RSAConference2019
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
attack.mitre.org

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

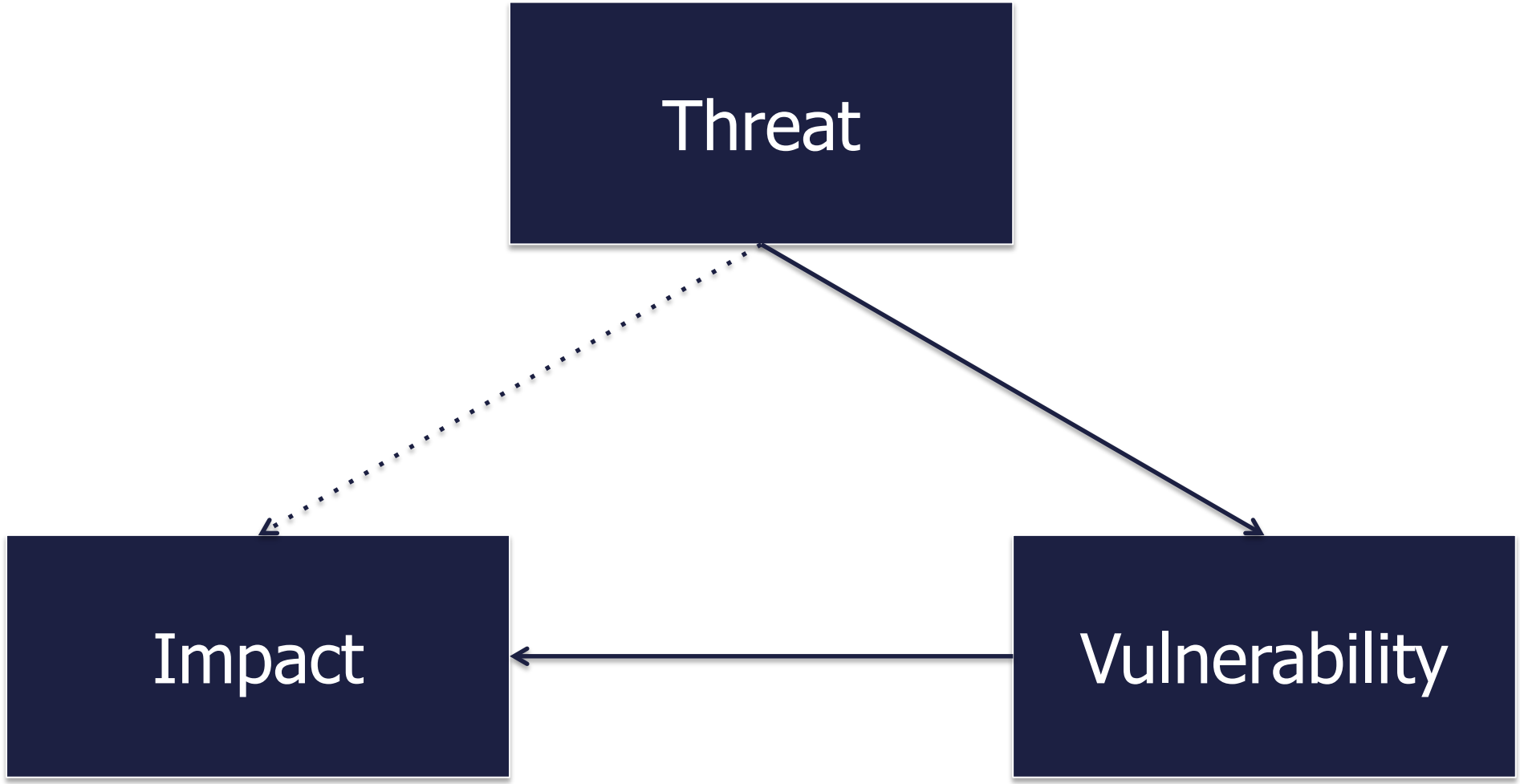
10% of all computers in UA destroyed !

Massive collateral damage: > 3 billion $

Threat Landscape 2019: Agile Adversaries

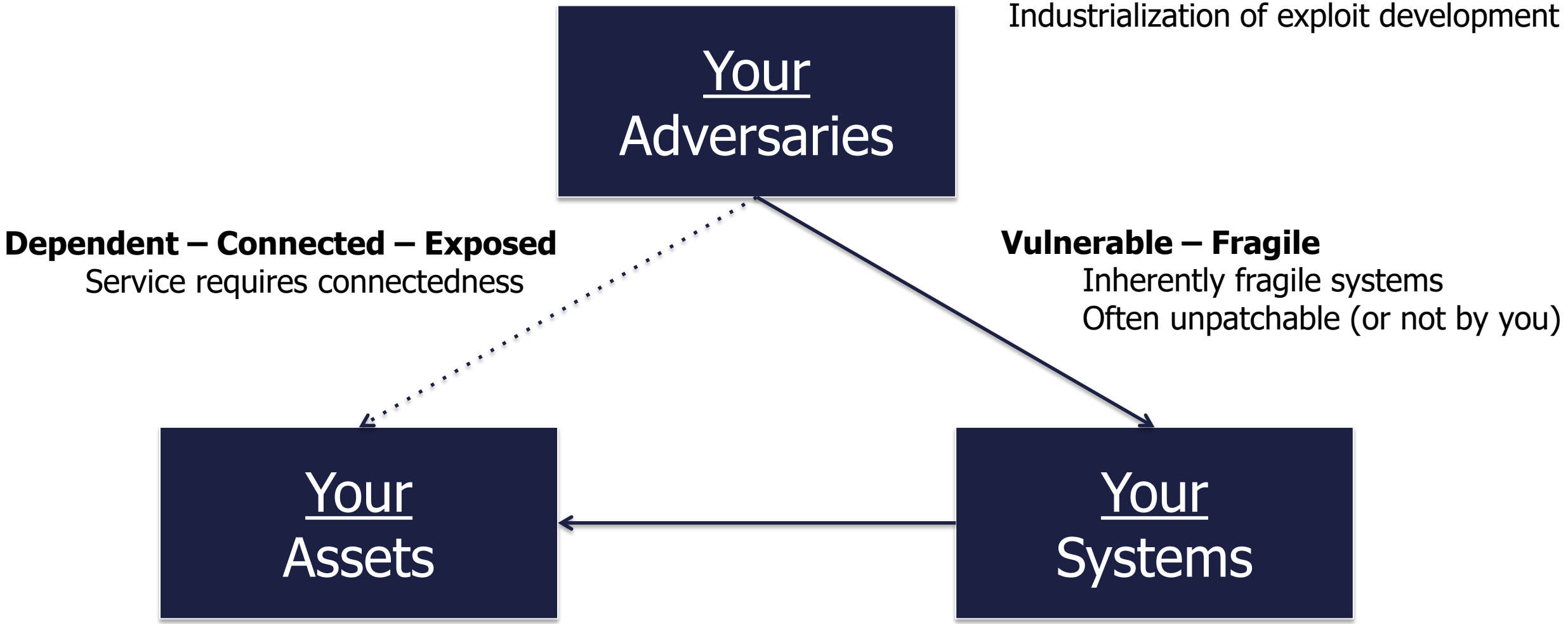
- Adaptive Adversary infrastructure
- Blending in with legitimate user
  - Using legitimate infrastructure components (PowerShell, Macros)
  - Abusing legitimate credentials
  - Replicating legitimate user behavior
- Fast uptake of new vulnerabilities and leaked tools

