From MITRE ATT&CK to Threat-Informed Defense

A community driven approach to advancing threat-informed defense

Jon Baker

May 24, 2023

MITRE ENGENUITY™ | Center for Threat Informed Defense

about me

Co-founder & Director of the Center for Threat-Informed Defense @ MITRE Engenuity

Former Department Manager - responsible MITRE’s Cyber Threat Intel and Adversary Emulation work program.

Led MITRE’s security automation work – CVE, OVAL, CPE, MAEC, CAPEC…

Started out as a software engineer

Working in the public interest to advance cybersecurity for all

MITRE ENGENUITY™ | Center for Threat Informed Defense

“Solving problems for a safer world”

MITRE	MITRE ENGENUITY™
Non-profit corporation	Subsidiary non-profit of MITRE
Founded in 1958	Founded in 2019
Operates in the public interest	Operates in the public interest
Primarily focused on US Government	Focused on global private sector
Creator of major cybersecurity public resources including CVE and ATT&CK	Home of the Center for Threat-Informed Defense, MITRE ATT&CK Defender and ATT&CK Evaluations programs

What is MITRE ATT&CK?

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Active Scanning	Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Adversary-in-the-Middle	Account Discovery	Exploitation of Remote Services	Adversary-in-the-Middle	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Gather Victim Host Information	Compromise Accounts	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Brute Force	Application Window Discovery	Internal Spearphishing	Archive Collected Data	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information	Compromise Infrastructure	External Remote Services	Deploy Container	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	BITS Jobs	Credentials from Password Stores	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Gather Victim Network Information	Develop Capabilities	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Build Image on Host	Exploitation for Credential Access	Container and Resource Discovery	Remote Service Session Hijacking	Automated Collection	Data Obfuscation	Exfiltration Over C2 Channel	Data Manipulation
Gather Victim Org Information	Establish Accounts	Phishing	Inter-Process Communication	Browser Extensions	Create or Modify System Process	Deobfuscate/Decode Files or Information	Forced Authentication	Domain Trust Discovery	Remote Services	Browser Session Hijacking	Dynamic Resolution	Exfiltration Over Other Network Medium	Defacement
Phishing for Information	Obtain Capabilities	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification	Deploy Container	Forge Web Credentials	File and Directory Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel	Exfiltration Over Physical Medium	Disk Wipe
Search Closed Sources	Stage Capabilities	Supply Chain Compromise	Scheduled Task/Job	Create Account	Escape to Host	Direct Volume Access	Input Capture	Group Policy Discovery	Software Deployment Tools	Data from Configuration Repository	Fallback Channels	Exfiltration Over Web Service	Endpoint Denial of Service
Search Open Technical Databases		Trusted Relationship	Shared Modules	Create or Modify System Process	Event Triggered Execution	Domain Policy Modification	Modify Authentication Process	Network Service Scanning	Taint Shared Content	Data from Information Repositories	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains		Valid Accounts	Software Deployment Tools	Event Triggered Execution	Exploitation for Privilege Escalation	Execution Guardrails	Network Sniffing	Network Share Discovery	Use Alternate Authentication Material	Data from Local System	Multi-Stage Channels		Inhibit System Recovery
Search Victim-Owned Websites			System Services	External Remote Services	Hijack Execution Flow	Exploitation for Defense Evasion	OS Credential Dumping	Network Sniffing		Data from Network Shared Drive	Non-Application Layer Protocol		Network Denial of Service
			User Execution	Hijack Execution Flow	Process Injection	File and Directory Permissions Modification	Steal or Forge Kerberos Tickets	Password Policy Discovery		Data from Removable Media	Non-Standard Port		Resource Hijacking
			Windows Management Instrumentation	Implant Internal Image	Scheduled Task/Job	Hide Artifacts	Steal Web Session Cookie	Peripheral Device Discovery		Data Staged	Protocol Tunneling		Service Stop
				Modify Authentication Process	Valid Accounts	Hijack Execution Flow	Two-Factor Authentication Interception	Permission Groups Discovery		Email Collection	Proxy		System Shutdown/Reboot
				Office Application Startup		Impair Defenses	Unsecured Credentials	Process Discovery		Input Capture	Remote Access Software		
				Pre-OS Boot		Indicator Removal on Host		Query Registry		Screen Capture	Traffic Signaling		
				Scheduled Task/Job		Indirect Command Execution		Remote System Discovery		Video Capture	Web Service		
				Server Software Component		Masquerading		Software Discovery					
				Traffic Signaling		Modify Authentication Process		System Information Discovery					
				Valid Accounts		Modify Registry		System Location Discovery					
						Modify System Image		System Network Configuration Discovery					
						Network Boundary Bridging							
						Obfuscated Files or Information							
						Pre-OS Boot							
						Process Injection							
						Reflective Code Loading							
						Rogue Domain Controller							
						Rootkit							
						Signed Binary Proxy Execution							
						Signed Script Proxy Execution							
						Subvert Trust Controls							
						Template Injection							
						Traffic Signaling							
						Trusted Developer Utilities Proxy Execution							
						Use Alternate Authentication Material							
						Valid Accounts							
						Virtualization/Sandbox Evasion							
						Weaken Encryption							
						XSL Script Processing							

ATT&CK®

A community-driven knowledgebase of adversary TTPs

MITRE ENGENUITY | Center for Threat Informed Defense

Poll: Describe your organization’s use of ATT&CK:

a) We are new to ATT&CK

b) We considering or plan to use ATT&CK

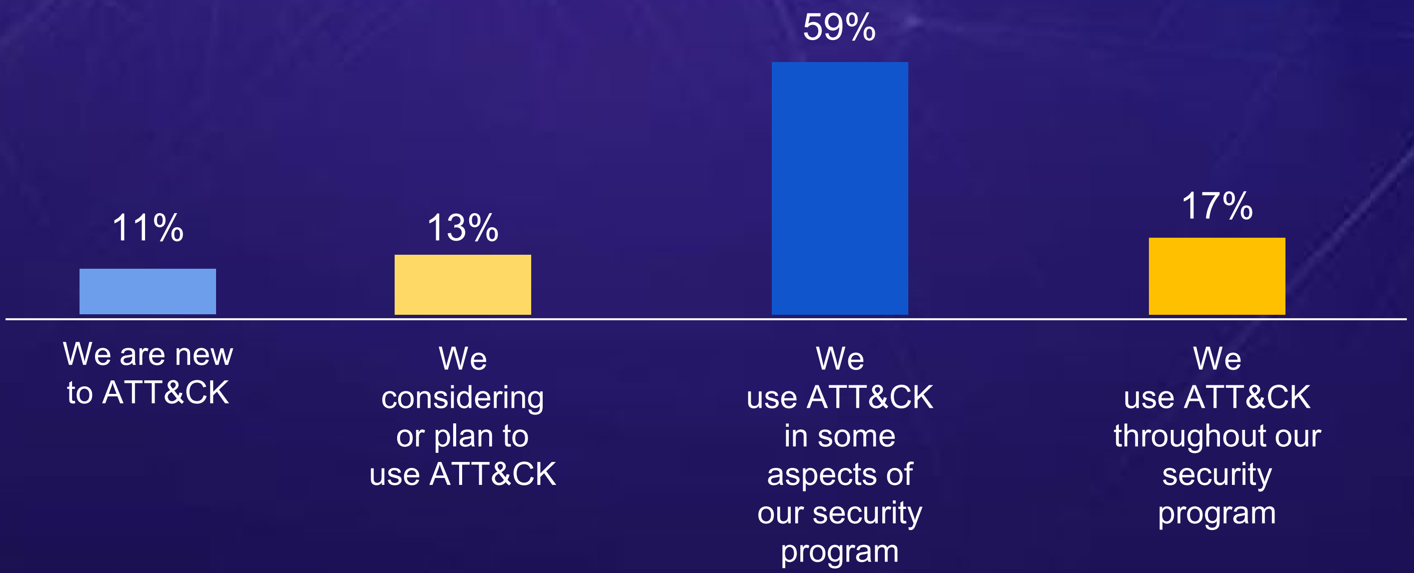
c) We use ATT&CK in some aspects of our security program

