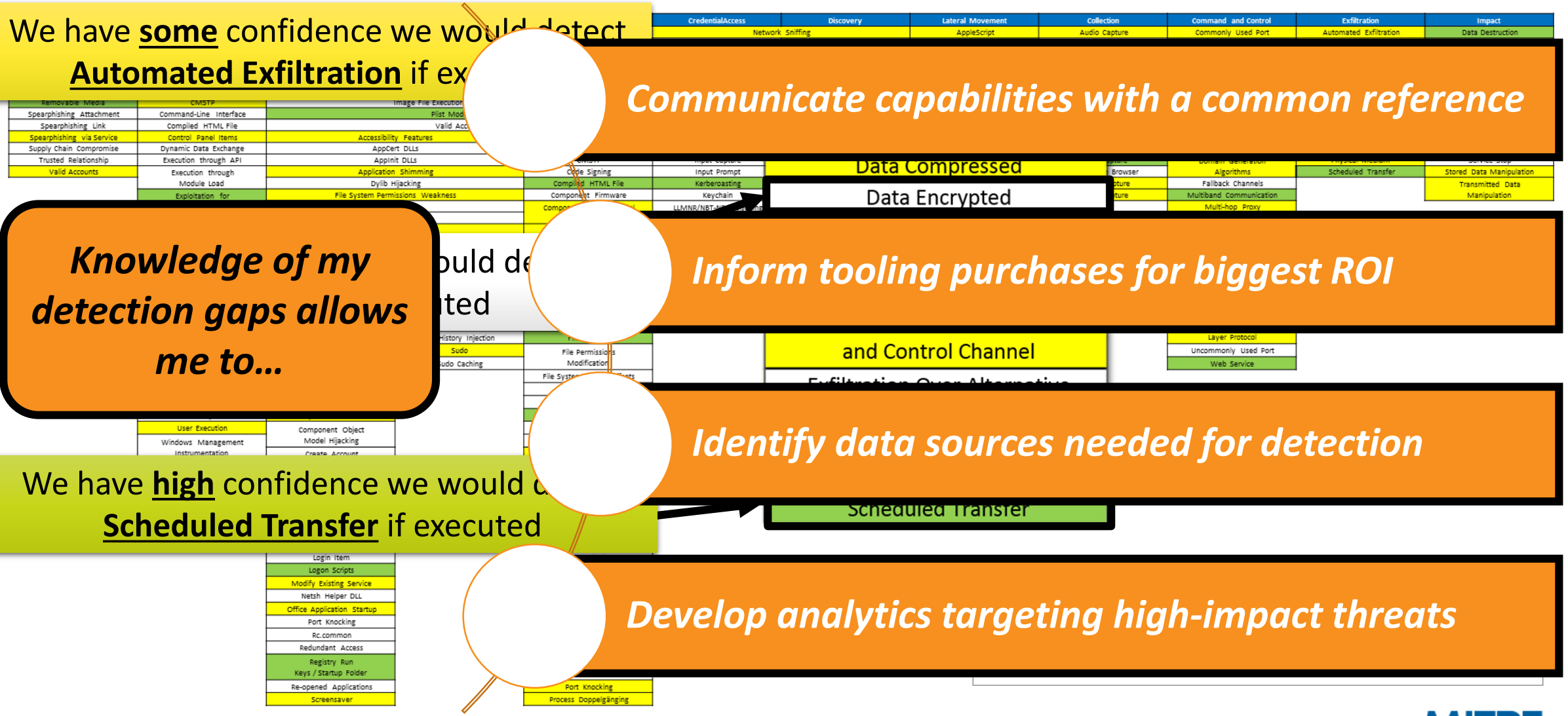
We have **high** confidence we would d **Scheduled Transfer** if executed

Communicate capabilities with a common reference

Inform tooling purchases for biggest ROI

Identify data sources needed for detection

Develop analytics targeting high-impact threats



© 2019 The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited 18-3288-11.

MITRE

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

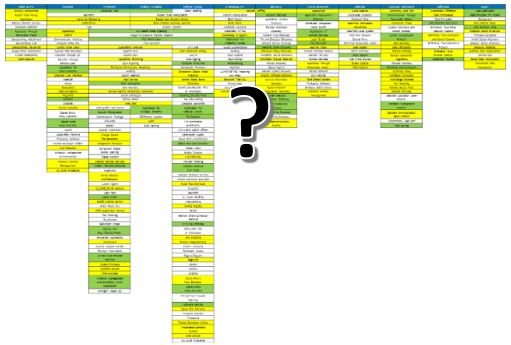
© 2019 The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited 18-3288-11.

MITRE

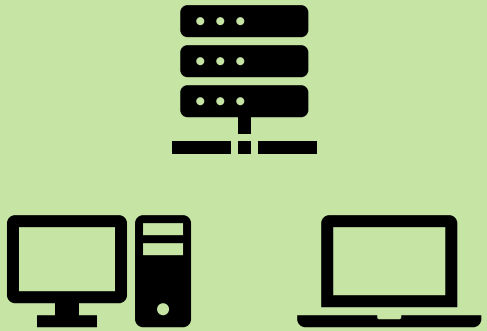
Getting Started: Using ATT&CK for Assessments

Bringing ATT&CK into the SOC

Security Operations Center:
Protecting Network



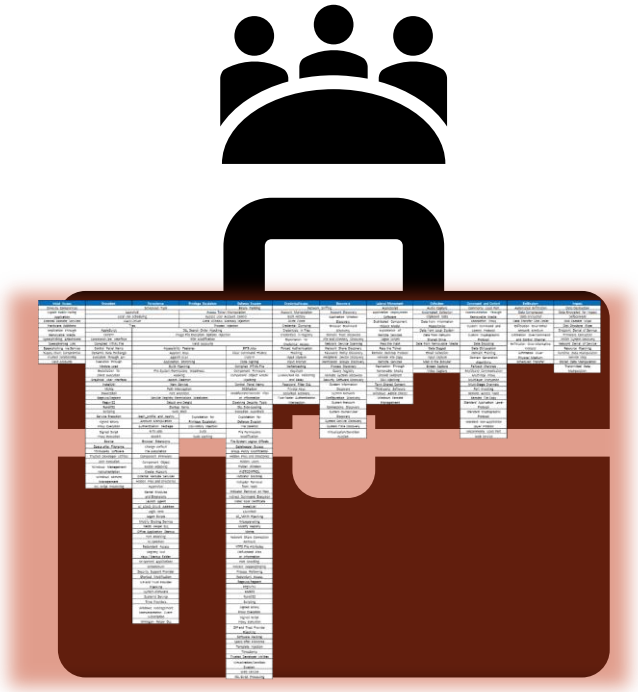
Defended: Network:
Performing Operational Need