Risk-Based Defense

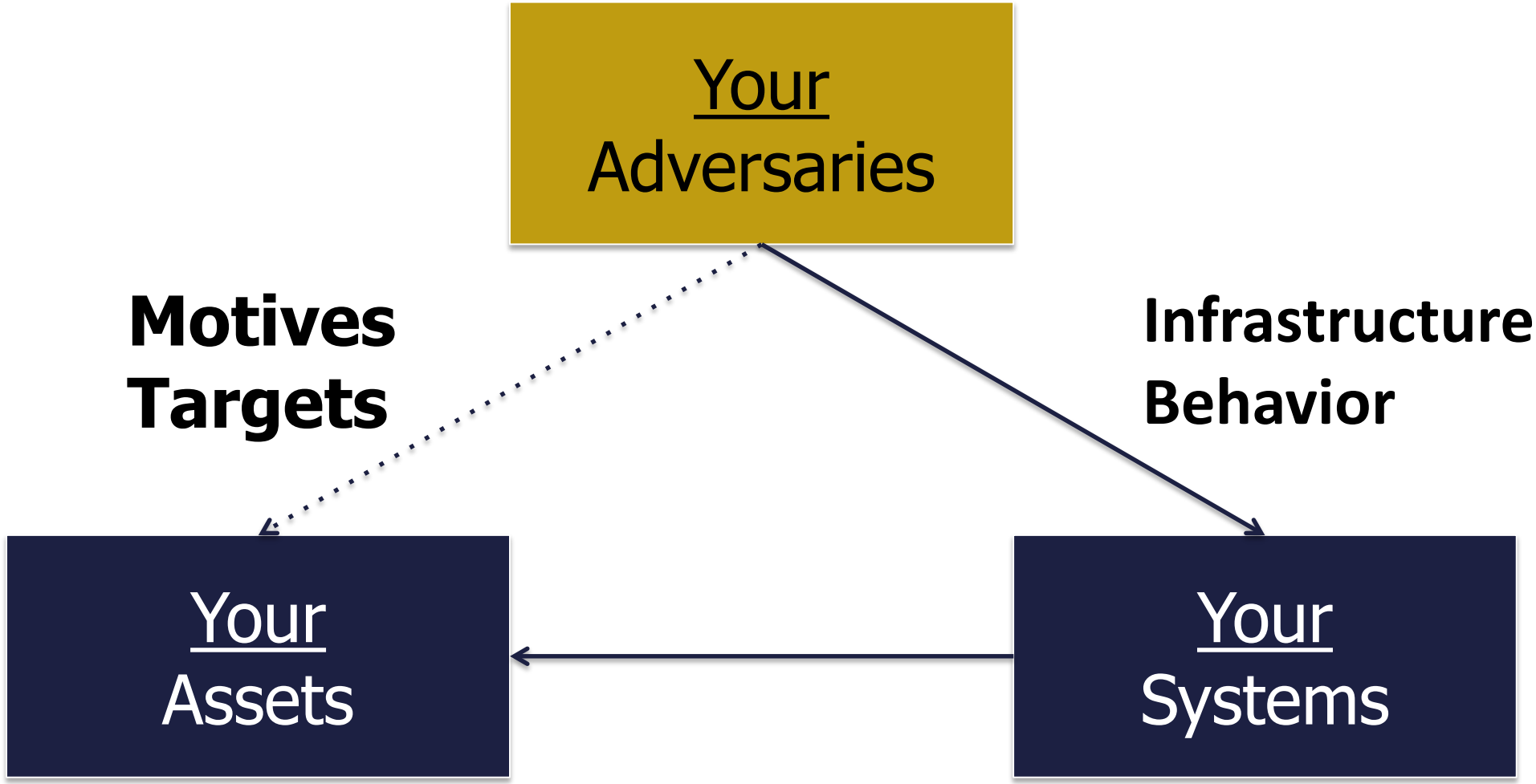


Threat-Informed Defense

Agile Adversaries
Industrialization of exploit development



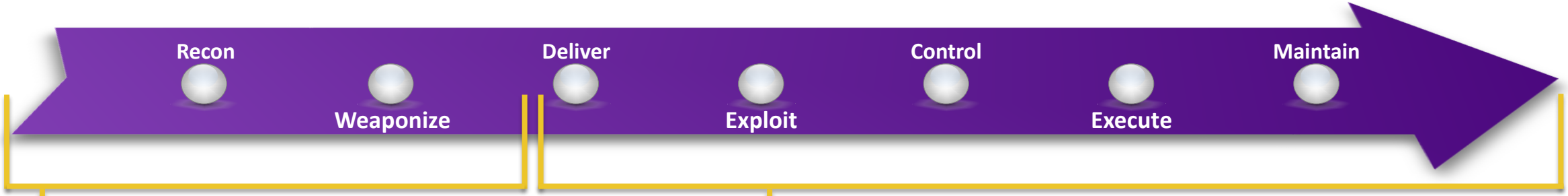
Identify Your Threats to Improve Your Defense



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!

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	AppInit 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

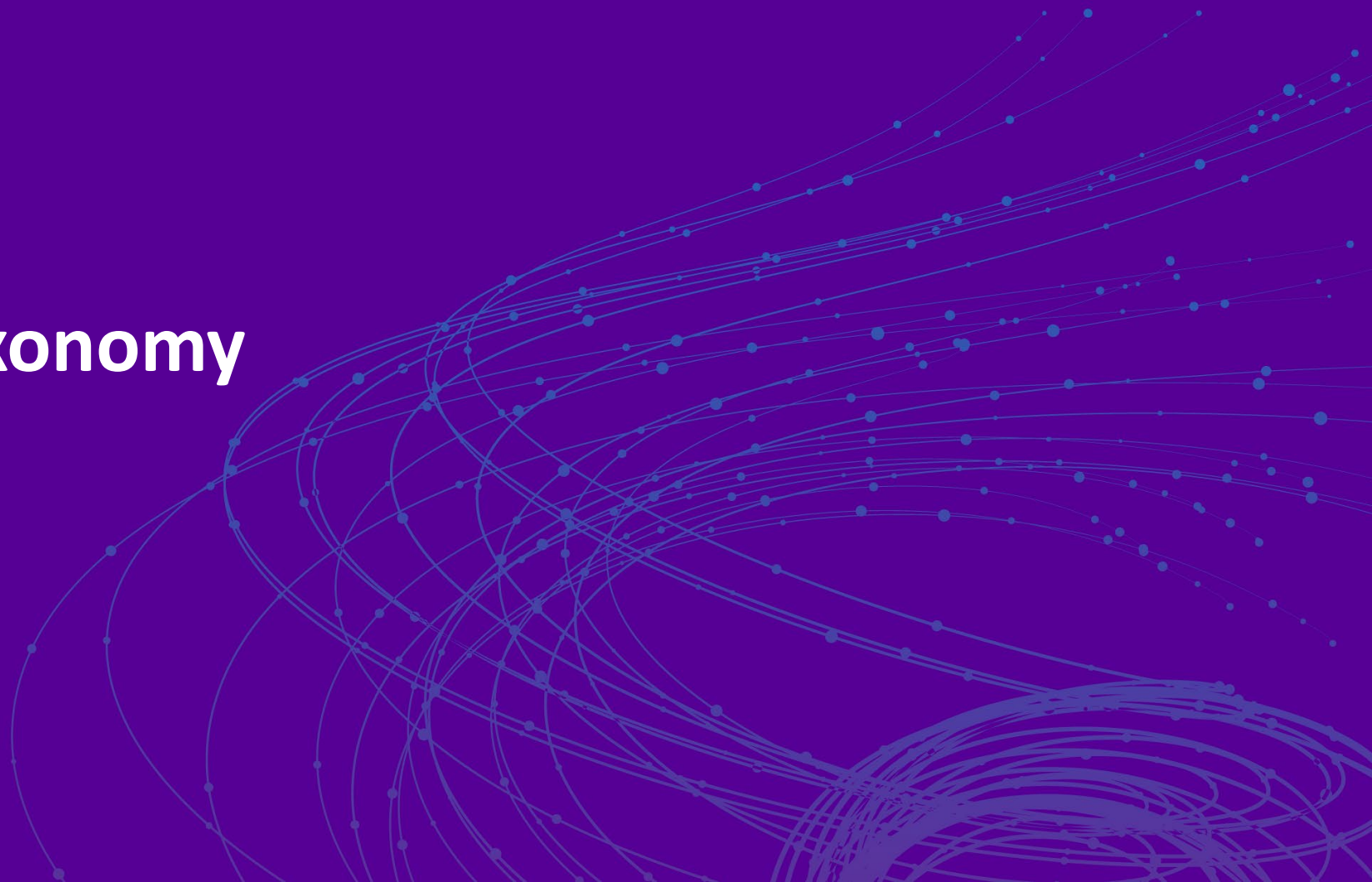
- Common Taxonomy

- 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

RSAConference2019

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	`~/.bash_profile` and `~/.bashrc` 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. `~/.bash_profile` is executed for login shells and `~/.bashrc` 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), `~/.bash_profile` is executed before the initial command prompt is returned to the user. After that, every time a new shell is opened, `~/.bashrc` 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 `runas`.
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