d) We use ATT&CK throughout our security program

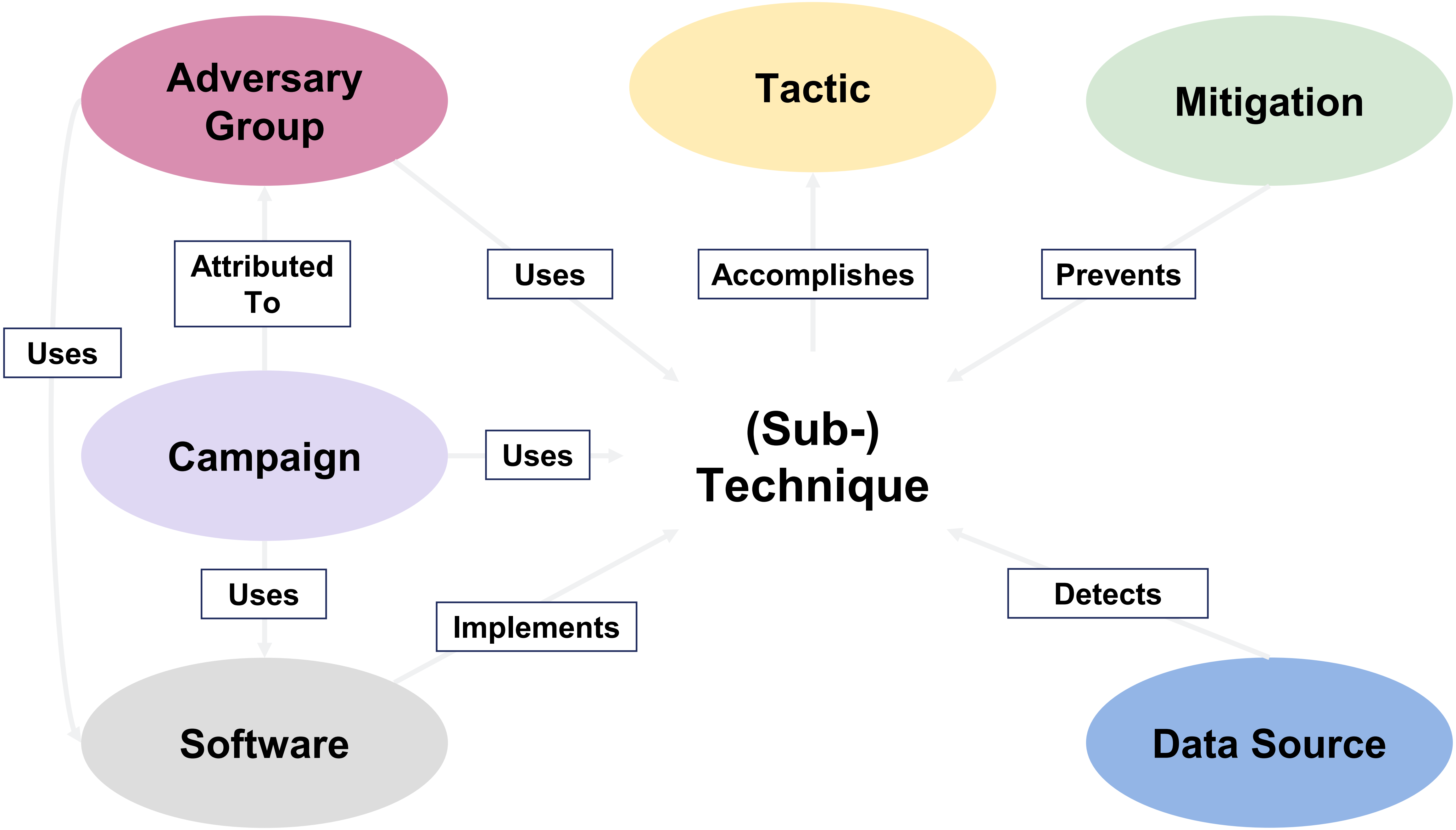
MITRE ENGENUITY

Center for Threat Informed Defense

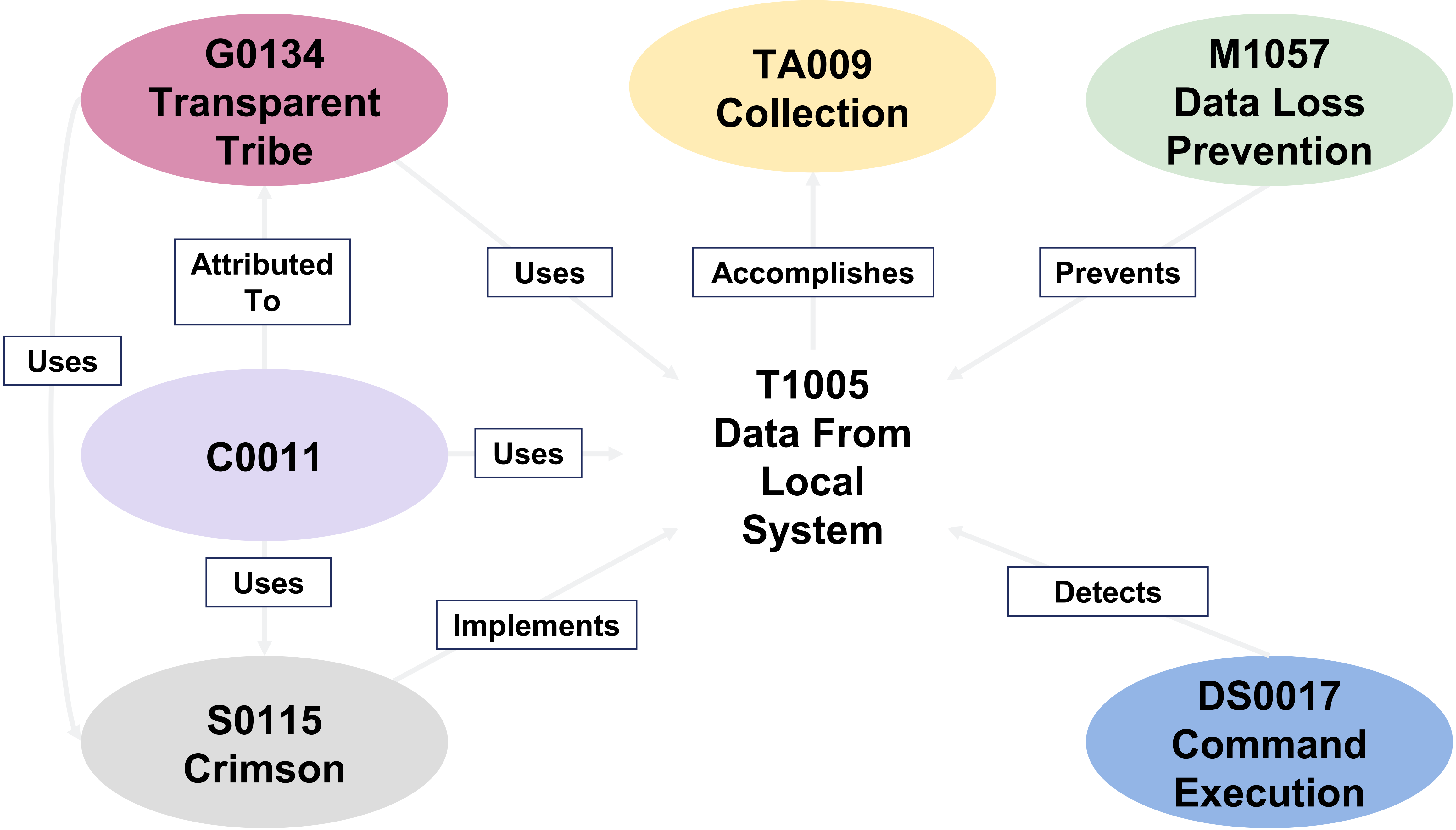
Poll Results: Describe your organization's use of ATT&CK:



