ASCENT SOLUTIONS

September 24th, 2022

# *Developing with MITRE ATT&CK*

Workshop @ Texas Cyber Summit 2022


**Brad Palm**
Director of Software

**Brian Greunke**
Director of Engineering

# Agenda

- Intro - ATT&CK Refresher
- Use Cases / Detections / Analytics
  - Why should we develop with ATT&CK
  - Module 1 Lab
- Framework and Protocols
  - How is ATT&CK organized, structured, and communicated?
  - Module 2 Lab
- Data
  - Where can we obtain ATT&CK data? What factors should be considered?
  - Module 3 Lab
- Versioning
  - How does ATT&CK handle versions/upgrades and why do we care?
  - Module 4 Lab
- Existing Tools
  - What does ATT&CK provide? What does our community provide?
  - Module 5 Lab
- Development Time
  - Real world examples / problems
  - Module 6 Lab

- Timeline:
  - 11:15am – 12:00pm
  - 12:00 – 12:10pm BREAK
  - 12:10 – 1pm
  - 1:00 – 1:10pm BREAK
  - 1:10 – 2:00pm
  - 2:00 – 2:15pm Questions

ASCENT SOLUTIONS

# *Brad Palm – Director of Software, Ascent Solutions*

**Brad Palm**

*Director of Software*

Prior to Product Leader at Ascent, Brad led all cyber services for his previous firm Pathfynder; and was lead strategist and threat hunter for his boutique consulting firm - BruteForce. Prior to life as a civilian, Brad spent 10 years in the Marine Corps as a Combat Engineer, Brad earned a Mechanical Engineering degree from the University of St. Thomas and holds a Master of Science in Computer Science from the Naval Postgraduate School and has certifications with numerous acronyms from various accreditation bodies.

**Selected Service Experience**

*Retail, Finance, Technology, Healthcare, Consumer Packaged Goods/Manufacturing, Government*

ASCENT SOLUTIONS

# *Brian Greunke – Director of Engineering, Ascent Solutions*

**Brian Greunke**

*Director of Engineering*

Over the past 15+ years, Brian has had an opportunity to approach technology from multiple vantage points as a software engineer, cloud architect, network analyst, pen tester, threat hunter, and leading teams doing all the above. Prior to building security products at Ascent, he was the Lead Developer for Recon InfoSec. And prior to that, he spent 10 years leading technical and security teams in the United States Marine Corps as a Communications Officer. Brian has a B.S. and M.S. in Computer Science.

# *Hand Raising Exercise - Briefly Share YOUR Current Experience Level*


- Are you leveraging ATT&CK in your organization?
- Are you coding in Python frequently for tasks?
- Are you a C-Suite/Executive/Senior-level/Strategic leader?
- Are you a Mid-level Manager/Leader/Operational leader?
- Are you Low-level Team Lead/Analyst/Tactical/Individual Contributor?

# ATT&CK Refresher

*If you haven't been exposed to the MATRIX, prepare to enter at hyper speed!*

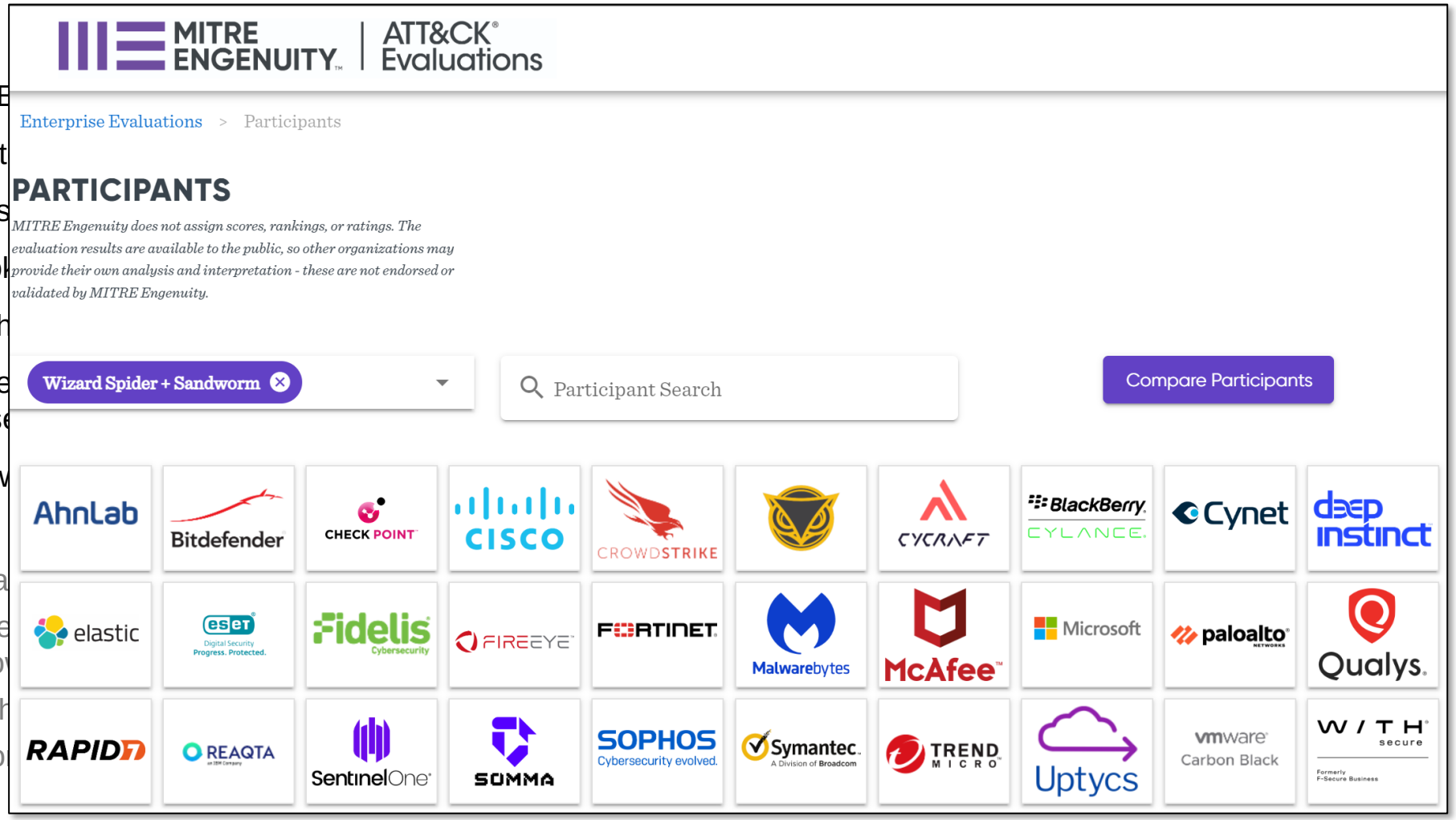
ASCENT SOLUTIONS

# What is ATT&CK

- ATT&CK® stands for MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)
- Created by MITRE in 2013 (released 2015) to be a globally-accessible knowledge base of adversary TTPs
- It is based on real-world observations (no pay wall like other CTI feeds)
- Attacker techniques are broken down into detail
- It continues to evolve with the threat landscape and sees updates at least once a quarter
- Used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community
- It has become the de-facto way in which we judge the coverage and efficacy of defensive products and services (MITRE Engenuity tests)
- Premise/Axioms:
  - You need to understand and observe your adversary in order to establish an appropriate defense
  - Successful and comprehensive threat detection requires understanding common adversary techniques, which ones pose a threat to your organization, and how to detect and mitigate these attacks
  - The amount of attack paths makes it nearly impossible for any single organization to monitor every single attack type
  - You need to be able to communicate threats and mitigations across – internally, externally, laterally, and hierarchically - different stakeholders

# What is ATT&CK

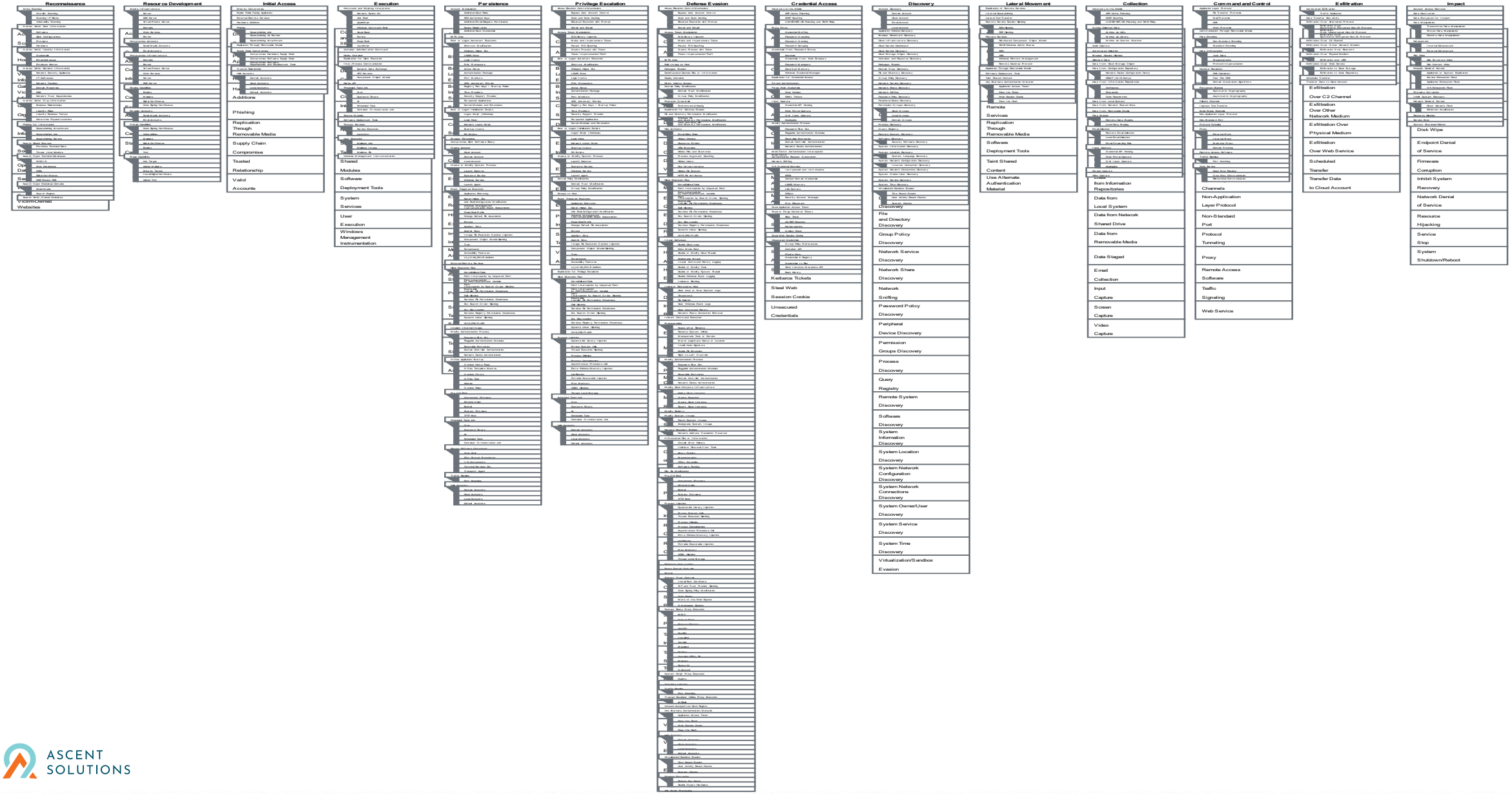
- ATT&CK® stands for MITRE
- Created by MITRE in 2013 t
- It is based on real-world obs
- Attacker techniques are brok
- It continues to evolve with th
- Used as a foundation for the cybersecurity product and se
- It has become the de-facto v
- Premise/Axioms:
  - You need to understand a
  - Successful and comprehe your organization, and hov
  - The amount of attack path
  - You need to be able to co stakeholders