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

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

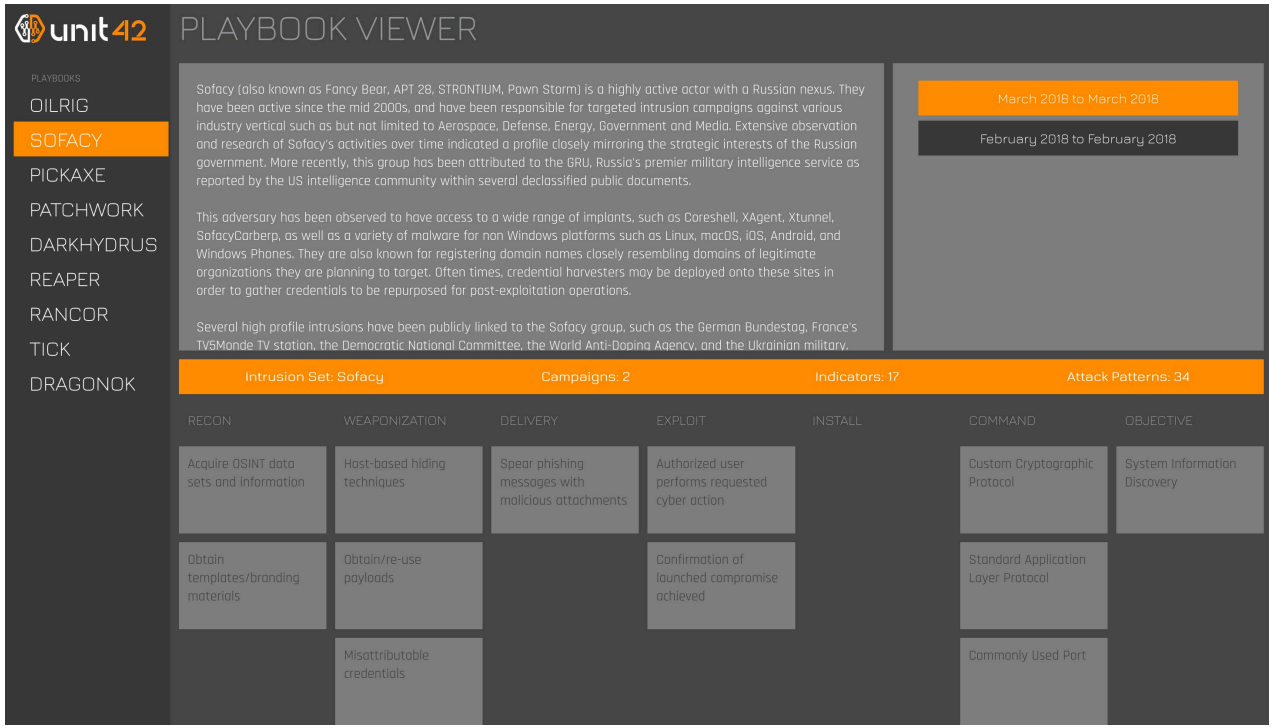
Contributors: Richard Gold, Digital Shadows

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]

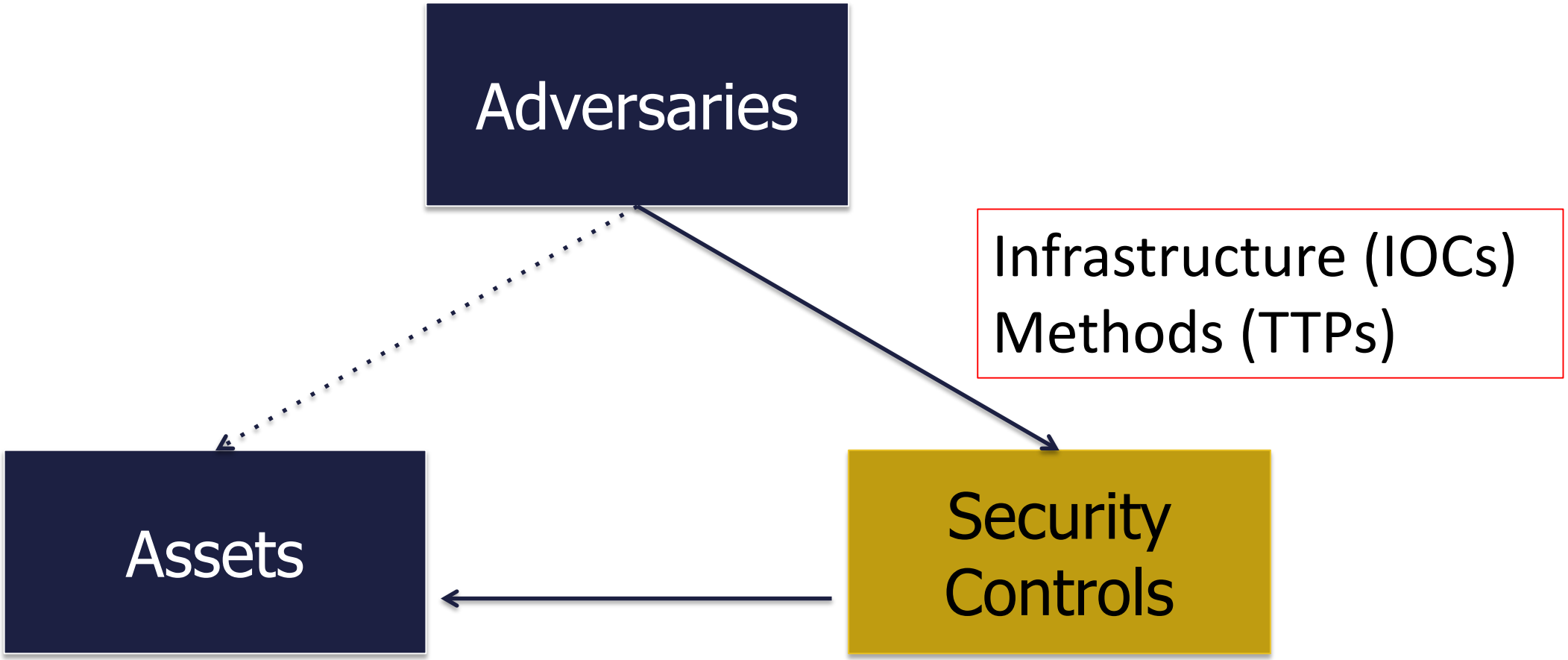
Vendors Use MITRE ATT&CK in their Reports