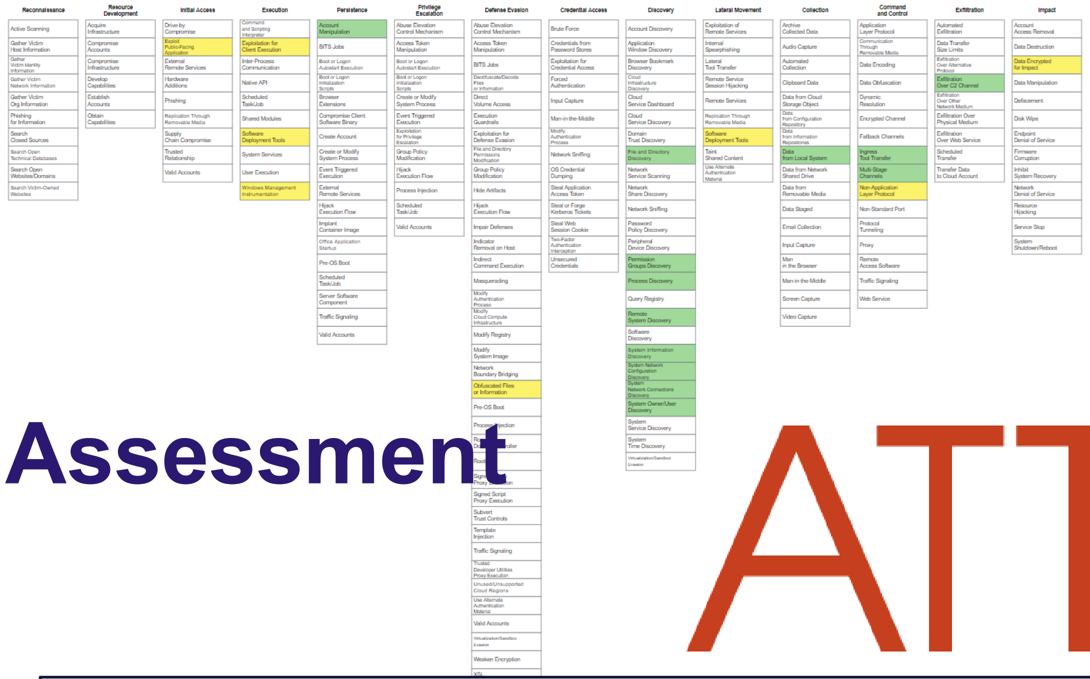
MITRE ENGENUITY™ | Center for Threat Informed Defense



MITRE ENGENUITY | Center for Threat Informed Defense



MITRE ENGENUITY | Center for Threat Informed Defense

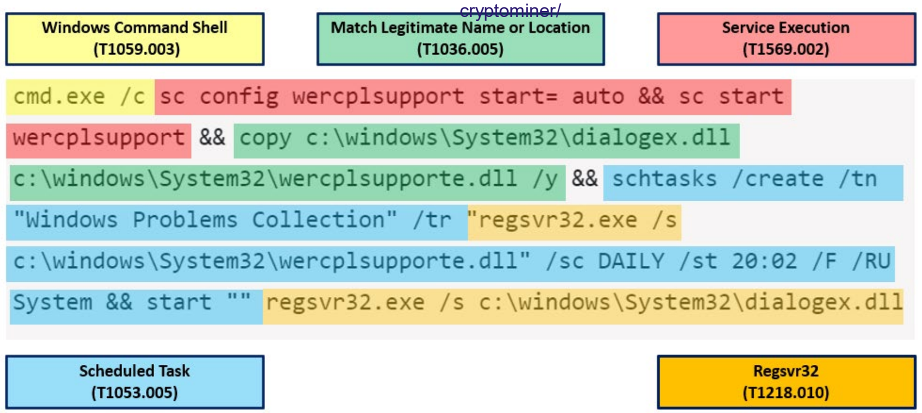

Reconnaissance
Resource Development
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command and Control
Exfiltration
Impact

Assessment

ATT&CK

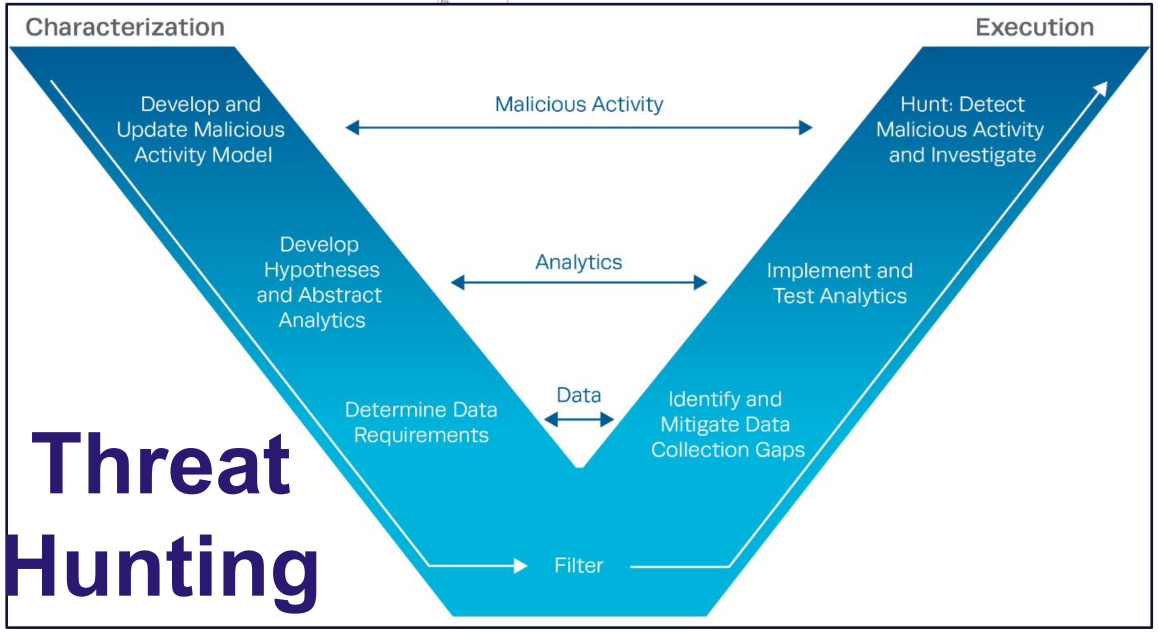
Cyber Threat Intel

https://redcanary.com/blog/blue-mockingbird-cryptominer/

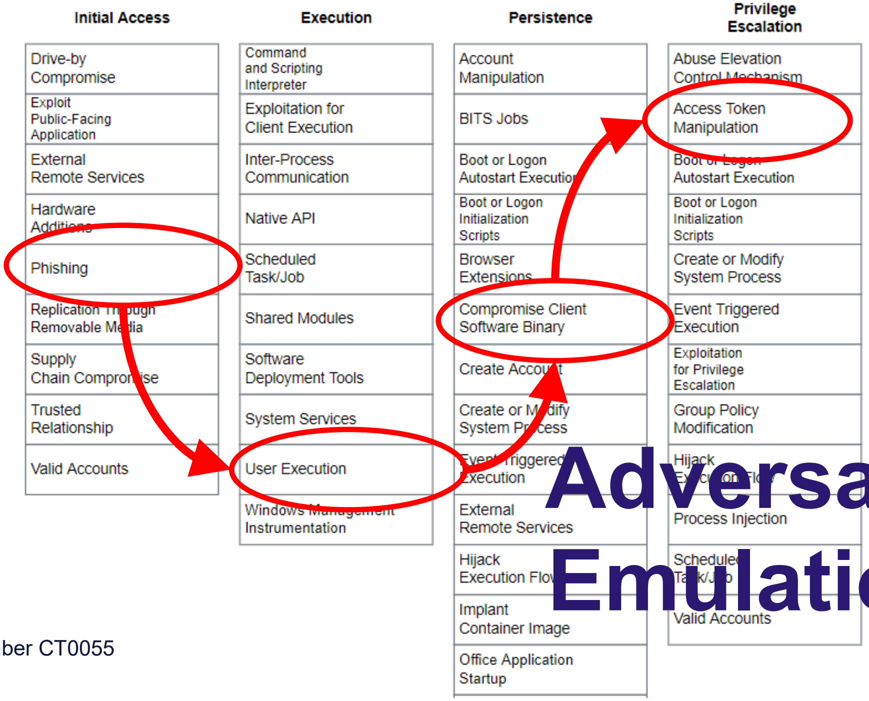

Windows Command Shell (T1059.003)
Match Legitimate Name or Location (T1036.005)
Service Execution (T1569.002)
Scheduled Task (T1053.005)
Regsvr32 (T1218.010)

```
cmd.exe /c sc config wercplsupport start= auto && sc start
wercplsupport && copy c:\windows\System32\dialogex.dll
c:\windows\System32\wercplsupporte.dll /y && schtasks /create /tn
"Windows Problems Collection" /tr "regsvr32.exe /s
c:\windows\System32\wercplsupporte.dll" /sc DAILY /st 20:02 /F /RU
System && start "" regsvr32.exe /s c:\windows\System32\dialogex.dll
```

