TIDAL

THREAT-INFORMED DEFENSE

So You've Decided to Use MITRE ATT&CK®: *Now What?*

November 30, 2022

PRESENTED BY:

Rich Struse, CTO
Scott Small, Director of CTI

Learning objectives

- Threat-informed defense and its applications
- The benefits and limitations of MITRE ATT&CK
- How to develop a threat-informed defense strategy

Note: All of the resources referenced in this presentation are freely-available community resources.

TIDAL

Threat-Informed Defense and its Applications

What is "Threat-Informed Defense"?

Threat-Informed Defense

"The systematic application and deep understanding of adversary tradecraft and technology to assess, organize and optimize your defenses."†

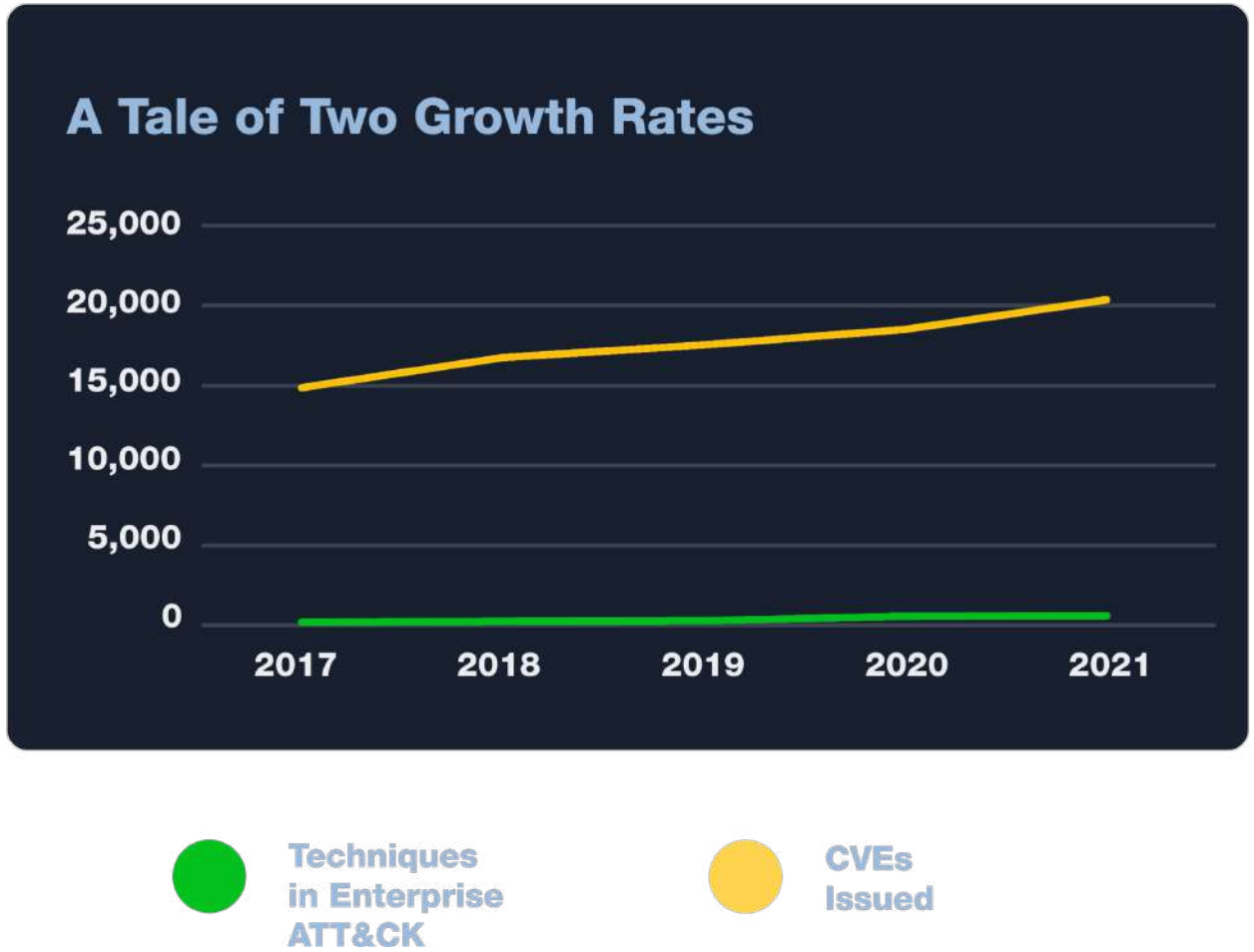
- Understanding adversary tactics, techniques and procedures is critical to effectively defending your systems
- Without this, you're left with defending against anything and everything
- Threat-Informed Defense helps you to prioritize where to allocate time and resources for security

† https://www.tidalcyber.com/blog/threat-informed-defense-what-is-it

TIDAL

Why is Threat-Informed Defense so important?

Because the Old Way Doesn't Work



- It is not feasible to ensure everything in your enterprise is always fully-patched against exploitable vulnerabilities

