Please ATT&CK My Intelligence!

Get inside the heads of your adversaries and win!

Mike McPhee
Principal Solutions Engineer – Security

CCIEx2 | CCDE | GSE
US Commercial

3 December 2024

Our session's roadmap...

- Whois
- Scary Stories
- Hacking fear with CTI
- ATT&CKing Intelligence
- Use CTI to flip the script
- Conclusion

About me

- Rochester NY (Garbage Plates and Kristen Wig!!!)
- 11 years with Cisco
- 12+ years designing C2 systems
- 6 years in US Navy – “Bubblehead”
- GSE #339 & SANS MSISE
- 10-year CCIE 41663 (R&S, Sec) & CCDE 20180018
- Homebrewer, woodworker

Scary stories...

“If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.”

Sun Tzu

CTI Afficionado, Author of "The Art of War”

Threat Intelligence? Oh wow, where do we start?

Global Threat Picture is complex and overwhelming

Dual-Use Tools

Cryptojacking

Ransomware

Unpatched Software

Data/IP Theft

Spyware/Malware

Code Bugs

Malvertising

Wiper Attacks

Drive by Downloads

Phishing

Rogue Software

Man in the Middle

Botnets

Exposed Datastores

Credential compromise

Advanced Persistent Threats

DDoS

Supply chain attacks

We need to narrow our focus

Don’t chase other peoples’ boogiemen

Are you driven by press or by your own threat picture?

- Likely tactics?
  - Everyone exposed to ransomware, phishing: the devil is in the details
  - Ex. Unlikely to see Quantum insert exploits on politically insignificant sites, Magecart in non-commerce, etc.
- Likely adversaries?
  - Threat actors usually concentrate on certain vertical/geography
  - Could be implicated by political affinity, downstream customers (e.g. ISPs for government, banks serving sector)
  - “Cui bono” = to whom will it benefit? Who can benefit from compromising you?
  - Don’t forget the wide-net aspect of threat actors (log4j/log4shell)
- Find and read up your most likely actors through incident reports and CTI

Hack your fear with CTI

What is Cyber Threat Intelligence?

- It is a chance to surprise the adversaries
  - Characterization of an attacker's behavior
  - Useful to inform defenses and reveal gaps
  - Can be fused with visibility to reveal situational awareness
- Where can we get CTI?
  - Vendors, via subscriptions and feeds
  - Open source and community provided/sourced
  - Your own infrastructure
- What CTI isn't:
  - A magic bullet
  - Only for large enterprises

Threat Hunting Maturity Model (HMM)

Stages help guide CTI progression in your environment

Level	Level 0 Initial	Level 1 Minimal	Level 2 Procedural	Level 3 Innovative	Level 4 Leading
Sophistication	- Relies primarily on automated reporting - Tools on default configs, little else	- Incorporates threat intelligence indicator searches. - Showing awareness, if not yet practicing CTI	- Follows analysis procedures created by others - Reliably repeatable practices	- Creates new data analysis procedures. - Dedicated hunters	- Automates most successful data analysis procedures - Hunters leveraging advanced collection & analytics
Data Collection	Little/none	Beginning CTI - Moderate/high level	High or very high level	High or very high level	High or very high level
Enablers	Security products	Integration (Detection), STIX/TAXII feeds	Integrated (Reponse), APIs/Scripts	Orchestration	Customized analytics tailored integrations

Threat Intelligence Use Case

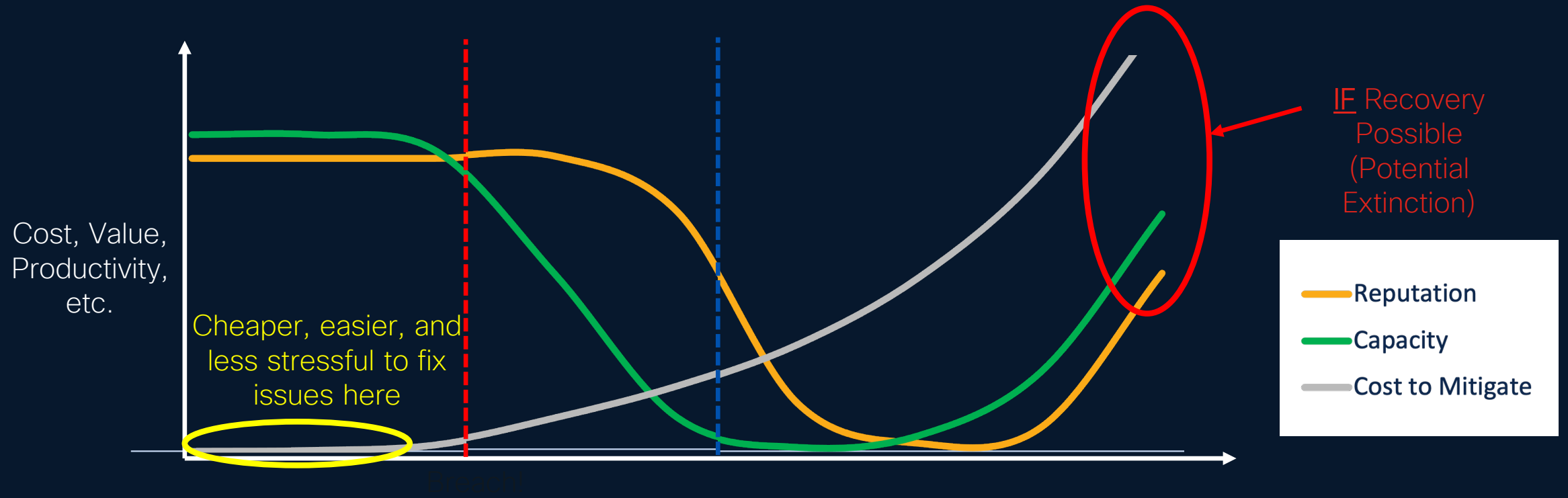
Detections & Analytics Use Case

Adversary Emulation Use Case

Gap Analysis & Engineering Use Case

Earlier detection = cheaper mitigation

- Predicting, deterring, and early detection reduce cost and workload



- Better to be “left of boom” – tackle problems before becoming acute!
- Earlier & effective controls = better performance, lower pressure/cost, preserved reputation
- CTI relieves pressure! Not just for Global corporations/governments…we all need it!

The 3 Main CTI Categories

A mix of them all will be key to your success and sanity

- Strategic: Sometimes the board needs to know about the monsters.
  - Tell them!
  - Use Risk Management and high-level insights to back strategy asks
- Tactical: What most of us think of – Indicators of Compromise
  - Domains, hashes, URLs, traffic signatures
  - Changes rapidly, but it is where we are forced to operate
- Operational: Wouldn't it be nice to truly know our adversary?
  - Behavioral focus
  - Tactics, Techniques and procedures are MUCH harder to change

If only we had something that taught us Operational CTI...