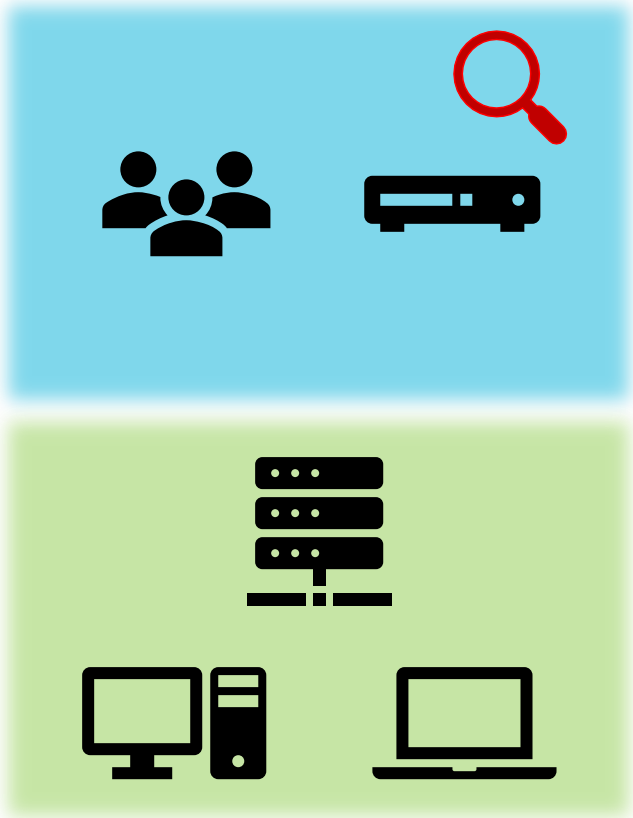


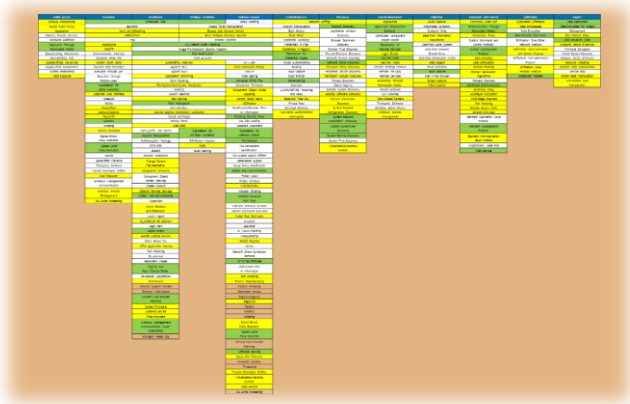
© 2019 The MITRE Corporation. All rights reserved.

MITRE

Solution: ATT&CK-based SOC Assessments







Third-party Assessment Team

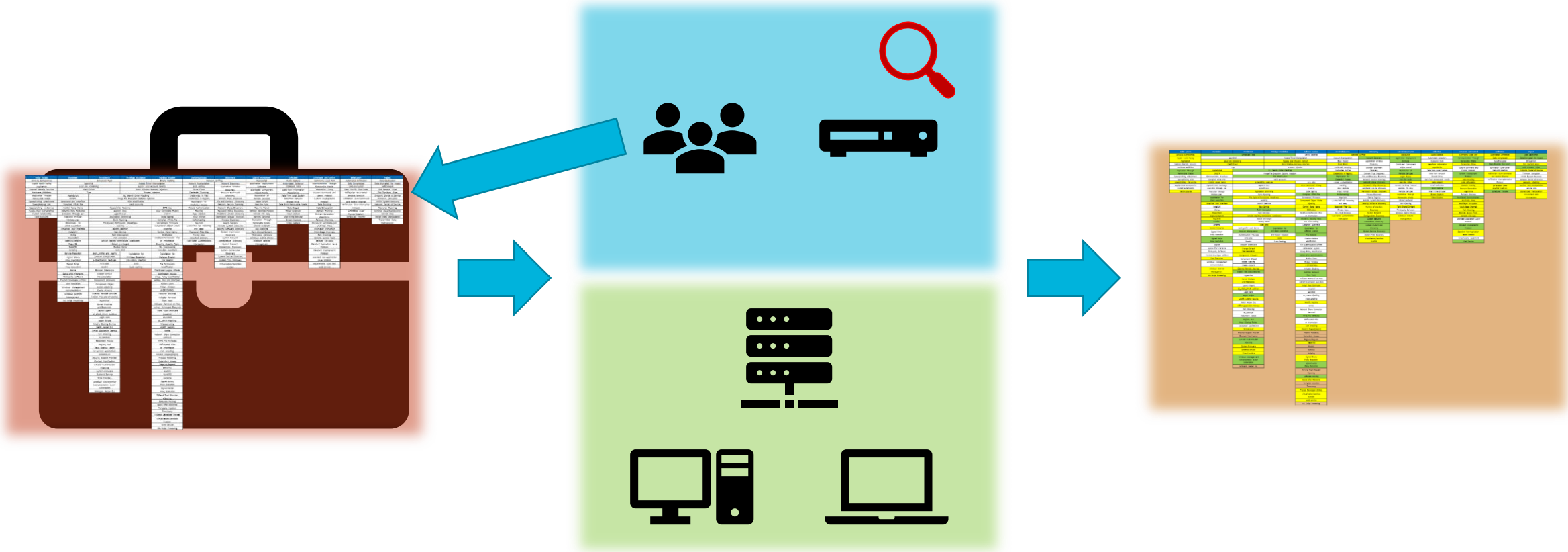
Target SOC Environment

Detection Heatmap

© 2019 The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited 18-3288-11.