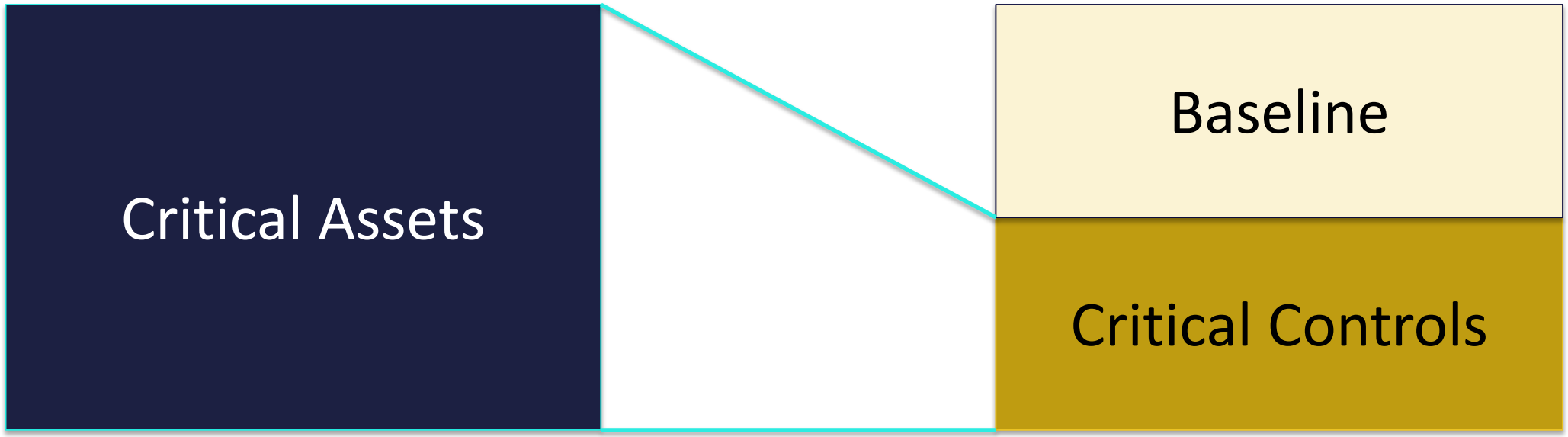
RSAConference2019

Prevention, Detection and Response

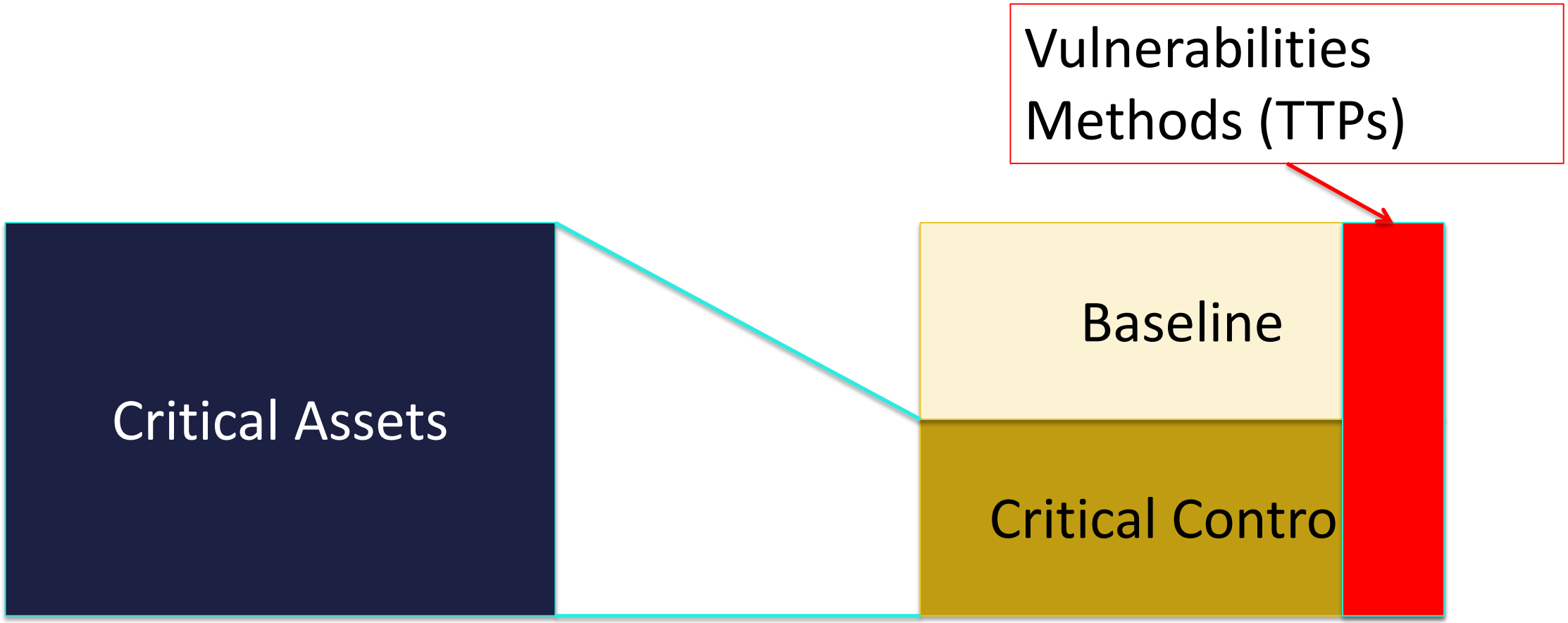
Understand Your Controls



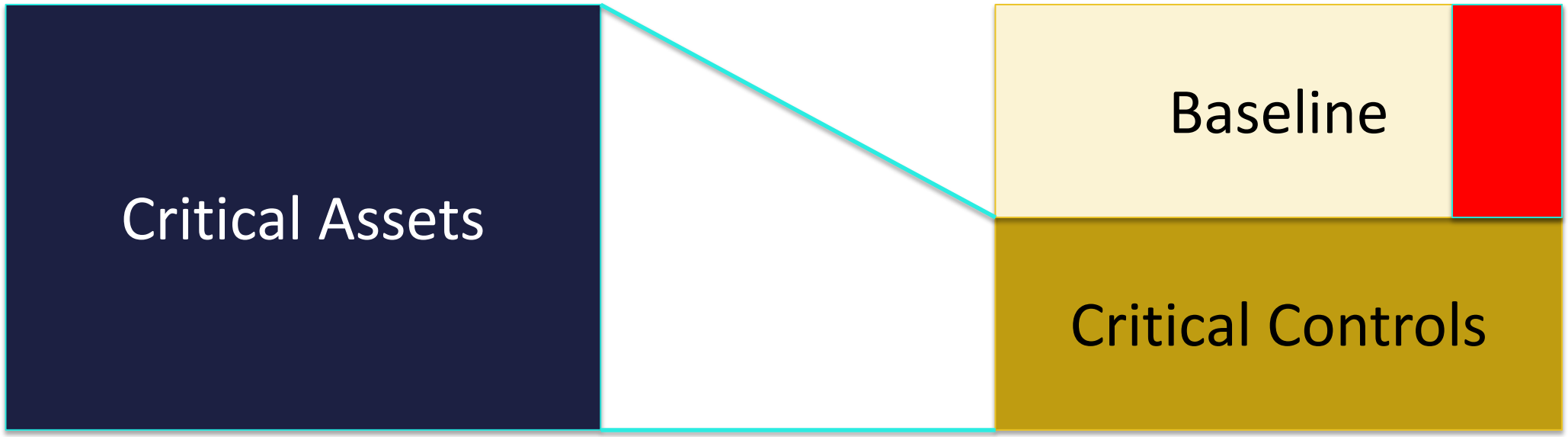
Critical Controls for Your Critical Assets