# What is ATT&CK

- ATT&CK® stands for MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)
- Created by MITRE in 2013 to be a globally-accessible knowledge base of adversary TTPs
- It is based on real-world observations (no pay wall like other CTI feeds)
- Attacker techniques are broken down into detail
- It continues to evolve with the threat landscape and sees updates at least once a quarter
- Used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community
- It has become the de-facto way in which we judge the coverage and efficacy of defensive products and services (MITRE Engenuity tests)
- Premise/Axioms:
  - You need to understand and observe your adversary in order to establish an appropriate defense
  - Successful and comprehensive threat detection requires understanding common adversary techniques, which ones pose a threat to your organization, and how to detect and mitigate these attacks
  - The amount of attack paths makes it nearly impossible for any single organization to monitor every single attack type
  - You need to be able to communicate threats and mitigations – internally, externally, laterally, and hierarchically positioned – across different stakeholders

# ATT&CK Enterprise Matrix



# ATT&CK TTPs Breakdown

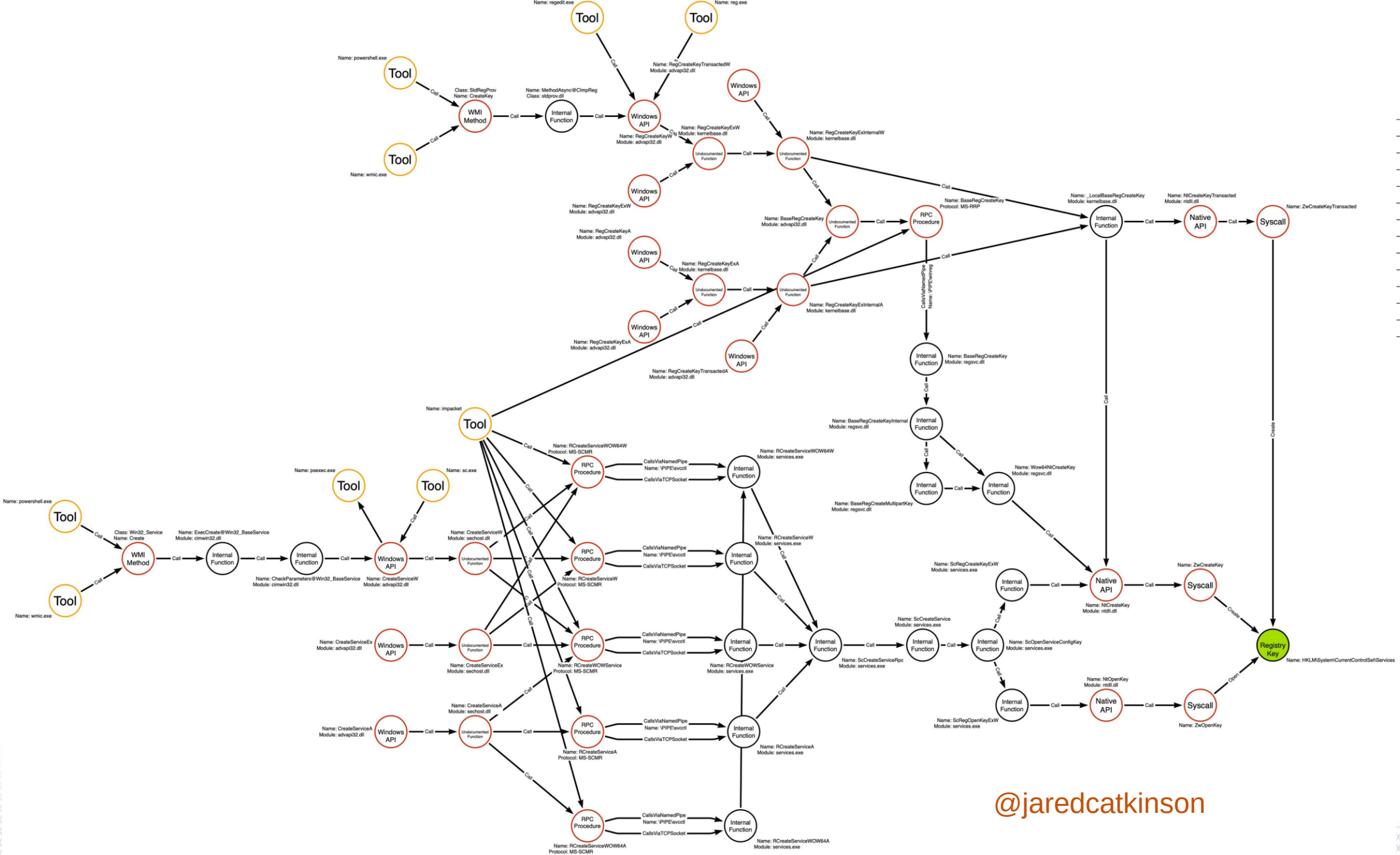
| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command And Control |
|---|---|---|---|---|---|---|---|---|---|---|
| 10 items | 31 items | 56 items | 28 items | 59 items | 20 items | 19 items | 17 items | 13 items | 9 items | 21 items |
| 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 | Binary Padding | Bash History | Application Window Discovery | Application Deployment Software | Automated Collection | Data Compressed | Communication Through Removable Media |
| Hardware Additions | Command-Line Interface | AppCert DLLs | AppCert DLLs | BITS Jobs | Brute Force | Browser Bookmark Discovery | Distributed Component Object Model | Clipboard Data | Data Encrypted | Connection Proxy |
| Replication Through Removable Media | Control Panel Items | AppInit DLLs | AppInit DLLs | Bypass User Account Control | Credential Dumping | File and Directory Discovery | Exploitation of Remote Services | Data from Information Repositories | Data Transfer Size Limits | Custom Command and Control Protocol |
| Spearphishing Attachment | Dynamic Data Exchange | Application Shimming | Application Shimming | Clear Command History | Credentials in Files | Network Service Scanning | Logon Scripts | Data from Local System | Exfiltration Over Alternative Protocol | Custom Cryptographic Protocol |
| Spearphishing Link | Execution through API | Authentication Package | Bypass User Account Control | CMSTP | Credentials in Registry | Network Share Discovery | Pass the Hash | Data from Network Shared Drive | Exfiltration Over Command and Control Channel | Data Encoding |
| Spearphishing via Service | Execution through Module Load | BITS Jobs | DLL Search Order Hijacking | Code Signing | Exploitation for Credential Access | Password Policy Discovery | Pass the Ticket | Data from Removable Media | Exfiltration Over Other Network Medium | Data Obfuscation |
| Supply Chain Compromise | Exploitation for Client Execution | Bootkit | Dylib Hijacking | Component Firmware | Forced Authentication | Peripheral Device Discovery | Remote Desktop Protocol | Data Staged | Exfiltration Over Physical Medium | Domain Fronting |
| Trusted Relationship | Graphical User Interface | Browser Extensions | Exploitation for Privilege Escalation | Component Object Model Hijacking | Hooking | Permission Groups Discovery | Remote File Copy | Email Collection | Scheduled Transfer | Fallback Channels |
| Valid Accounts | InstallUtil | Change Default File Association | Extra Window Memory Injection | Control Panel Items | Input Capture | Process Discovery | Remote Services | Input Capture | | Multi-hop Proxy |
| | Launchctl | Component Firmware | File System Permissions Weakness | DCShadow | Input Prompt | Query Registry | Replication Through Removable Media | Man in the Browser | | Multi-Stage Channels |
| | Local Job Scheduling | Component Object Model Hijacking | Hooking | Deobfuscate/Decode Files or Information | Kerberoasting | Remote System Discovery | Shared Webroot | Screen Capture | | Multilayer Encryption |
| | Mshta | Create Account | Image File Execution Options Injection | DLL Search Order Hijacking | Keychain | Security Software Discovery | SSH Hijacking | Video Capture | | Port Knocking |
| | PowerShell | DLL Search Order Hijacking | Launch Daemon | DLL Side-Loading | LLMNR/NBT-NS Poisoning | System Information Discovery | Taint Shared Content | | | Remote Access Tools |
| | Regsvcs/Regasm | Dylib Hijacking | New Service | Exploitation for Defense Evasion | Network Sniffing | System Network Configuration Discovery | Third-party Software | | | Remote File Copy |
| | Regsvr32 | External Remote Services | Path Interception | Extra Window Memory Injection | Password Filter DLL | System Network Connections Discovery | Windows Admin Shares | | | Standard Application Layer Protocol |
| | Rundll32 | File System Permissions Weakness | Plist Modification | File Deletion | Private Keys | System Owner/User Discovery | Windows Remote Management | | | Standard Cryptographic Protocol |
| | Scheduled Task | Hidden Files and Directories | Port Monitors | File System Logical Offsets | Replication Through Removable Media | System Service Discovery | | | | Standard Non-Application Layer Protocol |
| | Scripting | Hooking | Process Injection | Gatekeeper Bypass | Securityd Memory | | | | | Uncommonly Used Port |
| | Service Execution | Hypervisor | Scheduled Task | Hidden Files and Directories | Two-Factor Authentication Interception | | | | | Web Service |
| | Signed Binary Proxy Execution | Image File Execution Options Injection | Service Registry Permissions Weakness | Hidden Users | | | | | | |
| | Signed Script Proxy Execution | Kernel Modules and Extensions | Setuid and Setgid | Hidden Window | | | | | | |
| | Source | Launch Agent | | HISTCONTROL | | | | | | |
| | Space after Filename | | | Image File Execution Options Injection | | | | | | |

