



San Francisco | March 4–8 | Moscone Center



SESSION ID: AIR-T07

ATT&CK in Practice A Primer to Improve Your Cyber Defense

Freddy Dezeure

CEO
Freddy Dezeure BVBA
@Fdezeure
www.freddydezeure.eu

Rich Struse

Chief Strategist Cyber Threat Intelligence
MITRE
[@MITREattack](https://www.mitre.org)
attack.mitre.org

#RSAC

Who Are We?

Freddy Dezeure

- Founder and Head of CERT-EU from 2011-2017
- Independent strategic advisor
- Advisor/Board Member CoreLight, SpyCloud, Intel471, CMD, Arctic Security, KEYP
- Community contributor



Rich Struse

- Chief Advanced Technology Officer DHS NCCIC 2012-2017
- MITRE, CTI Chief Strategist
- Director Oasis, Co-chair CTI Technical Committee
- Community contributor

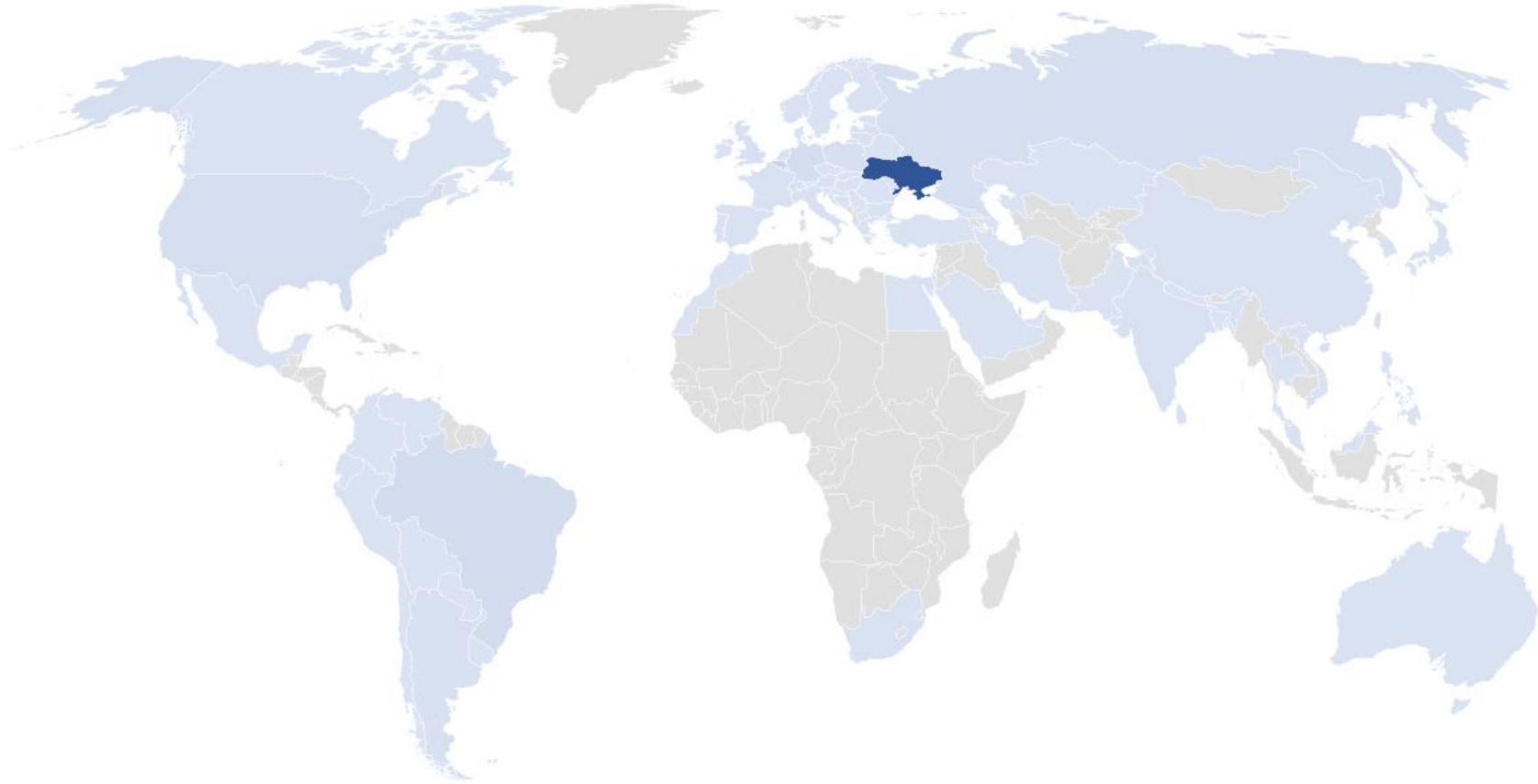


(Not)Petya



- June 2017
- Destructive intent
- Initial infection via accounting software
- Spreading using a leaked NSA tool

Geographic distribution of Petya encounters



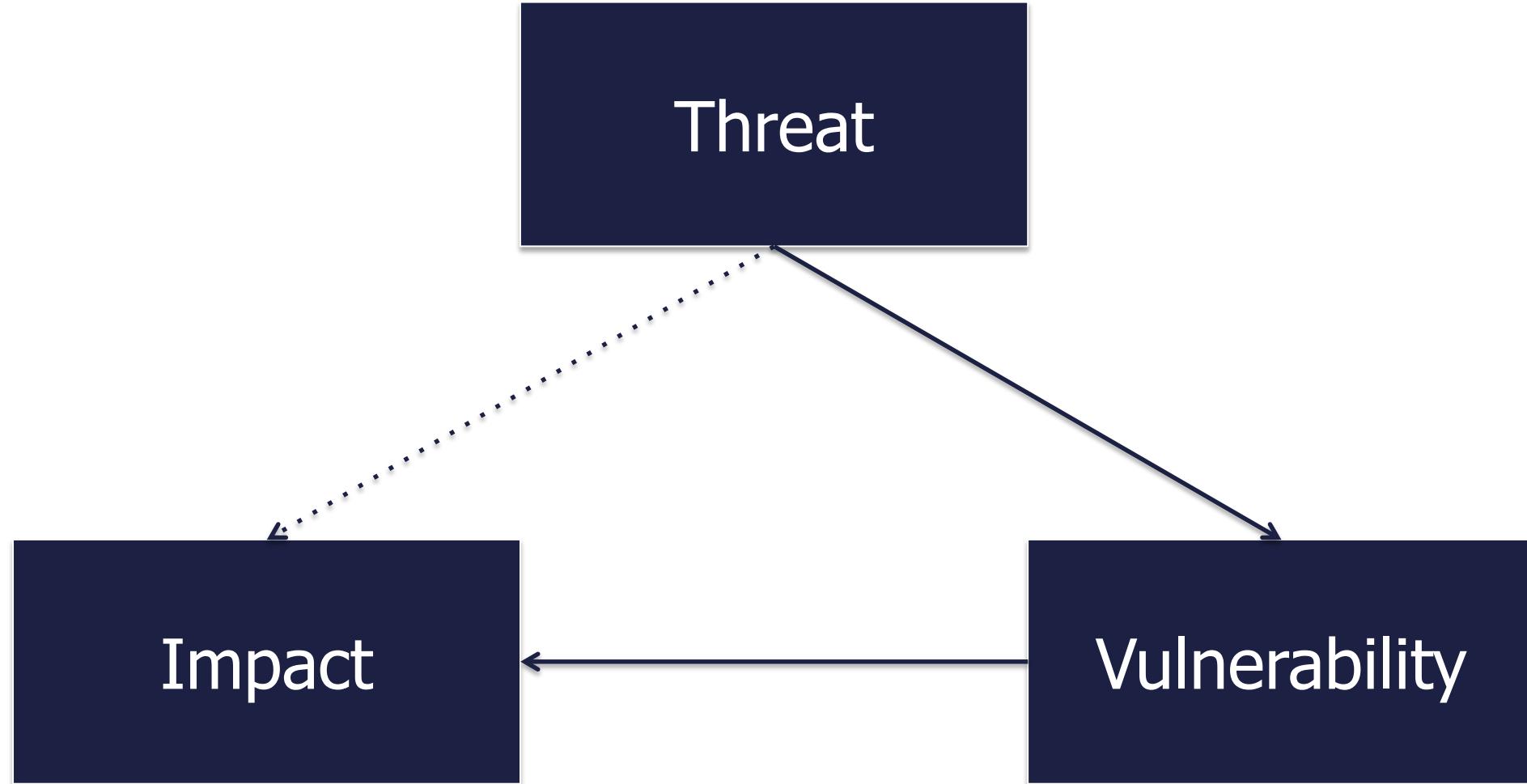
10% of all computers in UA destroyed !