MITRE

Solution: ATT&CK-based SOC Assessments



Internal Assessment Team

Target SOC Environment

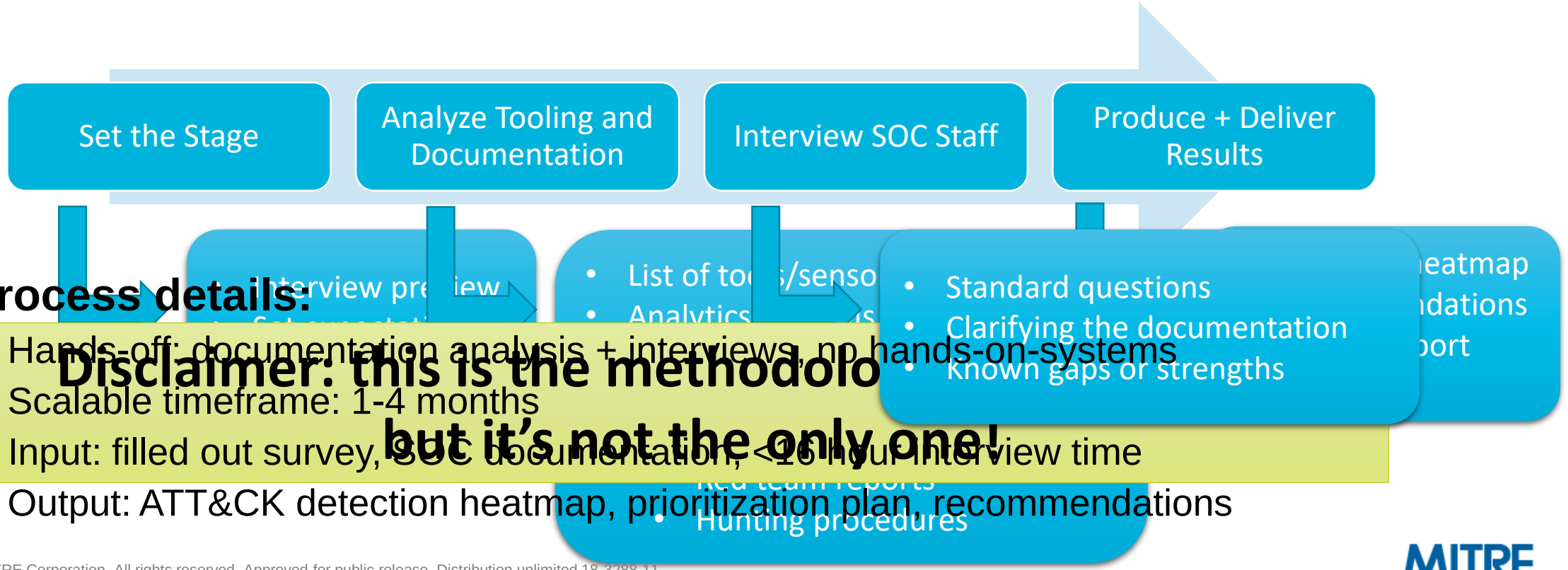
Detection Heatmap

© 2019 The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited 18-3288-11.

MITRE

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



- **Process details:**
  - Hands-off: documentation analysis + interviews, no hands-on-systems
  - Scalable timeframe: 1-4 months
  - Input: filled out survey, SOC documentation, <16 hour interview time
  - Output: ATT&CK detection heatmap, prioritization plan, recommendations

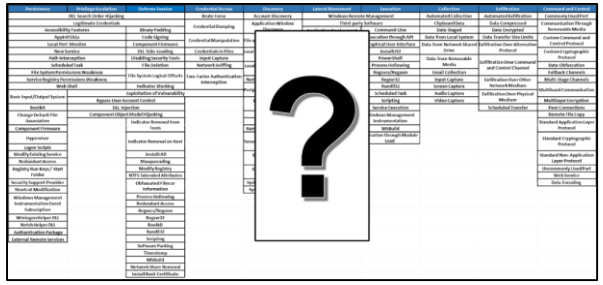
Disclaimer: this is the methodolo
but it's not the only one!

© 2019 The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited 18-3288-11.

MITRE

Experiences with ATT&CK-Based SOC Assessments

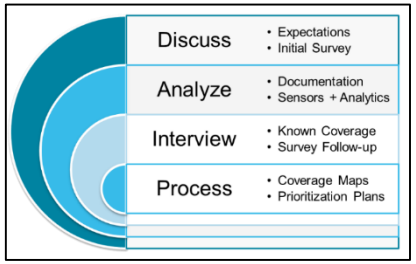
- **First run in 2017**



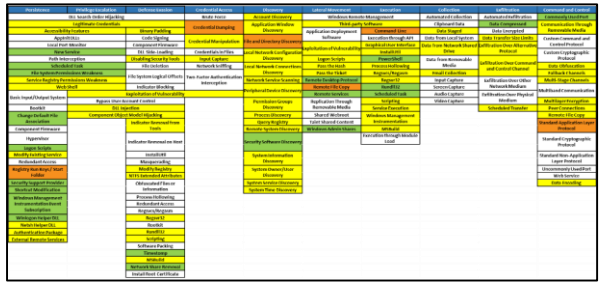
- **Since then:**

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



© 2019 The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited 18-3288-11.

MITRE

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: <u>if you're bringing ATT&CK into a SOC, make sure you set the right expectations, particularly if you're doing an assessment</u>**

© 2019 The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited 18-3288-11.

MITRE

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

© 2019 The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited 18-3288-11.

MITRE

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**

© 2019 The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited 18-3288-11.

MITRE

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***

© 2019 The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited 18-3288-11.

MITRE

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

© 2019 The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited 18-3288-11.

MITRE

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**

© 2019 The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited 18-3288-11.

MITRE

Conducting an ATT&CK-based SOC Assessment

3. Producing the Heatmap

Pick a Good Scoring Scheme For Your Heatmap

Legend

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

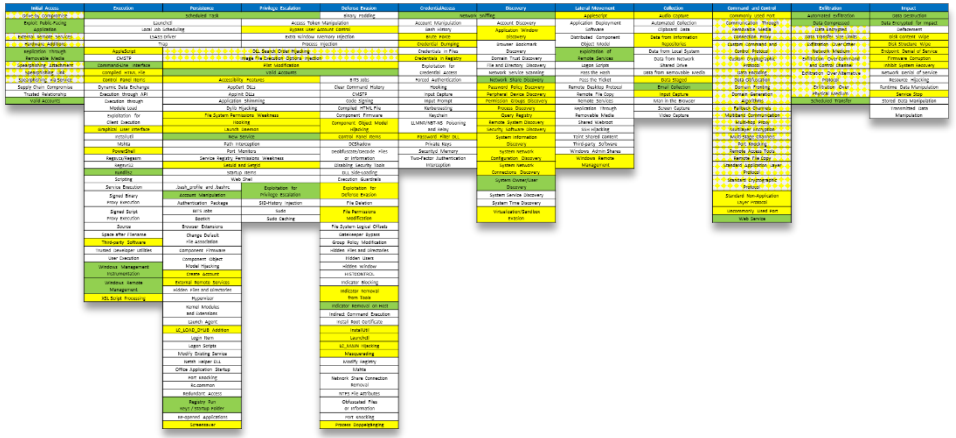
© 2019 The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited 18-3288-11.

MITRE

Pick a Good Scoring Scheme For Your Heatmap

- Regardless of ATT&CK use case, have a good scoring scheme!
  - Too much of a good thing becomes confusing
- Define categories that are relevant to your use case
  - Easy to get lost in labels
- Avoid mixing category types (confidence + likelihood + ease of use is messy)
  - Remember: your goal is to paint broad strokes
- Know your audience: leadership wants big picture, stakeholder needs 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