**Tactics**

**Techniques – inside a technique/sub-technique are Procedures (TTPs)**

## *ATT&CK Terminology*

- **Tactics:** describe the immediate technical objectives (the "**what**") attackers are trying to achieve, such as gaining Initial Access, maintaining Persistence, or establishing Command and Control. Invariably, attackers must use multiple tactics to successfully complete an attack (e.g., Killchain).
- **Techniques**: describe the "**how**"—the methods attackers use to achieve a tactic. All tactics in each matrix have multiple techniques; the Enterprise matrix breaks some techniques down further into sub-techniques. An example of this is the Phishing technique attackers use to gain Initial Access (a tactic). Phishing's three associated sub-techniques are Spearphishing Attachment, Spearphishing Link, and Spearphishing via [a] Service.
  - *Macro view*
- **Procedures**: describe the specific implementations of techniques and sub-techniques APTs have used (sometimes in clever or novel ways), or it can refer to specific malware or other tools attackers have used.
  - Often found in the Intel report, as there is no room for all possible procedures currently in the ATT&CK matrix
  - When mapping to ATT&CK, analysts will have to find the bucket that best fits the procedure if it is not well known
  - *Micro view*




@jaredcatkinson

# *Why Use ATT&CK*

- As security practitioners we are facing an intractable (wicked hard) problem
  - We must “eat the elephant” / “boil the ocean” (pick your analogy) and defend against all the threats 24/7
  - ATT&CK provides a logical and data-driven approach that provides us some certainty and confidence in the strategy we are crafting for our organizations
- By leveraging ATT&CK, our SecOps teams can:
  - Design adversary emulation atomic tests
  - Prepare red teaming engagement objectives
  - Inform behavioral analytics and detection development
  - Support defensive gap assessments
  - Bring consistency and transparency to SOC maturity assessments
  - Enrich cyber threat intelligence programs
  - Improve communication across teams and throughout the security industry
- Motivation / value proposition for the ATT&CK framework
  - Security has not been solved and some will argue we haven’t made much of a dent since FW/AV
  - Keeping pace with the adversary is HARD
  - Cyber Threat Intelligence (CTI) analysts and operations are expensive
  - Intel requirements collection, analysis, and dissemination is HARD
  - Operationalizing external & internal intelligence is very HARD

## *Common Objections Heard*

*It isn't tailored for our org*

*If its open source, won't the adversary stop using those TTPs*

*We don't have enough internal expertise to operationalize*

It is the goal to outgrow/outpace the ATT&CK team's intel/release cycles

*Most won't….*

*We don't have time and resources to categorize and correlate incidents*

*Not another framework!*

*We can't afford to replace or reconfigure our tools to work with ATT&CK*

ASCENT SOLUTIONS

## *Who Uses ATT&CK*

- Strategic (C-Suite, high-level executives, boards)
  - CISO briefing the board, "*pictures good, code bad*"
  - Select and manage security service partners (MSSPs, cloud providers, product vendors)
  - Insurance providers / policies
  - Partnerships, M&As
- Operational (mid-level management)
  - Cybersecurity road mapping (gap analysis)
  - What hires/budget do I need to plan for to continue our cybersecurity journey
  - What trends/emerging threats should we align to (tracking threats relevant to business/industry)
- Tactical (SOC staff, analysts, team leads)
  - What things to we need to hire/spend/build **today** to better defend ourselves against attacker X
  - All the SecOps team – red, blue, purple, CTI, threat hunt, insider threat
    - *AND* builders/devs

## *How Teams Use ATT&CK*

- Cyber Threat intelligence
  - Intel-driven defenses
  - Tracking business/asset specific adversaries
- Detection Engineering / Purple Teaming
  - Maintain tactical advantage (home field)
  - Continuous improvement
- Adversary emulation
  - Recreating an attack path to determine defensive coverage or gaps
  - Adversary emulation plans can be as discrete as an atomic technique that you are trying to test for, or it could be a whole adversary profile and all their known exploits/tooling
- Threat Hunting
  - Generating hypotheses / reoccurring hunt candidates
  - Determining data sources of interest to detect bad
- Dev/Builders
  - Education
  - Proactive defense

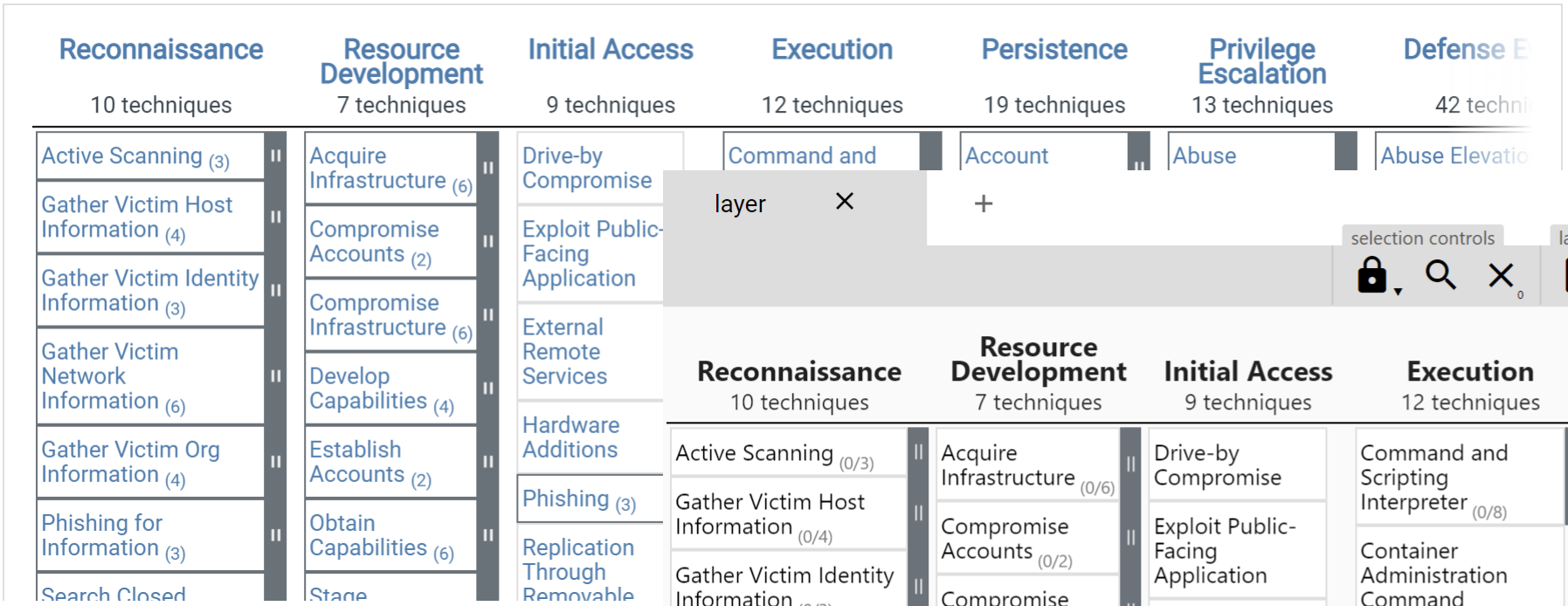
- Matrix - Matrix - Enterprise | MITRE ATT&CK®
  - Enterprise (explore filters for tech platforms)
  - Mobile (explore filters for tech platforms)
  - ICS
- Zoom in on Tactics, Techniques, Sub-Techniques pages
- Groups / Software
- Mitigations
- Data Sources