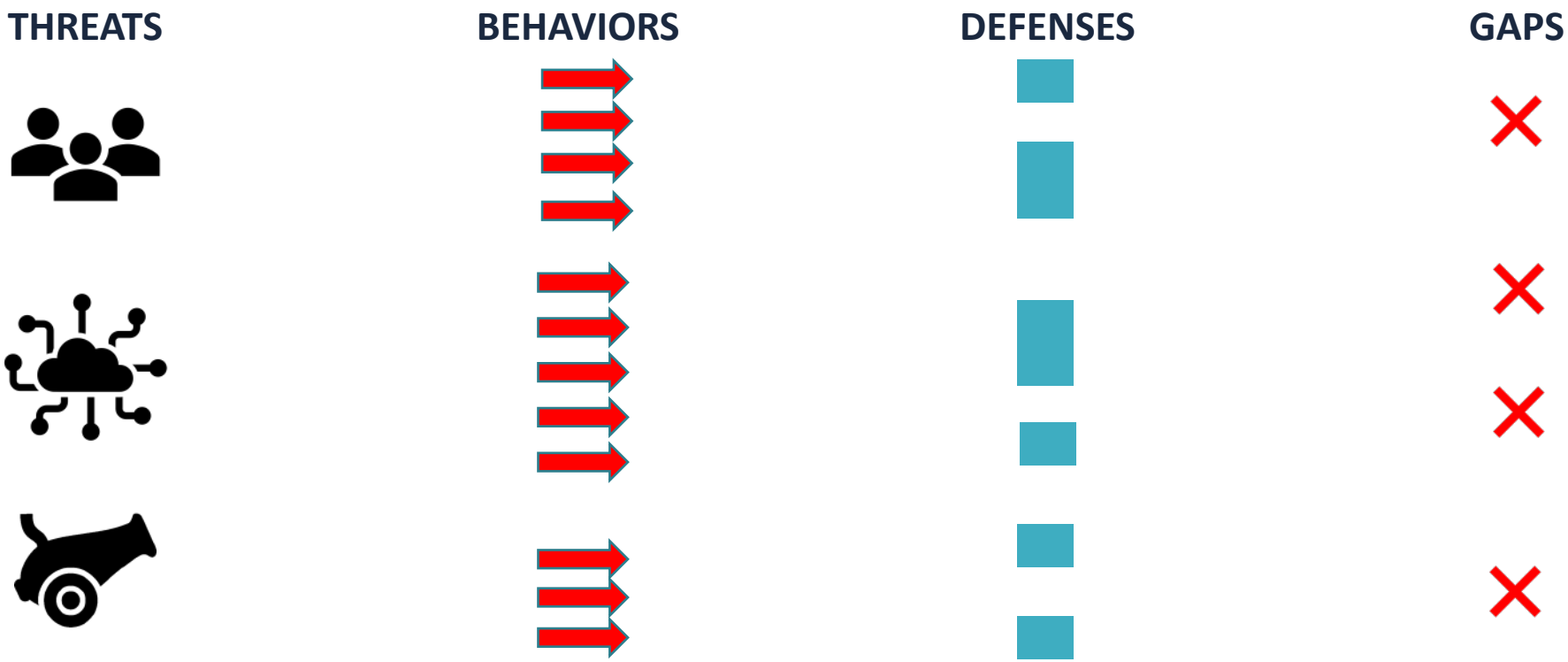
TIDAL

Supports Focus & Prioritization

- Threat-Informed Defense allows defenders to focus and prioritize their activities and investments, based on:
  - Specific threats they face including groups, software, campaigns – translated into the specific behaviors they employ
  - How existing defenses stack up against those behaviors
  - Identify key gaps

TIDAL

Mind the Gap(s)!



TIDAL

What is the MITRE ATT&CK knowledge base?

MITRE ATT&CK

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.†

- ATT&CK is the globally-accepted encyclopedia of adversary behaviors
- ATT&CK serves as a common language to facilitate communication within and between organizations
- ATT&CK is made freely-available by the non-profit MITRE Corporation

† https://attack.mitre.org/

TIDAL

MITRE ATT&CK: The Basics

Tactics: the "why" of an adversary's behavior – their technical objective

…

Persistence

Privilege Escalation

Credential Access

Lateral Movement

…

Techniques: the "how" of an adversary's behavior – the actions they take to achieve their objective

Create Account

Cloud Account

Domain Account

Local Account

Brute Force

Input Capture

Network Sniffing

Procedures: commands/APIs and parameters used

Sub-Techniques: more specific versions of some techniques

† https://attack.mitre.org/

TIDAL

MITRE ATT&CK: The Basics

Reconnaissance (10 techniques)	Resource Development (7 techniques)	Initial Access (9 techniques)	Execution (12 techniques)	Persistence (19 techniques)	Privilege Escalation (13 techniques)	Defense Evasion (39 techniques)	Credential Access (15 techniques)	Discovery (27 techniques)	Lateral Movement (9 techniques)	Collection (17 techniques)	Command and Control (16 techniques)	Exfiltration (9 techniques)	Impact (13 techniques)
Active Scanning ≡	Acquire Infrastructure ≡	Valid Accounts ≡	Scheduled Task/Job ≡			Modify Authentication Process ≡		System Service Discovery	Remote Services ≡	Data from Local System	Data Obfuscation ≡	Exfiltration Over Other Network Medium ≡	Data Destruction
Gather Victim Host Information ≡	Compromise Accounts ≡	Replication Through Removable Media	Windows Management Instrumentation	Valid Accounts ≡			Network Sniffing		Software Deployment Tools	Data from Removable Media	Fallback Channels		Data Encrypted for Impact
	Compromise Infrastructure ≡			Hijack Execution Flow ≡			OS Credential Dumping ≡	Application Window Discovery ≡			Application Layer Protocol ≡	Scheduled Transfer	Service Stop
Gather Victim Identity Information ≡	Develop Capabilities ≡	Trusted Relationship	Software Deployment Tools	Boot or Logon Initialization Scripts ≡		Direct Volume Access	Input Capture ≡		Replication Through Removable Media	Input Capture ≡	Proxy ≡	Data Transfer Size Limits	Inhibit System Recovery
	Establish Accounts ≡	Supply Chain Compromise ≡		Create or Modify System Process ≡		Rootkit	Brute Force ≡	System Network Configuration Discovery ≡		Data Staged ≡	Communication Through Removable Media	Exfiltration Over C2 Channel	Defacement ≡
Gather Victim Network Information ≡	Obtain Capabilities ≡	Hardware Additions	Shared Modules	Event Triggered Execution ≡		Obfuscated Files or Information ≡	Two-Factor Authentication Interception		Internal Spearphishing	Screen Capture			Firmware Corruption
	Stage Capabilities ≡	Exploit Public-Facing Application	User Execution ≡	Boot or Logon Autostart Execution ≡				System Owner/User Discovery	Use Alternate Authentication Material ≡	Email Collection ≡	Web Service ≡	Exfiltration Over Physical Medium ≡	Resource Hijacking
Gather Victim Org Information ≡			Exploitation for Client Execution	Account Manipulation ≡	Process Injection ≡		Exploitation for Credential Access			Clipboard Data	Multi-Stage Channels		Network Denial of Service ≡
		Phishing ≡		External Remote Services	Access Token Manipulation ≡			System Network Connections Discovery	Lateral Tool Transfer	Automated Collection	Ingress Tool Transfer	Exfiltration Over Web Service ≡	Endpoint Denial of Service ≡
Phishing for Information ≡		External Remote Services	System Services ≡	Office Application Startup ≡	Abuse Elevation Control Mechanism ≡		Steal Web Session Cookie		Taint Shared Content	Audio Capture	Data Encoding ≡		System Shutdown/Reboot
Search Closed Sources ≡		Drive-by Compromise	Command and Scripting Interpreter ≡	Create Account ≡	Domain Policy Modification ≡		Unsecured Credentials ≡	Permission Groups Discovery ≡	Exploitation of Remote Services	Video Capture	Traffic Signaling ≡	Automated Exfiltration ≡	Account Access Removal
Search Open Technical Databases ≡				Browser Extensions	Escape to Host	Indicator Removal on Host ≡	Credentials from Password Stores ≡			Man in the Browser	Remote Access Software	Exfiltration Over Alternative Protocol ≡	Disk Wipe ≡
			Native API	Traffic Signaling ≡	Exploitation for Privilege Escalation	Modify Registry		File and Directory Discovery	Remote Service Session Hijacking ≡	Data from Information Repositories ≡	Dynamic Resolution ≡		Data Manipulation ≡
Search Open Websites/Domains ≡			Inter-Process Communication ≡	BITS Jobs		Trusted Developer Utilities Proxy Execution ≡	Steal or Forge Kerberos Tickets ≡				Non-Standard Port	Transfer Data to Cloud Account	
				Server Software Component ≡		Traffic Signaling ≡		Peripheral Device Discovery		Man-in-the-Middle ≡	Protocol Tunneling		
Search Victim-Owned Websites			Container Administration Command	Pre-OS Boot ≡		Signed Script Proxy Execution ≡	Forced Authentication	Network Share Discovery		Archive Collected Data ≡	Encrypted Channel ≡		
				Compromise Client Software Binary		Rogue Domain Controller	Steal Application Access Token	Password Policy Discovery		Data from Network Shared Drive	Non-Application Layer Protocol		
			Deploy Container	Implant Container Image		Indirect Command Execution	Man-in-the-Middle ≡	Browser Bookmark Discovery		Data from Cloud Storage Object			
				Modify Authentication Process ≡		BITS Jobs	Forge Web Credentials ≡	Virtualization/Sandbox Evasion ≡		Data from Configuration Repository ≡			
						XSL Script Processing		Cloud Service Dashboard					
						Template Injection		Software Discovery ≡					
						File and Directory Permissions Modification ≡		Query Registry					
						Virtualization/Sandbox Evasion ≡		Remote System Discovery					
						Unused/Unsupported Cloud Regions		Network Service Scanning					
						Use Alternate Authentication Material ≡		Process Discovery					
						Impair Defenses ≡		System Information Discovery					
						Hide Artifacts ≡		Account Discovery ≡					
						Masquerading ≡		System Time Discovery					
						Deobfuscate/Decode Files or Information		Domain Trust Discovery					
						Signed Binary Proxy Execution ≡		Cloud Service Discovery					
						Exploitation for Defense Evasion		Container and Resource Discovery					
						Execution Guardrails ≡		Cloud Infrastructure Discovery					
						Modify Cloud Compute Infrastructure ≡		System Location Discovery					
						Pre-OS Boot ≡							
						Subvert Trust Controls ≡							
						Build Image on Host							
						Deploy Container							
						Modify System Image ≡							
						Network Boundary Bridging ≡							
						Weaken Encryption ≡							