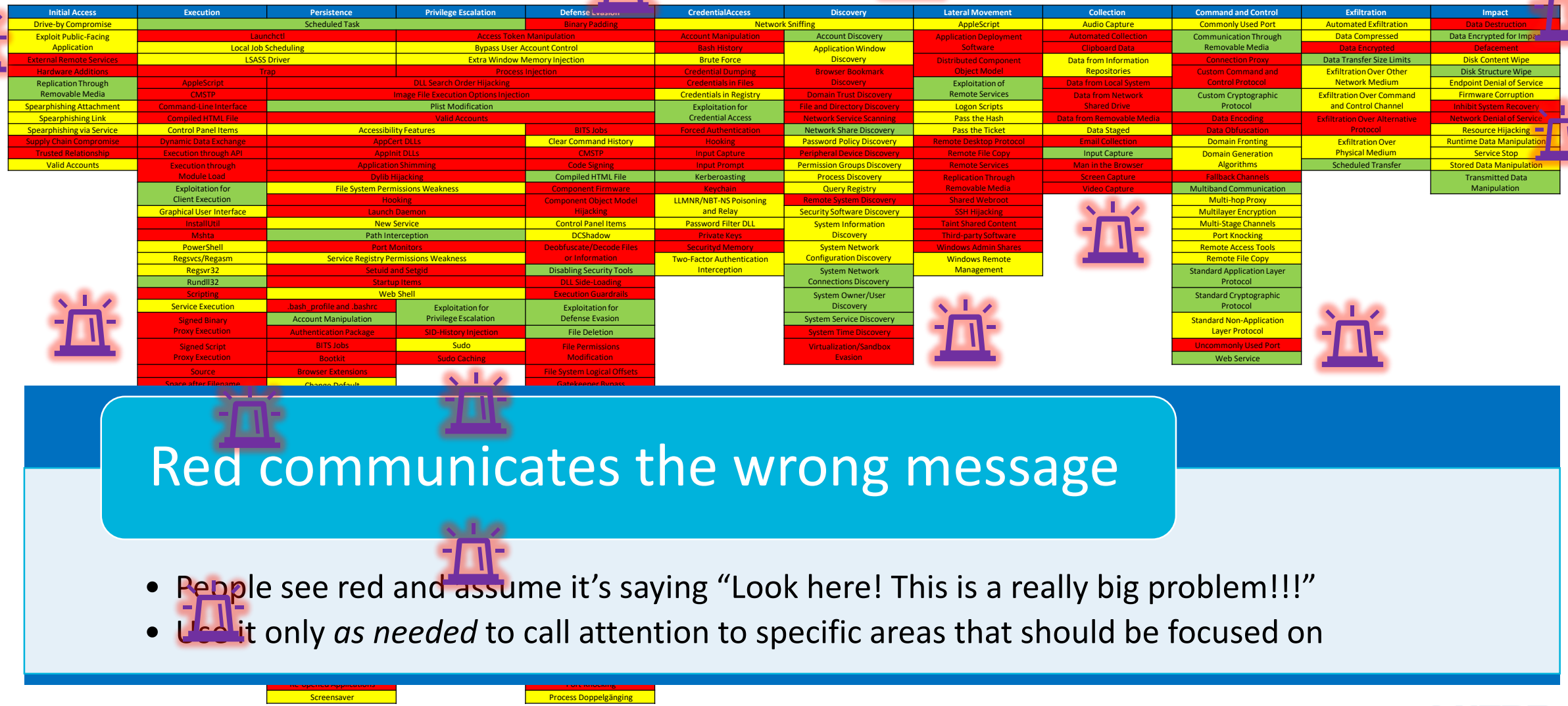
© 2019 The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited 18-3288-11.

MITRE

Heatmaps: Avoiding Red

Legend

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



Red communicates the wrong message

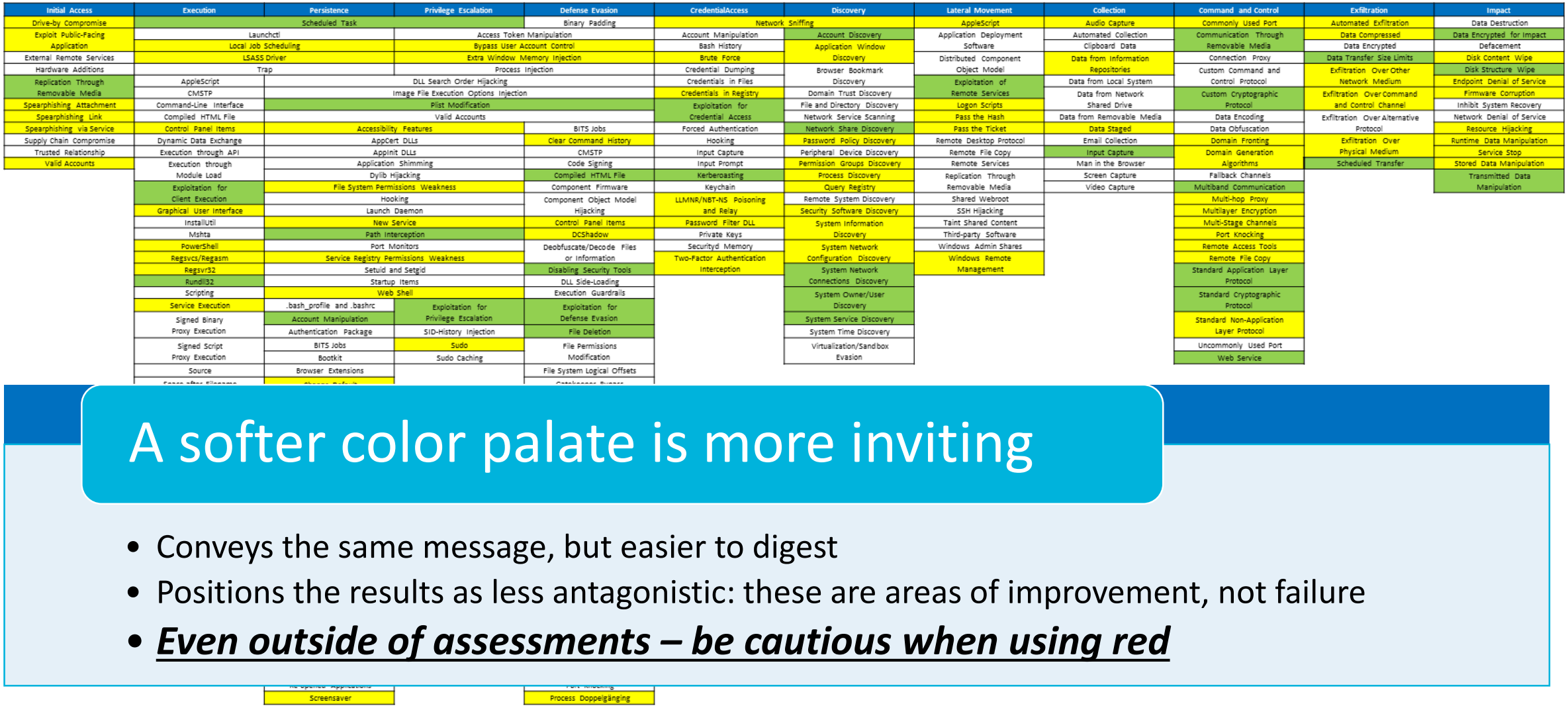
- People see red and assume it's saying "Look here! This is a really big problem!!!"
- Use it only *as needed* to call attention to specific areas that should be focused on

© 2019 The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited 18-3288-11.