Massive collateral damage: > 3 billion \$

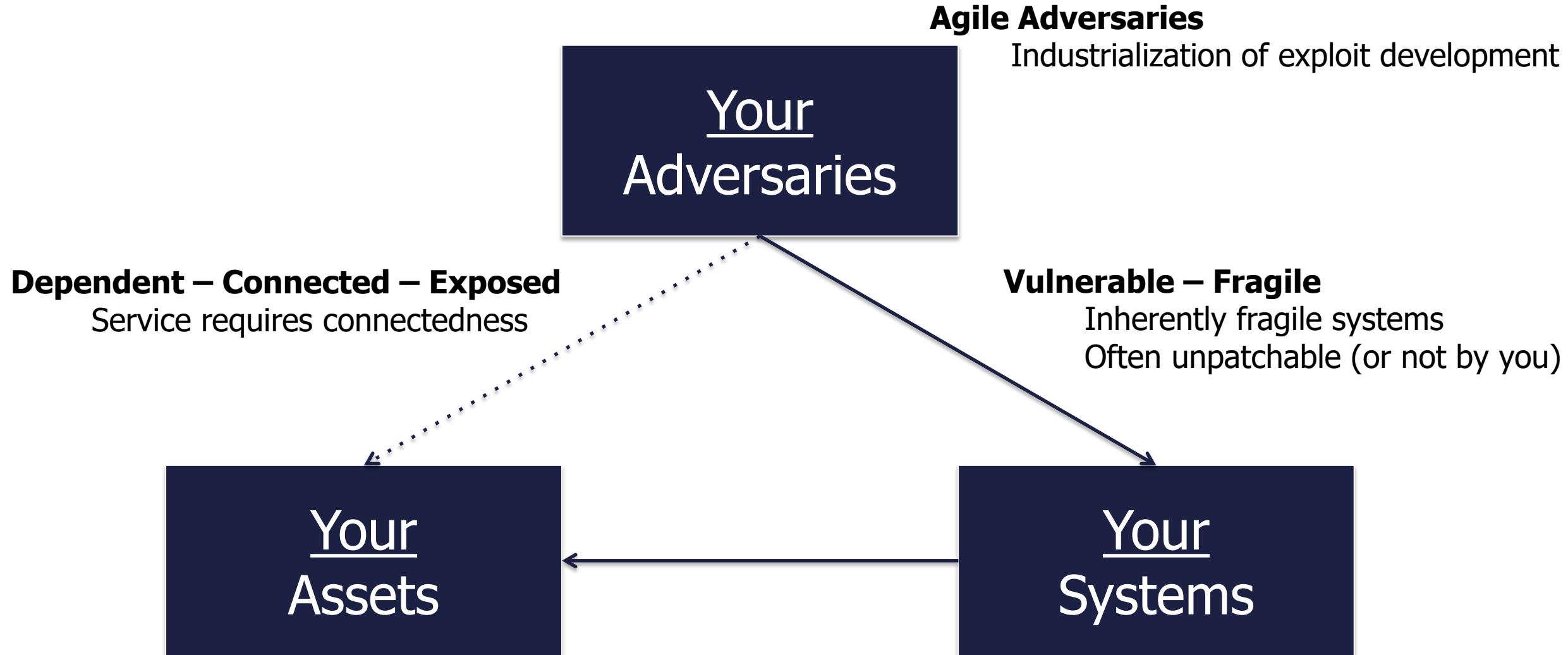
Threat Landscape 2019: Agile Adversaries

- Adaptive Adversary infrastructure
- Blending in with legitimate user
 - Using legitimate infrastructure components (PowerShell, Macros)
 - Abusing legitimate credentials
 - Replicating legitimate user behavior
- Fast uptake of new vulnerabilities and leaked tools

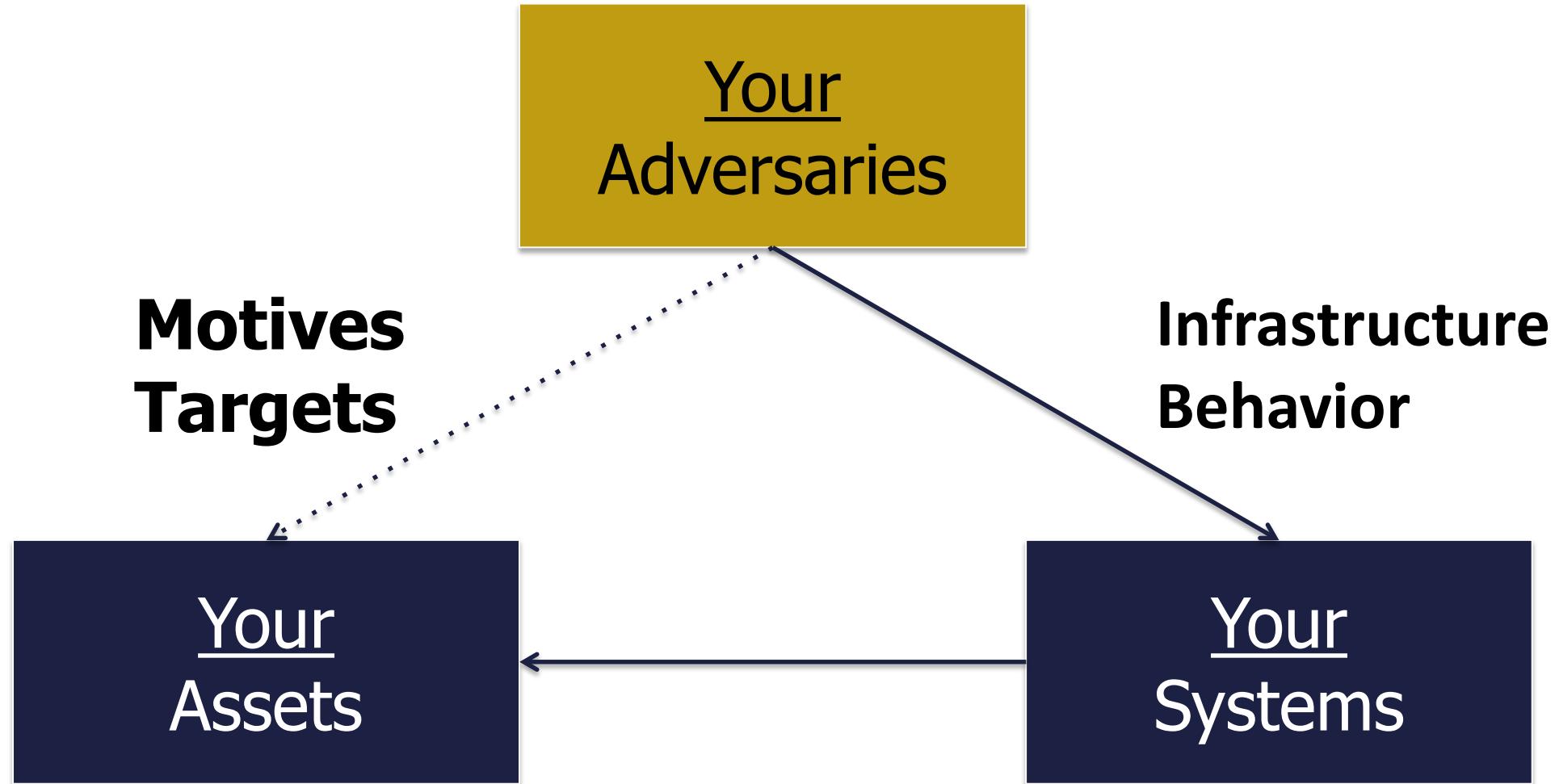
Risk-Based Defense



Threat-Informed Defense



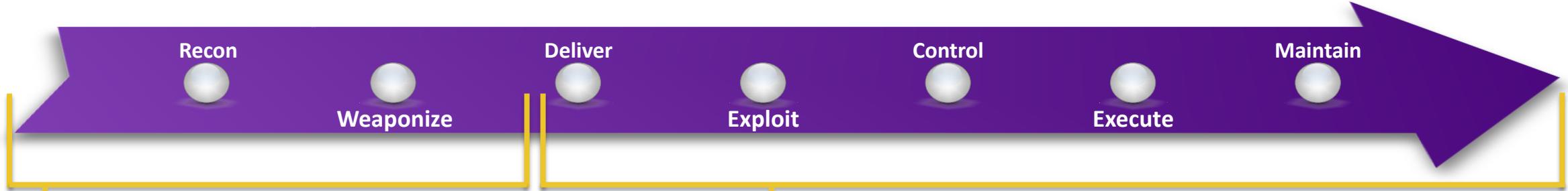
Identify Your Threats to Improve Your Defense



Use Threat Intelligence in Your Defense

- Identify Your Critical Assets
 - Who would be interested in them?
 - Why?
- Maximize the benefit of observing Your Adversaries' Infrastructure
 - Increase the quality and timeliness of Indicators of Compromise (IOCs)
 - Make them actionable (COA)
- Observe Your Adversaries' Behavior
 - Techniques, Tactics and Procedures (TTPs)
 - Deploy in prevention, detection, response

Decomposing the ATT&CK



PRE-ATT&CK

- Priority Definition
 - Planning, Direction
- Target Selection
- Information Gathering
 - Technical, People, Organizational
- Weakness Identification
 - Technical, People, Organizational
- Adversary OpSec
- Establish & Maintain Infrastructure
- Persona Development
- Build Capabilities
- Test Capabilities
- Stage Capabilities

ATT&CK for Enterprise

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Exfiltration
- Command and Control

Check out the results from our first round of ATT&CK Evaluations at attackevals.mitre.org!

MATRICES

PRE-ATT&CK

Enterprise

[All Platforms](#)

Linux

macOS

Windows

Mobile

[Home](#) > [Matrices](#) > [Enterprise](#)[Launch the ATT&CK™ Navigator](#) ↗

Enterprise Matrix

The full ATT&CK Matrix™ below includes techniques spanning Windows, Mac, and Linux platforms and can be used to navigate through the knowledge base.

Last Modified: 2018-10-17T00:14:20.652Z

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	ApnInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol

Polling Question 1

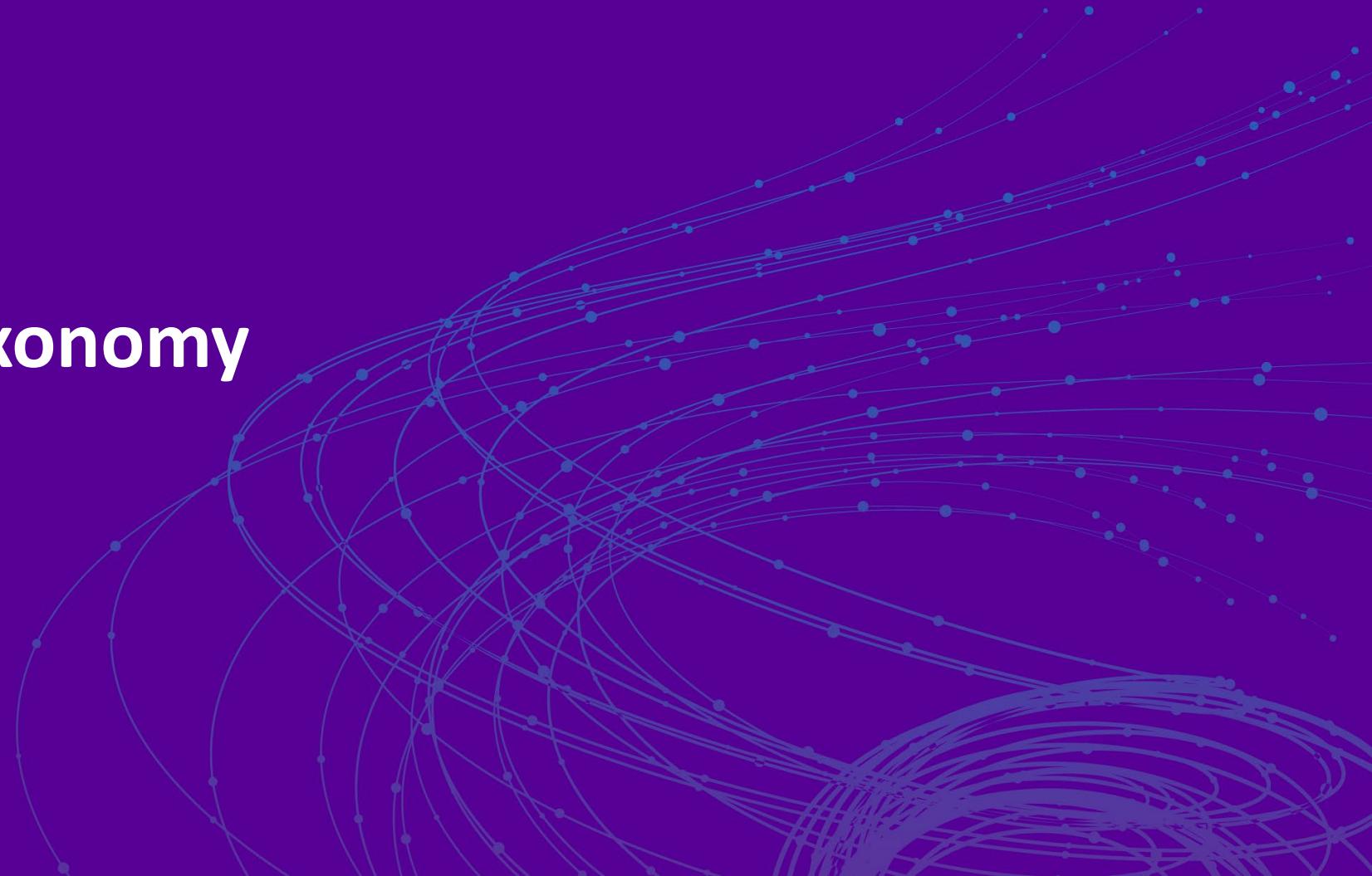
- AIR-T07
- Is your organisation currently using the ATT&CK Framework?
 - A. Yes
 - B. No
 - C. I don't know
- Results

MITRE ATT&CK Key Added Values

- Common Taxonomy
- Prioritization in Prevention, Detection and Response
 - No need to implement the whole matrix
 - Not all the techniques are equal to you
- Easier Sharing of Insights

RSA®Conference2019

Common Taxonomy



Taxonomy

- Common language to describe TTPs
- Knowledge base of observed TTPs
- Continuously updated
- Vendor agnostic
- Widely adopted by the community

Enterprise Tactics

ID	Name	Description
TA0001	Initial Access	The initial access tactic represents the vectors adversaries use to gain an initial foothold within a network.
TA0002	Execution	The execution tactic represents techniques that result in execution of adversary-controlled code on a local or remote system. This tactic is often used in conjunction with initial access as the means of executing code once access is obtained, and lateral movement to expand access to remote systems on a network.
TA0003	Persistence	Persistence is any access, action, or configuration change to a system that gives an adversary a persistent presence on that system. Adversaries will often need to maintain access to systems through interruptions such as system restarts, loss of credentials, or other failures that would require a remote access tool to restart or alternate backdoor for them to regain access.
TA0004	Privilege Escalation	Privilege escalation is the result of actions that allows an adversary to obtain a higher level of permissions on a system or network. Certain tools or actions require a higher level of privilege to work and are likely necessary at many points throughout an operation. Adversaries can enter a system with unprivileged access and must take advantage of a system weakness to obtain local administrator or SYSTEM/root level privileges. A user account with administrator-like access can also be used. User accounts with permissions to access specific systems or perform specific functions necessary for adversaries to achieve their objective may also be considered an escalation of privilege.
TA0005	Defense Evasion	Defense evasion consists of techniques an adversary may use to evade detection or avoid other defenses. Sometimes these actions are the same as or variations of techniques in other categories that have the added benefit of subverting a particular defense or mitigation. Defense evasion may be considered a set of attributes the adversary applies to all other phases of the operation.

Enterprise Techniques

ID	Name	Description
T1156	.bash_profile and .bashrc	<code>~/.bash_profile</code> and <code>~/.bashrc</code> are executed in a user's context when a new shell opens or when a user logs in so that their environment is set correctly. <code>~/.bash_profile</code> is executed for login shells and <code>~/.bashrc</code> is executed for interactive non-login shells. This means that when a user logs in (via username and password) to the console (either locally or remotely via something like SSH), <code>~/.bash_profile</code> is executed before the initial command prompt is returned to the user. After that, every time a new shell is opened, <code>~/.bashrc</code> is executed. This allows users more fine grained control over when they want certain commands executed.
T1134	Access Token Manipulation	Windows uses access tokens to determine the ownership of a running process. A user can manipulate access tokens to make a running process appear as though it belongs to someone other than the user that started the process. When this occurs, the process also takes on the security context associated with the new token. For example, Microsoft promotes the use of access tokens as a security best practice. Administrators should log in as a standard user but run their tools with administrator privileges using the built-in access token manipulation command <code>runas</code> .
T1015	Accessibility Features	Windows contains accessibility features that may be launched with a key combination before a user has logged in (for example, when the user is on the Windows logon screen). An adversary can modify the way these programs are launched to get a command prompt or backdoor without logging in to the system.
T1087	Account Discovery	Adversaries may attempt to get a listing of local system or domain accounts.

Example T1060: Registry Run Keys / Start Folder

- **Description:** Adding an entry to the "run keys" in the Registry or startup folder will cause the program referenced to be executed when a user logs in.[1] The program will be executed under the context of the user and will have the account's associated permissions level. [etc...]
- **Platform:** Windows
- **Permissions required:** User, Administrator
- **Detection:**
 - Monitor Registry for changes to run keys that do not correlate with known software, patch cycles, etc.
 - Monitor the start folder for additions or changes.
 - Tools such as Sysinternals Autoruns may also be used to detect system changes that could be attempts at persistence, including listing the run keys' Registry locations and startup folders.[52]
- **Mitigation:**
 - Identify and block potentially malicious software that may be executed through run key or startup folder persistence using whitelisting[47] tools like AppLocker[48][49] or Software Restriction Policies[50] where appropriate.[51]
- **Data Sources:** Windows Registry, File monitoring
- **Examples:** 68 groups and software examples

Understand Your Adversaries' Behavior

- Identify Your Adversaries of interest
- Which techniques do they use and which traces to they leave?
- “Track” them with intelligence from the community and security vendors

Thanks to all of our ATT&CKcon participants. [All sessions are here](#), and individual presentations will be posted soon.

GROUPS

Overview

admin@338

APT1

APT12

APT16

APT17

APT18

APT19

APT28

APT29

APT3

APT30

APT32

APT33

APT37

Axiom

BlackOasis

BRONZE BUTLER

Carbanak

Charming Kitten

Cleaver

Cobalt Group

Home > Groups

Groups

Groups are sets of related intrusion activity that are tracked by a common name in the security community. Groups are also sometimes referred to as campaigns or intrusion sets. Some groups have multiple names associated with the same set of activities due to various organizations tracking the same set of activities by different names. Organizations' group definitions may be only partially overlapping and may be in disagreement on specific activity.

Groups are mapped to publicly reported technique use and referenced in the ATT&CK threat model. Groups are also mapped to reported software used during intrusions.

Name	Alias	Description
admin@338	admin@338	admin@338 is a China-based cyber threat group. It has previously used newsworthy events as lures to deliver malware and has primarily targeted organizations involved in financial, economic, and trade policy, typically using publicly available RATs such as PoisonIvy , as well as some non-public backdoors.
APT1	APT1, Comment Crew, Comment Group, Comment Panda	APT1 is a Chinese threat group that has been attributed to the 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department, commonly known by its Military Unit Cover Designator (MUCD) as Unit 61398.
APT12	APT12, IXESHE, DynCalc, Numbered Panda, DNSCALC	APT12 is a threat group that has been attributed to China.
APT16	APT16	APT16 is a China-based threat group that has launched spearphishing campaigns targeting Japanese and Taiwanese organizations.
APT17	APT17, Deputy Dog	APT17 is a China-based threat group that has conducted network intrusions against U.S. government entities, the defense industry, law firms, information technology companies, mining companies, and non-government organizations.

APT28

APT28 is a threat group that has been attributed to Russia's Main Intelligence Directorate of the Russian General Staff by a July 2018 U.S. Department of Justice indictment. This group reportedly compromised the Hillary Clinton campaign, the Democratic National Committee, and the Democratic Congressional Campaign Committee in 2016 in an attempt to interfere with the U.S. presidential election. [\[1\]](#) [\[2\]](#) [\[3\]](#) [\[4\]](#) [\[5\]](#) [\[6\]](#) [\[7\]](#) [\[8\]](#) [\[9\]](#)

ID: G0007

Aliases: APT28, Sednit, Sofacy, Pawn Storm, Fancy Bear, STRONTIUM, Tsar Team, Threat Group-4127, TG-4127

Contributors: Richard Gold, Digital Shadows

Version: 1.0

Alias Descriptions

Name	Description
APT28	[4] [5] [3] [28] [12] [2]
Sednit	This designation has been used in reporting both to refer to the threat group and its associated malware. [6] [5] [28] [2]
Sofacy	This designation has been used in reporting both to refer to the threat group and its associated malware. [4] [5] [3] [12] [2]
Pawn Storm	[5] [12]
Fancy Bear	[3] [28] [12] [2]
STRONTIUM	[28] [12]
Tsar Team	[12]
Threat Group-4127	[5]
TG-4127	[5]

Vendors Use MITRE ATT&CK in their Reports



PLAYBOOK VIEWER

PLAYBOOKS
OILRIG
SOFACY
PICKAXE
PATCHWORK
DARKHYDRUS
REAPER
RANCOR
TICK
DRAGONOK

Sofacy (also known as Fancy Bear, APT 28, STRONTIUM, Pawn Storm) is a highly active actor with a Russian nexus. They have been active since the mid 2000s, and have been responsible for targeted intrusion campaigns against various industry vertical such as but not limited to Aerospace, Defense, Energy, Government and Media. Extensive observation and research of Sofacy's activities over time indicated a profile closely mirroring the strategic interests of the Russian government. More recently, this group has been attributed to the GRU, Russia's premier military intelligence service as reported by the US intelligence community within several declassified public documents.