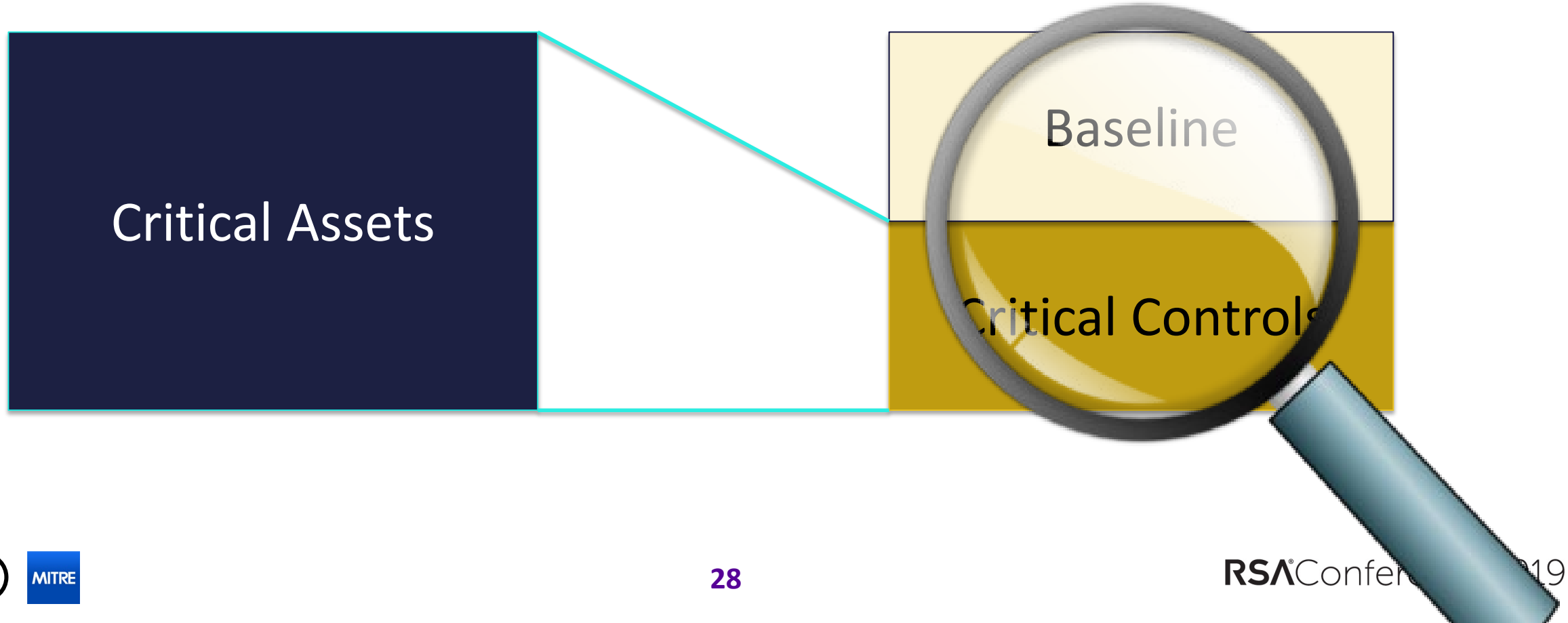
Monitor and Discover Exposure



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

stages: act
platforms: windows

legend

- Lazarus
- APT15
- Common techniques

Initial Access (10 items)	Execution (25 items)	Persistence (41 items)	Privilege Escalation (21 items)	Defense Evasion (49 items)	Credential Access (16 items)	Discovery (19 items)	Lateral Movement (15 items)	Collection (13 items)	Exfiltration (9 items)	Command And Control (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	Exploitation 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	Logon Scripts	Data from Information Repositories	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	BITS Jobs	Bypass User Account Control	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Exploitation for Client Execution	Bootkit	DLL Search 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	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Peripheral Device Discovery	Remote File Copy	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Permission Groups Discovery	Remote Services	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	LSASS Driver	Component Firmware	File System Permissions Weakness	DCShadow	Kerberoasting	Process Discovery	Replication Through Removable Media	Input Capture		Multi-hop Proxy
	Mshta	Component Object Model Hijacking	Hooking	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning	Query Registry	Shared Webroot	Man in the Browser		Multi-Stage Channels
	PowerShell	Create Account	Image File Execution Options Injection	Disabling Security Tools	Network Sniffing	Remote System Discovery	Taint Shared Content	Screen Capture		Multiband Communication
	Regsvcs/Regasm	DLL Search Order Hijacking	New Service	DLL Search Order Hijacking	Password Filter DLL	Security Software Discovery	Third-party Software	Video Capture		Multilayer Encryption
	Regsvr32	External Remote Services	Path Interception	DLL Side-Loading	Private Keys	System Information Discovery	Windows Admin Shares			Remote Access Tools
	Rundll32	File System Permissions Weakness	Port Monitors	Exploitation for Defense Evasion	Replication Through Removable Media	System Network Configuration Discovery	Windows Remote Management			Remote File Copy
	Scheduled Task	Hidden Files and Directories	Process 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 Folder		Mshta						
		Scheduled Task		Network Share Connection Removal						
		Screensaver		NTFS File Attributes						
		Security Support Provider		Obfuscated Files or Information						
		Service Registry Permissions Weakness		Process Doppelgänging						
		Shortcut Modification		Process Hollowing						
		SIP and Trust Provider Hijacking		Process Injection						
		System Firmware		Redundant Access						
		Time Providers		Regsvcs/Regasm						
		Valid Accounts		Regsvr32						
		Web Shell		Rootkit						
		Windows Management Instrumentation Event Subscription		Rundll32						

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	Exploitation 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	Logon Scripts	Data from Information Repositories	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	BITS Jobs	Bypass User Account Control	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Exploitation for Client Execution	Bootkit	DLL Search 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	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Peripheral Device Discovery	Remote File Copy	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Permission Groups Discovery	Remote Services	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	LSASS Driver	Component Firmware	File System Permissions Weakness	DCShadow	Kerberoasting	Process Discovery	Replication Through Removable Media	Input Capture		Multi-hop Proxy
	Mshta	Component Object Model Hijacking	Hooking	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning	Query Registry	Shared Webroot	Man in the Browser		Multi-Stage Channels
	PowerShell	Create Account	Image File Execution Options Injection	Disabling Security Tools	Network Sniffing	Remote System Discovery	Taint Shared Content	Screen Capture		Multiband Communication
	Regsvcs/Regasm	DLL Search Order Hijacking	New Service	DLL Search Order Hijacking	Password Filter DLL	Security Software Discovery	Third-party Software	Video Capture		Multilayer Encryption
	Regsvr32	External Remote Services	Path Interception	DLL Side-Loading	Private Keys	System Information Discovery	Windows Admin Shares			Remote Access Tools
	Rundll32	File System Permissions Weakness	Port Monitors	Exploitation for Defense Evasion	Replication Through Removable Media	System Network Configuration Discovery	Windows Remote Management			Remote File Copy
	Scheduled Task	Hidden Files and Directories	Process 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						
				Masquerading						

+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	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	Exploitation 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	Logon Scripts	Data from Information Repositories	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	BITS Jobs	Bypass User Account Control	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Exploitation for Client Execution	Bootkit	DLL Search 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	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Peripheral Device Discovery	Remote File Copy	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Permission Groups Discovery	Remote Services	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	LSASS Driver	Component Firmware	File System Permissions Weakness	DCShadow	Kerberoasting	Process Discovery	Replication Through Removable Media	Input Capture		Multi-hop Proxy
	Mshta	Component Object Model Hijacking	Hooking	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning	Query Registry	Shared Webroot	Man in the Browser		Multi-Stage Channels
	PowerShell	Create Account	Image File Execution Options Injection	Disabling Security Tools	Network Sniffing	Remote System Discovery	Taint Shared Content	Screen Capture		Multiband Communication
	Regsvcs/Regasm	DLL Search Order Hijacking	New Service	DLL Search Order Hijacking	Password Filter DLL	Security Software Discovery	Third-party Software	Video Capture		Multilayer Encryption
	Regsvr32	External Remote Services	Path Interception	DLL Side-Loading	Private Keys	System Information Discovery	Windows Admin Shares			Remote Access Tools
	Rundll32	File System Permissions Weakness	Port Monitors	Exploitation for Defense Evasion	Replication Through Removable Media	System Network Configuration Discovery	Windows Remote Management			Remote File Copy
	Scheduled Task	Hidden Files and Directories	Process 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						
				Masquerading						

Analytics Instead of Indicators

Detect known bad
Artifact-driven
Fewer false positives
More atomic
Higher quantity