Threat Hunting

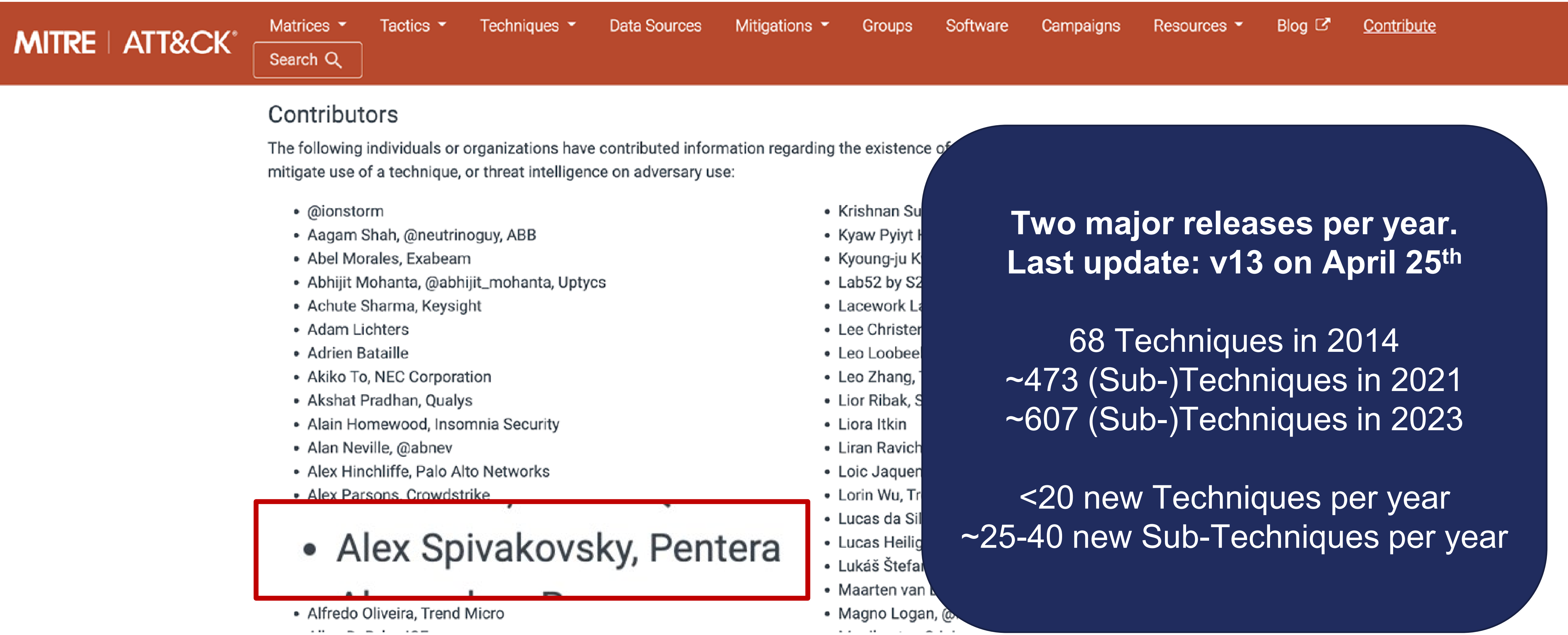

Characterization
Execution
Develop and Update Malicious Activity Model
Malicious Activity
Hunt: Detect Malicious Activity and Investigate
Develop Hypotheses and Abstract Analytics
Analytics
Implement and Test Analytics
Determine Data Requirements
Data
Identify and Mitigate Data Collection Gaps
Filter

Adversary Emulation



Initial Access	Execution	Persistence	Privilege Escalation
Drive-by Compromise	Command and Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation
External Remote Services	Inter-Process Communication	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution
Hardware Additions	Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts
Phishing	Scheduled Task/Job	Browser Extensions	Create or Modify System Process
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution
Supply Chain Compromise	Software Deployment Tools	Create Account	Exploitation for Privilege Escalation
Trusted Relationship	System Services	Create or Modify System Process	Group Policy Modification
Valid Accounts	User Execution	Event Triggered Execution	Hijack Execution Flow
	Windows Management Instrumentation	External Remote Services	Process Injection
		Hijack Execution Flow	Scheduled Task/Job
		Implant Container Image	Valid Accounts
		Office Application Startup	

ATT&CK is community driven



Contributors

The following individuals or organizations have contributed information regarding the existence of mitigate use of a technique, or threat intelligence on adversary use:

- @ionstorm
- Aagam Shah, @neutrinoguy, ABB
- Abel Morales, Exabeam
- Abhijit Mohanta, @abhijit_mohanta, Uptycs
- Achute Sharma, Keysight
- Adam Lichters
- Adrien Bataille
- Akiko To, NEC Corporation
- Akshat Pradhan, Qualys
- Alain Homewood, Insomnia Security
- Alan Neville, @abnev
- Alex Hinchliffe, Palo Alto Networks
- Alex Parsons, Crowdstrike
- Alex Spivakovsky, Pentera
- Alfredo Oliveira, Trend Micro

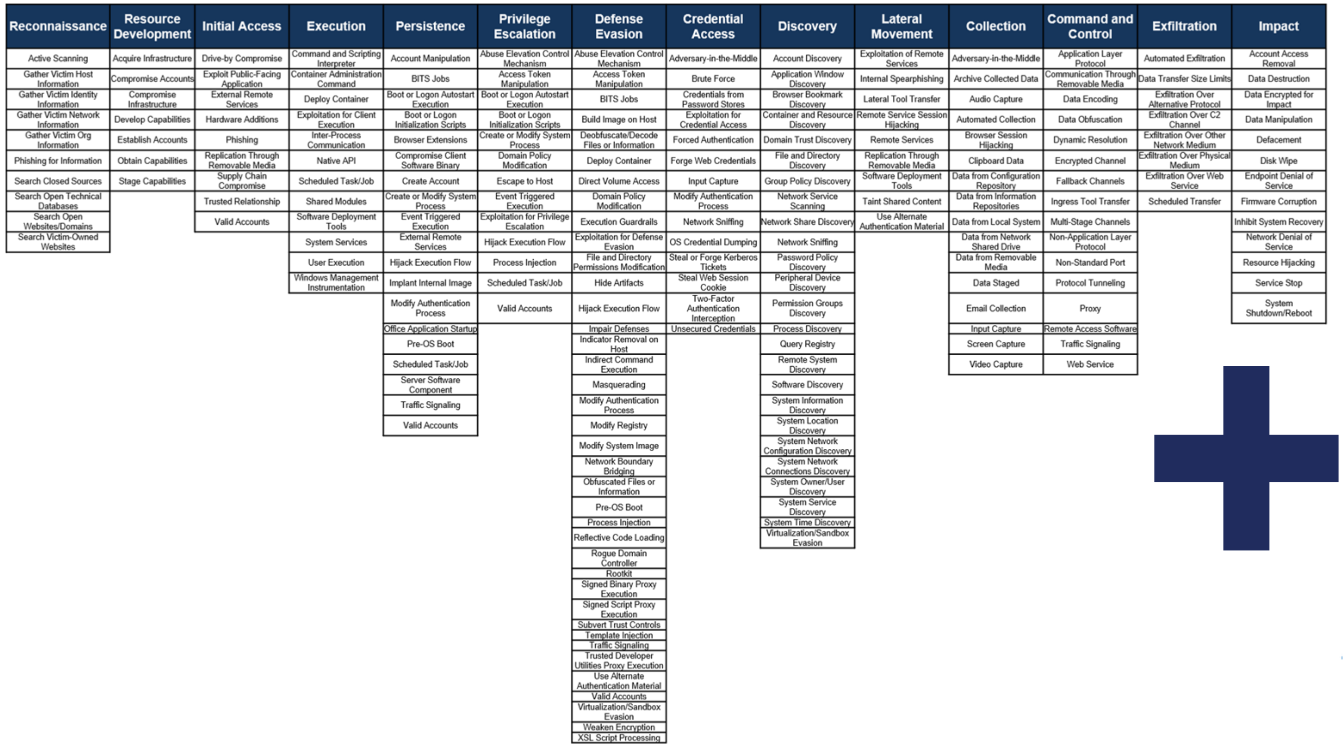
- Krishnan Su
- Kyaw Pyiyt H
- Kyoung-ju K
- Lab52 by S2
- Lacework La
- Lee Christen
- Leo Loobeel
- Leo Zhang, T
- Lior Ribak, S
- Liora Itkin
- Liran Ravich
- Loic Jaquen
- Lorin Wu, Tr
- Lucas da Sil
- Lucas Heilig
- Lukáš Štefa
- Maarten van
- Magno Logan, @