This adversary has been observed to have access to a wide range of implants, such as Coreshell, XAgent, Xtunnel, SofacyCarberp, as well as a variety of malware for non Windows platforms such as Linux, macOS, iOS, Android, and Windows Phones. They are also known for registering domain names closely resembling domains of legitimate organizations they are planning to target. Often times, credential harvesters may be deployed onto these sites in order to gather credentials to be repurposed for post-exploitation operations.

Several high profile intrusions have been publicly linked to the Sofacy group, such as the German Bundestag, France's TV5Monde TV station, the Democratic National Committee, the World Anti-Doping Agency, and the Ukrainian military.

Intrusion Set: Sofacy Campaigns: 2 Indicators: 17 Attack Patterns: 34

RECON	WEAPONIZATION	DELIVERY	EXPLOIT	INSTALL	COMMAND	OBJECTIVE
Acquire OSINT data sets and information	Host-based hiding techniques	Spear phishing messages with malicious attachments	Authorized user performs requested cyber action	Custom Cryptographic Protocol	System Information Discovery	
Obtain templates/branding materials	Obtain/re-use payloads		Confirmation of launched compromise achieved	Standard Application Layer Protocol		
	Misattributable credentials			Commonly Used Port		

unit42 PRIME Mitre ATT&CK APT28 Actors

Filter result APT28 Clear Filter

Table Kill Chain Flat

The screenshot shows a grid of 48 cards representing various MITRE ATT&CK tactics and techniques for the APT28 threat actor. The grid is organized into three tabs: Table, Kill Chain, and Flat. The Table tab is currently selected. The cards include:

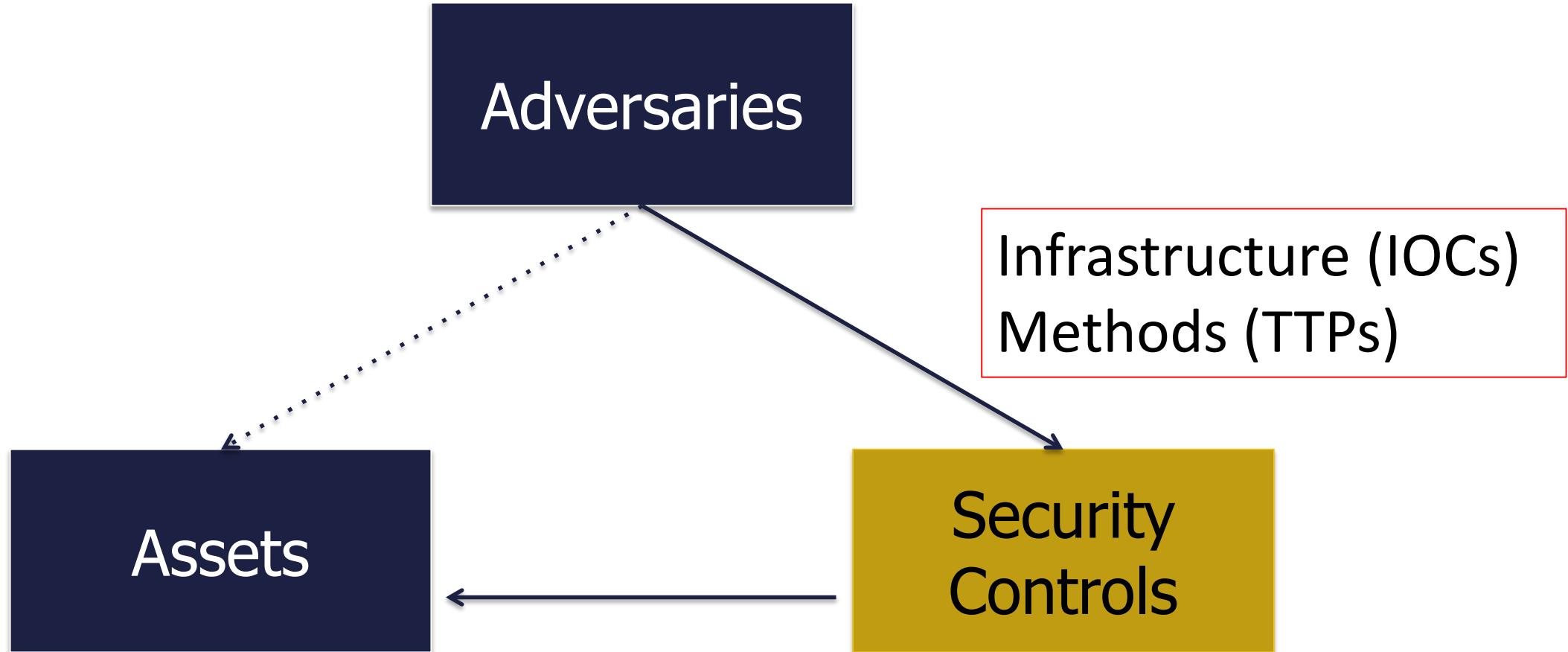
- Discovery: File and Directory Discovery (Rules: 33)
- Discovery: Peripheral Device Discovery (Rules: 0)
- Discovery: Process Discovery (Rules: 0)
- Discovery: System Information Discovery (Rules: 10)
- Discovery: System Owner/User Discovery (Rules: 9)
- Initial Access: Replication Through Removable Media (Rules: 9)
- Initial Access: Spearphishing Attachment (Rules: 14)
- Initial Access: Valid Accounts (Rules: 10)
- Credential Access: Credential Dumping (Rules: 34)
- Credential Access: Credentials in Files (Rules: 56)
- Credential Access: Network Sniffing (Rules: 15)
- Credential Access: Replication Through Removable Media (Rules: 9)
- Privilege Escalation: Access Token Manipulation (Rules: 6)
- Privilege Escalation: Exploitation for Privilege Escalation (Rules: 26)
- Privilege Escalation: Defense Evasion (Rules: 15)
- Defense Evasion: Component Object Model Hijacking (Rules: 2)
- Defense Evasion: Component Object Model Hijacking (Rules: 2)
- Defense Evasion: Deobfuscate/Decode Files or Scripts (Rules: 11)
- Defense Evasion: Hidden Files and Directories (Rules: 22)
- Defense Evasion: Indicator Removal on Host (Rules: 11)
- Defense Evasion: Persistence (Rules: 11)
- Persistence: Bootkit (Rules: 11)
- Persistence: Hidden Files and Directories (Rules: 22)
- Persistence: Logon Scripts (Rules: 11)
- Persistence: Office Application Startup (Rules: 8)
- Persistence: Valid Accounts (Rules: 60)
- Command and Control: Communication Through Removable Media (Rules: 6)
- Command and Control: Connection Privacy (Rules: 14)
- Command and Control: Data Obfuscation (Rules: 9)
- Command and Control: Remote File Copy (Rules: 152)
- Command and Control: Standard Application Layer Protocol (Rules: 44)
- Latent Movement: Exploit Remote Services (Rules: 3)
- Latent Movement: File Copy (Rules: 152)
- Latent Movement: Persistence (Rules: 42)
- Execution: Runfile (Rules: 42)
- Execution: Scripting (Rules: 51)
- Execution: User Execution (Rules: 603)
- Execution: Dynamic Data Exchange (Rules: 0)