# *Use Cases / Detections / Analytics*

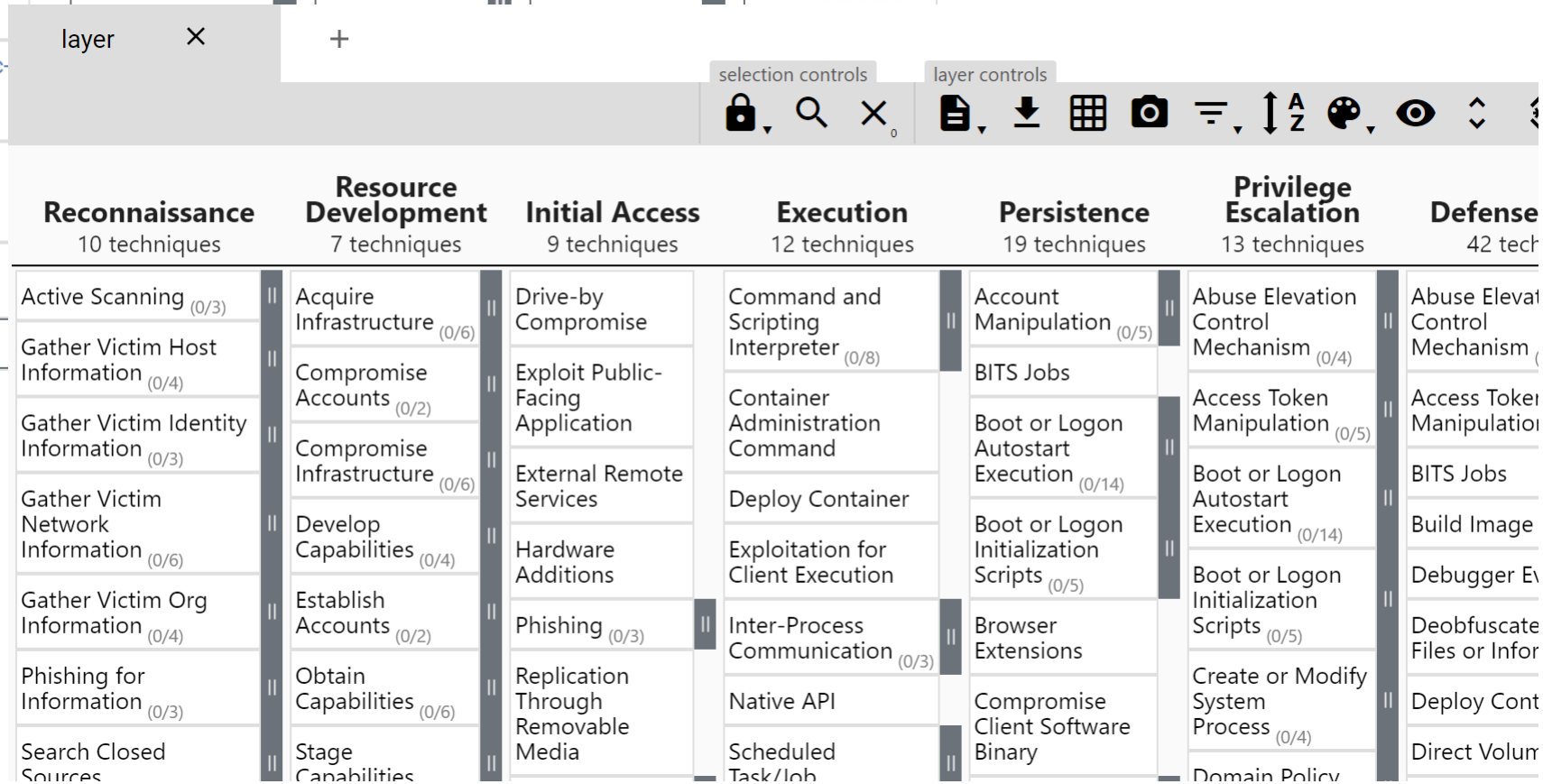
*Why develop with ATT&CK?*

ASCENT SOLUTIONS

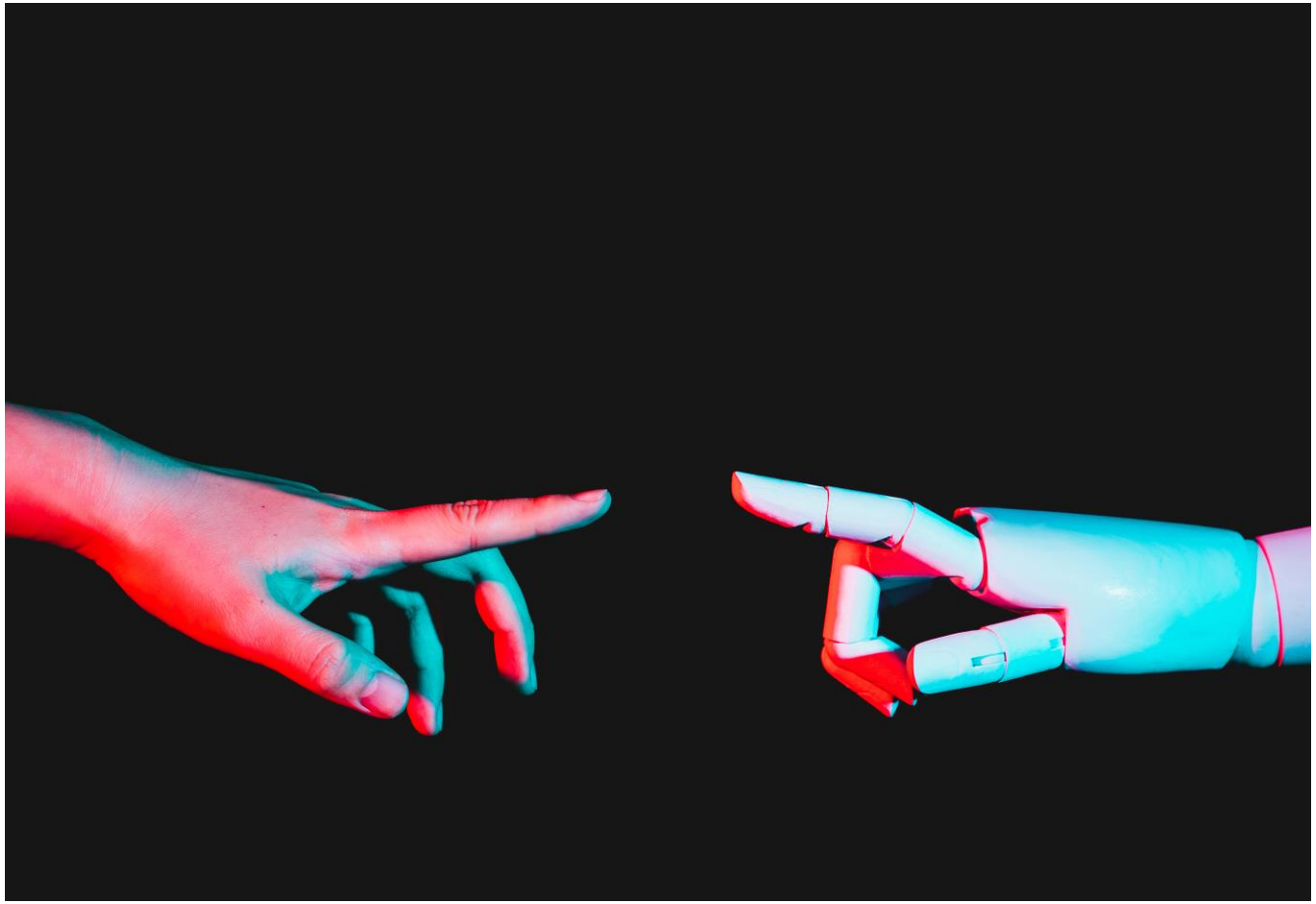
# *Isn't ATT&CK Just…*




+



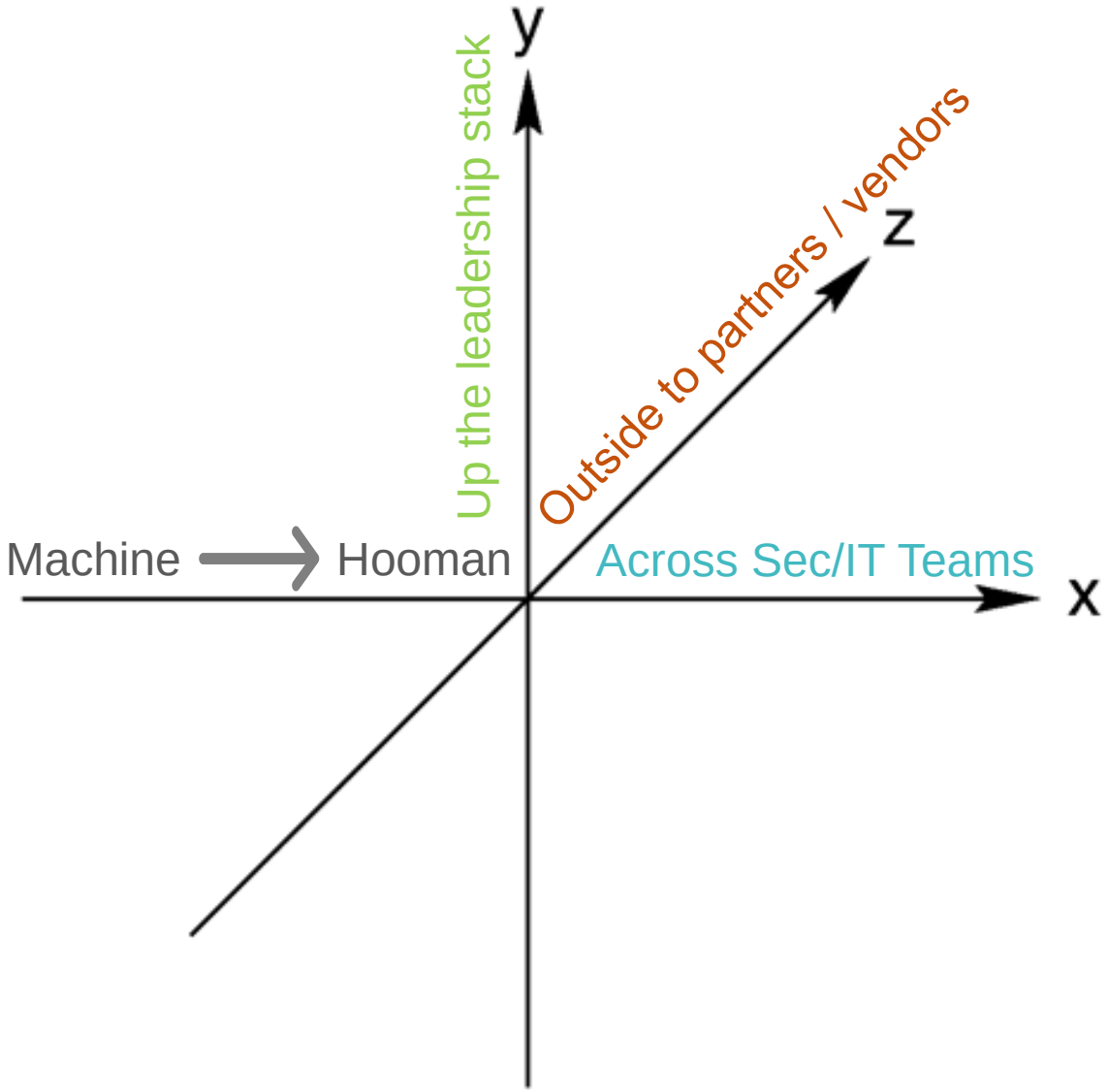
# *Humans and Machines are Speaking ATT&CK*