Two major releases per year.
Last update: v13 on April 25th

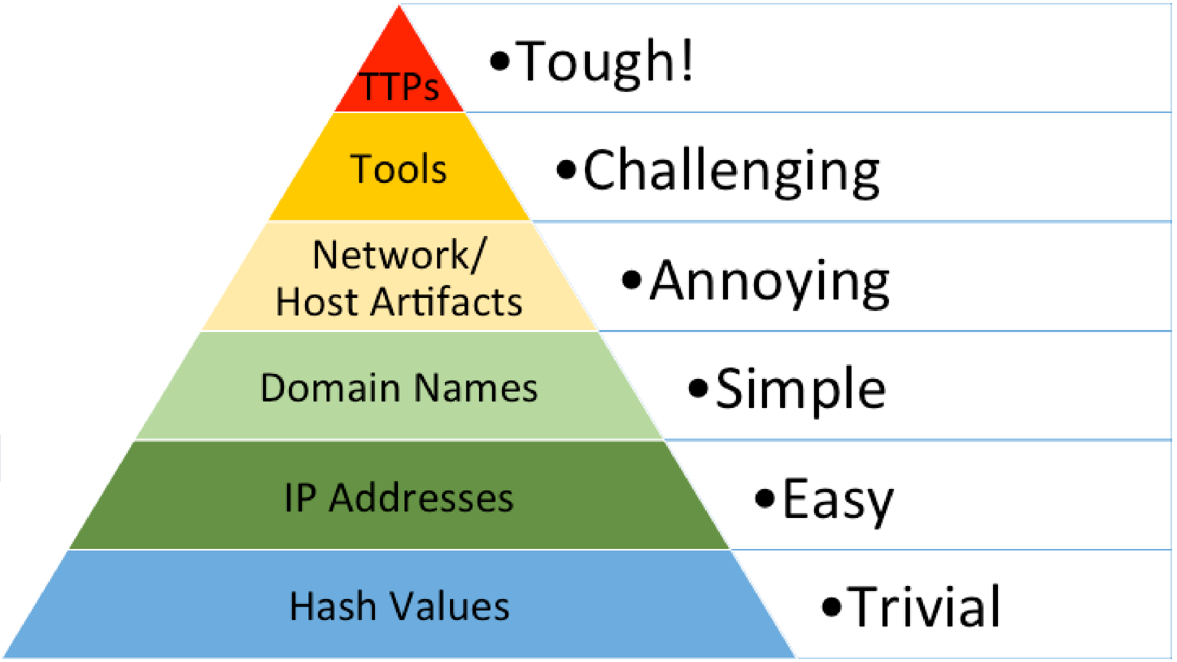
68 Techniques in 2014
~473 (Sub-)Techniques in 2021
~607 (Sub-)Techniques in 2023

<20 new Techniques per year
~25-40 new Sub-Techniques per year

MITRE ENGENUITY | Center for Threat Informed Defense



Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Active Scanning	Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Adversary-in-the-Middle	Account Discovery	Exploitation of Remote Services	Adversary-in-the-Middle	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Gather Victim Host Information	Compromise Accounts	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Brute Force	Application Window Discovery	Internal Spearphishing	Archive Collected Data	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information	Compromise Infrastructure	External Remote Services	Deploy Container	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	BITS Jobs	Credentials from Password Stores	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Gather Victim Network Information	Develop Capabilities	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Build Image on Host	Exploitation for Credential Access	Container and Resource Discovery	Remote Service Session Hijacking	Automated Collection	Data Obfuscation	Exfiltration Over C2 Channel	Data Manipulation
Gather Victim Org Information	Establish Accounts	Phishing	Inter-Process Communication	Browser Extensions	Create or Modify System Process	Deobfuscate/Decode Files or Information	Forced Authentication	Domain Trust Discovery	Remote Services	Browser Session Hijacking	Dynamic Resolution	Exfiltration Over Other Network Medium	Defacement
Phishing for Information	Obtain Capabilities	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification	Deploy Container	Forge Web Credentials	File and Directory Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel	Exfiltration Over Physical Medium	Disk Wipe
Search Closed Sources	Stage Capabilities	Supply Chain Compromise	Scheduled Task/Job	Create Account	Escape to Host	Direct Volume Access	Input Capture	Group Policy Discovery	Software Deployment Tools	Data from Configuration Repository	Fallback Channels	Exfiltration Over Web Service	Endpoint Denial of Service
Search Open Technical Databases		Trusted Relationship	Shared Modules	Create or Modify System Process	Event Triggered Execution	Domain Policy Modification	Modify Authentication Process	Network Service Scanning	Taint Shared Content	Data from Information Repositories	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains		Valid Accounts	Software Deployment Tools	Event Triggered Execution	Exploitation for Privilege Escalation	Execution Guardrails	Network Sniffing	Network Share Discovery	Use Alternate Authentication Material	Data from Local System	Multi-Stage Channels		Inhibit System Recovery
Search Victim-Owned Websites			System Services	External Remote Services	Hijack Execution Flow	Exploitation for Defense Evasion	OS Credential Dumping	Network Sniffing		Data from Network Shared Drive	Non-Application Layer Protocol		Network Denial of Service
			User Execution	Hijack Execution Flow	Process Injection	File and Directory Permissions Modification	Steal or Forge Kerberos Tickets	Password Policy Discovery		Data from Removable Media	Non-Standard Port		Resource Hijacking
			Windows Management Instrumentation	Implant Internal Image	Scheduled Task/Job	Hide Artifacts	Steal Web Session Cookie	Peripheral Device Discovery		Data Staged	Protocol Tunneling		Service Stop
				Modify Authentication Process	Valid Accounts	Hijack Execution Flow	Two-Factor Authentication Interception	Permission Groups Discovery		Email Collection	Proxy		System Shutdown/Reboot
				Office Application Startup		Impair Defenses	Unsecured Credentials	Process Discovery		Input Capture	Remote Access Software		
				Pre-OS Boot		Indicator Removal on Host		Query Registry		Screen Capture	Traffic Signaling		
				Scheduled Task/Job		Indirect Command Execution		Remote System Discovery		Video Capture	Web Service		
				Server Software Component		Masquerading		Software Discovery					
				Traffic Signaling		Modify Authentication Process		System Information Discovery					
				Valid Accounts		Modify Registry		System Location Discovery					
						Modify System Image		System Network Configuration Discovery					
						Network Boundary Bridging		System Network Connections Discovery					
						Obfuscated Files or Information		System Owner/User Discovery					
						Pre-OS Boot		System Service Discovery					
						Process Injection		System Time Discovery					
						Reflective Code Loading		Virtualization/Sandbox Evasion					
						Rogue Domain Controller							
						Rootkit							
						Signed Binary Proxy Execution							
						Signed Script Proxy Execution							
						Subvert Trust Controls							
						Template Injection							
						Traffic Signaling							
						Trusted Developer Utilities Proxy Execution							
						Use Alternate Authentication Material							
						Valid Accounts							
						Virtualization/Sandbox Evasion							
						Weaken Encryption							
						XSL Script Processing							



* Pyramid of Pain by David Bianco http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

ATT&CK and the “Pyramid of Pain”