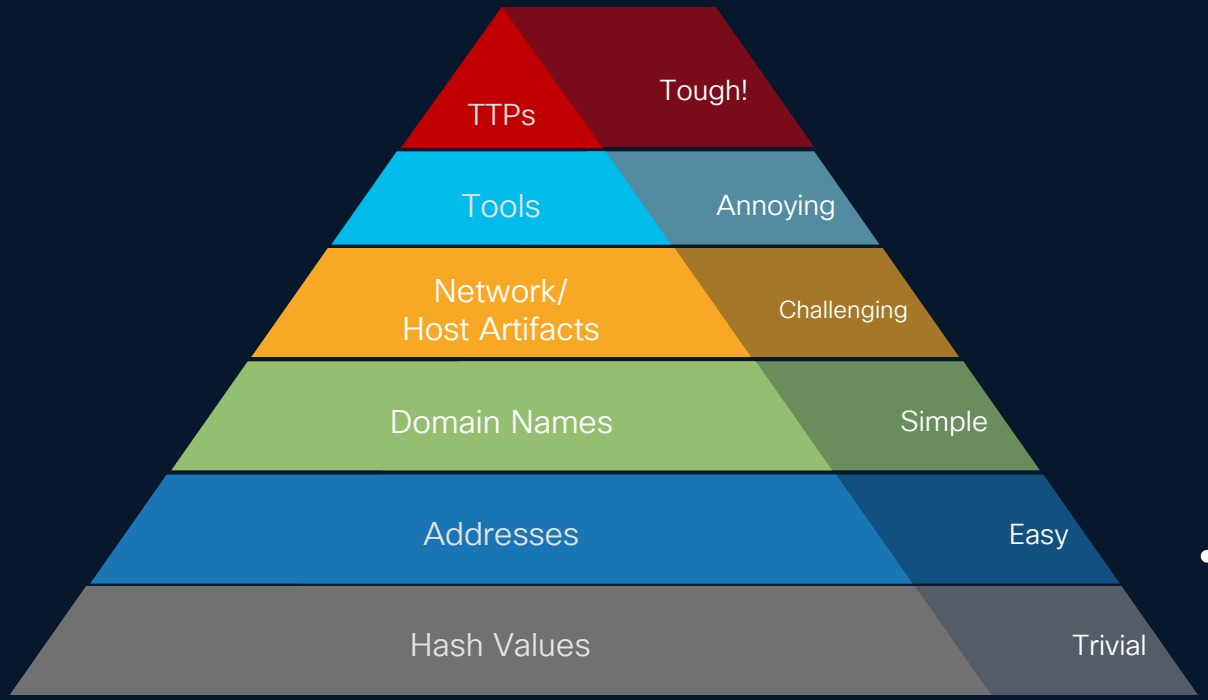
ATT&CKing Intelligence

Get to know your fear with MITRE's ATT&CK

- Who is MITRE Corporation?
  - Not-for-profit, US company with multiple federally funded R&D centers (FFRDCs)
  - Public-private partnerships in many areas, including cybersecurity
  - Same folks who brought us CVE database/list
- What is ATT&CK
  - **A**dversarial **T**actics, **T**echniques, **&** **C**ommon **K**nowledge
  - Born in 2013 to document tactics, techniques, and procedures (TTPs) that APTs use on Windows networks
  - Globally-accessible knowledge base
  - Used for the development of specific threat models & methodologies in the private sector, in government, and in the cybersecurity product and service community.

ATT&CK changes our focus

Concentrate on the root of the problem to achieve security enlightenment

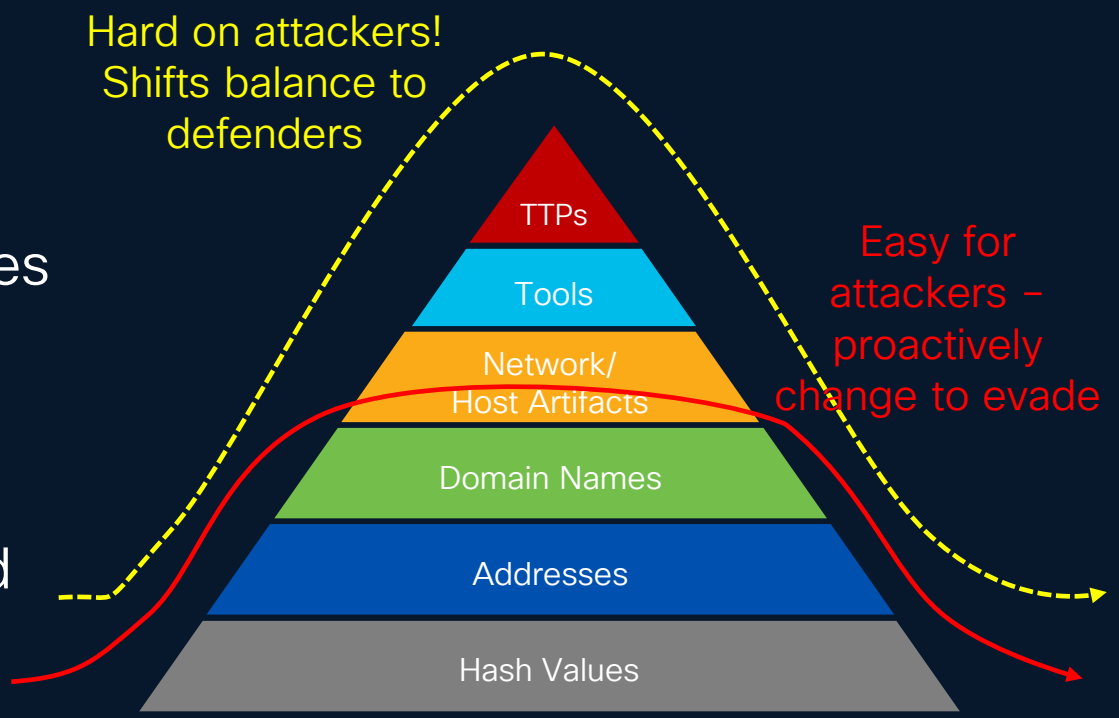


From David Biacco (Splunk, a Cisco Company):
https://www.eventtracker.com/blog/2015/february/the-pyramid-of-pain/

- TTPs, a.k.a. “The Problem”:
  - Good: TTPs behaviors ingrained in adversary – much harder to modify
  - Bad: Behavior defies checking boxes
  - HARD to tackle = conceptual, prone to false positives/negatives without good context
- IOCs, a.k.a. “The Symptom”:
  - Good: Generally, focus on are easily tracked attributes – “tangible”
  - Bad: easily tracked attributes are easily changed – Attacker advantage

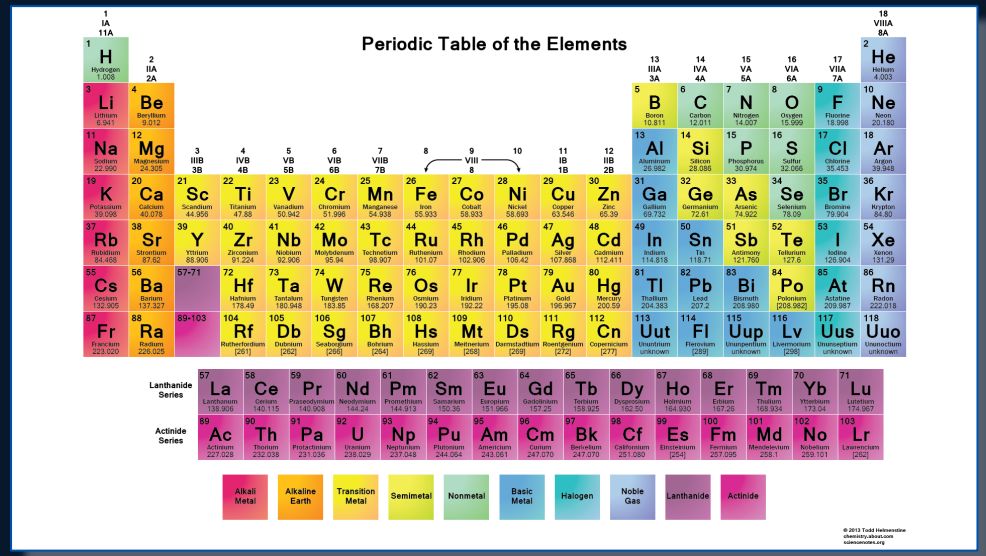
Push the adversary to change
Why should the defender always sweat it out?