≡ Has sub-techniques

MITRE ATT&CK®
Enterprise Framework

attack.mitre.org

† https://attack.mitre.org/

TIDAL

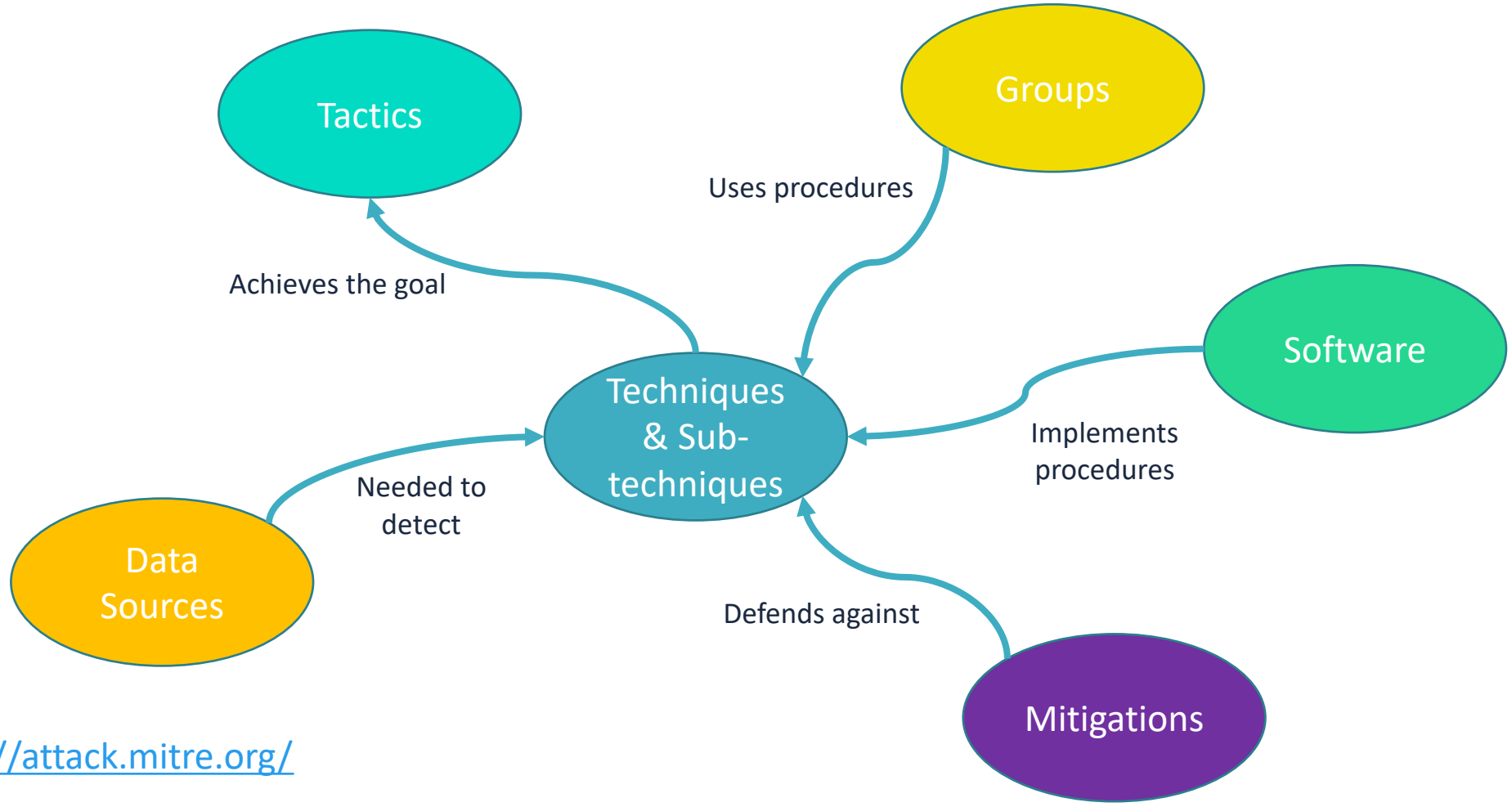
MITRE ATT&CK: Additional Data Resources

- **Groups**: Adversary groups linked to the techniques and software they employ
  - **Procedures**: specific examples of adversary implementations of techniques
- **Software**: Both malware and tools that adversaries use to achieve their objectives
- **Data Sources/Components**: Classification of data types mapped to the techniques they can be used to detect
- **References**: Published reporting cited to support inclusion in ATT&CK

† https://attack.mitre.org/

TIDAL

MITRE ATT&CK: Connecting the Dots



† https://attack.mitre.org/

TIDAL

MITRE ATT&CK: Benefits & Limitations

ATT&CK Benefits

- Provides a common foundation for threat-informed defense across geographic and sectorial boundaries
- Level of abstraction – tactics, techniques and sub-techniques balances specificity with manageable size/scope
- Vibrant community with many freely-available resources