A global shift towards increasing the cost for the adversary

Threat-Informed Defense

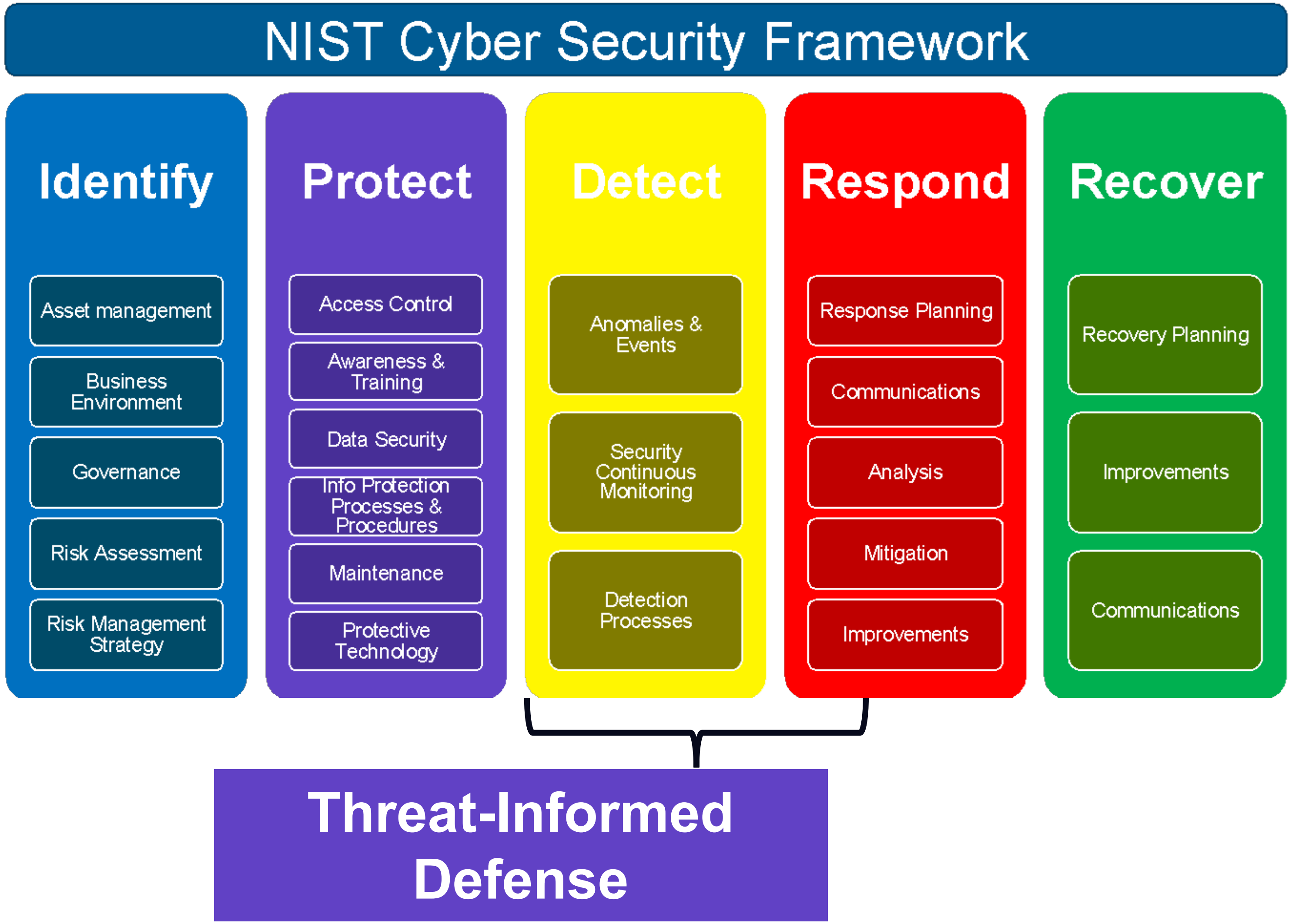
MITRE ENGENUITY

Center for Threat Informed Defense

What is Threat-Informed Defense?

The systematic application of a deep understanding of adversary tradecraft and technology to improve defenses.

Where does it fit?

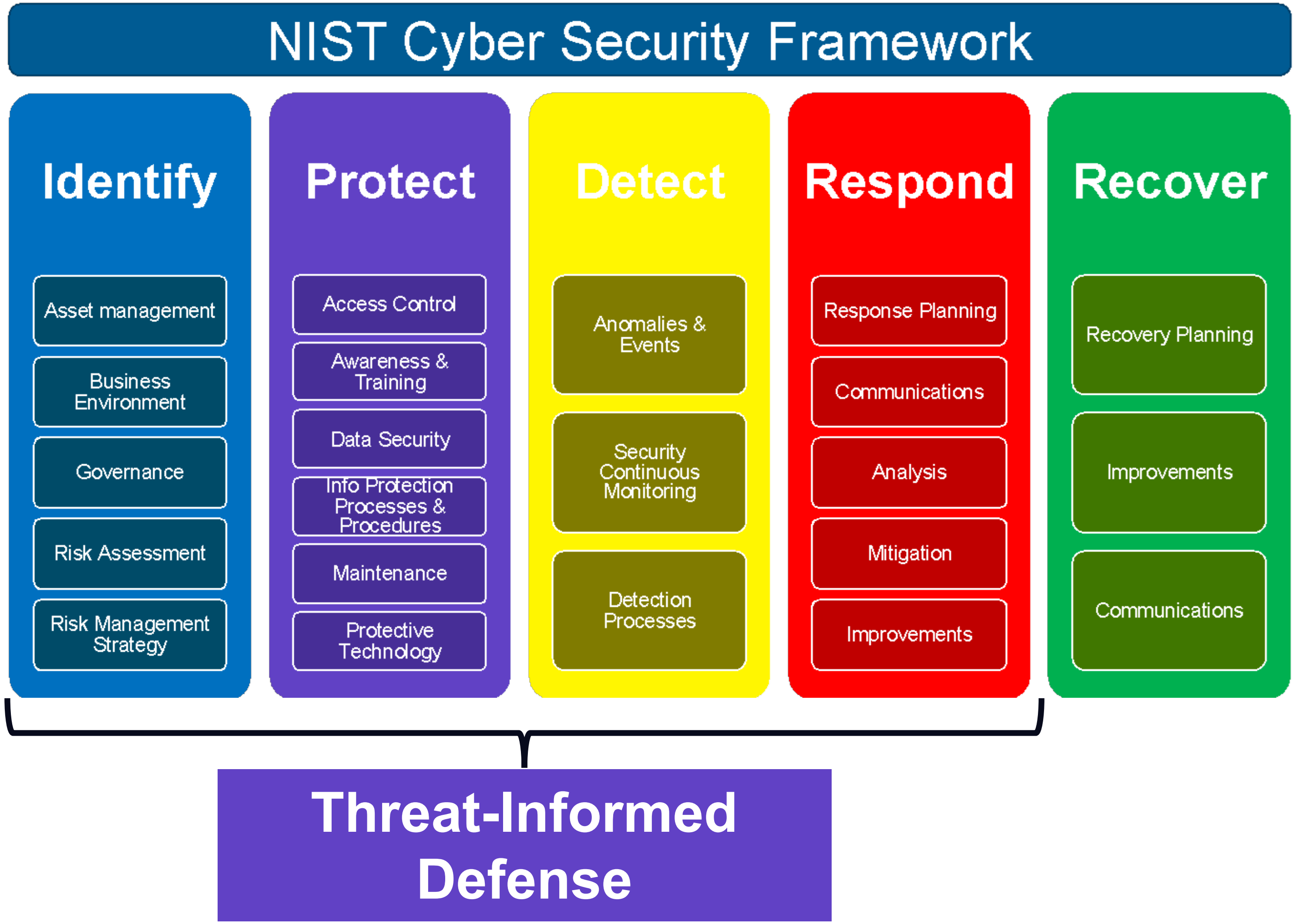


NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset management	Access Control	Anomalies & Events	Response Planning	Recovery Planning
Business Environment	Awareness & Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes & Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

Threat-Informed Defense

Where does it fit?