- Time-based security: protection buys time.
  - Will always fail – must detect and remediate before that happens
  - Pt > Dt + Rt
- Forcing TTP changes → harder on adversaries
  - Changing TTP (or tooling) takes time, depletes resources, and exhausts funds
  - Strategic shifts create more detectable events
- Adversaries may leave, or become frustrated
- Defenders can – with commitment – work to force the paradigm shift

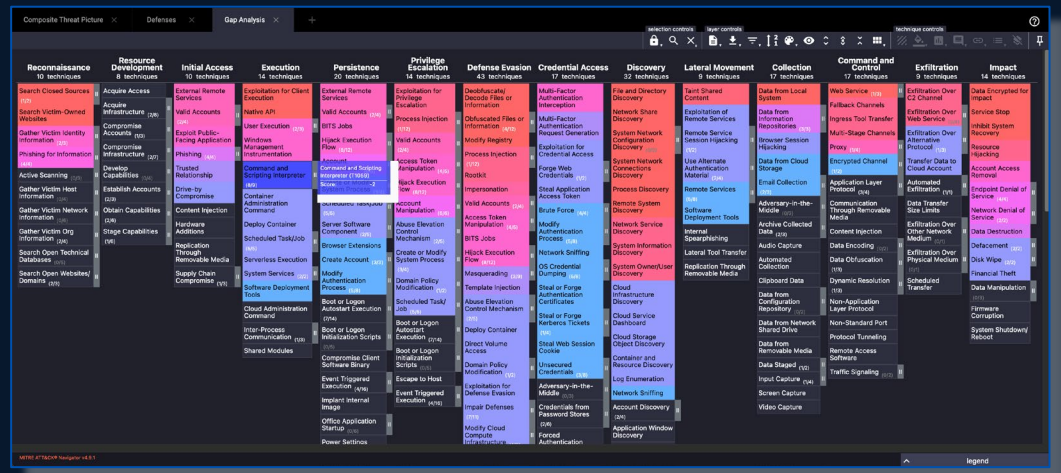


The alchemy of adversarial behavior

Techniques are the elements, bonded together to form APT patterns



- Groups (similar behavior/valence band)
- Elements and their oxidation states
- MSDS Sheets
- Molecules
- Compounds drastically different than elements that form them



- Tactics (base on similar adversarial goals)
- Techniques and their Sub-Techniques
- Mitigations
- Adversaries
- Adversaries drastically different despite using similar techniques but in different ways

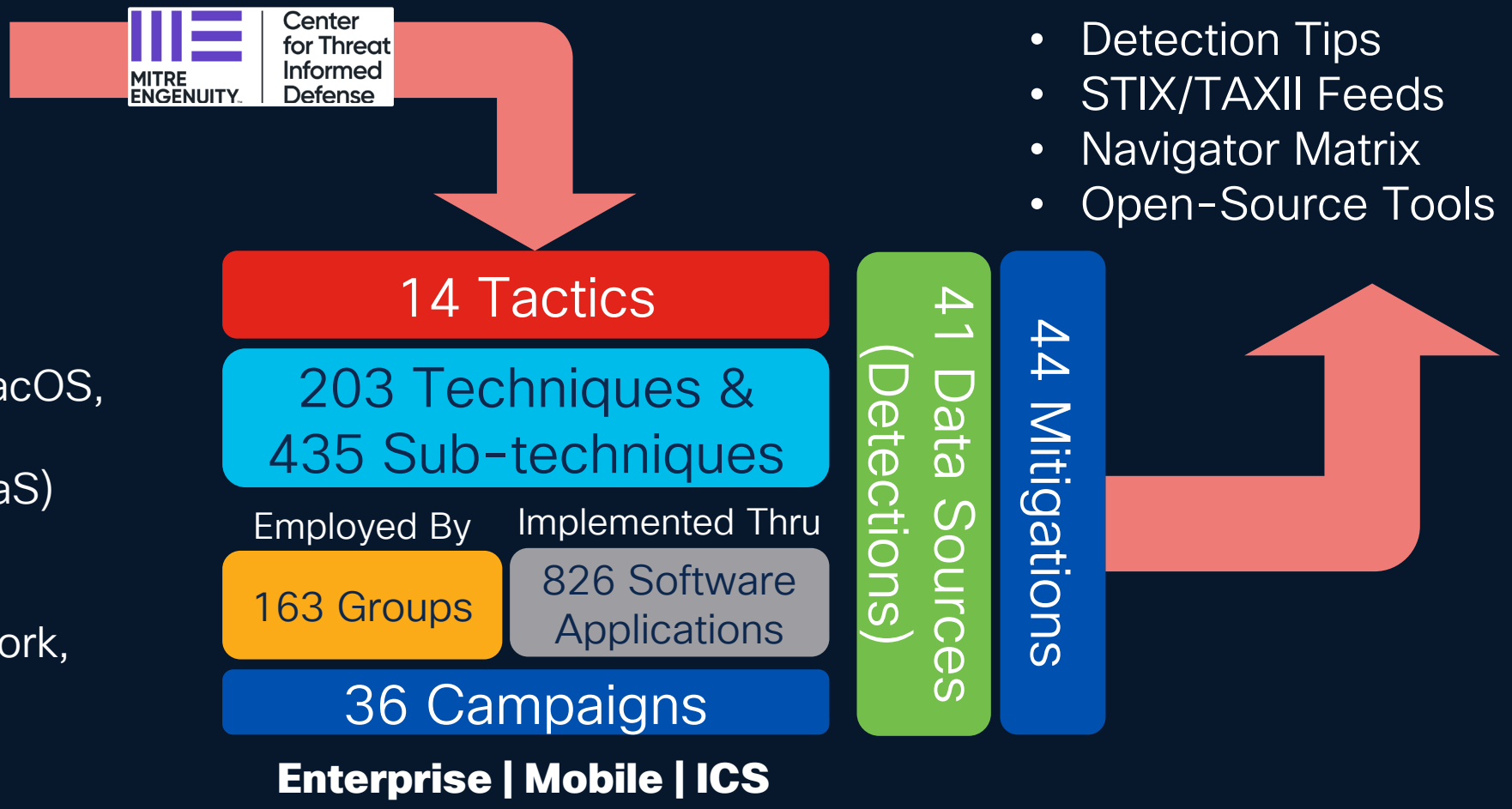
What is inside ATT&CK?