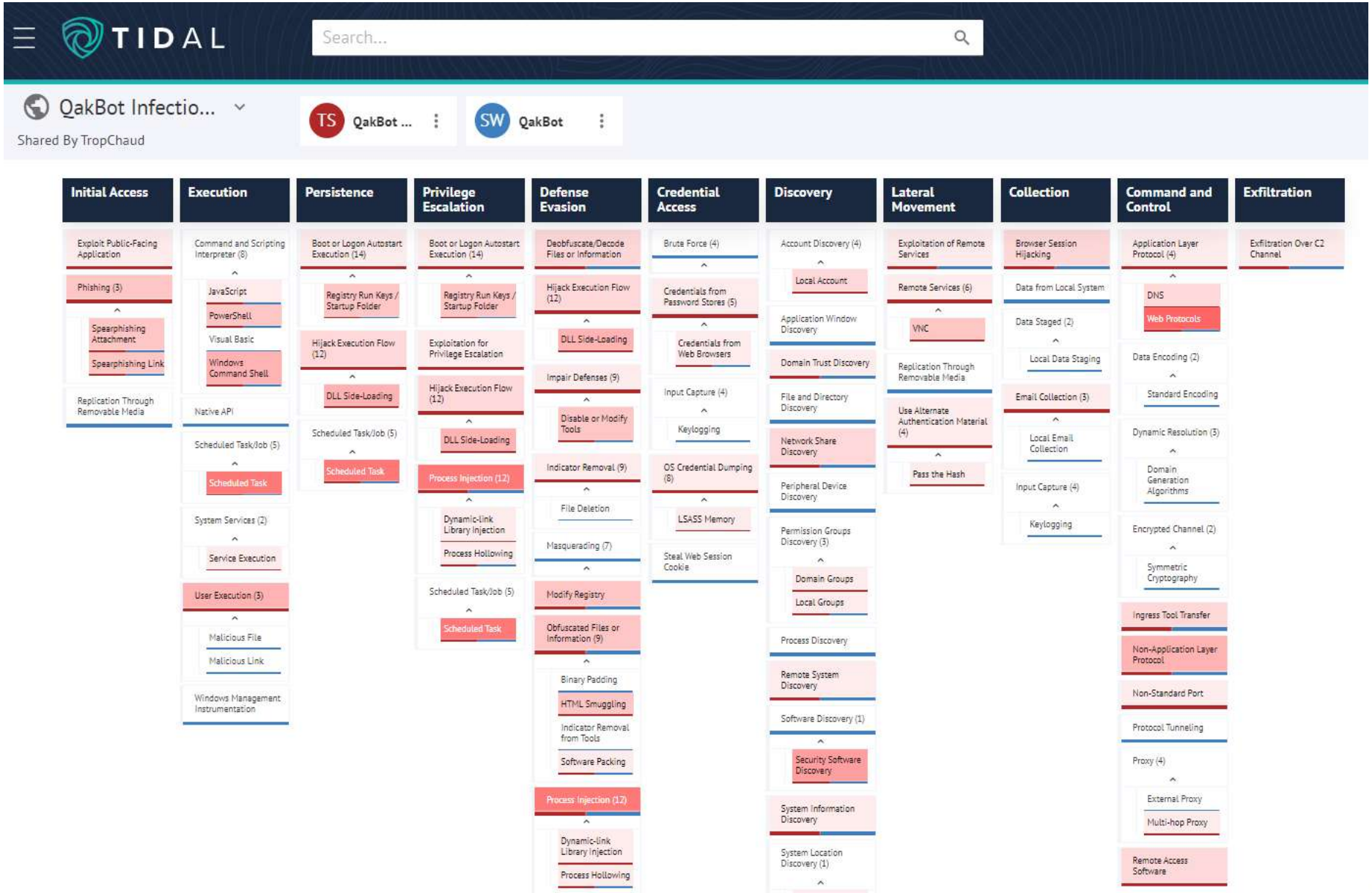
TIDAL

ATT&CK Realities

- MITRE relies on open-source reporting and community contributions as their inputs
  - Implication: it isn’t exhaustive (but nothing is) – think of it as a great starting point
- MITRE updates ATT&CK twice a year
  - Typically in April & October
- Level of abstraction – tactics, techniques and sub-techniques may not convey enough detail (i.e. procedures)
- Not all ATT&CK techniques are created equal
  - Some techniques are more important than others

TIDAL

ATT&CK Realities



TIDAL

Implementing Threat-Informed Defense

Step One: Identify your threats: Groups

TIDAL

Search...

Draft

GR APT29

Home > Groups

Groups

Search in groups | Motivation | Suspected Attribution: Russia | Observed Sectors: Energy | Observed Countries

Name	Associated Groups	Motivation	Suspected Attribution	Observed Sectors	Observed Countries	Add to Matrix
APT28	SNAKEMACKEREL, Swallowtail, Group 74 ...		Russia	Aerospace, Chemical, Defense ...	Afghanistan , France ...	
APT29	IRON RITUAL, IRON HEMLOCK, Dark Halo ...	Cyber Espionage	Russia	Aerospace, Education, Energy ...	Austria , Brazil ...	
Dragonfly	TEMP.Isotope, DYMALLOY, TG-4192 ...	Cyber Espionage	Russia	Energy, Government, Travel Services	France , Germany ...	
Sandworm Team	ELECTRUM, IRON VIKING, BlackEnergy (Group) ...	Destruction	Russia	Energy, Government	France , Georgia ...	
Wizard Spider	UNC1878, TEMP.MixMaster, Grim Spider	Financial Gain	Russia	Aerospace, Agriculture, Automotive ...	Australia , Belgium ...	

TIDAL

Step One: Identify your threats: Groups

TIDAL

Search...

Draft

GR APT29

Home > Groups > APT29

Groups

APT29

REMOVE FROM MATRIX

Suspected Attribution: Russia

Motivation: Cyber Espionage

Observed Countries: Austria, Brazil, China, France, Germany, Hungary, Japan, Republic of Korea, Mexico, Netherlands, New Zealand, Norway, Portugal, Spain, Turkey, Ukraine, United Kingdom, United States, Uzbekistan

Observed Sectors: Aerospace, Education, Energy, Financial Services, Government, Insurance, Legal, Manufacturing, Media, NGOs, Non Profit, Pharmaceuticals, Technology, Telecommunications, Think Tanks

Sources: MITRE, Tidal Cyber

APT29 is threat group that has been attributed to Russia's Foreign Intelligence Service (SVR).[White House Imposing Costs RU Gov April 2021][UK Gov Malign RIS Activity April 2021] They have operated since at least 2008, often targeting government networks in Europe and NATO member countries, research institutes, and think tanks. APT29 reportedly compromised the Democratic National Committee starting in the summer of 2015.[F-Secure The Dukes][GRIZZLY STEPPE JAR][Crowdstrike DNC June 2016][UK Gov UK Exposes Russia SolarWinds April 2021]

In April 2021, the US and UK governments attributed the SolarWinds supply chain compromise cyber operation to the SVR; public statements included citations to APT29, Cozy Bear, and The Dukes.[NSA Joint Advisory SVR SolarWinds April 2021][UK NSCS Russia SolarWinds April 2021] Victims of this campaign included government, consulting, technology, telecom, and other organizations in North America, Europe, Asia, and the Middle East. Industry reporting referred to the actors involved in this campaign as UNC2452, NOBELIUM, StellarParticle, and Dark Halo.[FireEye SUNBURST Backdoor December 2020][MSTIC NOBELIUM Mar 2021][CrowdStrike SUNSPOT Implant January 2021][Volexity SolarWinds][Cybersecurity Advisory SVR TTP May 2021]

Associated Groups (11) | Techniques (106) | Software (47) | References (49)

Name	Description
AADInternals	[MSTIC Nobelium Oct 2021]

TIDAL

Step One: Identify your threats: Software

TIDAL

Search...

Draft

GR APT29

SW Cobalt S...