RSA®Conference2019

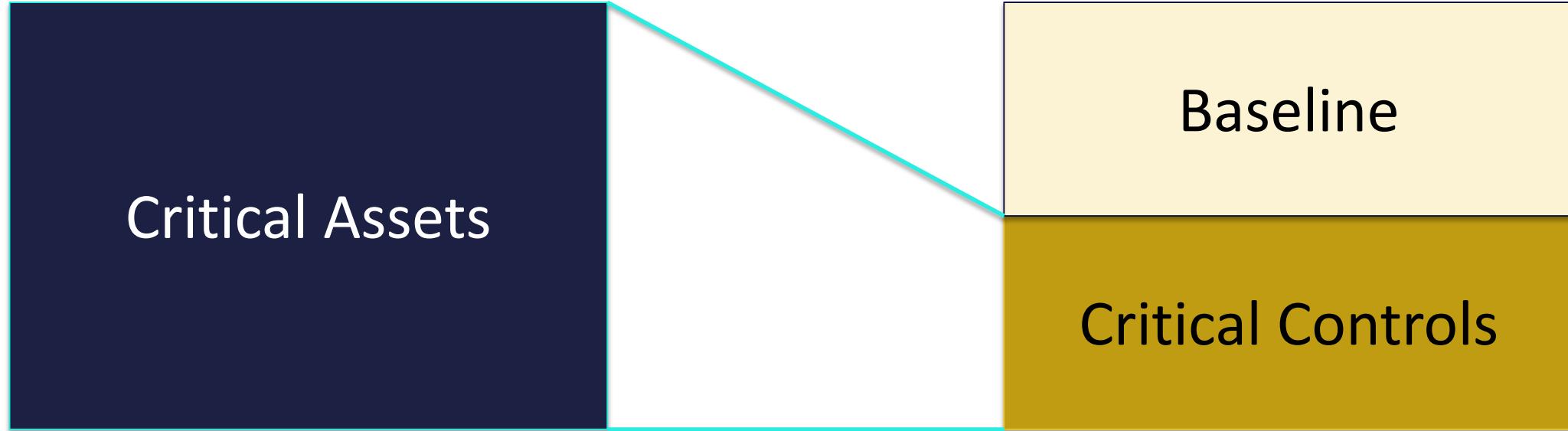
Prevention, Detection and Response



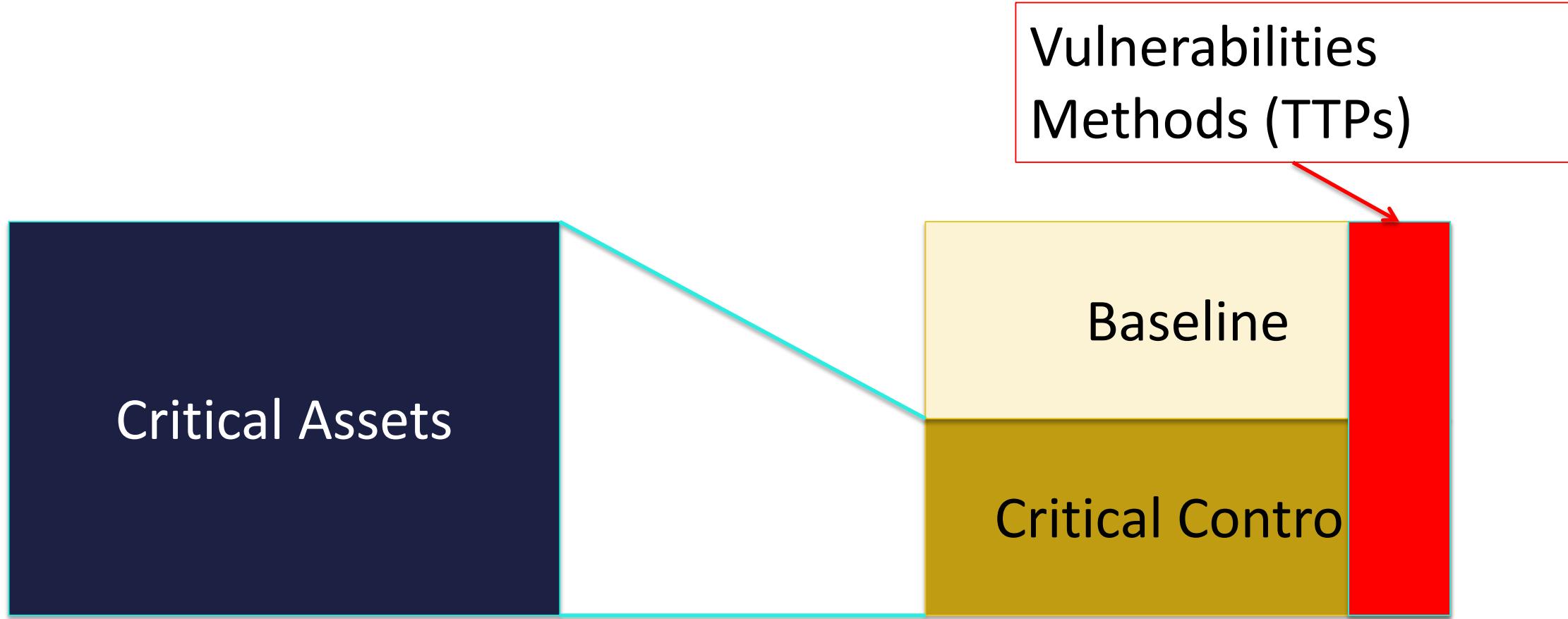
Understand Your Controls



Critical Controls for Your Critical Assets



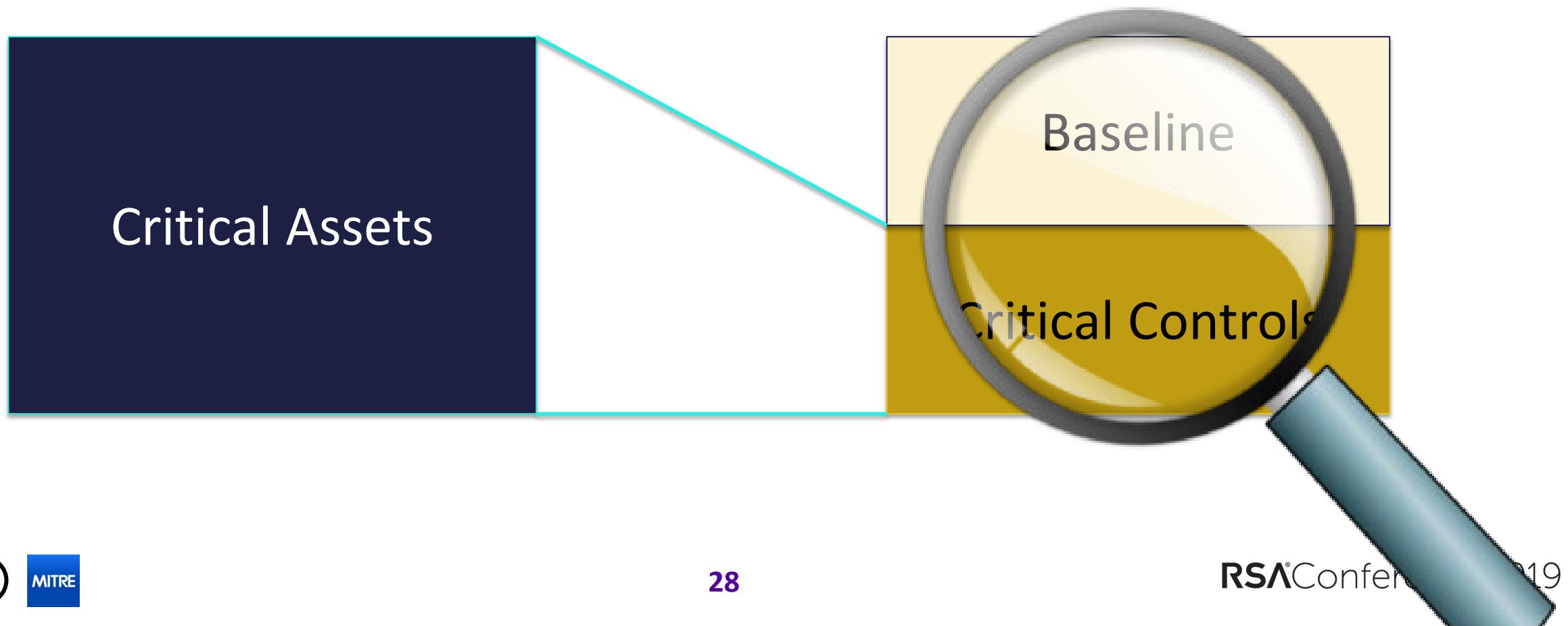
Monitor and Discover Exposure



Adapt Your Controls



Validate Your Controls



How Does CIS 6 Help You in Prevention?

Understand Your Detection

- Gain Visibility
 - Priorities in log collection
- Design Analytics
 - Write them with knowledge of Your Adversaries
 - Get them from the community
- Deploy
 - Detect / Hunt / Refine

Determine Overlaps between Your Adversaries

Lazarus/APT15			filters				legend					
			stages: act platforms: windows				 Lazarus  APT15  Common techniques					
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control		
10 items	25 items	41 items	21 items	49 items	16 items	19 items	15 items	13 items	9 items	20 items		
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Automated Exfiltration	Commonly Used Port		
Exploit Public-Facing Application	Command-Line Interface	AppCert DLLs	Accessibility Features	Binary Padding	Brute Force	Application Window Discovery	Distributed Component Object Model	Automated Collection	Data Compromised	Communication Through Removable Media		
Hardware Addition	Control Panel Items	AppInit DLLs	AppInit DLLs	BITB Jobs	Credential Dumping	Browser Bookmark Discovery	Exfiltration of Remote Services	Clipboard Data	Data Encrypted	Connection Proxy		
Replication Through Removable Media	Dynamic Data Exchange	Application Shimming	AppInit DLLs	Bypass User Account Control	Credentials in Files	File and Directory Discovery	Login Scripts	Data from Information Resources	Data Transfer Size Limits	Custom Command and Control Protocol		
Spearphishing Attachment	Execution through API	Authentication Package	Application Shimming	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol		
Spearphishing Link	Execution through Module Load	BITB Jobs	Bypass User Account Control	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Network Shared Class	Exfiltration Over Command and Control Channel	Data Encoding		
Spearphishing via Service	Exploitation for Client Execution	Bootkit	DLL Session Order Hijacking	Component Firmware	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation		
Supply Chain Compromise	Graphical User Interface	Browser Extensions	Exploit for Privilege Escalation	Component Object Model Hijacking	Hooking	Peripheral Device Discovery	Remote File Copy	Data Staged	Exfiltration Over Physical Medium	Domain Fronting		
Treated Relationship	Install Util	Change Default File Associations	Core Window Memory	Control Panel Items	Input Capture	Permission Group Discovery	Remote Services	Email Collection	Scheduled Transfer	Fallback Channels		
Valid Accounts	LSASS Driver	Component Firmware	Core System Permissions Weakness	DCShadow	Kerberoasting	Process Discovery	Replication Through Removable Media	Input Capture		Multiprop Proxy		
	Mimik	Component Object Model Hijacking	Hosting		LLMNR/NBTNS Poisoning	Query Registry	Shared Webroot	Man in the Browser		Multistage Channels		
	PowerShell	Create Account	Image File Execution Options Injection		Distilling Security Tools	Network Sniffing	Remote System Discovery	Screen Capture		Multiband Communication		
	Regexec/Regasm	DLL Search Order Hijacking	New Service		DLL Search Order Hijacking	Password Filter DLL	Security Software Discovery	Video Capture		Multi-layer Encryption		
	Regsv32	External Remote Services	Path Interception		DLL Side-Loading	Private Keys	System Information Discovery	Windows Admin Shares		Remote Access Tools		
	Rundl02	File System Persistence Weakness	Port Monitors		Exploration for Defense Evasion	Registration Through Removable Media	System Network Configuration Discovery	Windows Remote Management		Remote File Copy		
	Scheduled Task	Hidden Files and Directories	Phishing Injection		Extra Window Memory Injection	Two-Factor Authentication Interception	System Network Connections Discovery			Standard Application Layer Protocol		
	Scripting	Hooking	Scheduled Task		File Deletion		System Owner/User Discovery			Standard Cryptographic Protocol		
	Service Execution	Hypervisor	Service Registry Permissions Weakness		File System Logical Offsets		System Service Discovery			Standard Non-Application Layer Protocol		
	Signed Binary Proxy Execution	Image File Execution Options Injection	SID-History Injection		Hidden Files and Directories		System Time Discovery			Uncommonly Used Port		
	Signed Script Proxy Execution	Logon Scripts	Valid Accounts		Image File Execution Options Injection					Web Service		
	Third-party Software	LSASS Driver	Web Shell		Indicator Blocking							
	Trusted Developer Utilities	Modify Existing Service			Indicator Removal from Tools							
	User Execution	Netsh Helper DLL			Indicator Removal on Host							
	Windows Management Instrumentation	New Service			Indirect Command Execution							
	Windows Remote Management	Office Application Startup			Install Root Certificate							
		Path Interception			InstallUtil							
		Port Monitors			Masquerading							
		Redundant Access			Modify Registry							
		Registry Run Keys / Start			Mimik							
		Scheduled Task			Network Share Connection Removal							
		Screensaver			NTFS File Attributes							
		Security Support Provider			Obfuscated File or Name							
		Service Registry Permissions Weakness			Process Doppelganging							
		Shrunk Modification			Process Hollowing							
		SIP and Trust Provider Hijacking			Process Injection							
		System Firmware			Redundant Access							
		Time Providers			Regexec/Regasm							
		Valid Accounts			Regsv32							
		Web Shell			Roskit							
		Windows Management Instrumentation			Rundl02							

Where do you get the highest impact?