Enterprise matrix as an example…

- Open-Source CTI
- Blog Entries
- MITRE R&D
- Community Feeds

Key platforms:

- OS: Windows, macOS, Linux
- Cloud (IaaS & SaaS)
- O365, Google Workspaces
- Containers, Network, VMs
- iOS & Android

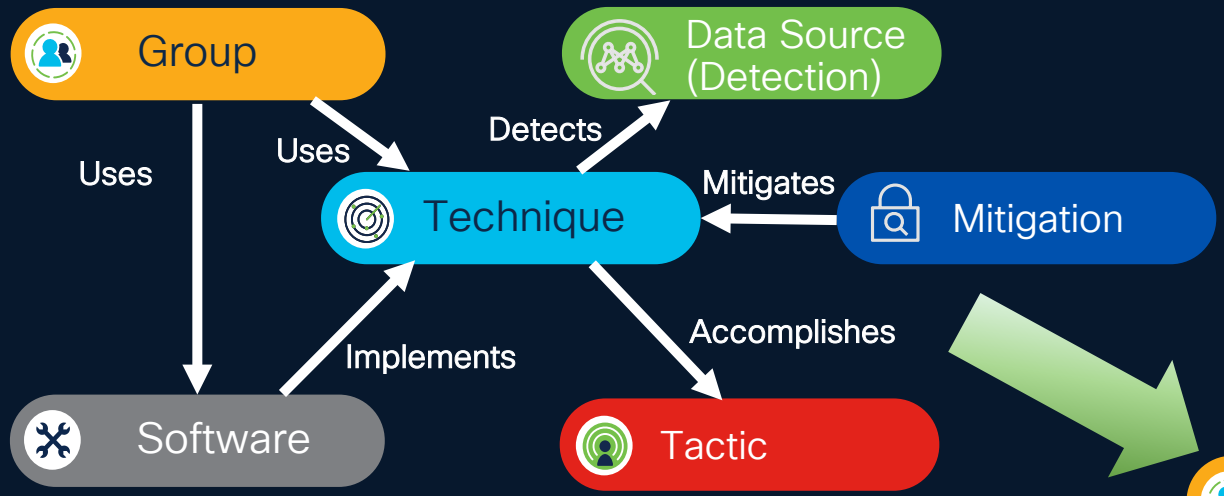


As of MITRE ATT&CK v16 (October 31, 2024)

- Detection Tips
- STIX/TAXII Feeds
- Navigator Matrix
- Open-Source Tools

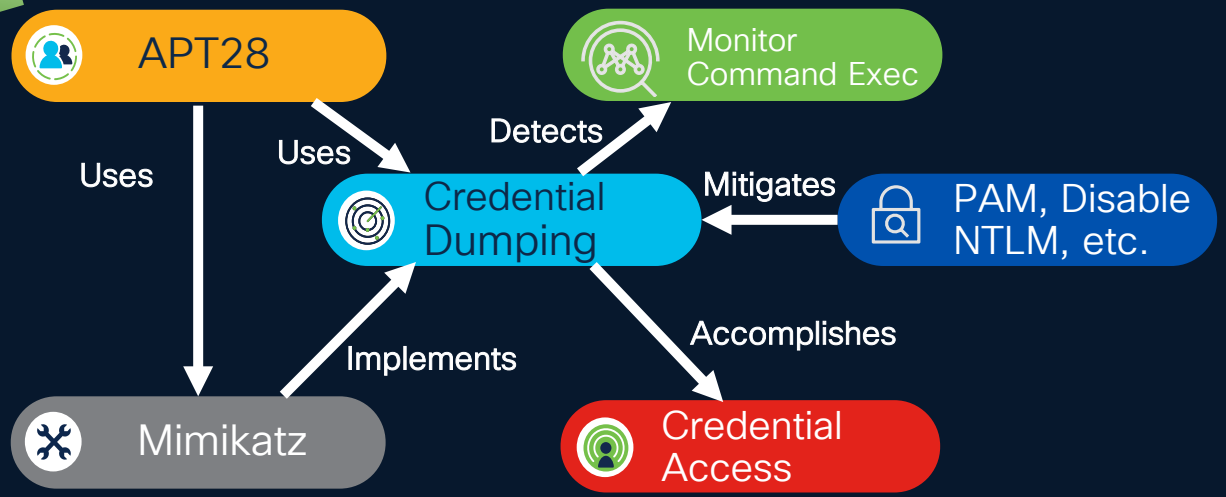
Understand your ATT&CK model relationships

MITRE's approach simplifies mapping goals to behaviors (a.k.a. TTPs)



MITRE Advice on Detection for T1003.001 (OS Credential Dumping: LSASS Memory)?

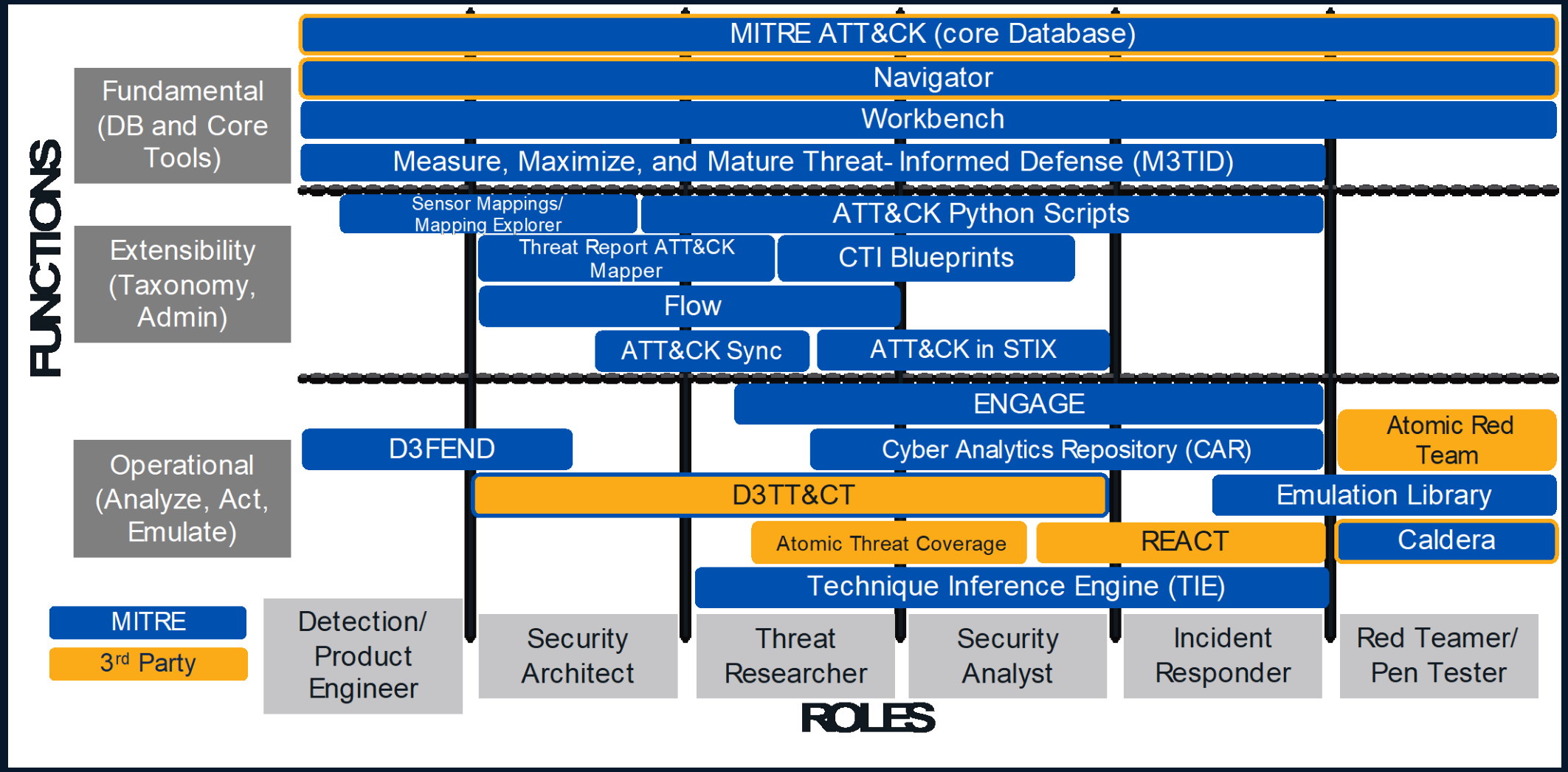
- Monitor event IDs 10, 4104, 4633 and 4688
- Find process where target = "*lsass.exe" AND source is taskmgr.exe