MITRE

Heatmaps: Avoiding Red

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



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	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		Bash History	Application Window Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	LSASS Driver		Extra Window Memory Injection		Brute Force	Browser Bookmark Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Trap		Process Injection		Credential Dumping	Domain Trust Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Other Network Medium	Disk Structure Wipe
Spearphishing Attachment	AppleScript	DLL Search Order Hijacking			Credentials in Files	File and Directory Discovery	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	CMSTP	Image File Execution Options Injection			Credentials in Registry	Network Service Scanning	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Alternative Protocol	Firmware Corruption
Spearphishing via Service	Command-Line Interface	Plist Modification			Exploitation for Credential Access	Network Share Discovery	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Compiled HTML File	Valid Accounts			Forced Authentication	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	Control Panel Items	Accessibility Features		BITS Jobs	Hooking	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Resource Hijacking
Valid Accounts	Dynamic Data Exchange	AppCert DLLs		Clear Command History	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multiband Communication		Runtime Data Manipulation
	Execution through API	AppInit DLLs		CMSTP	Input Prompt	Process Discovery	Shared Webroot	Screen Capture	Multi-hop Proxy		Service Stop
	Execution through Module Load	Application Shimming		Code Signing	Kerberoasting	Query Registry	SSH Hijacking	Video Capture	Multilayer Encryption		Stored Data Manipulation
	Exploitation for Client Execution	Dylib Hijacking		Compiled HTML File	Keychain	Remote System Discovery	Taint Shared Content		Multi-Stage Channels		Transmitted Data Manipulation
	Graphical User Interface	File System Permissions Weakness		Component Firmware	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	Third-party Software		Port Knocking		
	InstallUtil	Hooking		Component Object Model Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools		
	Mshta	Launch Daemon		Control Panel Items	Private Keys	System Network Configuration Discovery	Windows Remote Management		Remote File Copy		
	PowerShell	New Service		DCShadow	Securityd Memory	System Network Connections Discovery			Standard Application Layer Protocol		
	Regsvcs/Regasm	Path Interception		Deobfuscate/Decode Files or Information	Two-Factor Authentication Interception	System Owner/User Discovery			Standard Cryptographic Protocol		
	Regsvr32	Port Monitors		Disabling Security Tools		System Service Discovery			Standard Non-Application Layer Protocol		
	Rundll32	Service Registry Permissions Weakness		DLL Side-Loading		System Time Discovery			Uncommonly Used Port		
	Scripting	Setuid and Setgid		Execution Guardrails		Virtualization/Sandbox Evasion			Web Service		
	Service Execution	Startup Items		Exploitation for Defense Evasion							
	Signed Binary Proxy Execution	Web Shell		File Deletion							
	Signed Script Proxy Execution	.bash_profile and .bashrc	Exploitation for Privilege Escalation	File Permissions Modification							
	Source	Account Manipulation	SID-History Injection	File System Logical Offsets							
		Authentication Package	Sudo								
		BITS Jobs	Sudo Caching								
		Bootkit									
		Browser Extensions									
		Screensaver		Process Doppelgänging							

A softer color palate 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***

© 2019 The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited 18-3288-11.

MITRE

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…

1. **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

2. **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

3. **<u>Remember: ATT&CK heatmaps are almost always approximations</u>**
   - 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

© 2019 The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited 18-3288-11.

MITRE

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

© 2019 The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited 18-3288-11.

MITRE

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

Legend

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

© 2019 The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited 18-3288-11.

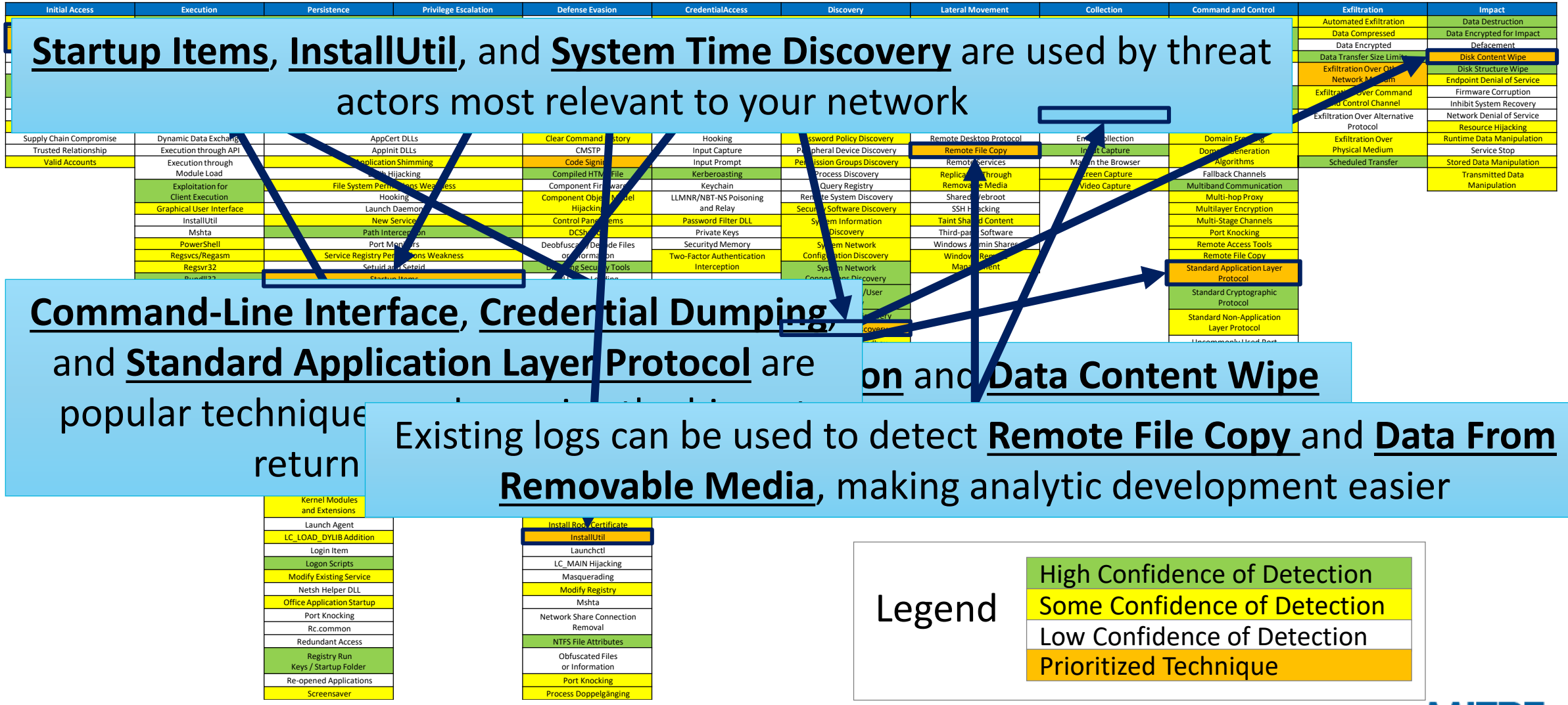
MITRE

Try to Focus Prioritization

Startup Items, **InstallUtil**, and **System Time Discovery** are used by threat actors most relevant to your network

Command-Line Interface, **Credential Dumping**, and **Standard Application Layer Protocol** are popular techniqu… return …on and **Data Content Wipe**

Existing logs can be used to detect **Remote File Copy** and **Data From Removable Media**, making analytic development easier



Legend

- High Confidence of Detection
- Some Confidence of Detection
- Low Confidence of Detection
- Prioritized Technique

© 2019 The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited 18-3288-11.

MITRE

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?

© 2019 The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited 18-3288-11.