Home > Software > Cobalt Strike

Software

Cobalt Strike

REMOVE FROM MATRIX

Type: malware

Platform(s): Linux, macOS, Windows

Source: MITRE

Cobalt Strike is a commercial, full-featured, remote access tool that bills itself as "adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors". Cobalt Strike's interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single, integrated system.[cobaltstrike manual]

In addition to its own capabilities, Cobalt Strike leverages the capabilities of other well-known tools such as Metasploit and Mimikatz.[cobaltstrike manual]

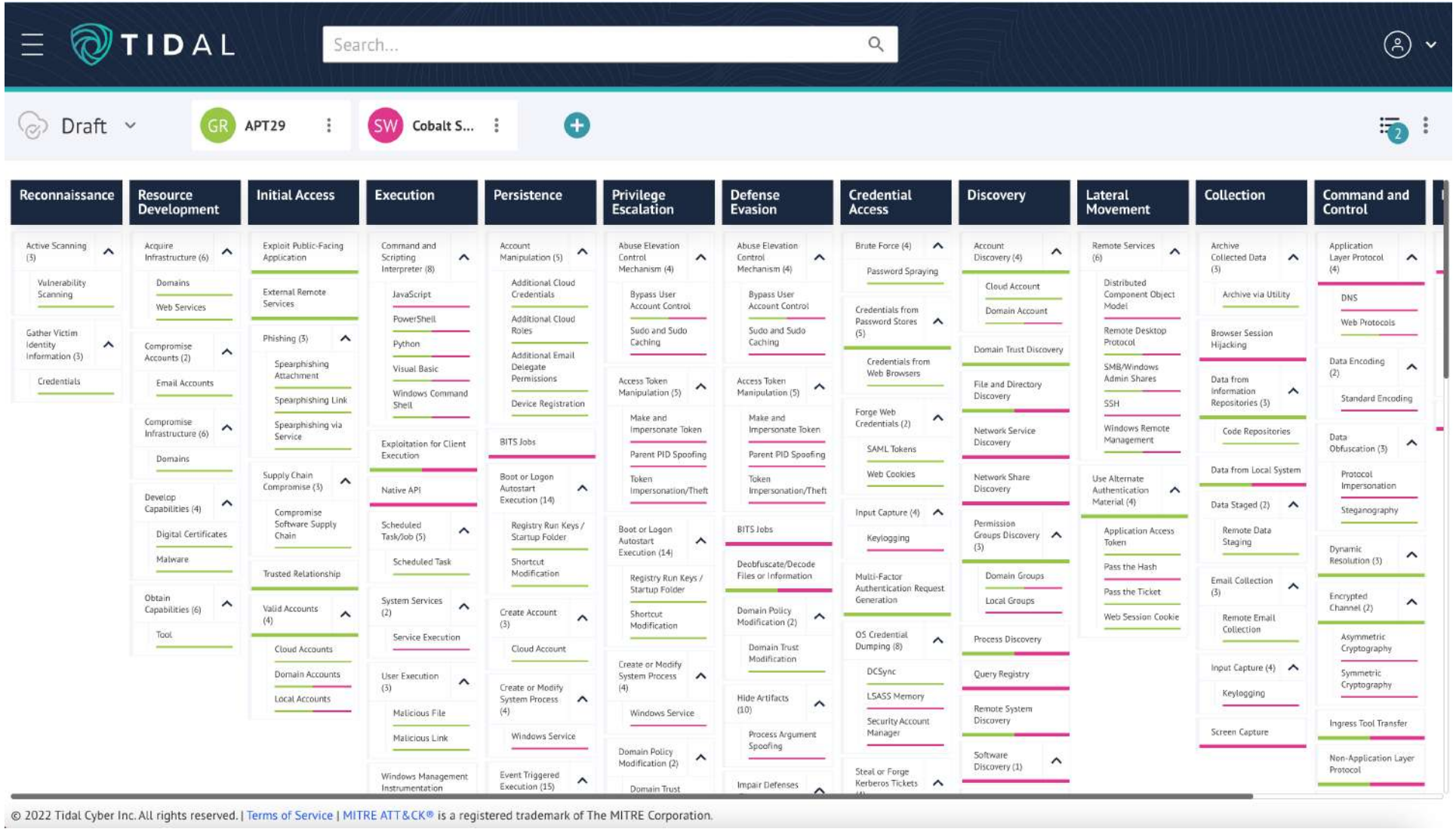
Associated Software (0) | Techniques (115) | Groups (28) | References (63)

There are no items to display

ID: S0154 **Version:** 1.8 **Created Date:** 14 December 2017 **Last Modified:** 25 February 2022, 06:58 PM GMT

TIDAL

Step One: Identify your threats: Combined



TIDAL

Step Two: Inventory your defenses: Detections

TIDAL

Search...

Draft

GR APT29

SW Cobalt S...

PR Sysmon...

Home > Product Registry > Olaf Hartong > Sysmon-Modular

Product

This item has been added to the matrix

REMOVE FROM MATRIX

Sysmon-Modular

Tactic(s) Covered: Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Impact

Capability Type(s): Detect

Vendor: Olaf Hartong

Product Version:

Source: Olaf Hartong

Sysmon-modular is a configuration repository, mapped to MITRE ATT&CK, to be used with Sysinternals Sysmon. The project has been set up in a modular fashion which allows for easier maintenance and the generation of specific configs. For instance, one for servers, one for workstations and one to only to be used in an Incident Response scenario. Please note this is a possible log entry that might lead to a detection, not in all cases will this be the only telemetry for that technique. Additionally there might be more techniques releated to that rule, there is only one mapped, this is the one deemed most likely by the author.

This product is licensed under the MIT License

Capabilities (142) Product Data Source (105)

Filter By : Detect

Capability	Type	Technique	Platform	Description	Availability

TIDAL

Step Two: Inventory your defenses: Tests

TIDAL

Search...

Draft

GR APT29 | SW Cobalt S... | PR Sysmon... | PR Invoke-...

Home > Product Registry > Atomic Red Team

Atomic Red Team

Last Updated: July 14, 2022

Source: Atomic Red Team

Atomic Red Team™ is a library of tests mapped to the MITRE ATT&CK® framework. Security teams can use Atomic Red Team to quickly, portably, and reproducibly test their environments.