- Detections or Mitigations can happen in Software, Technique, or Tactics
- https://www.mitre.org/publications/technical-papers/mitre-attack-design-and-philosophy

ATT&CK is also an ecosystem of projects

Open-Source CTI has a lot of applications!



Want a copy? https://github.com/mjmcphee/attack-rosetta

In ATT&CK, we finally have a common language

It is for everyone!

- Sharing of intel across all disciplines, vendors, personas, etc.
- No need to switch contexts with different teams
- Unlike other frameworks, pretty broadly accepted across geographies/verticals

Vendor-agnostic: Helps all get along in multi-vendor environments

- Can form a fair(er) approach to evaluating capabilities
- Offers means by which to fuse information from disparate sources
- Well supported in Threat Intelligence Platforms, SIEMs, and XDRs (especially ours)

Easier to grasp

- Focuses on the enemy
- Roughly aligns to series of events and behaviors

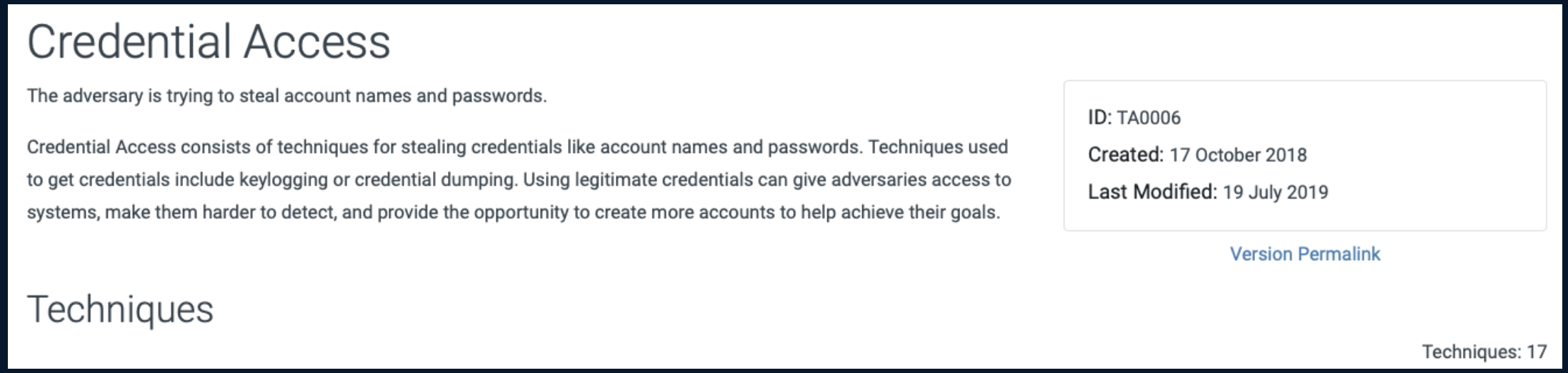
The 5 W's of threat modeling

My English teacher would be so proud...

• Who is threatening us?	Group
• Why are they doing it?	Tactic
• What are they doing?	Technique
• How are they doing it?	Procedure and/or Software
• Where can we prevent it?	Mitigation
• When are we going to notice?	Detection

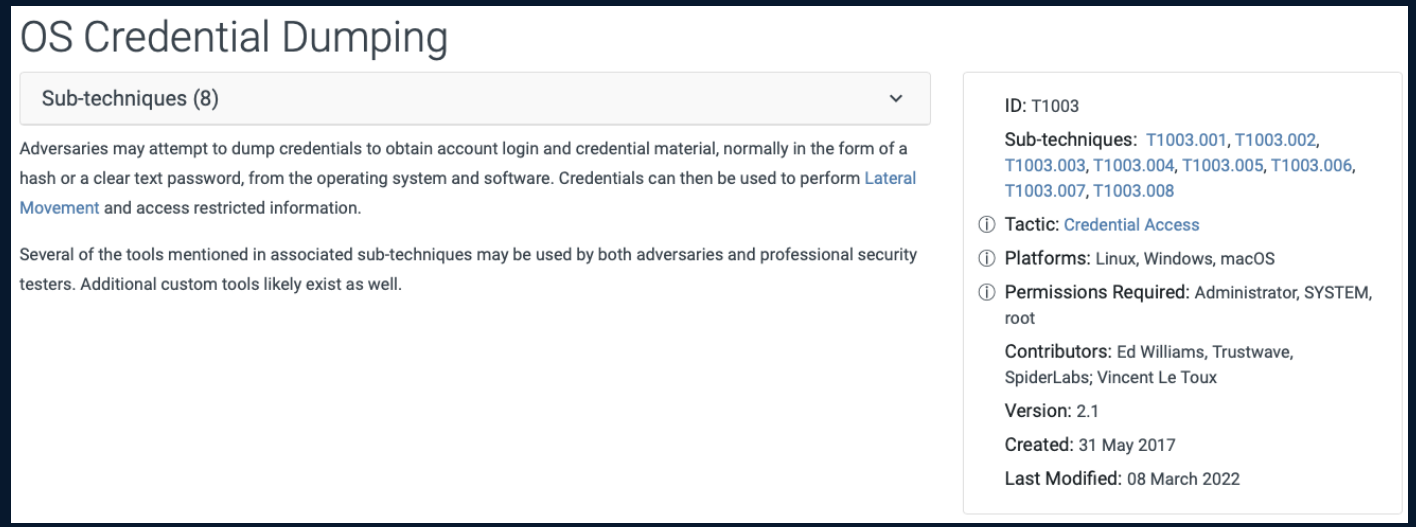
What is a Tactic

- Tactics represent the "why" of an ATT&CK technique or sub-technique.
- The adversary's tactical goal: the reason for performing an action.
- Example: an adversary may want to achieve credential access.
- There are currently 14 Enterprise Tactics



What is a Technique

- Techniques represent 'how' an adversary achieves a tactical goal by performing an action.
- Example: an adversary may dump credentials to achieve credential access.
- There are currently:
  - 196 Techniques
  - 411 Sub-techniques



What is a Sub Technique

- More specific description of the adversarial behavior used to achieve a goal.
- Lower level than a technique.
- Example: an adversary may dump credentials by accessing the Local Security Authority (LSA) Secrets.