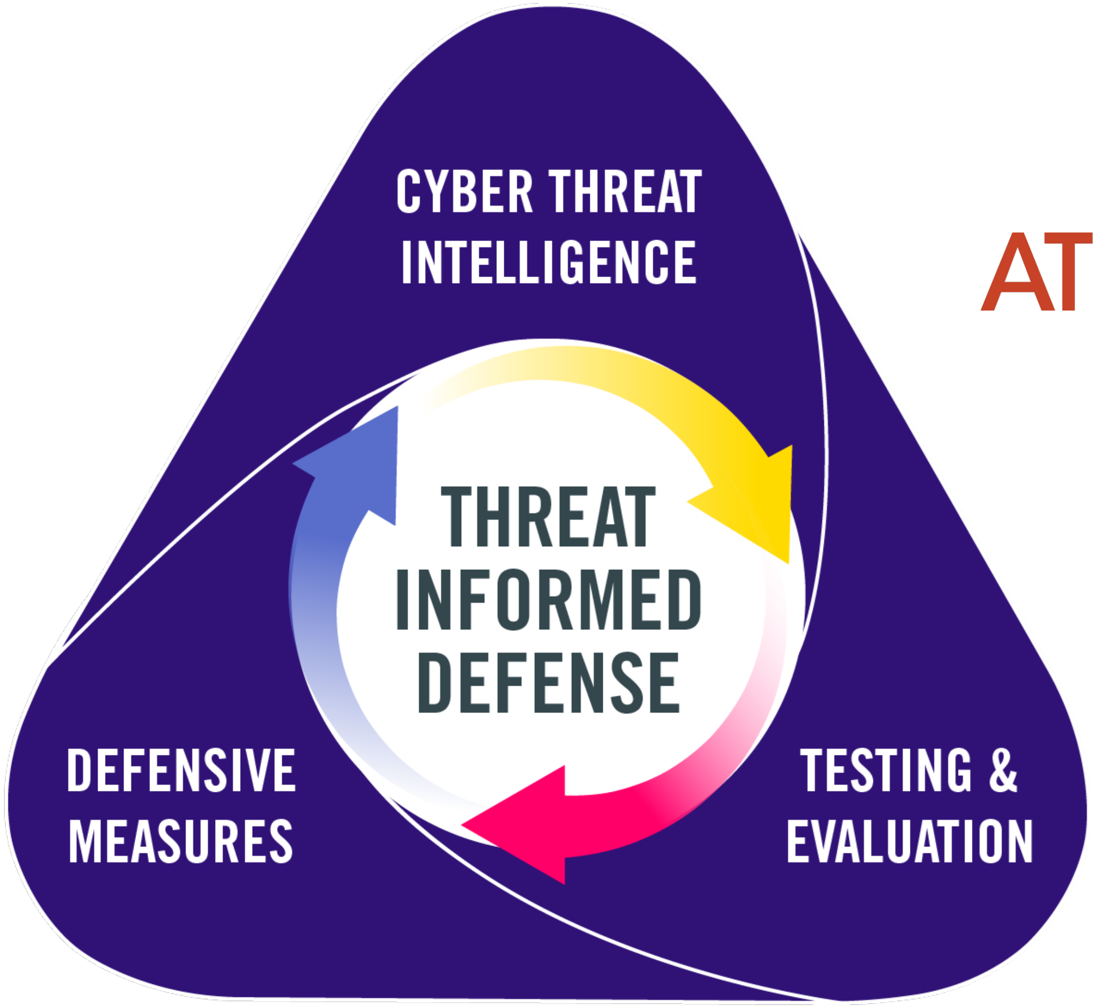


NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset management	Access Control	Anomalies & Events	Response Planning	Recovery Planning
Business Environment	Awareness & Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes & Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

Threat-Informed Defense

Threat-Informed Defense Cycle



ATT&CK® is at the core of threat-informed defense

Threat-informed defense is a continuous process.

As our defenses improve, our environments change, and adversaries evolve, the cycle continues.

Poll: Continual test & evaluation of your organization's defenses is…

a) a under consideration.

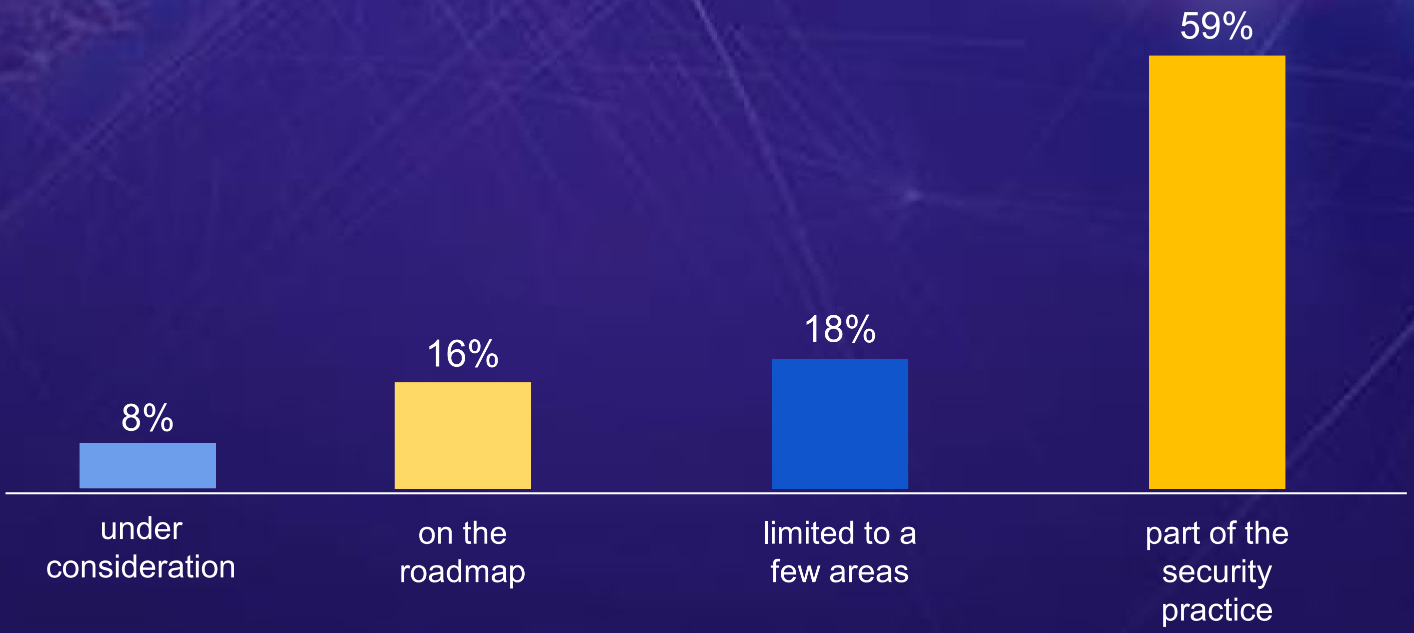
b) on the roadmap.

c) limited to a few areas.

d) part of the security practice.

MITRE ENGENUITY | Center for Threat Informed Defense

Poll Answer: Continual test & evaluation of your organization's defenses is…

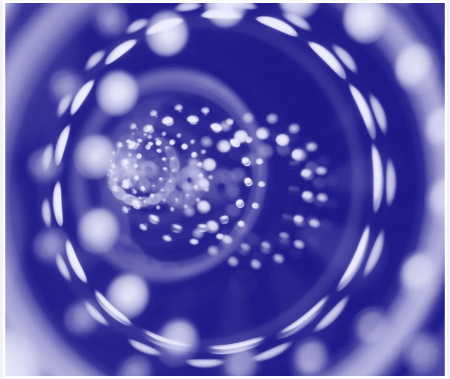


MITRE ENGENUITY
Center for Threat Informed Defense

Threat-Informed Defense is…

MITRE
ENGENUITY™

Center
for Threat
Informed
Defense



A lens, through which, you can understand your security posture

A way to think about your security architecture and operations

A way to prioritize your security strategy and investments

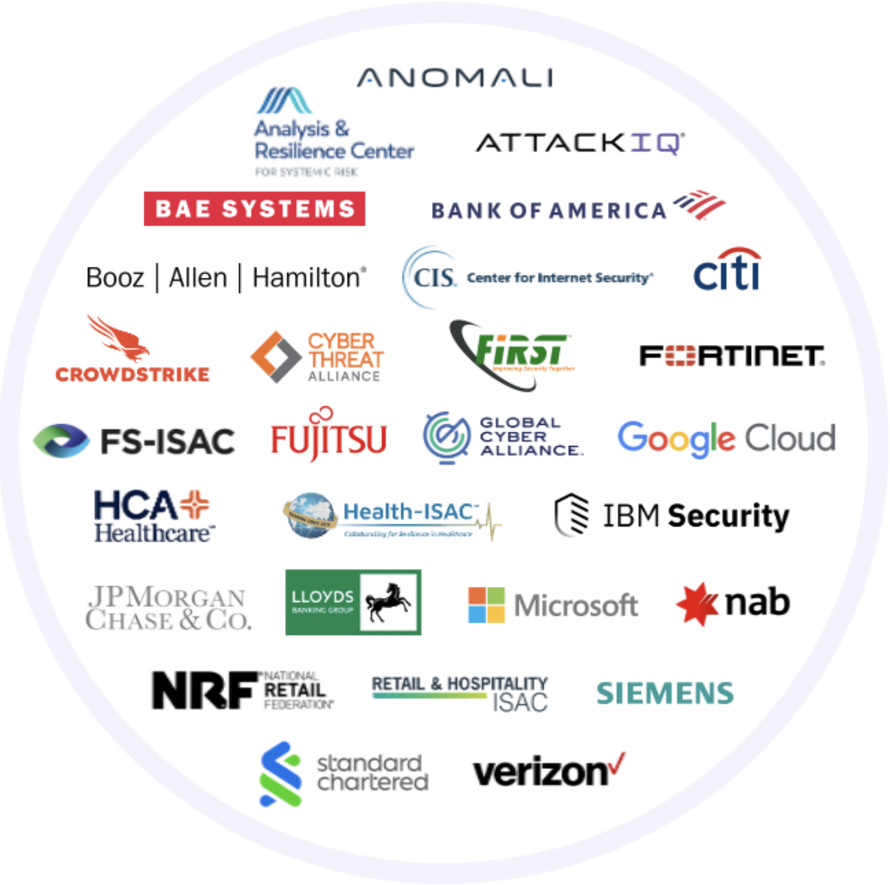
A way of assessing the effectiveness of your security investments

think like an attacker

How do we scale threat-informed defense?