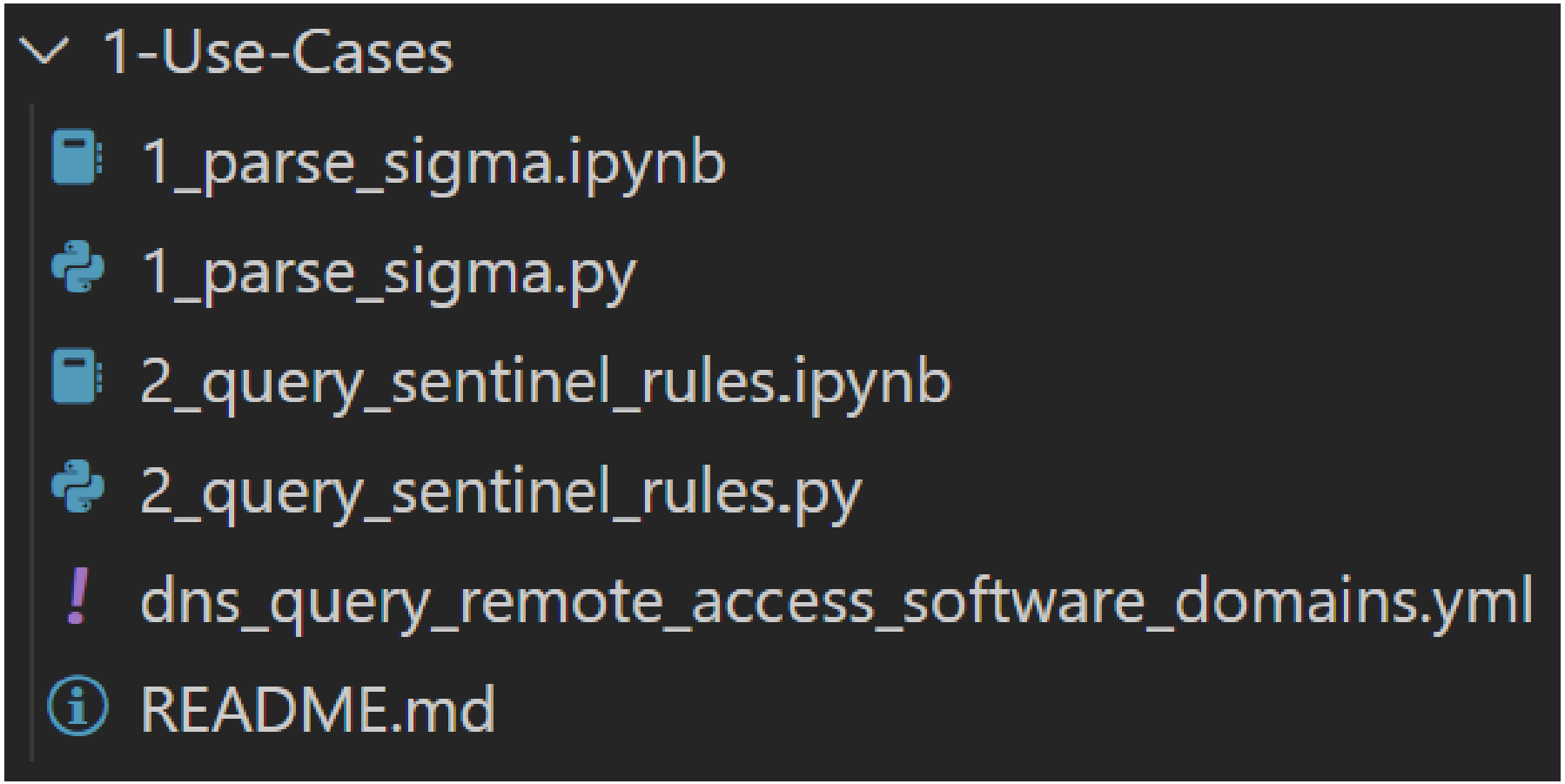
## *How Does ATT&CK Help My Organization*

- It has become the lexicon in which the cyber security industry communicates and collaborates on combating adversary methods. ALLOWS effective communication, via a shared language:
  - Across teams, from analyst up to leadership
  - With security partners and vendors (removes ambiguity of detection coverage and efficacy in products/solutions)
  - Between software and products
  - Amongst offensive and defensive internal teams
- ENABLES strategic, operational, and tactical level decision making:
  - Drives gap analysis
  - Focuses and prioritizes defensive efforts
  - Supports data-driven decisions
  - Informs build vs. buy choices
  - Purple teaming and continuous defensive improvements
- FUELS an intel-driven and threat-informed approach to security operations:
  - Identifying attacker behavior
  - Assessing defensive coverage
  - Analyzing opportunities to disrupt
  - Purposefully designing mitigations and detections

# *3D Communication*



## *Module 1 Lab*



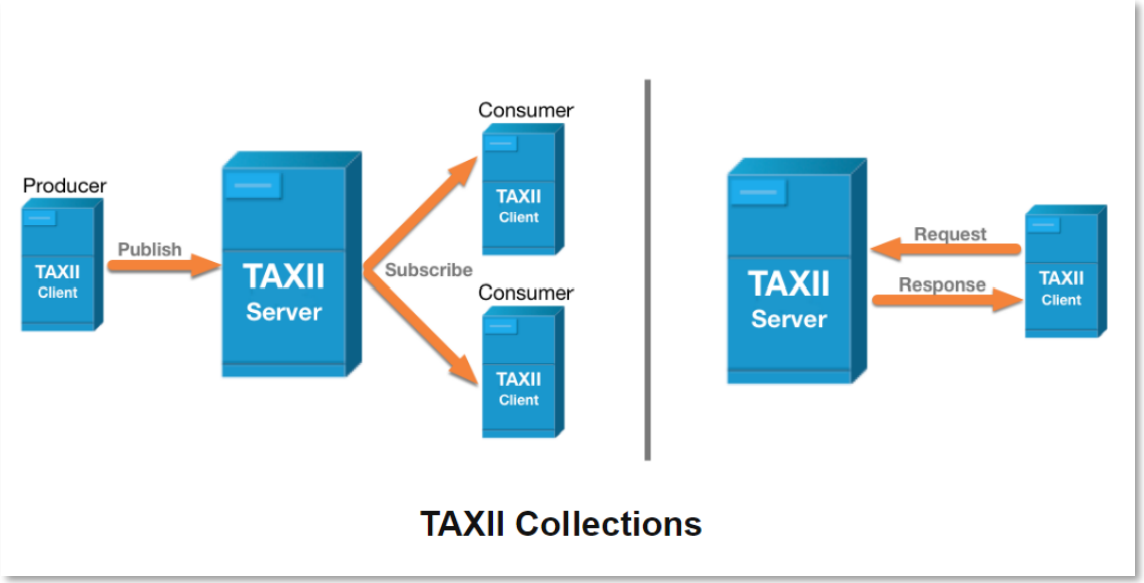
# *Framework and Protocols*

*How is ATT&CK organized, structured, and communicated?*

ASCENT SOLUTIONS

# *STIX / TAXII*


**STIX Relationship Example**




**TAXII Collections**

https://oasis-open.github.io/cti-documentation/

# *ATT&CK -> STIX Mapping*

| ATT&CK concept | STIX object type | Custom type? |
|---|---|---|
| Matrix | `x-mitre-matrix` | yes |
| Tactic | `x-mitre-tactic` | yes |
| Technique | attack-pattern | no |
| Sub-technique | attack-pattern where `x_mitre_is_subtechnique = true` | no |
| Procedure | relationship where `relationship_type = "uses"` and `target_ref` is an `attack-pattern` | no |
| Mitigation | course-of-action | no |
| Group | intrusion-set | no |
| Software | malware or tool | no |
| Collection[1] | `x-mitre-collection` | yes |
| Data Source | `x-mitre-data-source` | yes |