OS Credential Dumping: LSA Secrets

Other sub-techniques of OS Credential Dumping (8)

Adversaries with SYSTEM access to a host may attempt to access Local Security Authority (LSA) secrets, which can contain a variety of different credential materials, such as credentials for service accounts.[1][2][3] LSA secrets are stored in the registry at `HKEY_LOCAL_MACHINE\SECURITY\Policy\Secrets`. LSA secrets can also be dumped from memory.[4]

Reg can be used to extract from the Registry. Mimikatz can be used to extract secrets from memory.[4]

ID: T1003.004

Sub-technique of: T1003

ⓘ Tactic: Credential Access

ⓘ Platforms: Windows

ⓘ Permissions Required: SYSTEM

Contributors: Ed Williams, Trustwave, SpiderLabs

Version: 1.0

Created: 21 February 2020

Last Modified: 21 April 2021

Version Permalink

What is a Procedure

- Procedures are the specific implementation the adversary uses for techniques or sub-techniques.
- Example: adversary uses PowerShell to inject into lsass.exe and scrape LSASS memory to dump credentials.
- "Procedure Examples" section of technique pages.

Procedure Examples

ID	Name	Description
S0677	AADInternals	AADInternals can dump secrets from the Local Security Authority.[5]
G0064	APT33	APT33 has used a variety of publicly available tools like LaZagne to gather credentials.[6][7]
S0050	CosmicDuke	CosmicDuke collects LSA secrets.[8]
S0488	CrackMapExec	CrackMapExec can dump hashed passwords from LSA secrets for the targeted system.[9]
G0035	Dragonfly	Dragonfly has dropped and executed SecretsDump to dump password hashes.[10][11]
S0008	gsecdump	gsecdump can dump LSA secrets.[12]

Use it or lose it!

So that's nice, but what can we do with it?

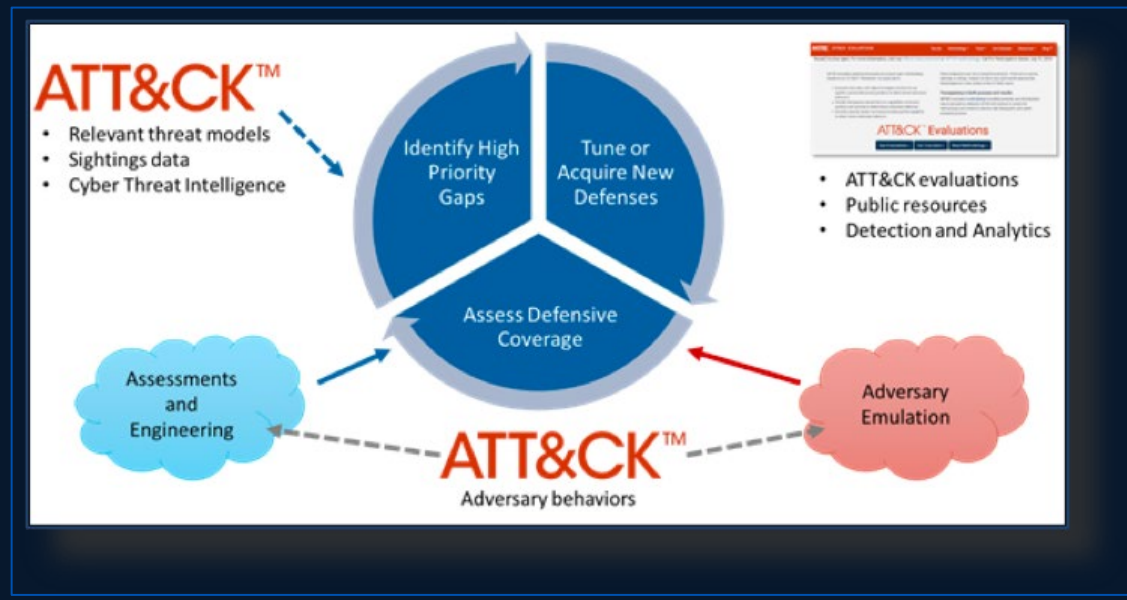
MITRE Envisioned 4 main use cases for the collected CTI

Early adopters =>attribution & CTI:

- Threat intelligence
- Detection and analytics
- Adversary emulation

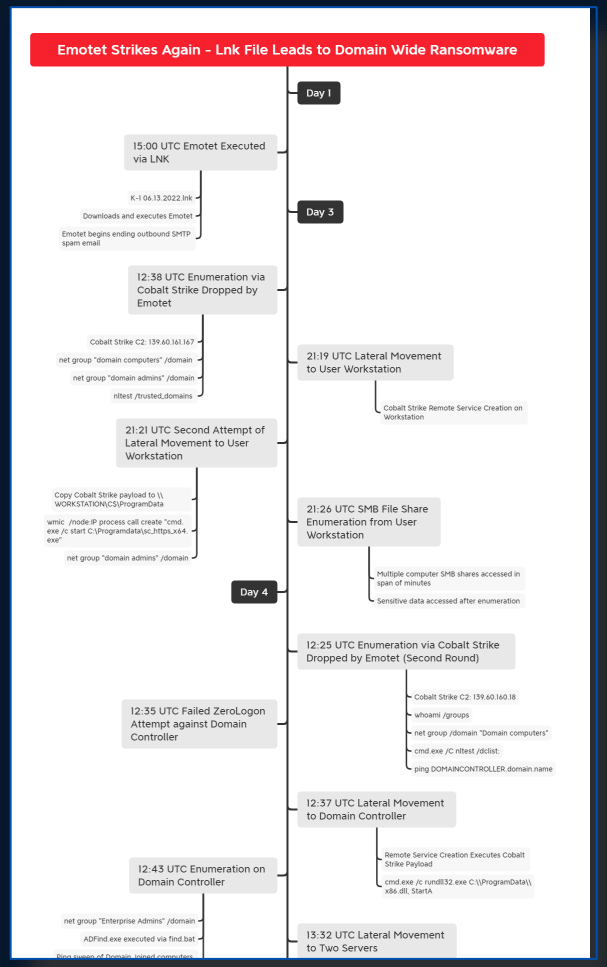
We're pre-sales. Let's also use ATT&CK to make things better!

- Assess coverage: do defenses stack up against the bad guys?
- Prioritize gaps: ID highest priorities
- Tune defenses: modify or acquire new!