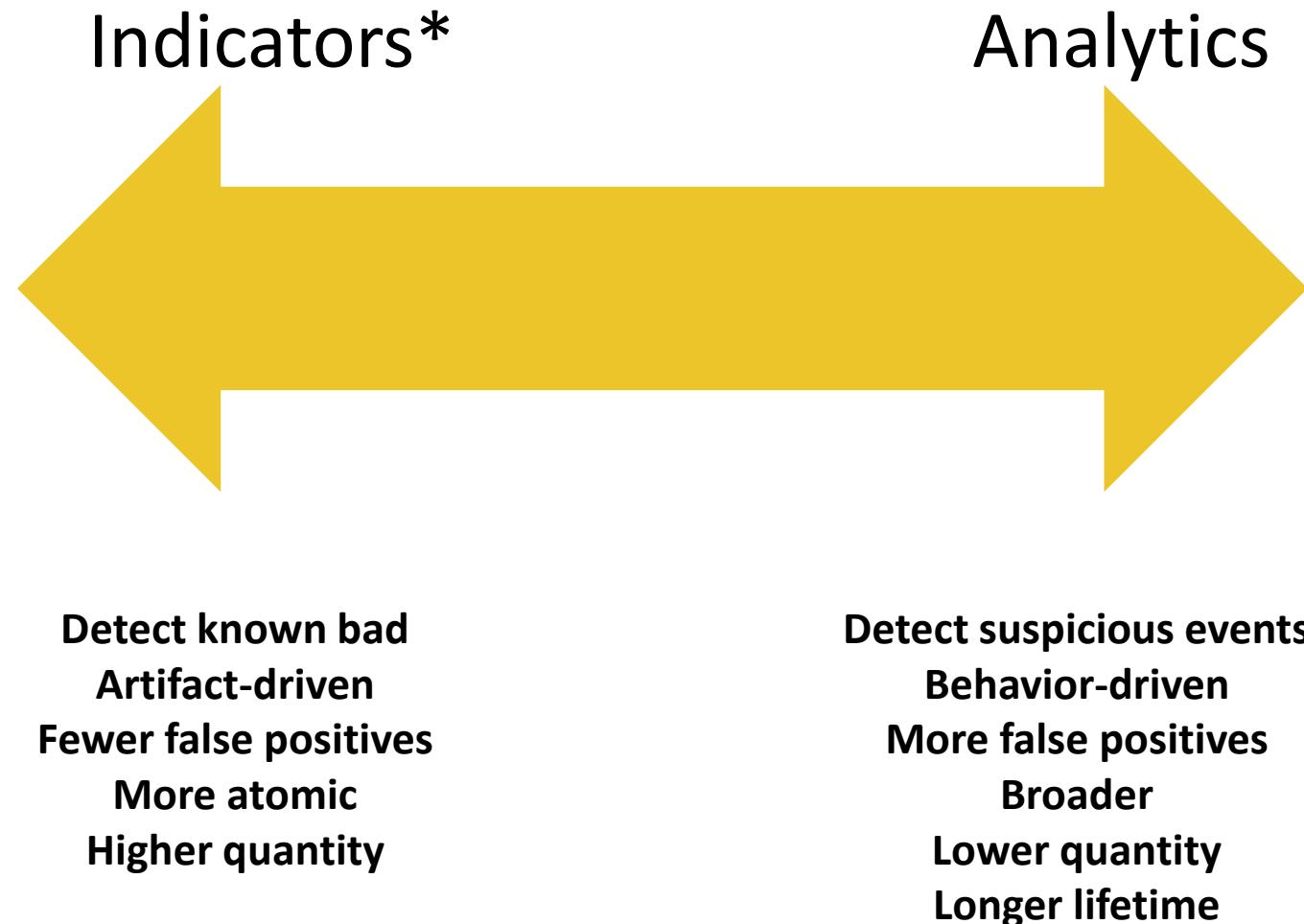
DC/DNS/Email logs

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	25 items	41 items	21 items	49 items	16 items	19 items	15 items	13 items	9 items	20 items
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	Command-Line Interface	AppCert DLLs	Accessibility Features	Binary Padding	Brute Force	Application Window Discovery	Distributed Component Object Model	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Control Panel Items	AppInit DLLs	AppCert DLLs	BITS Jobs	Credential Dumping	Browser Bookmark Discovery	Clipboard Data	Data Encrypted	Connection Proxy	
Replication Through Removable Media	Dynamic Data Exchange	Application Shimming	AppInit DLLs	Bypass User Account Control	Credentials in Files	Exploitation of Remote Services	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol	
Spearphishing Attachment	Execution through API	Authentication Package	Apnst	CMSTP	Credentials in Registry	File and Directory Discovery	Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
	Execution through Module Load	BITS Jobs	Application Shimming	Code Signing	Exploitation for Credential Access	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing Link	Exploitation for Client Execution	Bootkit	Bypass User Account Control	Component Firmware	Forced Authentication	Network Share Discovery	Pass the Ticket	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Spearphishing via Service	Graphical User Interface	Browser Extensions	DLL Search Order Hijacking	Component Object Model Hijacking	Hooking	Remote Desktop Protocol	Remote File Copy	Data Staged	Domain Fronting	
Supply Chain Compromise	InstallUtil	Change Default File Association	Control Panel Items	Control Panel Items	Input Capture	Password Policy Discovery	Email Collection	Exfiltration Over Physical Medium	Fallback Channels	
Trusted Relationship	LSASS Driver	Component Firmware	Exploitation for Privilege Escalation	DCShadow	Kerberoasting	Peripheral Device Discovery	Remote Services	Input Capture	Exfiltration Over Multi-hop Proxy	
	Mshba	Component Object Model Hijacking	Extra Window Memory Injection	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Scheduled Transfer	Multi-Stage Channels
Valid Accounts	PowerShell	Create Account	File System Permissions Weakness	Disabling Security Tools	Network Sniffing	Process Discovery	Shared Webroot	Screen Capture		Multiband Communication
	Regsvcs/Regasm	DLL Search Order Hijacking	Hijacking	DLL Search Order Hijacking	Password Filter DLL	Query Registry	Taint Shared Content	Video Capture		Multilayer Encryption
	Regsvr32	External Remote Services	Hooking	DLL Side-Loading	Private Keys	Remote System Discovery	Third-party Software			Remote Access Tools
	Rundll32	File System Permissions Weakness	Image File Execution Options Injection	Exploitation for Defense Evasion	Replication Through Removable Media	Windows Admin Shares				Remote File Copy
	Scheduled Task	Hidden Files and Directories	New Service	Extra Window Memory Injection	Two-Factor Authentication Interception	Security Software Discovery	Windows Remote Management			Standard Application Layer Protocol
	Scripting	Path Interception	File Deletion			System Information Discovery				Standard Cryptographic Protocol
	Service Execution	Port Monitors	File System Logical Offsets			System Network Configuration Discovery				Standard Non-Application Layer Protocol
	Signed Binary Proxy Execution	Process Injection	Hidden Files and Directories			System Network Connections Discovery				Uncommonly Used Port
	Signed Script Proxy Execution	Process Injection	Image File Execution Options Injection			System Owner/User Discovery				Web Service
	Third-party Software	Service Registry	Indicator Blocking			System Service Discovery				
Trusted Developer Utilities	Logon Scripts	Permissions Weakness	Indicator Removal from Tools			System Time Discovery				
User Execution	LSASS Driver	SID-History Injection	Indicator Removal on Host							
Windows Management Instrumentation	Modify Existing Service	Valid Accounts	Indirect Command Execution							
Windows Remote Management	Netsh Helper DLL	Web Shell	Install Root Certificate							
	New Service		InstallUtil							
	Office Application Startup		Masquerading							
	Path Interception									