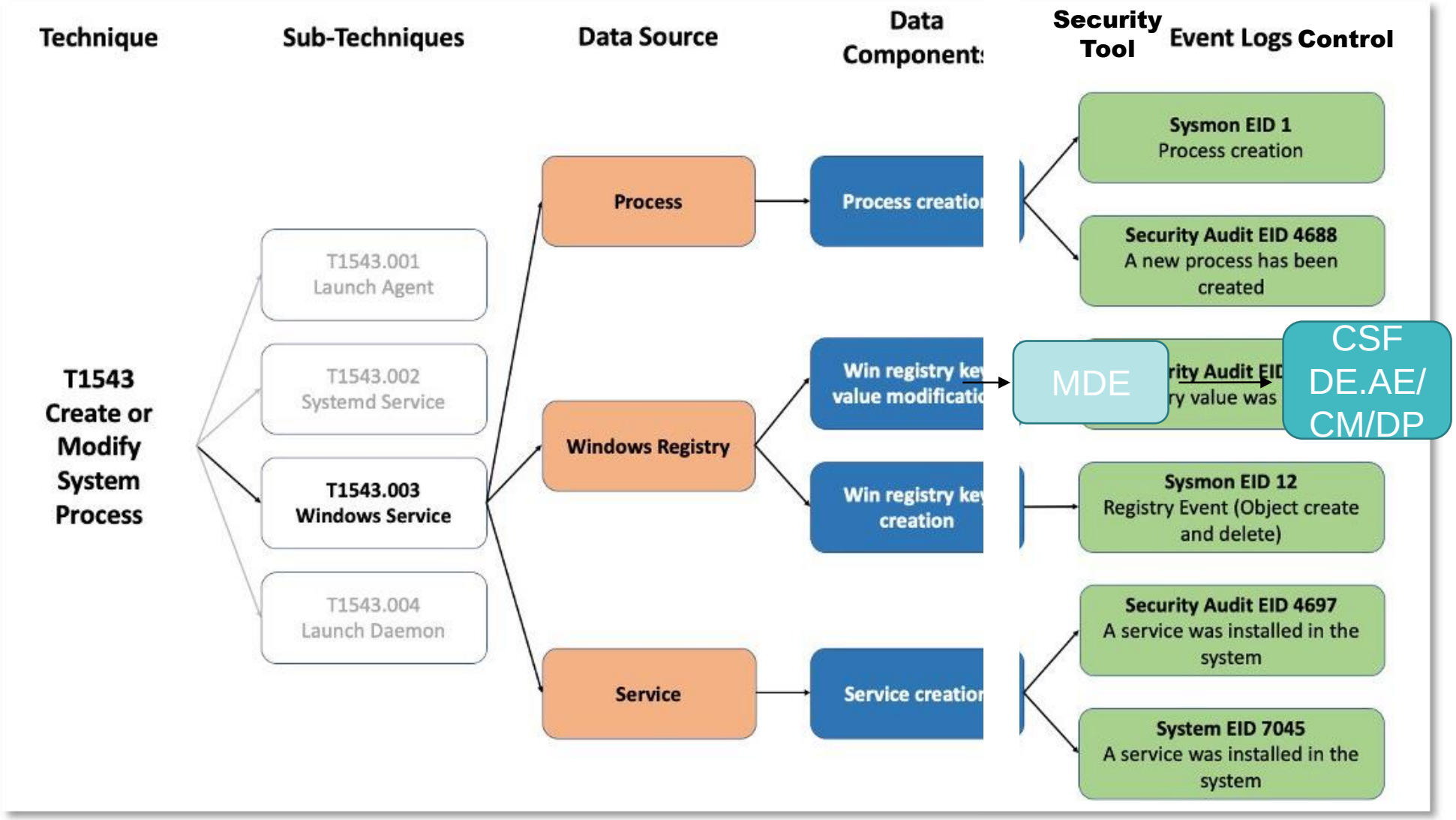
https://github.com/mitre-attack/attack-stix-data/blob/master/USAGE.md

ASCENT SOLUTIONS

## *Data Sources*

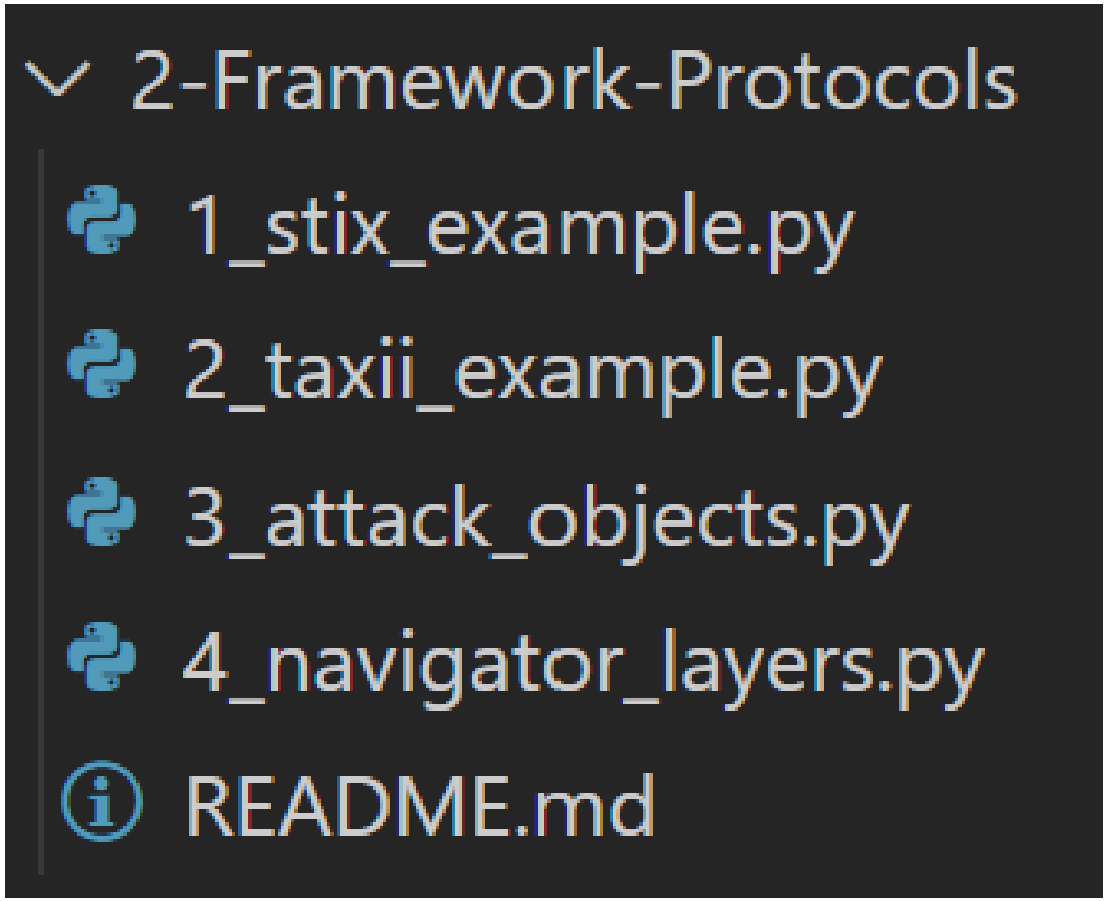
- How we bridge observed offensive actions to potential defensive countermeasures (prevention / detection)
- Bi-directional flow is a key mental model to embrace and exploit:
  - Threat -> {DRIVES} <- Detection/Use Case/Analytic -> {REQUIRES} <- Visibility -> {BUILT ON} <- Data Sources

# *Data Sources Cont'd*




https://medium.com/mitre-attack/defining-attack-data-sources-part-ii-1fc98738ba5b