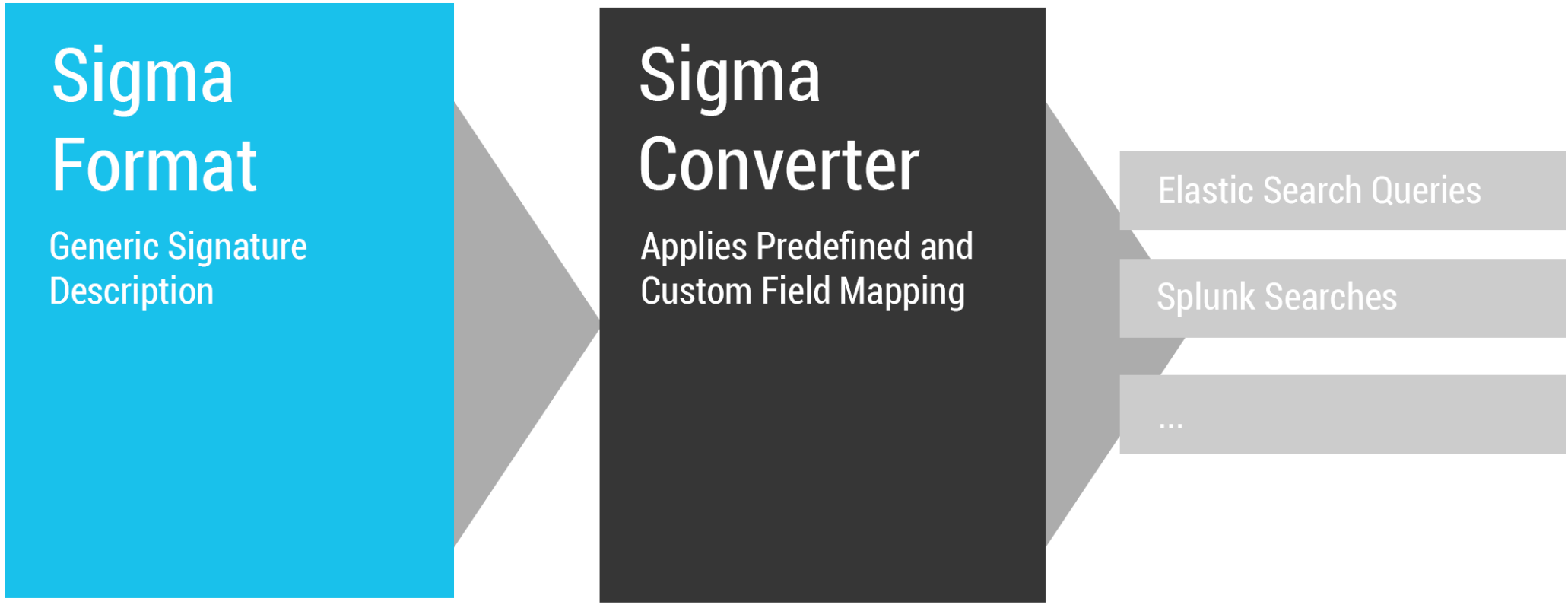
Detect suspicious events
Behavior-driven
More false positives
Broader
Lower quantity
Longer lifetime