MITRE

Give Tangible Recommendations

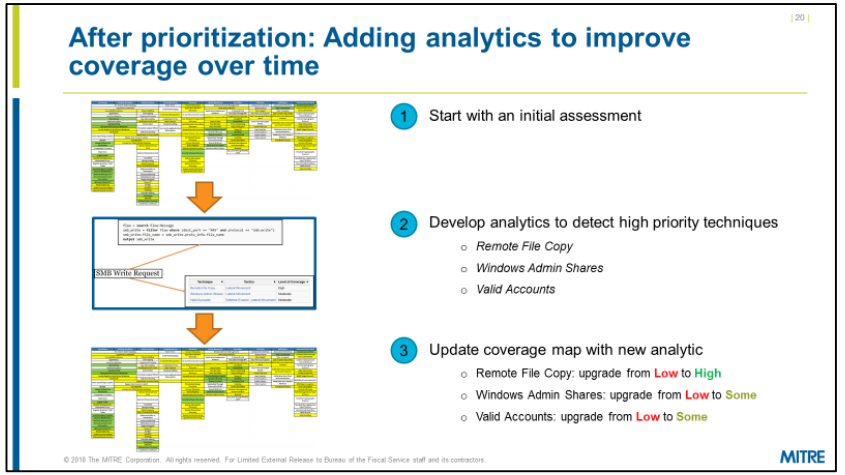
It's easy to give recommendations!

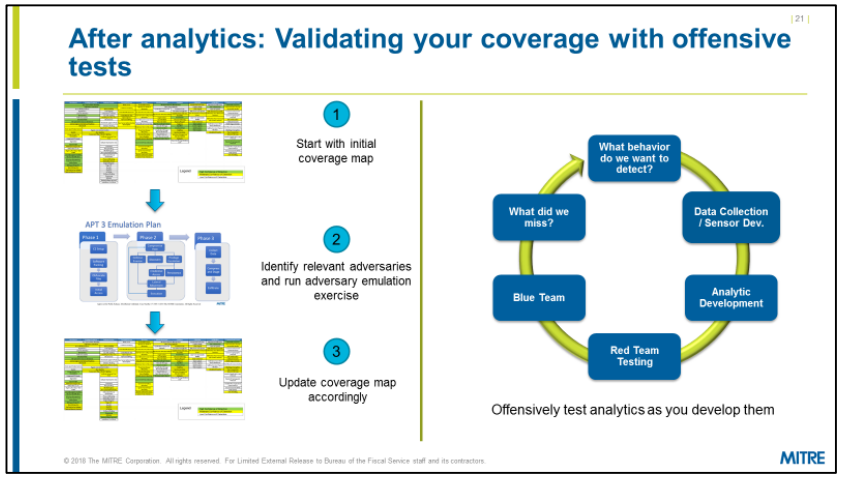
…but it's hard to give targeted ones

(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**

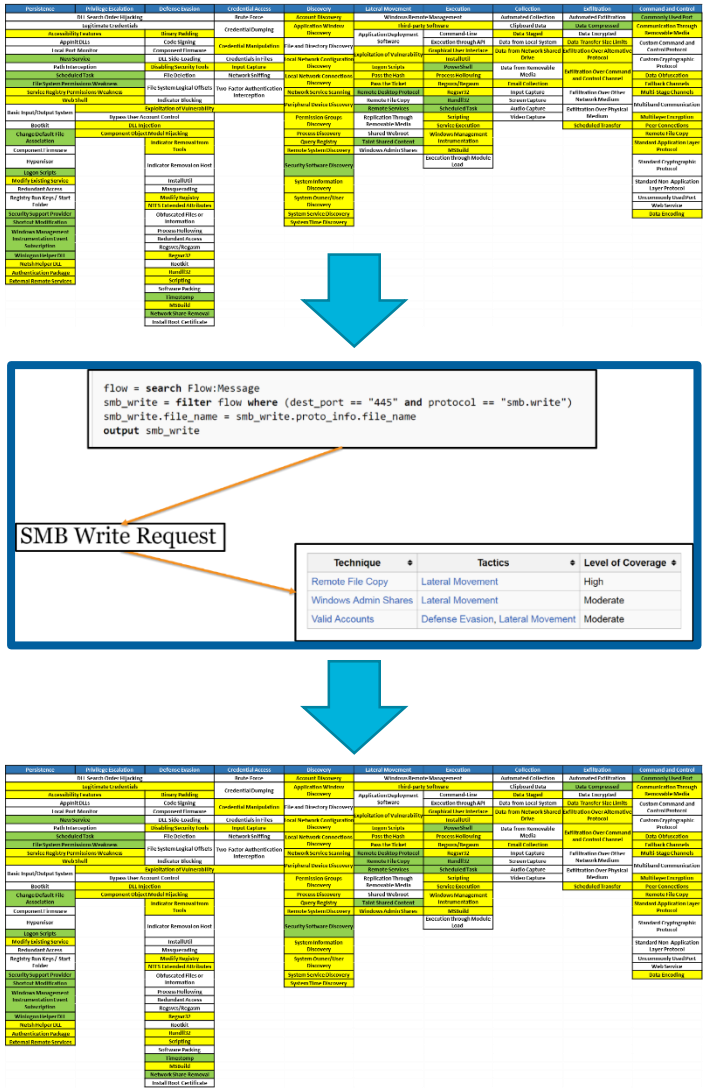




© 2019 The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited 18-3288-11.

MITRE

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**

© 2019 The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited 18-3288-11.

MITRE

Summary: Addressing Hard Challenges

Revisiting the Hard Problems

ATT&CK™
Adversarial Tactics, Techniques & Common Knowledge

SOC Survey Summary, SANS Security Operations Summit 2018
https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1532969860.pdf

© 2019 The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited 18-3288-11.

MITRE

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

© 2019 The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited 18-3288-11.

MITRE

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

© 2019 The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited 18-3288-11.

MITRE

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

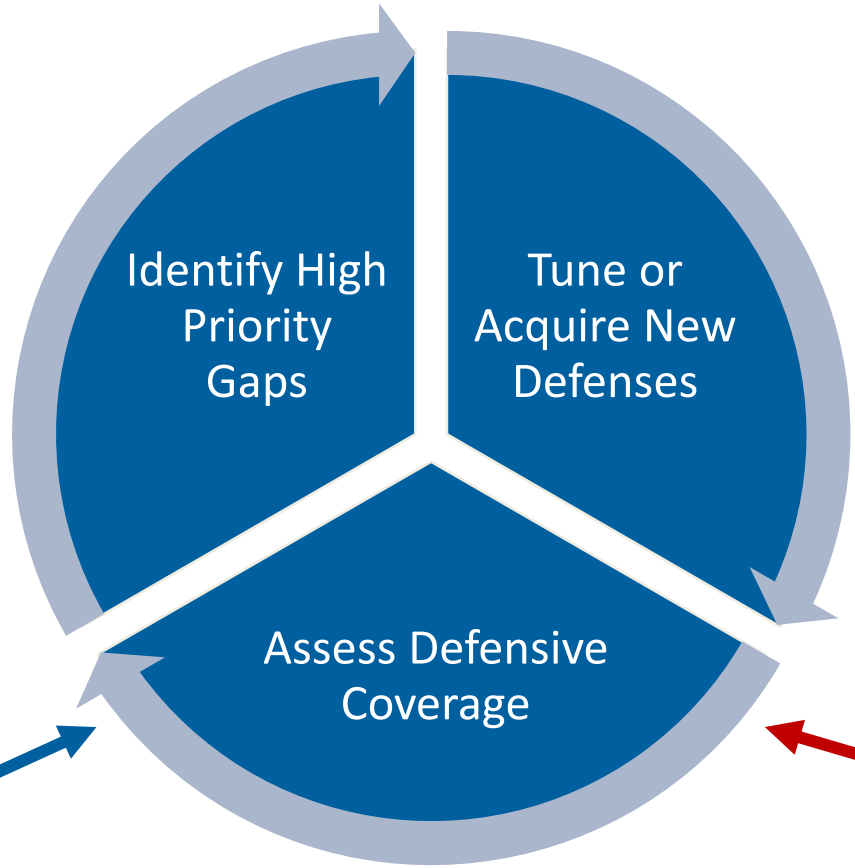
© 2019 The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited 18-3288-11.