Using ATT&CK for Threat Intelligence

Open-source CTI to augment in-house threat researchers



"If you know the enemy and know yourself, you need not fear the result of a hundred battles."- Sun Tzu

- Focus on enriching threat picture and learning about adversaries.
- Improves decision making and response, usually needs in-house analysts
- Great vendor-agnostic blog: https://thedfirreport.com

Using ATT&CK for Detection and Analytics

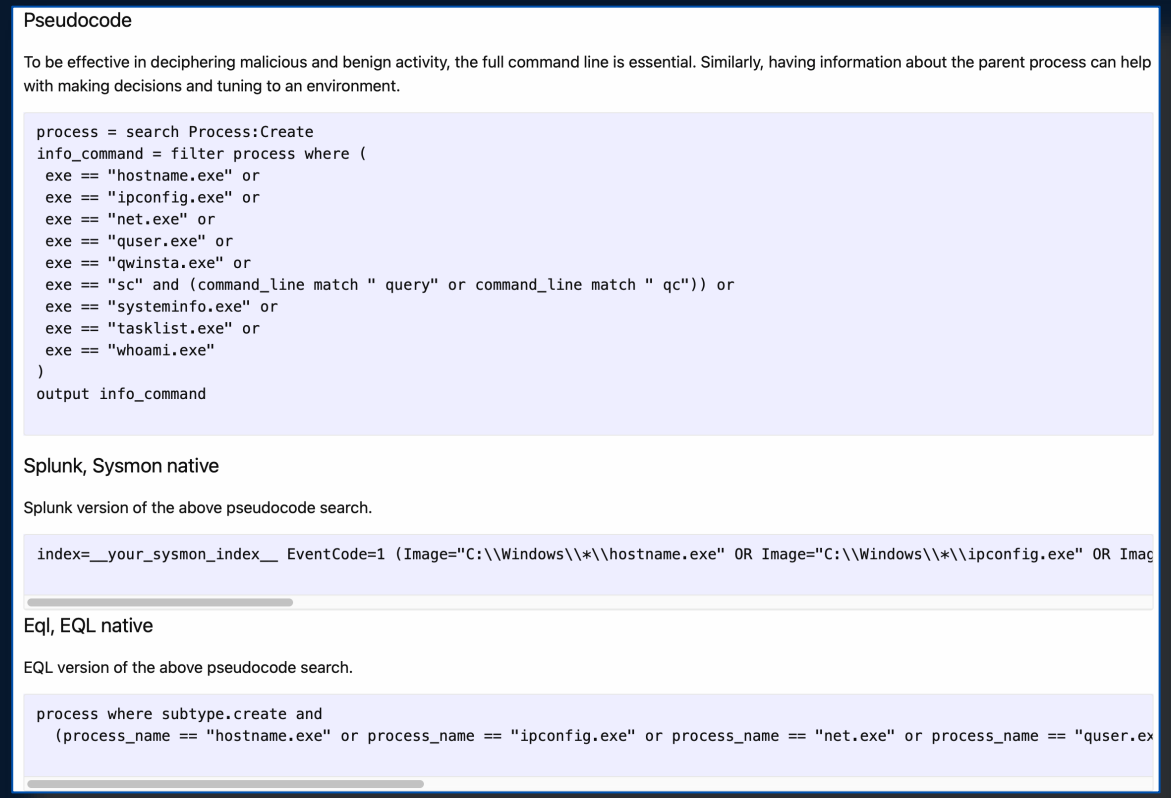
Takes detection beyond globally known signatures

- Guide log analysis and packet capture
- Logs and captures reveal behaviors

Focus on deeper use of available tools:

- CLI and process logging, Packet capture
- Logs - auth, syslog, etc. (Sigma tool, ELK, etc.)
- File Integrity & Registry monitoring

Check out MITRE's Cyber Analytics Repository!
https://car.mitre.org



Pseudocode

To be effective in deciphering malicious and benign activity, the full command line is essential. Similarly, having information about the parent process can help with making decisions and tuning to an environment.

```
process = search Process:Create
info_command = filter process where (
 exe == "hostname.exe" or
 exe == "ipconfig.exe" or
 exe == "net.exe" or
 exe == "quser.exe" or
 exe == "qwinsta.exe" or
 exe == "sc" and (command_line match " query" or command_line match " qc")) or
 exe == "systeminfo.exe" or
 exe == "tasklist.exe" or
 exe == "whoami.exe"
)
output info_command
```

Splunk, Sysmon native

Splunk version of the above pseudocode search.

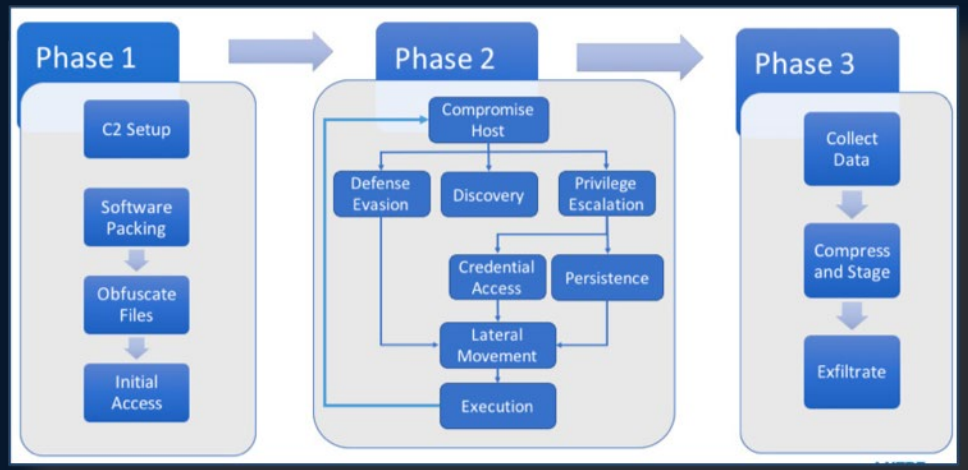
```
index=__your_sysmon_index__ EventCode=1 (Image="C:\\Windows\\*\\hostname.exe" OR Image="C:\\Windows\\*\\ipconfig.exe" OR Imag
```

Eql, EQL native

EQL version of the above pseudocode search.

```
process where subtype.create and
  (process_name == "hostname.exe" or process_name == "ipconfig.exe" or process_name == "net.exe" or process_name == "quser.ex
```

Using ATT&CK for Adversary Emulation



APT13 Operational Flow

Used by Red & Purple Teams

- Improves efficacy of in-house Red Team
- Helps scope and collaborate with external Red Team
- Purple Teams often unite around TTP-based exercises

Embedded details in ATT&CK lead through each group's progression

Useful in pitting defenses against a look-alike adversary

More time-consuming, but valuable in uncovering misconfiguration, gaps, etc.