*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

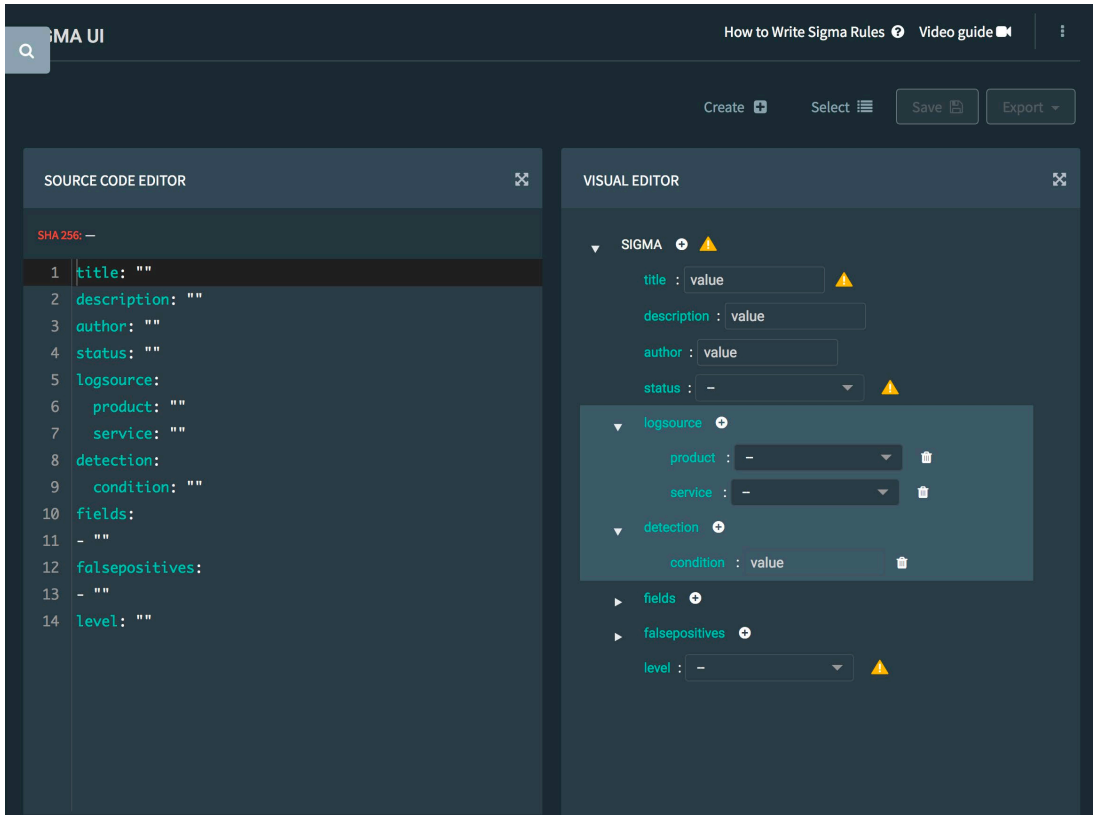
Convert your Analytics in Pseudo-Code



https://github.com/Neo23x0/sigma

Community Tools

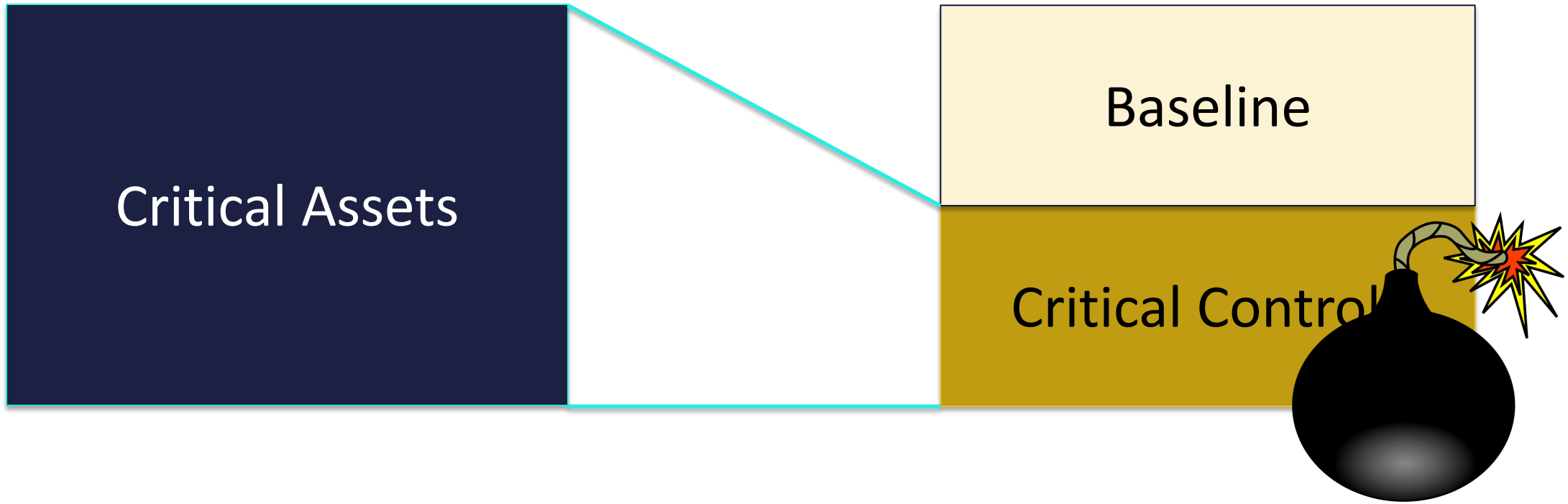
SIGMA Editor



Atomic Threat Coverage

Analytics Documentation

Test Your Controls

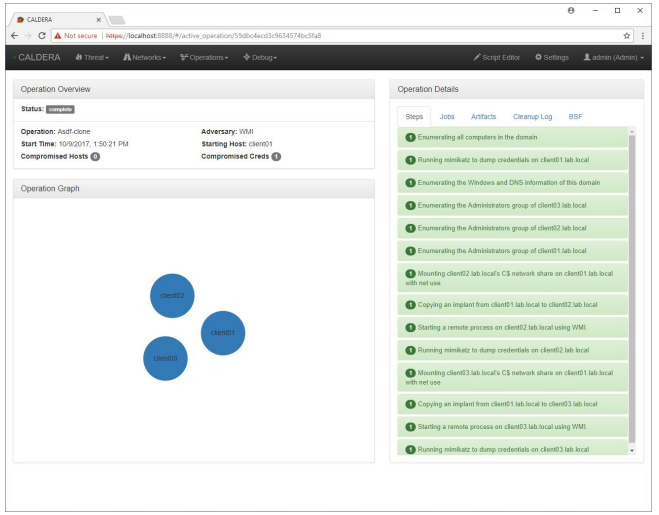


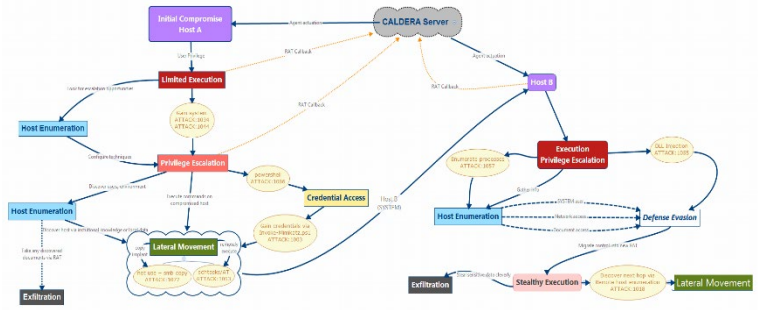
Red Team Tools

- Active testing of controls using MITRE ATT&CK
  - MITRE Caldera
  - Endgame RTA
  - Red Canary Atomic Red Team
  - Uber Metta

CALDERA

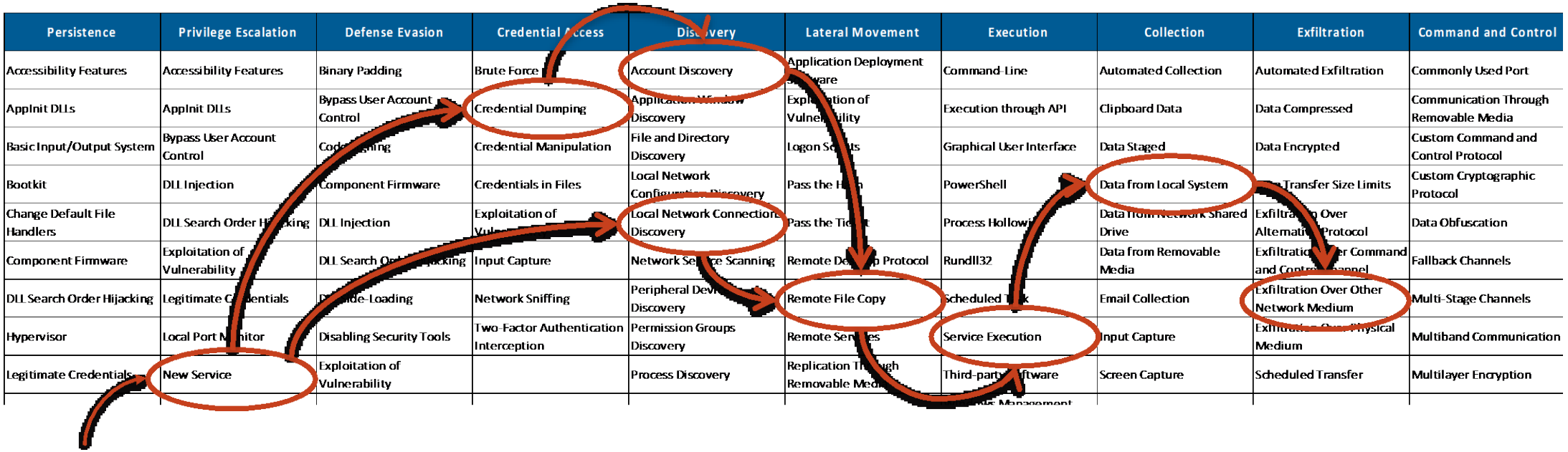
- Automated adversary emulation
  - Safely replicate realistic adversary behavior
  - Repeatable testing and verification of prevention/detection
- Features
  - Uses ATT&CK to create Adversary profiles
  - Uses AI and modeling to make decisions about actions
  - Self-cleans after operation completes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





Emulate Adversaries

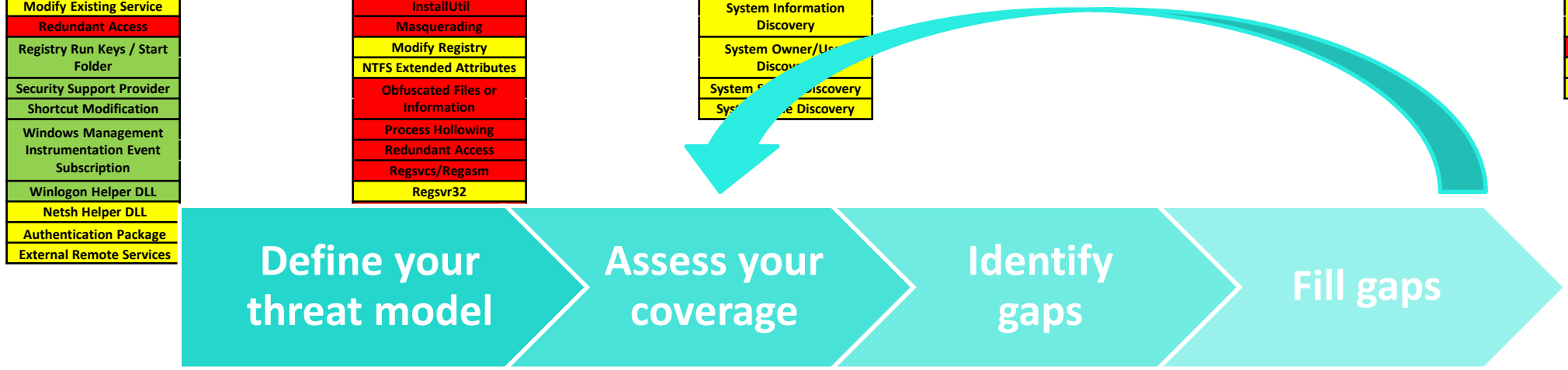
- Connect techniques in attack sequence
- Test patterns of behavior focusing on defense effectiveness
- Triage events



Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Accessibility Features	Accessibility Features	Binary Padding	Brute Force	Account Discovery	Application Deployment Software	Command-Line	Automated Collection	Automated Exfiltration	Commonly Used Port
AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Application Window Discovery	Exploitation of Vulnerability	Execution through API	Clipboard Data	Data Compressed	Communication Through Removable Media
Basic Input/Output System	Bypass User Account Control	Code Signing	Credential Manipulation	File and Directory Discovery	Logon Scripts	Graphical User Interface	Data Staged	Data Encrypted	Custom Command and Control Protocol
Bootkit	DLL Injection	Component Firmware	Credentials in Files	Local Network Configuration Discovery	Pass the Hash	PowerShell	Data from Local System	Data Transfer Size Limits	Custom Cryptographic Protocol
Change Default File Handlers	DLL Search Order Hijacking	DLL Injection	Exploitation of Vulnerability	Local Network Connections Discovery	Pass the Ticket	Process Hollowing	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	Data Obfuscation
Component Firmware	Exploitation of Vulnerability	DLL Search Order Hijacking	Input Capture	Network Service Scanning	Remote Desktop Protocol	Rundll32	Data from Removable Media	Exfiltration Over Command and Control Channel	Fallback Channels
DLL Search Order Hijacking	Legitimate Credentials	Dylib Hijacking	Network Sniffing	Peripheral Device Discovery	Remote File Copy	Scheduled Task	Email Collection	Exfiltration Over Other Network Medium	Multi-Stage Channels
Hypervisor	Local Port Monitor	Disabling Security Tools	Two-Factor Authentication Interception	Permission Groups Discovery	Remote Services	Service Execution	Input Capture	Exfiltration Over Physical Medium	Multiband Communication
Legitimate Credentials	New Service	Exploitation of Vulnerability		Process Discovery	Replication Through Removable Media	Third-party Software	Screen Capture	Scheduled Transfer	Multilayer Encryption
						Windows Management			

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			Application Deployment Software	Command-Line	Data Staged	Data Encrypted	
AppInit DLLs		Code Signing	Credential Manipulation	File and Directory Discovery		Execution through API	Data from Local System	Data Transfer Size Limits	Custom Command and Control Protocol
Local Port Monitor		Component Firmware			Exploitation of Vulnerability	Graphical User Interface	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	
New Service		DLL Side-Loading	Credentials in Files	Local Network Configuration Discovery		InstallUtil			Custom Cryptographic Protocol
Path Interception		Disabling Security Tools	Input Capture		Logon Scripts	PowerShell	Data from Removable Media	Exfiltration Over Command and Control Channel	
Scheduled Task		File Deletion	Network Sniffing	Local Network Connections Discovery	Pass the Hash	Process Hollowing			Data Obfuscation
File System Permissions Weakness		File System Logical Offsets	Two-Factor Authentication Interception		Pass the Ticket	Regsvcs/Regasm	Email Collection		Fallback Channels
Service Registry Permissions Weakness				Network Service Scanning	Remote Desktop Protocol	Regsvr32	Input Capture	Exfiltration Over Other Network Medium	Multi-Stage Channels
Web Shell		Indicator Blocking		Peripheral Device Discovery	Remote File Copy	Rundll32	Screen Capture		Multiband Communication
Basic Input/Output System	Exploitation of Vulnerability				Remote Services	Scheduled Task	Audio Capture	Exfiltration Over Physical Medium	
Bootkit	Bypass User Account Control			Permission Groups Discovery	Replication Through Removable Media	Scripting	Video Capture		Multilayer Encryption
Change Default File Association	DLL Injection			Process Discovery	Shared Webroot	Service Execution		Scheduled Transfer	Peer Connections
Component Firmware	Component Object Model Hijacking	Indicator Removal from Tools		Query Registry	Taint Shared Content	Windows Management Instrumentation			Remote File Copy
Hypervisor		Indicator Removal on Host		Remote System Discovery	Windows Admin Shares	MSBuild			Standard Application Layer Protocol
Logon Scripts				Security Software Discovery		Execution through Module Load			Standard Cryptographic Protocol
Modify Existing Service		InstallUtil		System Information Discovery					Standard Non-Application Layer Protocol
Redundant Access		Masquerading		System Owner/User Discovery					Uncommonly Used Port
Registry Run Keys / Start Folder		Modify Registry		System Service Discovery					Web Service
Security Support Provider		NTFS Extended Attributes		System Time Discovery					Data Encoding
Shortcut Modification		Obfuscated Files or Information							
Windows Management Instrumentation Event Subscription		Process Hollowing							
Winlogon Helper DLL		Redundant Access							
Netsh Helper DLL		Regsvcs/Regasm							
Authentication Package		Regsvr32							
External Remote Services									



Filter

APT3 Evaluations

CarbonBlack

Carbon Black.

Carbon Black | Response

CounterTack

GoSecure CounterTack

CounterTack

CrowdStrike

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

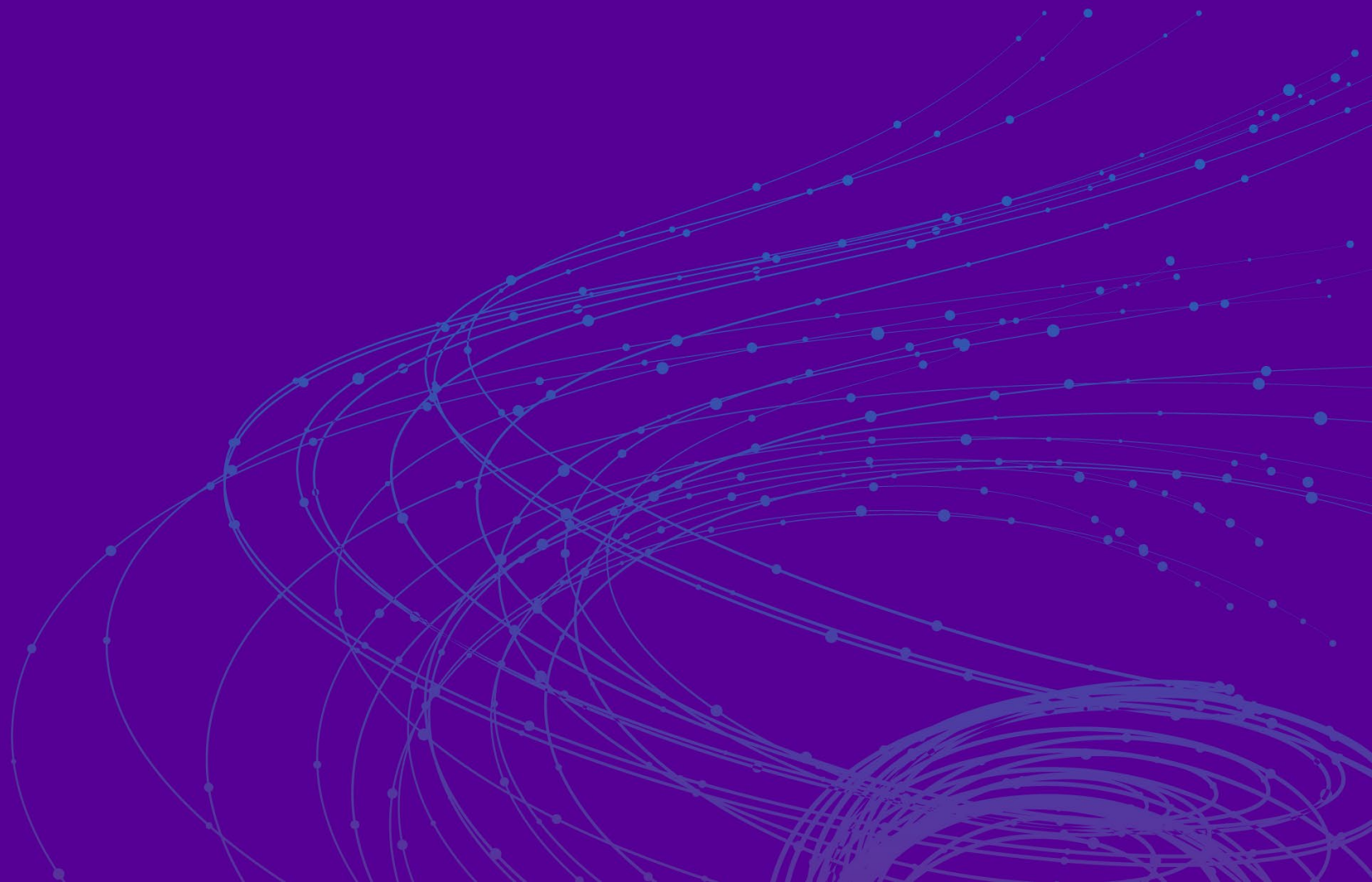
SentinelOne

Polling Question 2

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

RSAConference2019

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

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)