+Proxy/Endpoint AV/Sysmon

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	25 items	41 items	21 items	49 items	16 items	19 items	15 items	13 items	9 items	20 items
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	Command-Line Interface	AppCert DLLs	Binary Padding	Brute Force	Application Window Discovery	Distributed Component Object Model	Automated Collection	Data Compressed	Communication Through Removable Media	
Hardware Additions	Control Panel Items	AppInit DLLs	Accessibility Features	BITS Jobs	Credential Dumping	Browser Bookmark Discovery	Clipboard Data	Data Encrypted		
Replication Through Removable Media	Dynamic Data Exchange	Application Shimming	AppCert DLLs	Bypass User Account Control	Credentials in Files	Exploitation of Remote Services	Data from Information Repositories	Data Transfer Size Limits	Connection Proxy	
Spearphishing Attachment	Execution through API	Authentication Package	AppInit DLLs	CMSTP	Credentials in Registry	File and Directory Discovery	Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Custom Command and Control Protocol
Spearphishing Link	Execution through Module Load	BITS Jobs	Application Shimming	Code Signing	Exploitation for Credential Access	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Custom Cryptographic Protocol	
Spearphishing via Service	Exploitation for Client Execution	Bootkit	Bypass User Account Control	Component Firmware	Forced Authentication	Network Share Discovery	Pass the Ticket	Data from Removable Media	Exfiltration Over Command and Control Channel	Data Encoding
Supply Chain Compromise	Graphical User Interface	Change Default File Association	Component Object Model Hijacking	Component Object Model Hijacking	Hooking	>Password Policy Discovery	Remote Desktop Protocol	Data Staged	Exfiltration Over Other Network Medium	Data Obfuscation
Trusted Relationship	InstallUtil	Component Firmware	Control Panel Items	Input Capture	Kerberoasting	Peripheral Device Discovery	Remote File Copy	Data from Removable Media	Domain Fronting	
Valid Accounts	LSASS Driver	Component Object Model Hijacking	DCShadow	LLMNR/NBT-NS Poisoning	LLMNR/NBT-NS Poisoning	Permission Groups Discovery	Email Collection	Exfiltration Over Physical Medium	Fallback Channels	
	Mshta	Create Account	Extra Window Memory Injection	Disabling Security Tools	Network Sniffing	Process Discovery	Input Capture	Scheduled Transfer	Multi-Stage Channels	
	PowerShell		File System Permissions Weakness	DLL Search Order Hijacking	Password Filter DLL	Query Registry	Taint Shared Content		Multiband Communication	
	Regsvcs/Regasm	DLL Search Order Hijacking	Hooking	Image File Execution Options Injection	Private Keys	Remote System Discovery	Third-party Software		Remote Access Tools	
	Regsvr32	External Remote Services		DLL Side-Loading	Replication Through Removable Media	Security Software Discovery	Windows Admin Shares		Remote File Copy	
	Rundll32	File System Permissions Weakness		Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Information Discovery			Standard Application Layer Protocol	
	Scheduled Task	Hidden Files and Directories		Extra Window Memory Injection	File Deletion	System Network Configuration Discovery			Standard Cryptographic Protocol	
	Scripting	Path Interception		Image File Execution Options Injection	File System Logical Offsets	System Network Connections Discovery			Standard Non-Application Layer Protocol	
				Indicator Blocking	Hidden Files and Directories	System Owner/User Discovery			Uncommonly Used Port	
	Service Execution	Hooking		Indicator Removal from Tools		System Service Discovery			Web Service	
	Signed Binary Proxy Execution	Hypervisor		Indicator Removal on Host		System Time Discovery				
	Signed Script Proxy Execution	Image File Execution Options Injection		Indirect Command Execution						
	Third-party Software	Scheduled Task		Install Root Certificate						
	Trusted Developer Utilities	Logon Scripts		InstallUtil						
	User Execution	LSASS Driver		Office Application Startup	Masquerading					
	Windows Management Instrumentation	Modify Existing Service								
	Netsh Helper DLL	New Service								
	Windows Remote Management	Path Interception								

Analytics Instead of Indicators



*good, fresh, indicators are useful too

Build an Analytic

- Read the ATT&CK documentation for the techniques you expect
 - Separate possible legitimate use from malicious use
 - Look for existing analytics in MITRE CAR or community sources
- Simulate the techniques
 - Carry out the techniques via your own testing or pre-written scripts
 - What does it look like in your logs?
- Write and iterate your analytics
 - Write your search, narrow down false positives, and iterate
 - Keep testing – check for a variety of ways it can be used, not just the easiest

Convert your Analytics in Pseudo-Code



SIGMA

Sigma Format

Generic Signature
Description

Sigma Converter

Applies Predefined and
Custom Field Mapping

Elastic Search Queries

Splunk Searches

...

<https://github.com/Neo23x0/sigma>

Community Tools

SIGMA Editor

The screenshot shows the SIGMA UI interface. At the top, there's a navigation bar with links for "How to Write Sigma Rules" and "Video guide". Below the navigation are buttons for "Create", "Select", "Save", and "Export". The interface is divided into two main sections: "SOURCE CODE EDITOR" on the left and "VISUAL EDITOR" on the right.

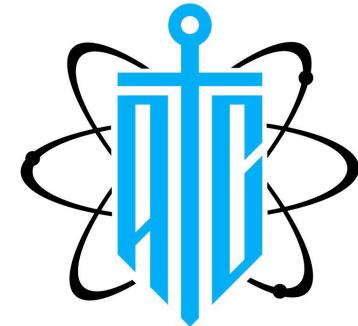
SOURCE CODE EDITOR:

```
SHA 256: --
1 title: ""
2 description: ""
3 author: ""
4 status: ""
5 logsource:
6   product: ""
7   service: ""
8 detection:
9   condition: ""
10 fields:
11 -
12 falsepositives:
13 -
14 level: ""
```

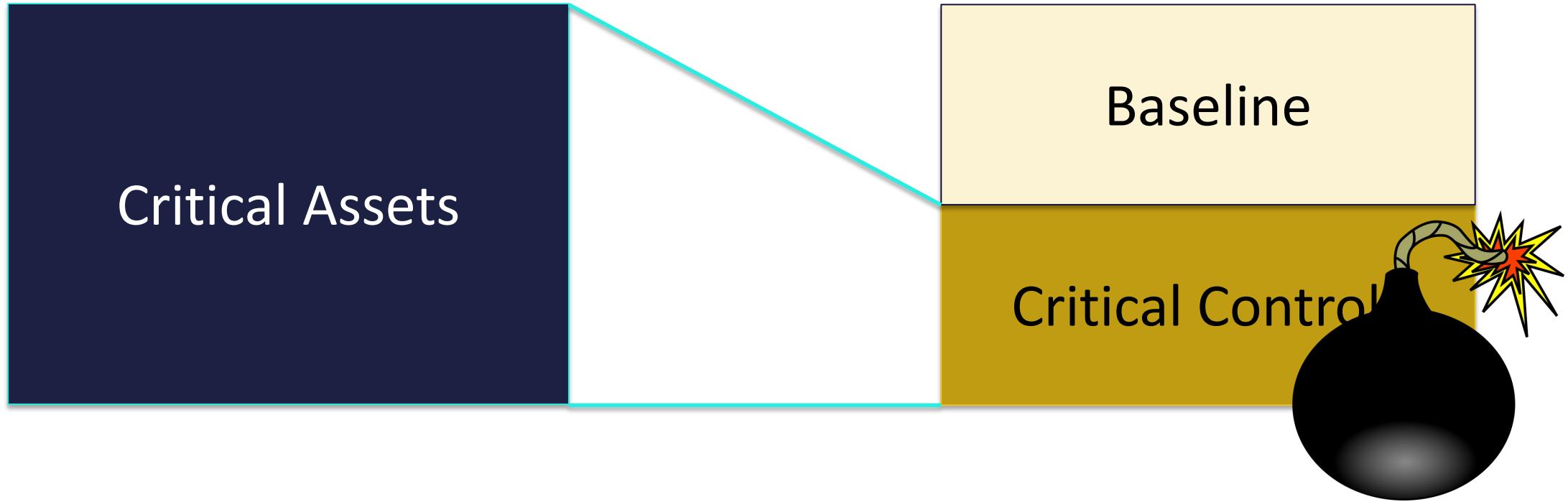
VISUAL EDITOR:

The visual editor displays the same Sigma rule structure. It includes fields for title, description, author, status, logsource (with product and service dropdowns), detection (with condition dropdown), fields, falsepositives, and level. Each field has a warning icon (yellow triangle with an exclamation mark) next to it.

Atomic Threat Coverage Analytics Documentation



Test Your Controls

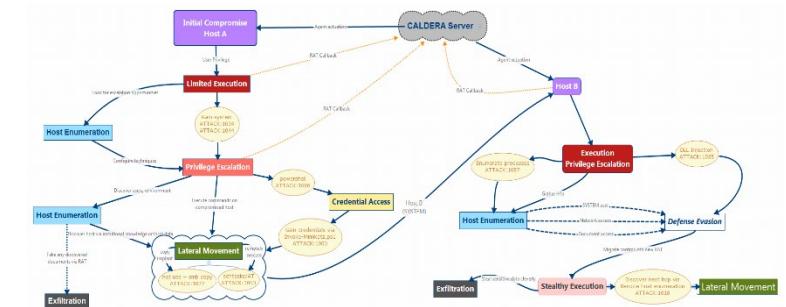
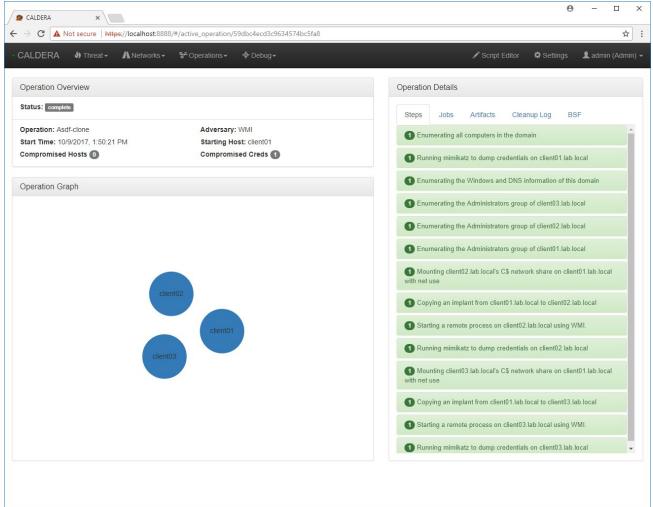


Red Team Tools

- Active testing of controls using MITRE ATT&CK
 - [MITRE Caldera](#)
 - [Endgame RTA](#)
 - [Red Canary Atomic Red Team](#)
 - [Uber Metta](#)

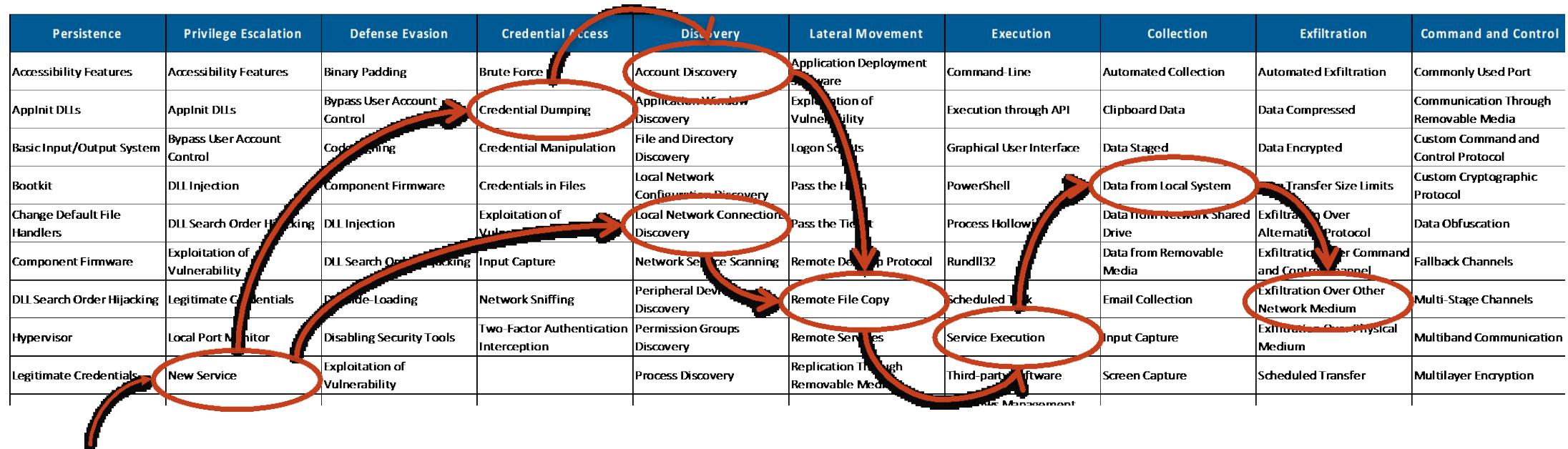
CALDERA

- Automated adversary emulation
 - Safely replicate realistic adversary behavior
 - Repeatable testing and verification of prevention/detection
- Features
 - Uses ATT&CK to create Adversary profiles
 - Uses AI and modeling to make decisions about actions
 - Self-cleans after operation completes
 - Low install overhead
 - Does not require extensive red team knowledge to operate