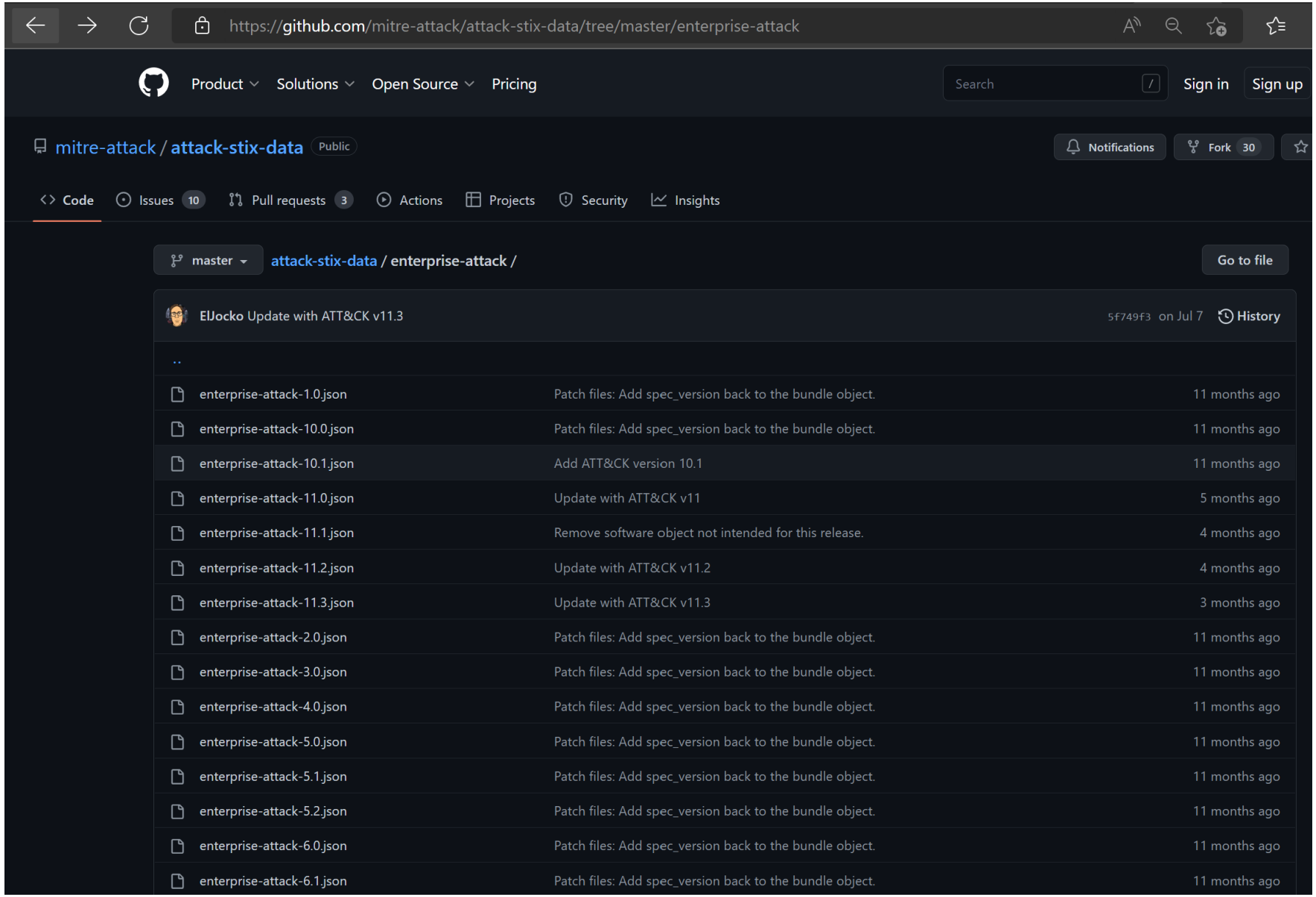
## *Module 2 Lab*



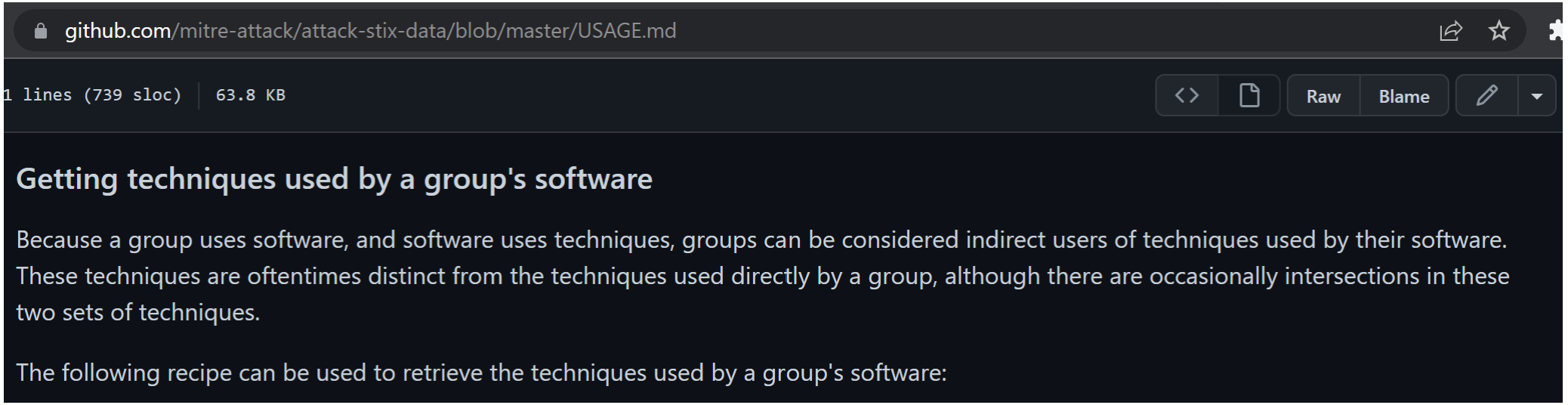
# Data

*Where can we obtain ATT&CK data? What factors should be considered?*

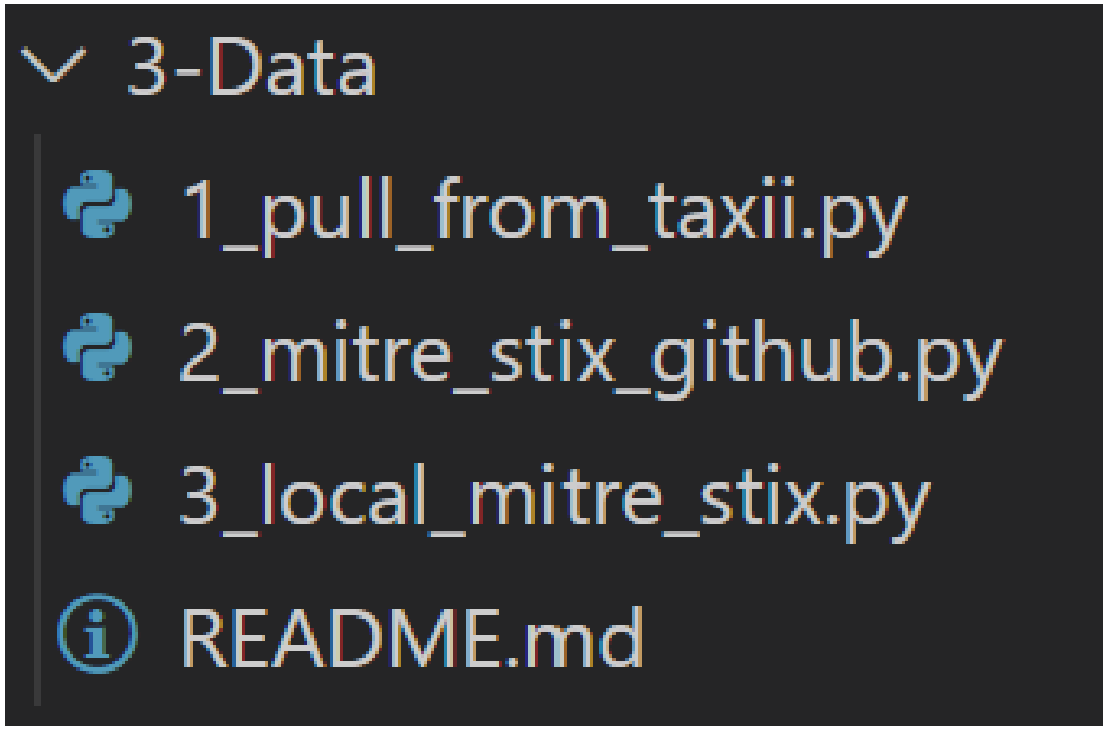
# Git Repo


https://github.com/mitre-attack/attack-stix-data/tree/master/enterprise-attack
Product
Solutions
Open Source
Pricing
Search
Sign in
Sign up
mitre-attack / attack-stix-data
Public
Notifications
Fork 30
Code
Issues 10
Pull requests 3
Actions
Projects
Security
Insights
master
attack-stix-data / enterprise-attack /
Go to file
ElJocko Update with ATT&CK v11.3
5f749f3 on Jul 7
History
..
enterprise-attack-1.0.json Patch files: Add spec_version back to the bundle object. 11 months ago
enterprise-attack-10.0.json Patch files: Add spec_version back to the bundle object. 11 months ago
enterprise-attack-10.1.json Add ATT&CK version 10.1 11 months ago
enterprise-attack-11.0.json Update with ATT&CK v11 5 months ago
enterprise-attack-11.1.json Remove software object not intended for this release. 4 months ago
enterprise-attack-11.2.json Update with ATT&CK v11.2 4 months ago
enterprise-attack-11.3.json Update with ATT&CK v11.3 3 months ago
enterprise-attack-2.0.json Patch files: Add spec_version back to the bundle object. 11 months ago
enterprise-attack-3.0.json Patch files: Add spec_version back to the bundle object. 11 months ago
enterprise-attack-4.0.json Patch files: Add spec_version back to the bundle object. 11 months ago
enterprise-attack-5.0.json Patch files: Add spec_version back to the bundle object. 11 months ago
enterprise-attack-5.1.json Patch files: Add spec_version back to the bundle object. 11 months ago
enterprise-attack-5.2.json Patch files: Add spec_version back to the bundle object. 11 months ago
enterprise-attack-6.0.json Patch files: Add spec_version back to the bundle object. 11 months ago
enterprise-attack-6.1.json Patch files: Add spec_version back to the bundle object. 11 months ago

# Note About Groups & TTPs & Software



# *Module 3 Lab*



# Versioning

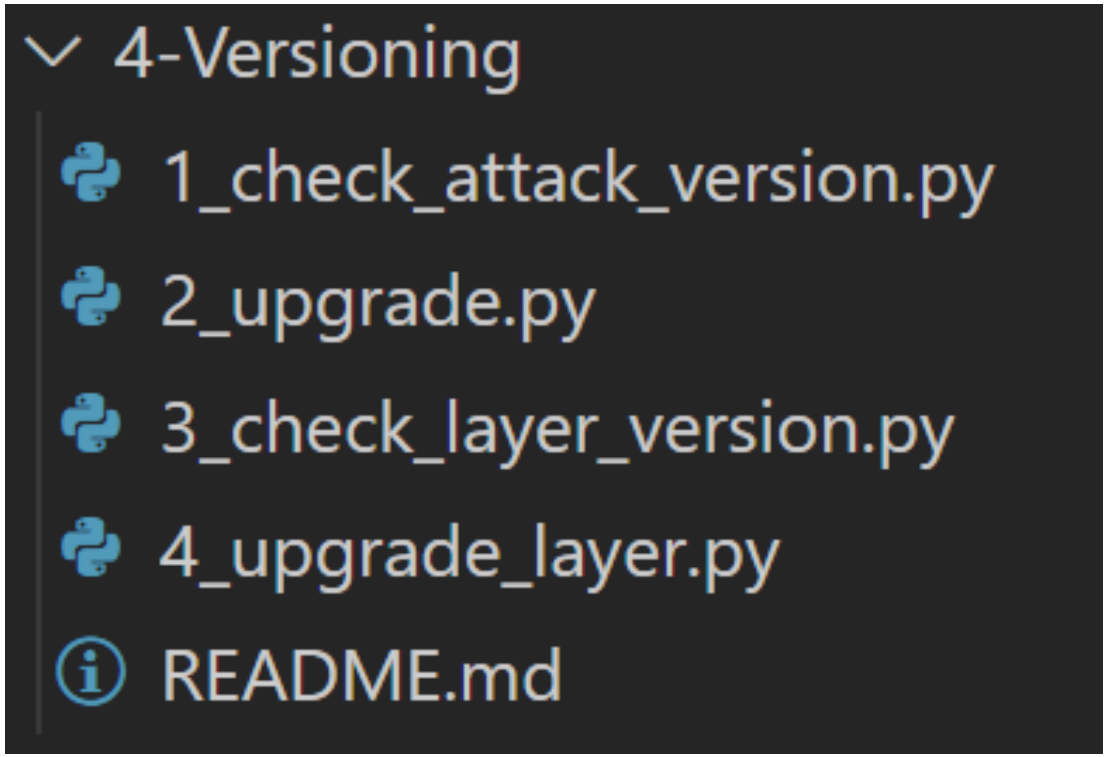
*How does ATT&CK handle versions/upgrades and why do we care?*