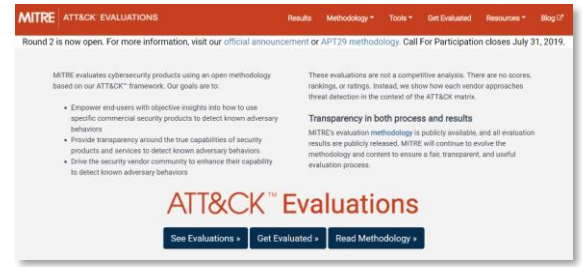
MITRE

Long-term: Following Up After an Assessment

ATT&CK™

- Relevant threat models
- Sightings data





- ATT&CK evaluations
- Public resources

ATT&CK-Based SOC Assessments

Adversary Emulation Exercises

ATT&CK™

Adversary behaviors

© 2019 The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited 18-3288-11.

MITRE

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 Evals**
  - https://attackevals.mitre.org/
- **ATT&CKcon**
  - https://www.mitre.org/attackcon
- **Blog**
  - https://medium.com/mitre-attack

© 2019 The MITRE Corporation. All rights reserved.

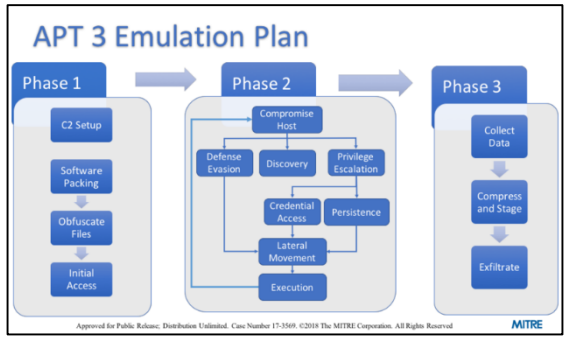
MITRE

Backup

© 2019 The MITRE Corporation. All rights reserved.

MITRE's Public ATT&CK Resources

Adversary Emulation Plans



attack.mitre.org/wiki/Adversary_Emulation_Plans

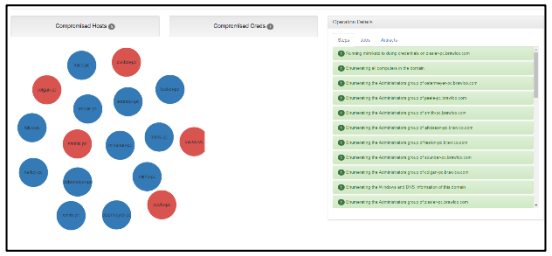
Public ATT&CK Knowledge Base

attack.mitre.org

ATT&CK Navigator

mitre.github.io/attack-navigator

CALDERA: Automated Adversary Emulation



https://github.com/mitre/caldera

Structured Content

STIX™

TAXII™

github.com/mitre/cti

cti-taxii.mitre.org

Conference Talks

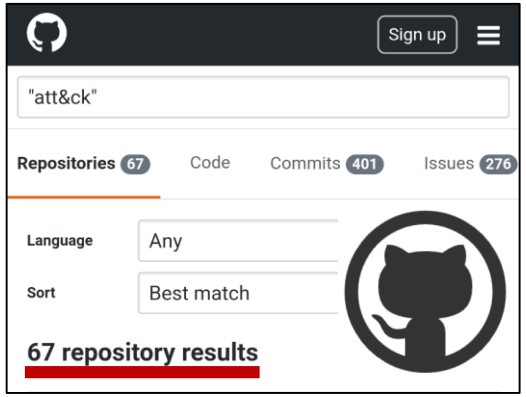
© 2019 The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited 18-3288-11.

MITRE

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 Loobeek, @leoloobeek
- 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

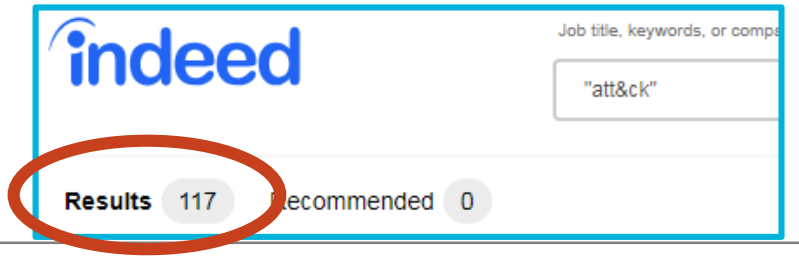


© 2019 The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited 18-3288-10.

MITRE

Who's using ATT&CK?

Job postings on Indeed as a proxy for usage



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

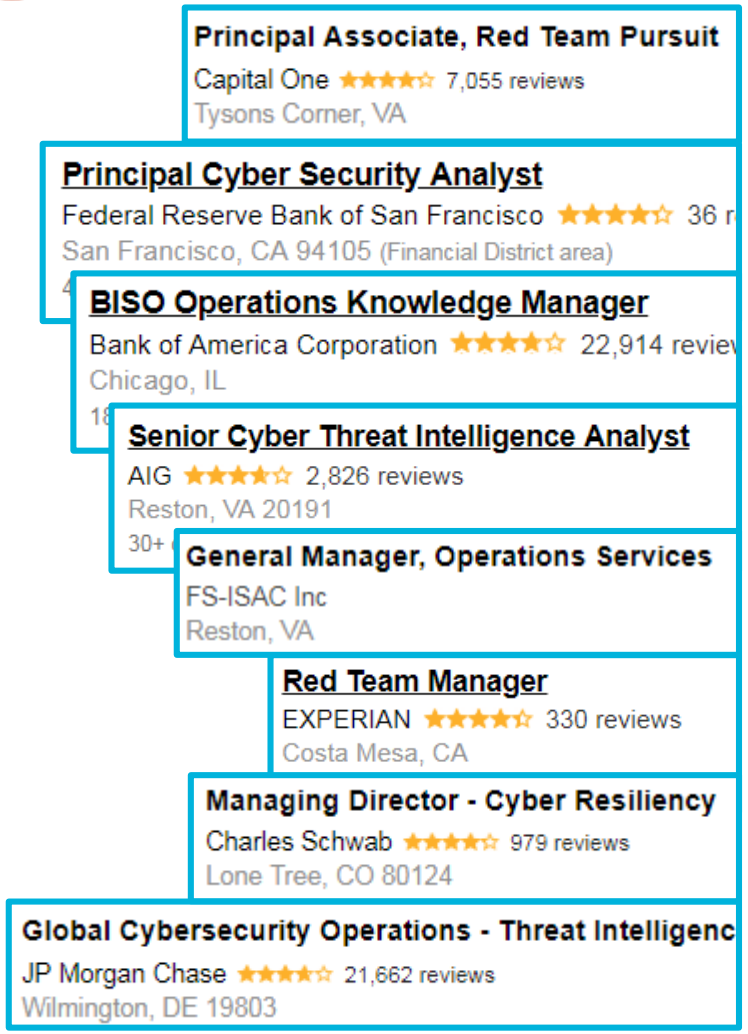
Retail
- Target
- Best Buy
- PepsiCo
- Under Armour

Defense
- Boeing
- Booz Allen
- Leidos

Media
- NBCUniversal
- Nielsen
- Cox
- Comcast

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

...and others!