Emulate Adversaries

- Connect techniques in attack sequence
- Test patterns of behavior focusing on defense effectiveness
- Triage events



Gap Analysis

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
DLL Search Order Hijacking			Brute Force	Account Discovery	Windows Remote Management	Automated Collection	Automated Exfiltration	Commonly Used Port	
Legitimate Credentials			Credential Dumping	Application Window Discovery	Third-party Software	Clipboard Data	Data Compressed	Communication Through Removable Media	
Accessibility Features	Binary Padding		Credential Manipulation	File and Directory Discovery	Application Deployment Software	Command-Line	Data Staged	Data Encrypted	
AppInit DLLs	Code Signing				Execution through API	Data from Local System	Data Transfer Size Limits	Custom Command and Control Protocol	
Local Port Monitor	Component Firmware				Graphical User Interface	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol	
New Service	DLL Side-Loading		Credentials in Files	Local Network Configuration Discovery	InstallUtil	Data from Removable Media	Exfiltration Over Command and Control Channel	Data Obfuscation	
Path Interception	Disabling Security Tools		Input Capture	Logon Scripts	PowerShell	Email Collection	Exfiltration Over Other Network Medium	Fallback Channels	
Scheduled Task	File Deletion		Network Sniffing	Pass the Hash	Process Hollowing	Input Capture	Exfiltration Over Physical Medium	Multi-Stage Channels	
File System Permissions Weakness	File System Logical Offsets		Two-Factor Authentication Interception	Pass the Ticket	Regsvcs/Regasm	Screen Capture	Scheduled Transfer	Multiband Communication	
Service Registry Permissions Weakness				Network Service Scanning	Remote Desktop Protocol	Regsvr32	Audio Capture	Multilayer Encryption	
Web Shell	Indicator Blocking			Remote File Copy	Rundll32	Video Capture	Execution over Module Load	Scheduled Transfer	
Basic Input/Output System	Exploitation of Vulnerability			Peripheral Device Discovery	Remote Services	Scheduled Task			
Bootkit	Bypass User Account Control				Scripting				
	DLL Injection				Service Execution				
Change Default File Association	Component Object Model Hijacking				Windows Management Instrumentation				
Component Firmware	Indicator Removal from Tools				MSBuild				
Hypervisor	Indicator Removal on Host								
Logon Scripts									
Modify Existing Service									
Redundant Access									
Registry Run Keys / Start Folder									
Security Support Provider									
Shortcut Modification									
Windows Management Instrumentation Event Subscription									
Winlogon Helper DLL									
Netsh Helper DLL									
Authentication Package									
External Remote Services									

Define your threat model

Assess your coverage

Identify gaps

Fill gaps

[Home](#) > [Evaluations](#)APT3 ▾ Evaluations

CarbonBlack

Carbon Black.[Carbon Black](#) [Response](#)

CounterTack

 GoSECURE
CounterTack[CounterTack](#)

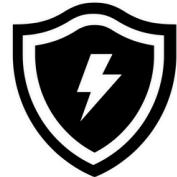
CrowdStrike

[CrowdStrike](#) [Falcon](#) [Endpoint Protection Standard Bundle](#)
[Overwatch](#) [Insight](#) [Prevent](#)

Endgame

ENDGAME.[Endgame](#)

Microsoft

**Windows
Defender ATP**[Microsoft](#) [Defender](#) [Windows Defender ATP](#)

RSA

RSA®[RSA](#) [NetWitness](#)

SentinelOne

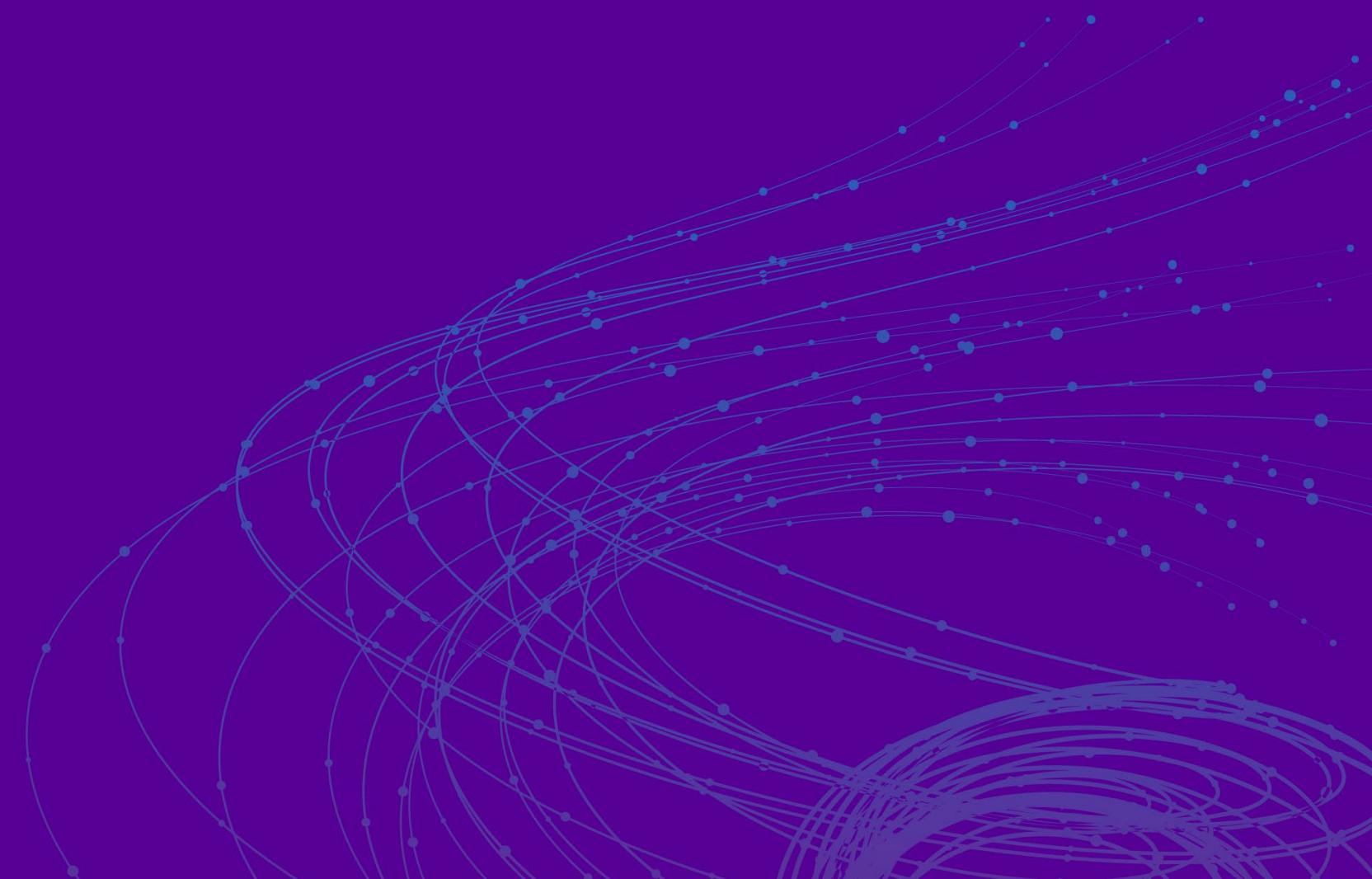
[SentinelOne](#)

Polling Question 2

- AIR-T07
- In which area do you think ATT&CK would be most useful?
 - A. Taxonomy
 - B. Prevention
 - C. Detection
- Results

RSA® Conference 2019

Share More



Share Insights and Contribute

- Sharing TTPs/analytics/SIGMA rules is easier than sharing IOCs
 - Higher level of abstraction
 - Better protection of the victim's identity
- It's also more useful
 - More context
 - More stable in time

EU ATT&CK User Community

- Mailing list -> opt in ? -> email to info@circl.lu
- Next workshop in Brussels 9-10 May 2019

Workshop - EU ATT&CK Community

Next workshop - event for EU ATT&CK Community

Polling Question 3

- AIR-T07
- What would be the most useful to operationalize ATT&CK??
 - A. Better Web Content
 - B. Webinars
 - C. Community Activities - Workshops
- Results

“Apply” Slide

- Next week you should:
 - Familiarize yourself with the ATT&CK documentation and resources
- In the first three months following this presentation you should:
 - Identify Your Adversaries
 - Identify and deploy at least three use cases in your organization
- Within six months you should:
 - Permeate the whole of your cyber defense using ATT&CK

Resources

- [ATT&CK repository](#) and [ATT&CK Navigator](#)
- STIX: <https://github.com/mitre/cti>
- TAXII: <https://cti-taxii.mitre.org/taxii>
- MITRE [Common Analytics Repository](#) and [CARET](#)
- [SIGMA](#) and [SIGMA rule collection](#) (Thomas Patzke, Florian Roth)
- [SIGMA Marketplace](#) and [Sigma Editor](#) (SOCPRIME)
- [Threathunter Playbook](#) (Roberto Rodriguez)
- [ThreatHunting](#) Splunk APP (Olaf Hartong)
- [Atomic Treat Coverage](#) Analytics documentation system (Tieto)