ASCENT SOLUTIONS

# Previous Versions

| Version | Start Date | End Date | Data | Release Notes |
|---|---|---|---|---|
| ATT&CK v11 (current version) | April 25, 2022 | n/a | v11.3 on MITRE/CTI | Updates — April 2022 |
| ATT&CK v10 | October 21, 2021 | April 24, 2022 | v10.1 on MITRE/CTI | Updates — October 2021 |
| ATT&CK v9 Data Sources | April 29, 2021 | October 20, 2021 | v9.0 on MITRE/CTI | Updates — April 2021 |
| ATT&CK v8 | October 27, 2020 | April 28, 2021 | v8.2 on MITRE/CTI | Updates — October 2020 |
| ATT&CK v7 Sub-Techniques | July 8, 2020 | October 26, 2020 | v7.2 on MITRE/CTI | Updates — July 2020 |
| ATT&CK v7-beta | March 31, 2020 | July 7, 2020 | v7.0-beta on MITRE/CTI | Updates — March 2020 |
| ATT&CK v6 | October 24, 2019 | March 30, 2020 | v6.3 on MITRE/CTI | Updates — October 2019 |
| ATT&CK v5 | July 31, 2019 | October 23, 2019 | v5.2 on MITRE/CTI | Updates — July 2019 |
| ATT&CK v4 | April 30, 2019 | July 30, 2019 | v4.0 on MITRE/CTI | Updates — April 2019 |
| ATT&CK v3 | October 23, 2018 | April 29, 2019 | v3.0 on MITRE/CTI | Updates — October 2018 |

# Module 4 Lab



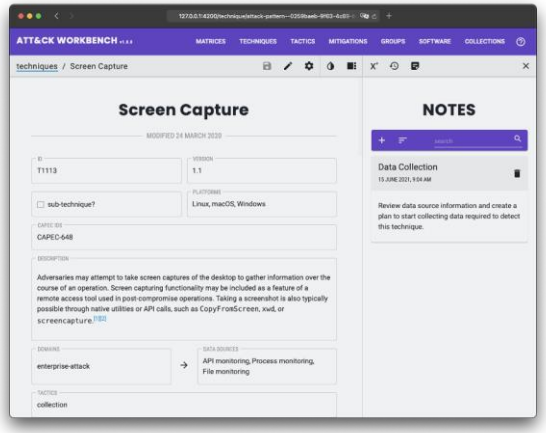
# Existing Tools

*What does ATT&CK provide? What does our community provide?*

ASCENT SOLUTIONS

## *ATT&CK Resources Page*

- ~~ATT&CK in STIX~~
- ATT&CK in Excel
- ATT&CK Navigator
- ATT&CK Python Utilities
- DeTT&CT
  - “mapping your blue team to ATT&CK”
  - Multi-level scoring, differentiation between visibility and detection and separation based on platforms and data sources
  - Allows you to score your data sources, visibility coverage, and detections WRT ATT&CK
- ATT&CK Workbench
  - Extending ATT&CK/Navigator



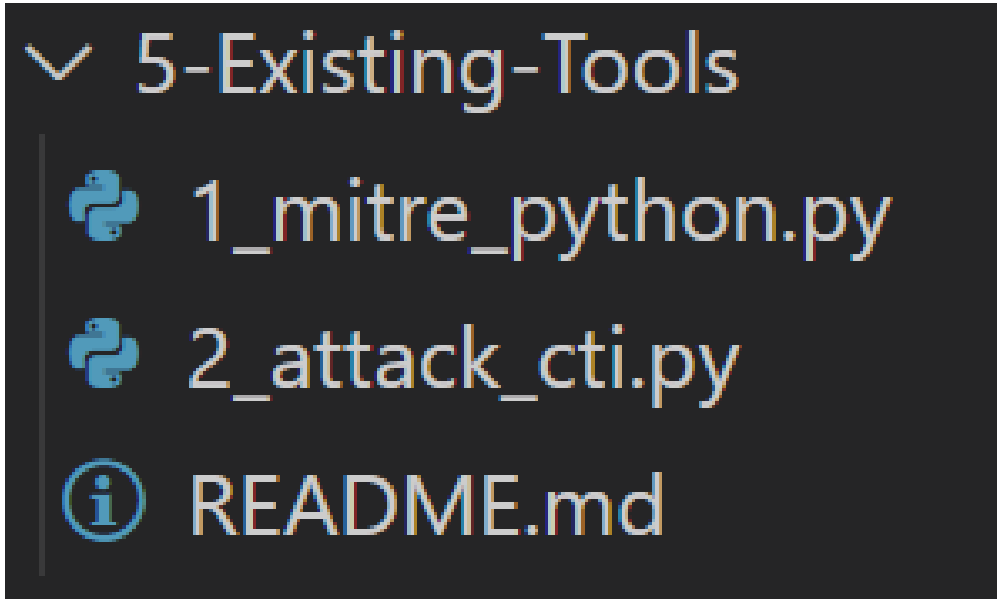

https://attack.mitre.org/resources/working-with-attack/

ASCENT SOLUTIONS

# *ATT&CK Navigator*

- Leveraging Navigator for analysis
  - ATT&CK® Navigator (mitre-attack.github.io)

# *Module 5 Lab*



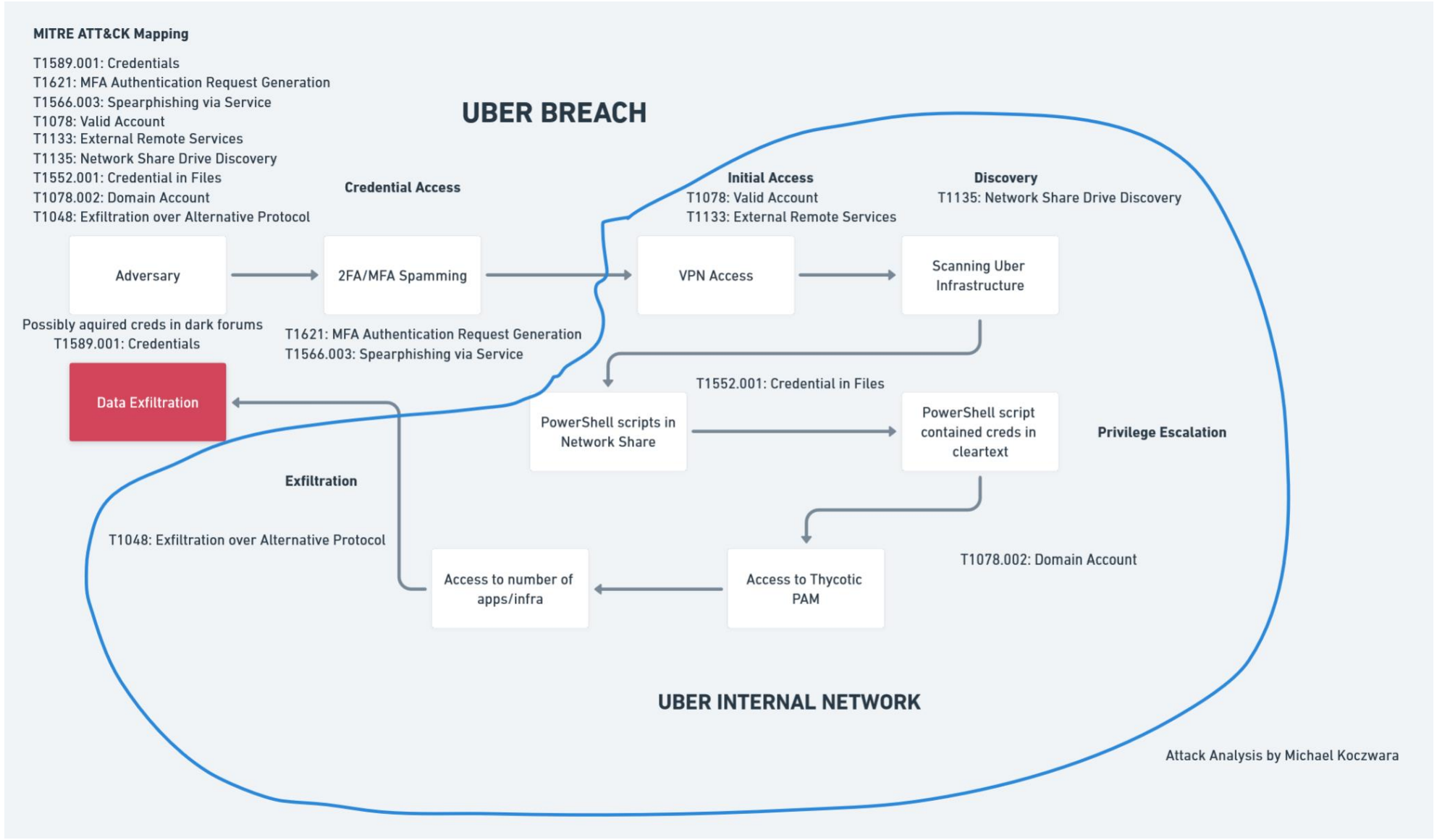
# Development Time

*Real World Examples / Problems*

ASCENT SOLUTIONS

# *Make it Your Own, Embrace It!*

# CTI / IR Work


MITRE ATT&CK Mapping
T1589.001: Credentials
T1621: MFA Authentication Request Generation
T1566.003: Spearphishing via Service
T1078: Valid Account
T1133: External Remote Services
T1135: Network Share Drive Discovery
T1552.001: Credential in Files
T1078.002: Domain Account
T1048: Exfiltration over Alternative Protocol
UBER BREACH
Credential Access
Initial Access
T1078: Valid Account
T1133: External Remote Services
Discovery
T1135: Network Share Drive Discovery
Adversary
2FA/MFA Spamming
VPN Access
Scanning Uber Infrastructure
Possibly aquired creds in dark forums
T1589.001: Credentials
T1621: MFA Authentication Request Generation
T1566.003: Spearphishing via Service
Data Exfiltration
T1552.001: Credential in Files
PowerShell scripts in Network Share
PowerShell script contained creds in cleartext
Privilege Escalation
Exfiltration
T1048: Exfiltration over Alternative Protocol
Access to number of apps/infra
Access to Thycotic PAM
T1078.002: Domain Account
UBER INTERNAL NETWORK
Attack Analysis by Michael Koczwara

# Module 6 Lab