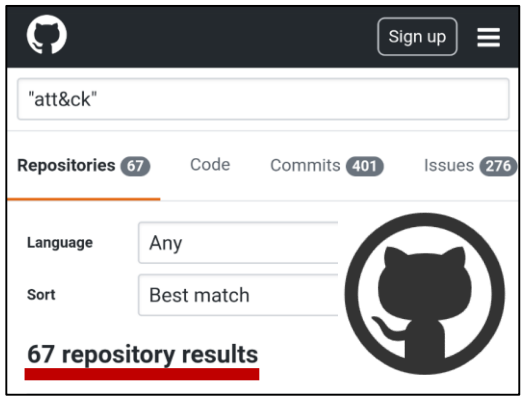
© 2019 The MITRE Corporation. All rights reserved.

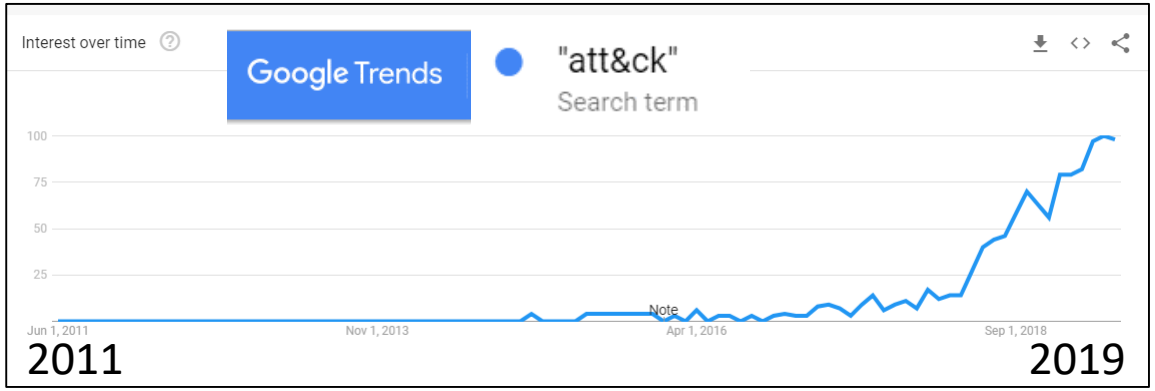
MITRE

ATT&CK in the Community

89 individuals + orgs contributing to ATT&CK!

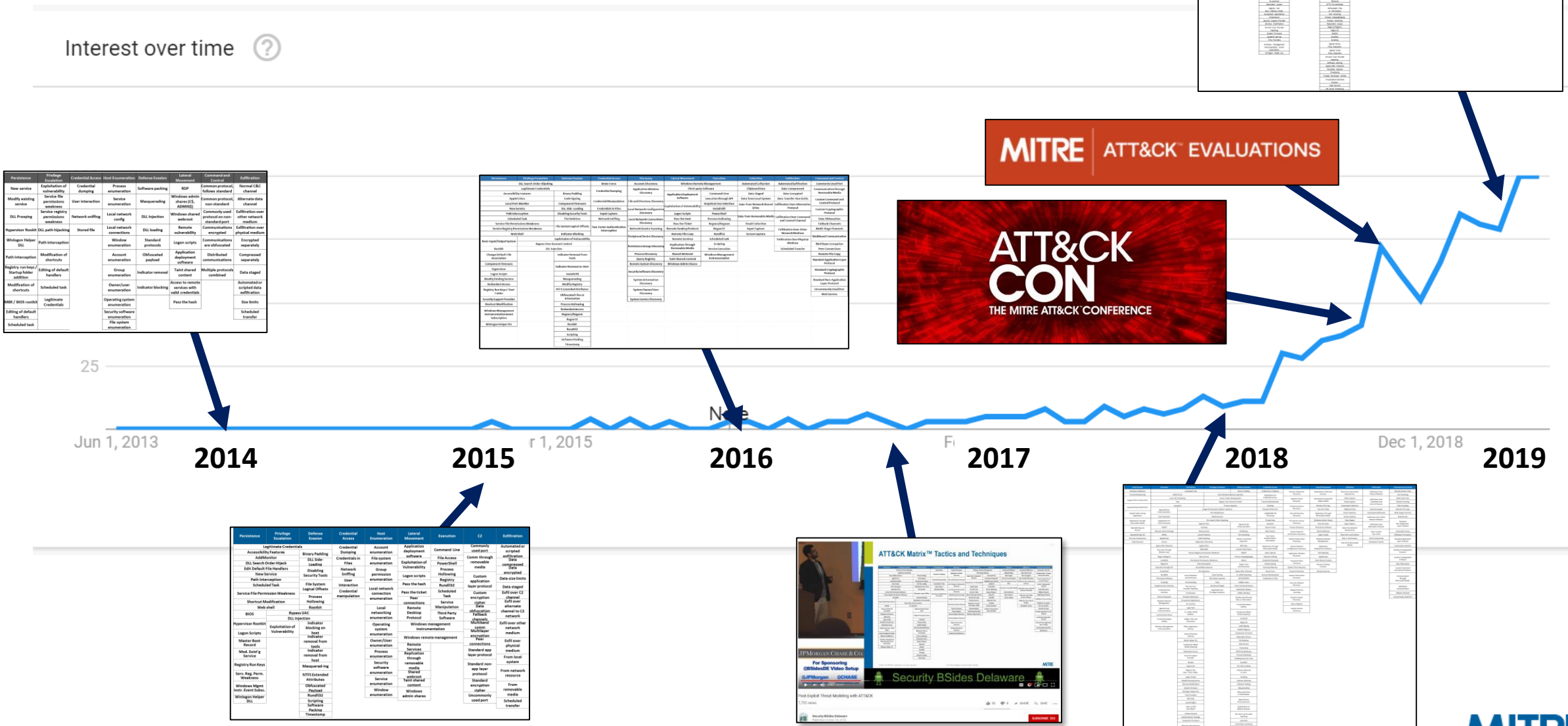
- Alain Homewood, Insomnia Security
- Alan Neville, @abnev
- Anastasios Pingios
- Andrew Smith, @jakx_
- Barry Shteiman, Exabeam
- Bartosz Jerzman
- Bryan Lee
- Carlos Borges, CIP
- Casey Smith
- Christiaan Beek, @ChristiaanBeek
- Cody Thomas, SpecterOps
- Craig Aitchison
- Daniel Oakley
- Darren Spruell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





© 2019 The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited 18-3288-10.

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



© 2019 The MITRE Corporation. All rights reserved.

MITRE