Capability Type: Test

ADD TO MATRIX | VISIT WEBSITE

Search in products

Capability Type

Products

Invoke-Atomic

Last Updated: 14 July 2022, 01:16 PM GMT

Product Version: v1.0.2

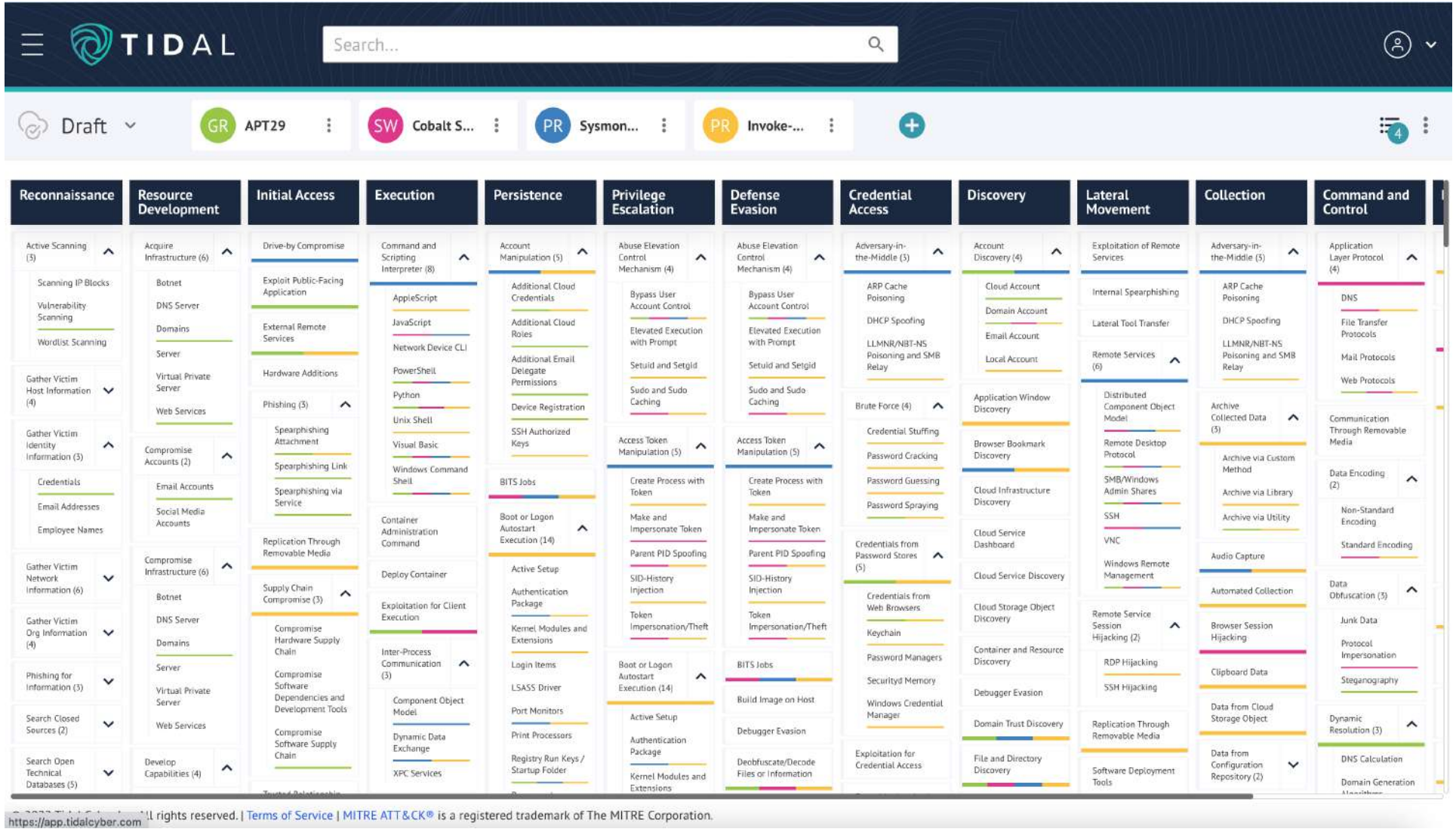
Tactics Covered: Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, Impact