The Center for Threat-Informed Defense conducts collaborative R&D projects that

improve cyber defense at scale



+

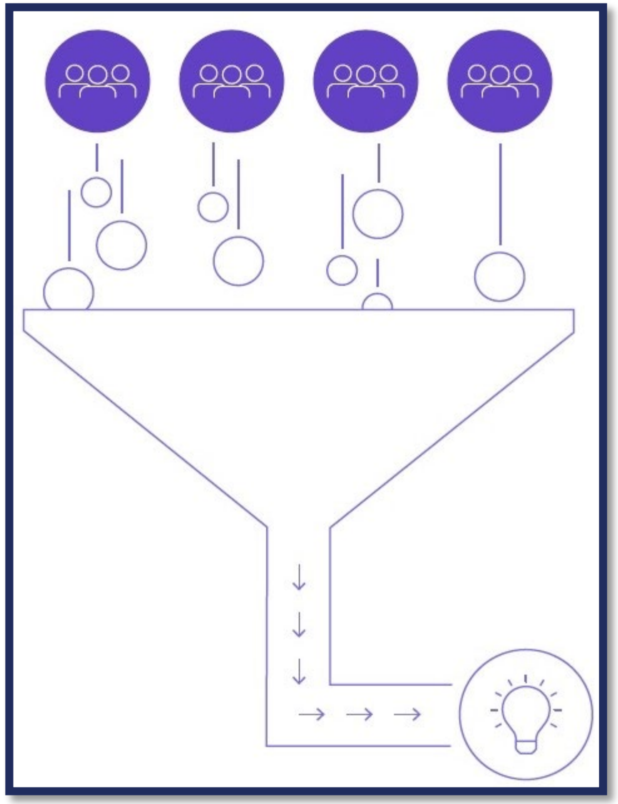
MITRE

SOLVING PROBLEMS
FOR A SAFER WORLD™

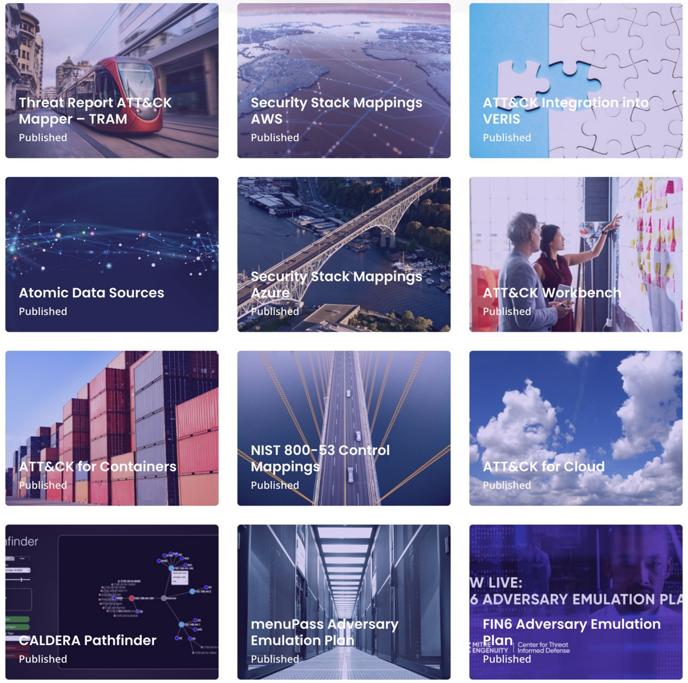
Membership is:

✓ Highly-sophisticated
✓ Global & cross-sector
✓ Non-governmental
✓ Committed to collaborative R&D in the public interest

A repeatable, scalable, approach to R&D built on **member-powered collaboration**



Systematically identify challenges



Threat Report ATT&CK Mapper – TRAM
Published

Security Stack Mappings AWS
Published

ATT&CK Integration into VERIS
Published

Atomic Data Sources
Published

Security Stack Mappings Azure
Published

ATT&CK Workbench
Published

ATT&CK for Containers
Published

NIST 800-53 Control Mappings
Published

ATT&CK for Cloud
Published

CALDERA Pathfinder
Published

menuPass Adversary Emulation Plan
Published

W LIVE:
6 ADVERSARY EMULATION PLA
FIN6 Adversary Emulation Plan
Published

Develop solutions together

MITRE ENGENUITY | Center for Threat Informed Defense

WHERE
DO I
START
?

Top ATT&CK Techniques

Problem

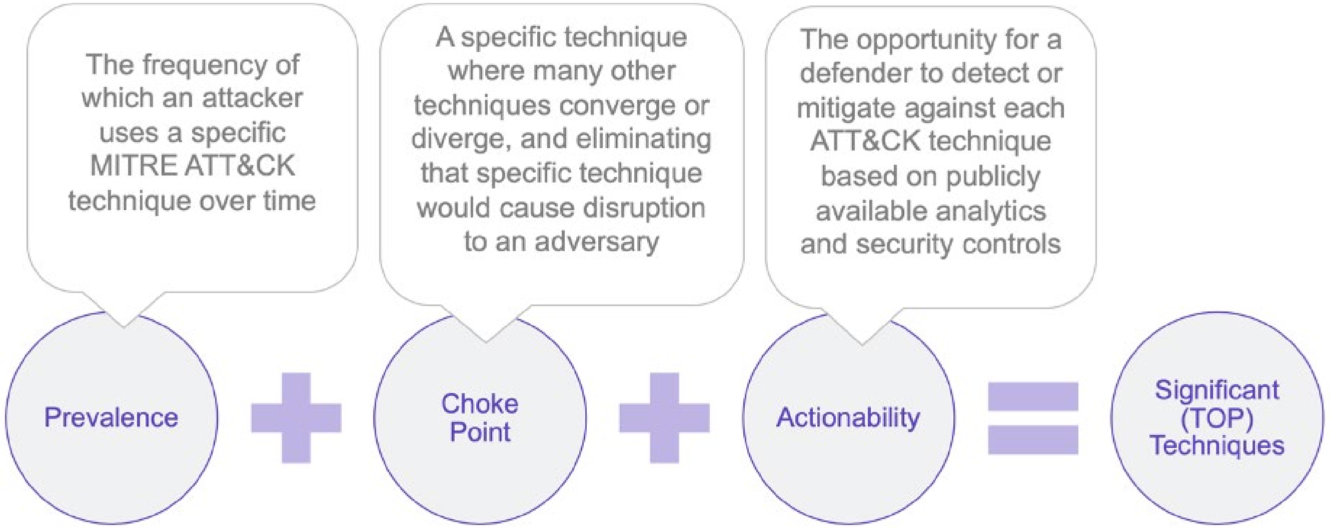
Defending against all ATT&CK techniques is simply not practical and, without guidance, determining which techniques to focus on is overwhelming.

Solution

Publish a methodology and tools to help defenders systematically prioritize ATT&CK techniques.

Impact

Defenders focus on the adversary behaviors that are most relevant to their organization and have the greatest effect on their security posture.



The frequency of which an attacker uses a specific MITRE ATT&CK technique over time

A specific technique where many other techniques converge or diverge, and eliminating that specific technique would cause disruption to an adversary

The opportunity for a defender to detect or mitigate against each ATT&CK technique based on publicly available analytics and security controls

Prevalence + Choke Point + Actionability = Significant (TOP) Techniques

https://top-attack-techniques.mitre-engenuity.org/

MITRE ENGENUITY | Center for Threat Informed Defense

Advance threat-informed defense with us

Center for Threat-Informed Defense

Spread the word to increase the impact of our work.

Use our work and tell us about it.

Check out the Impact Report

https://ctid.mitre-engenuity.org/impact-report/

Share your ideas to inform the R&D program.

Advance the research program by joining us.

Follow our R&D

https://ctid.mitre-engenuity.org/our-work/

MITRE ATT&CK: https://attack.mitre.org/

Free ATT&CK Training: https://mitre-engenuity.org/mad/

MITRE ENGENUITY | Center for Threat Informed Defense

Let’s change the game!

jbaker@mitre-engenuity.org

https://www.linkedin.com/in/jonathanobaker/

https://ctid.mitre-engenuity.org/

MITRE ENGENUITY

Center for Threat Informed Defense