Capability Type: Test 1069

REMOVE FROM MATRIX | VIEW DETAIL

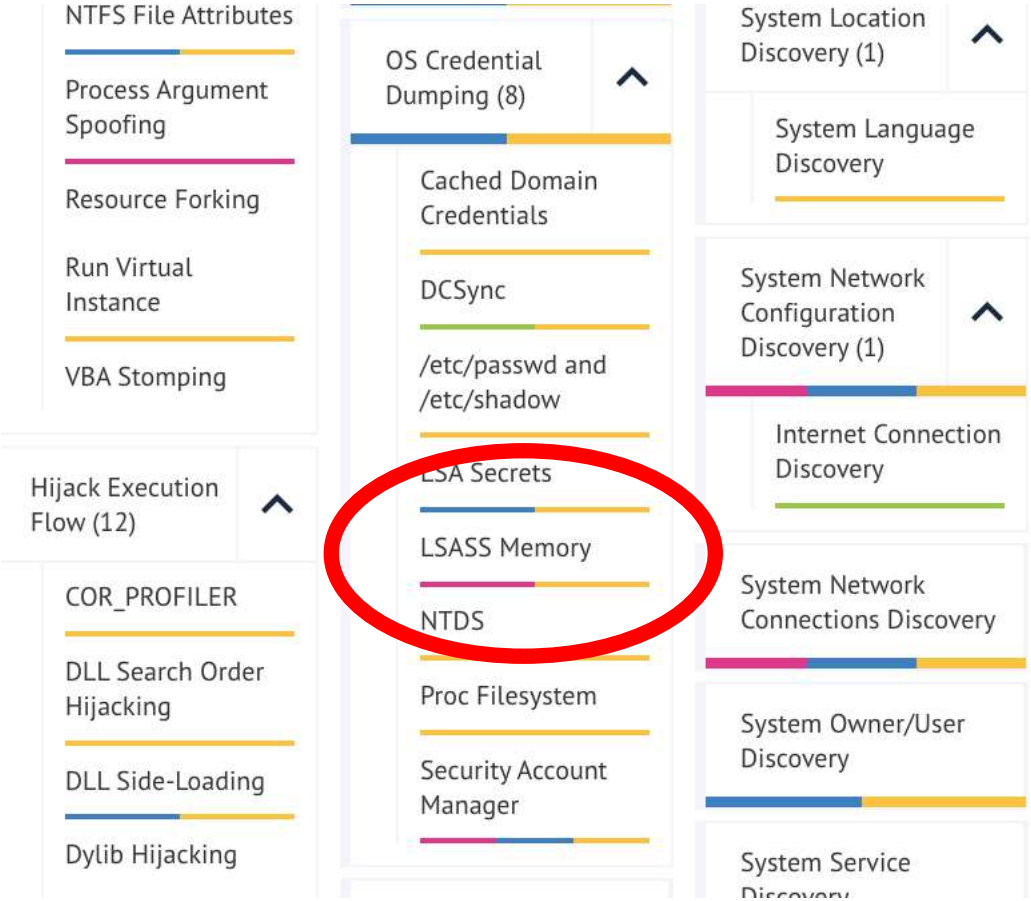
TIDAL

Step Three: Assess your Coverage



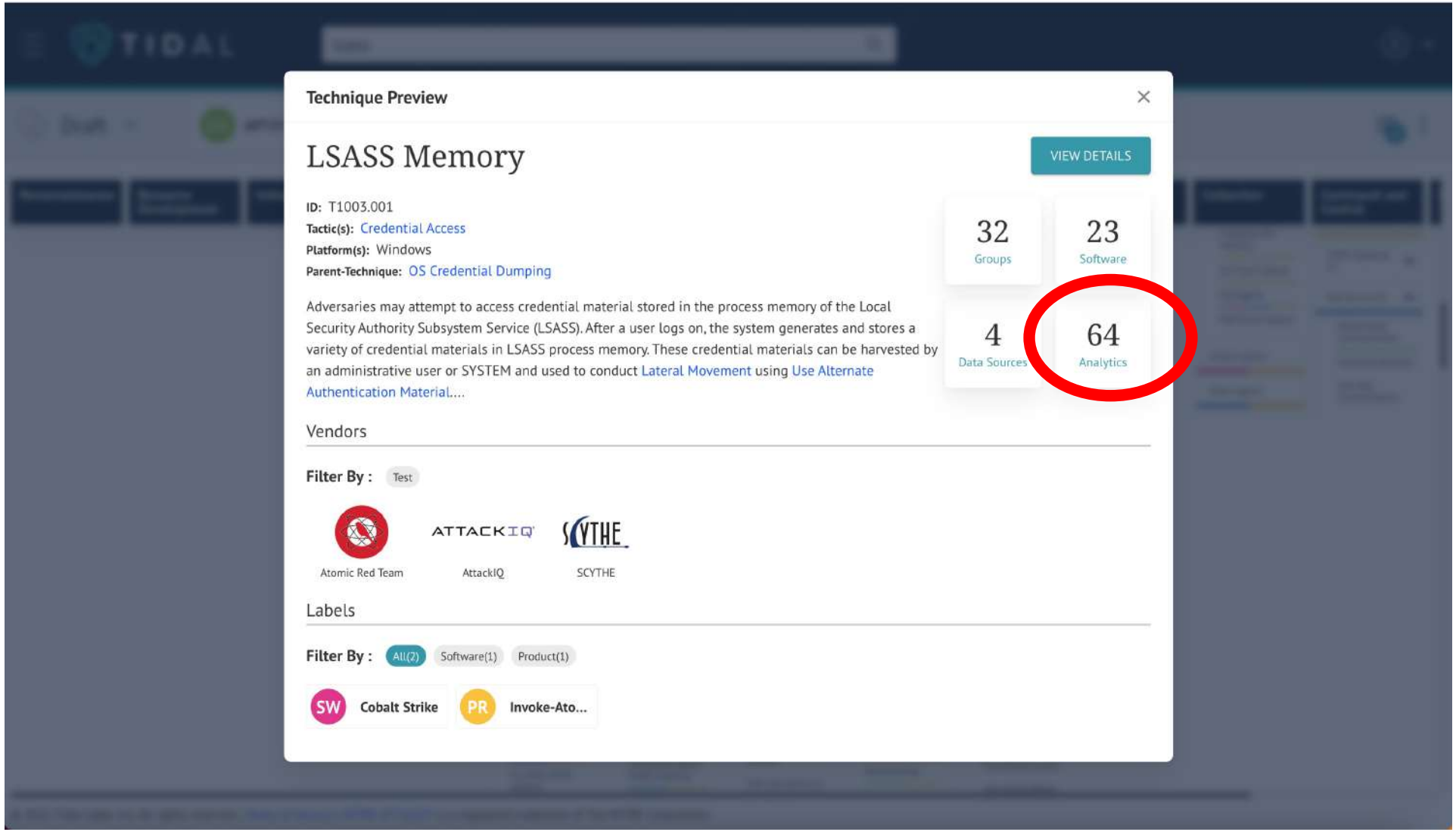
TIDAL

Step Four: Address Gaps – LSASS



TIDAL

Step Four: Address Gaps – OSS Analytics



TIDAL

Step Four: Address Gaps – OSS Analytics

TIDAL

lsass

Draft | GR APT29 | SW Cobalt S... | PR Sysmon... | PR Invoke-...

Home > Tactics > Credential Access > OS Credential Dumping > LSASS Memory

Sub-Techniques

LSASS Memory

ID: T1003.001

Tactic(s): Credential Access

Platform(s): Windows

Parent-Technique: OS Credential Dumping

Source: MITRE, Tidal Cyber

Adversaries may attempt to access credential material stored in the process memory of the Local Security Authority Subsystem Service (LSASS). After a user logs on, the system generates and stores a variety of credential materials in LSASS process memory. These credential materials can be harvested by an administrative user or SYSTEM and used to conduct Lateral Movement using Use Alternate Authentication Material.

As well as in-memory techniques, the LSASS process memory can be dumped from the target host and analyzed on a local system.

For example, on the target host use procdump:

- `procdump -ma lsass.exe lsass_dump`

Locally, mimikatz can be run using:

- `sekurlsa::Minidump lsassdump.dmp`
- `sekurlsa::logonPasswords`

Built-in Windows tools such as comsvcs.dll can also be used:

- `rundll32.exe C:\Windows\System32\comsvcs.dll MiniDump PID lsass.dmp full`[Volexity Exchange Marauder March 2021][Symantec Attacks Against Government Sector]

Windows Security Support Provider (SSP) DLLs are loaded into LSSAS process at system start. Once loaded into the LSA, SSP DLLs have access to encrypted and plaintext passwords that are stored in Windows, such as any logged-on user's Domain password or smart card PINs. The SSP configuration is stored in two Registry keys: `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Security Packages` and `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\OSConfig\Security Packages`. An adversary may modify these Registry keys to add new SSPs, which will be loaded the next time the system boots, or when the AddSecurityPackage Windows API function is called.[Graeber 2014]

The following SSPs can be used to access credentials:

- Msv: Interactive logons, batch logons, and service logons are done through the MSV authentication package.
- Wdigest: The Digest Authentication protocol is designed for use with Hypertext Transfer Protocol (HTTP) and Simple Authentication Security Layer (SASL) exchanges.[TechNet Blogs Credential Protection]
- Kerberos: Preferred for mutual client-server domain authentication in Windows 2000 and later.
- CredSSP: Provides SSO and Network Level Authentication for Remote Desktop Services.[TechNet Blogs Credential Protection]

Vendors (3) | Groups (32) | Software (23) | Data Sources (4) | References (62) | Analytics (64)

TIDAL

Step Four: Address Gaps- Add Sigma rules

github.com/SigmaHQ/sigma/blob/7853f93862304e65310e0c292ebb211f715857cb/rules/windows/process_access/proc_access_win_cred_dump_lsass_access.yml

SigmaHQ / sigma Public

Sponsor | Notifications | Fork 1.6k | Star 5.5k

Code | Issues 76 | Pull requests 24 | Discussions | Actions | Wiki | Security | Insights

7853f93862 | sigma / rules / windows / process_access / proc_access_win_cred_dump_lsass_access.yml | Go to file

phantinuss fix: FPs found in testing environment ✓ | Latest commit 9475153 on Jun 20 | History

3 contributors

Executable File | 130 lines (130 sloc) | 4.56 KB | Raw | Blame

```yaml
title: Credentials Dumping Tools Accessing LSASS Memory
id: 32d0d3e2-e58d-4d41-926b-18b520b2b32d
status: experimental
description: Detects process access LSASS memory which is typical for credentials dumping tools
author: Florian Roth, Roberto Rodriguez, Dimitrios Slamaris, Mark Russinovich, Thomas Patzke, Teymur Kheirkhabarov, Sherif Eldeeb, James Dickenson, Aleksey Pota
    oscd.community (update)
date: 2017/02/16
modified: 2022/06/20
references:
    - https://onedrive.live.com/view.aspx?resid=D026B4699190F1E6!2843&ithint=file%2cpptx&app=PowerPoint&authkey=!AMvCRTKB_V1J5ow
    - https://cyberwardog.blogspot.com/2017/03/chronicles-of-threat-hunter-hunting-for_22.html
    - https://www.slideshare.net/heirhabarov/hunting-for-credentials-dumping-in-windows-environment
    - http://security-research.dyndns.org/pub/slides/FIRST2017/FIRST-2017_Tom-Ueltschi_Sysmon_FINAL_notes.pdf
tags:
    - attack.credential_access
    - attack.t1003.001
    - attack.s0002
    - car.2019-04-004
logsource:
    category: process_access
    product: windows
detection:
    selection:
        TargetImage|endswith: '\lsass.exe'
        GrantedAccess|startswith:
            - '0x40'
            # - '0x1000'  # minimum access requirements to query basic info from service
            # - '0x1400'
            - '0x100000'
```

TIDAL

Step Five: Verify Defenses – run ART tests

TIDAL

Search...

LOGIN SIGN UP

Draft

GR APT29 | SW Cobalt S... | PR Sysmon... | PR Invoke-...

REMOVE FROM MATRIX

Invoke-Atomic

Tactic(s) Covered: Credential Access
Capability Type(s): Test
Vendor: Atomic Red Team
Product Version: v1.0.2
Source: Atomic Red Team

Invoke-AtomicRedTeam is a PowerShell module to execute tests as defined in the atomics folder of Red Canary's Atomic Red Team project. Visit the GitHub repository for Invoke-Atomic for installation and usage instructions.

This product is licensed under the MIT license

Capabilities (12) Product Data Source (0)

Filter By : Test Capabilities shown for "**LSASS Memory**"

Capability	Type	Technique	Platform	Description	Availability
Create Mini Dump of LSASS.exe using ProcDump	Test	LSASS Memory	Windows	The memory of lsass.exe is often dumped for offline c...	Default-Off
Dump LSASS with .Net 5 createdump.exe	Test	LSASS Memory	Windows	This test uses the technique describe in this tweet (ht...	Default-Off
Dump LSASS.exe Memory using comsvcs.dll	Test	LSASS Memory	Windows	The memory of lsass.exe is often dumped for offline c...	Default-Off

TIDAL

Step Six: Go To Step 1

- Threat-Informed Defense is an iterative, continuous process
- The environment is always changing
  - Evolution in threats – new groups, new behaviors, new malware
  - Evolution in defenses – new detections, new tests, new analytics
  - New public reporting of both

TIDAL

Putting it All Together into a Threat-Informed Strategy

Foundational Elements

Threat Model(s)	*The adversary groups, campaigns, software and specific behaviors of concern*	→ Specific behaviors
Inventory of Defenses	*Protections, detections, mitigations, responses and tests deployed*	→ Specific behaviors

TIDAL

Building a Threat Model

- Goal: Identify the threats to your organization and map those to specific behaviors you can defend against
- Sources of intelligence to drive threat modeling:
  - OSINT / Commercial threat intel sources – based on targeting of sector, geography and technology platforms
  - ISACs/ISAOs
  - Internal knowledge – past incidents, ongoing reconnaissance and probing, etc.

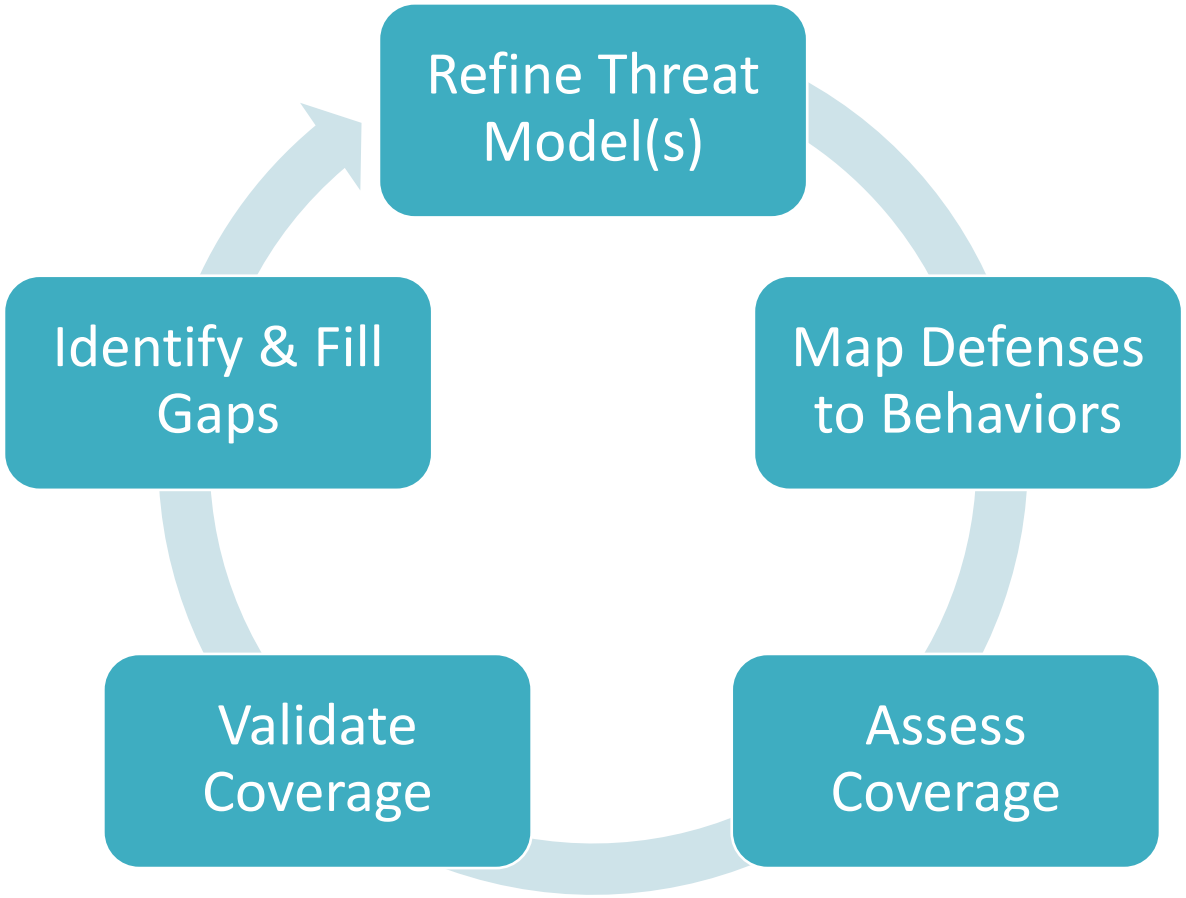
TIDAL

Inventory your Defenses

- Goal: Identify the security policies, controls and technologies deployed and map those to the specific behaviors they are effective against
- Helpful to segment by the type of defense:
  - **Mitigation**: prevents a behavior from being employed
  - **Protection**: blocks a specific behavior from achieving its objective
  - **Detection**: alerts when a behavior is seen in use
  - **Response**: takes corrective action when a behavior is detected
  - **Test**: verify if a specific defense is operating normally

TIDAL

Continuous Evaluation & Adaptation



TIDAL

Closing Thoughts

ATT&CK is a *Means*, not an *End*.

- Don’t try to achieve 100% coverage of the entire ATT&CK matrix – you will fail
- ATT&CK isn’t a checklist to be blindly followed
- Focus on ATT&CK as the glue that helps you connect and organize your understanding of what adversaries do IRL
- Understand that ATT&CK isn’t exhaustive and embrace the fact that you’ll want to extend it for yourself

TIDAL

Threat-Informed Defense is a Journey

- Embrace the iterative and continuous nature of threat-informed defense
- Align people, processes and technology to support this ongoing set of activities
- Measure your progress and use that to course correct

TIDAL

Select Community Resources

- MITRE ATT&CK: attack.mitre.org
- Tidal Cyber Community Edition: app.tidalcyber.com
- Atomic Red Team: atomicredteam.io
- SIGMA: github.com/SigmaHQ/sigma
- Sysmon Modular: github.com/olafhartong/sysmon-modular

TIDAL

Inventory your Defenses

- Goal: Identify the security policies, controls and technologies deployed and map those to the specific behaviors they are effective against
- Helpful to segment by the type of defense:
  - **Mitigation**: prevents a behavior from being employed
  - **Protection**: blocks a specific behavior from achieving its objective
  - **Detection**: alerts when a behavior is seen in use
  - **Response**: takes corrective action when a behavior is detected
  - **Test**: verify if a specific defense is operating normally

TIDAL

Thank You!