Using ATT&CK for Assessments & Engineering

Taking stock of what gaps need filling and how successful solutions will be

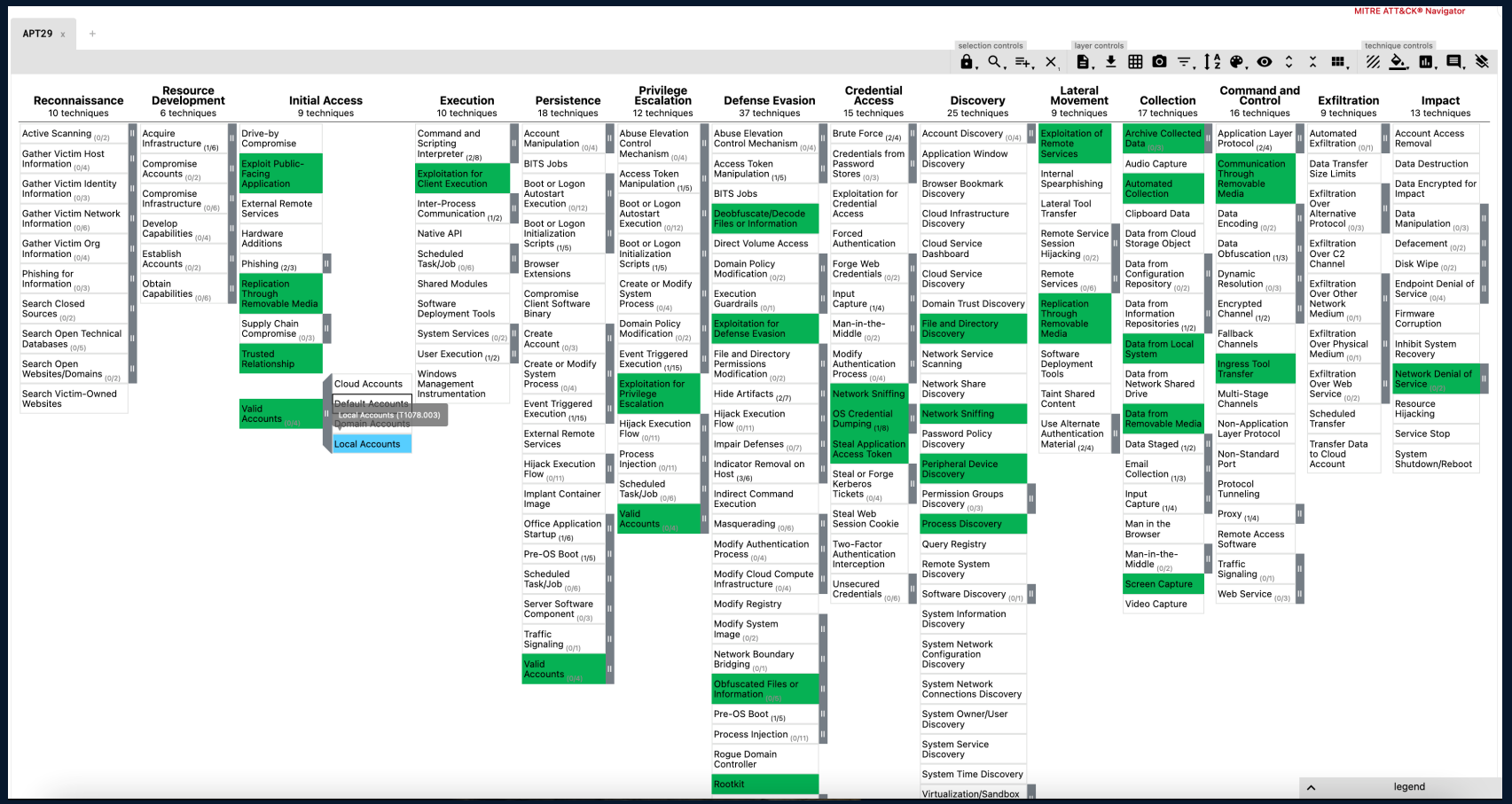
THIS is the most widely applicable use case across segments & verticals

- Possible for organizations of all sizes
- Crawl-Walk-Run -> 3-levels based on maturity

Cisco's XDR and portfolio are quickly moving to assist here

- Enrichment of alerts with TTPs
- Coverage mapping
- Building rulesets and policy sets based on APTs or Tactics

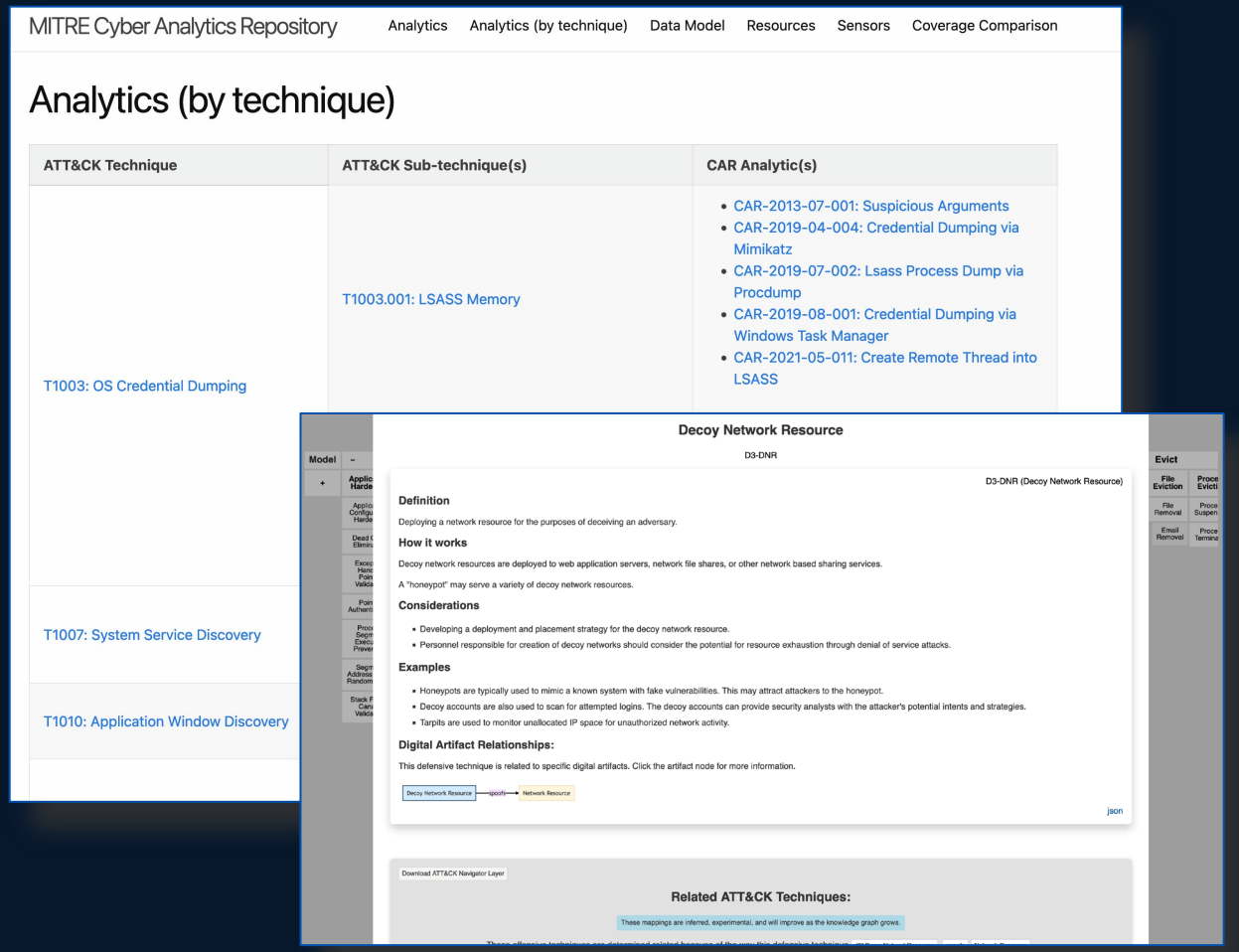
ATT&CK Navigator a versatile tool for our needs



- https://mitre-attack.github.io/attack-navigator/
- Want to dig deeper? Check my YouTube demo: https://youtu.be/76n6jTTiOU8

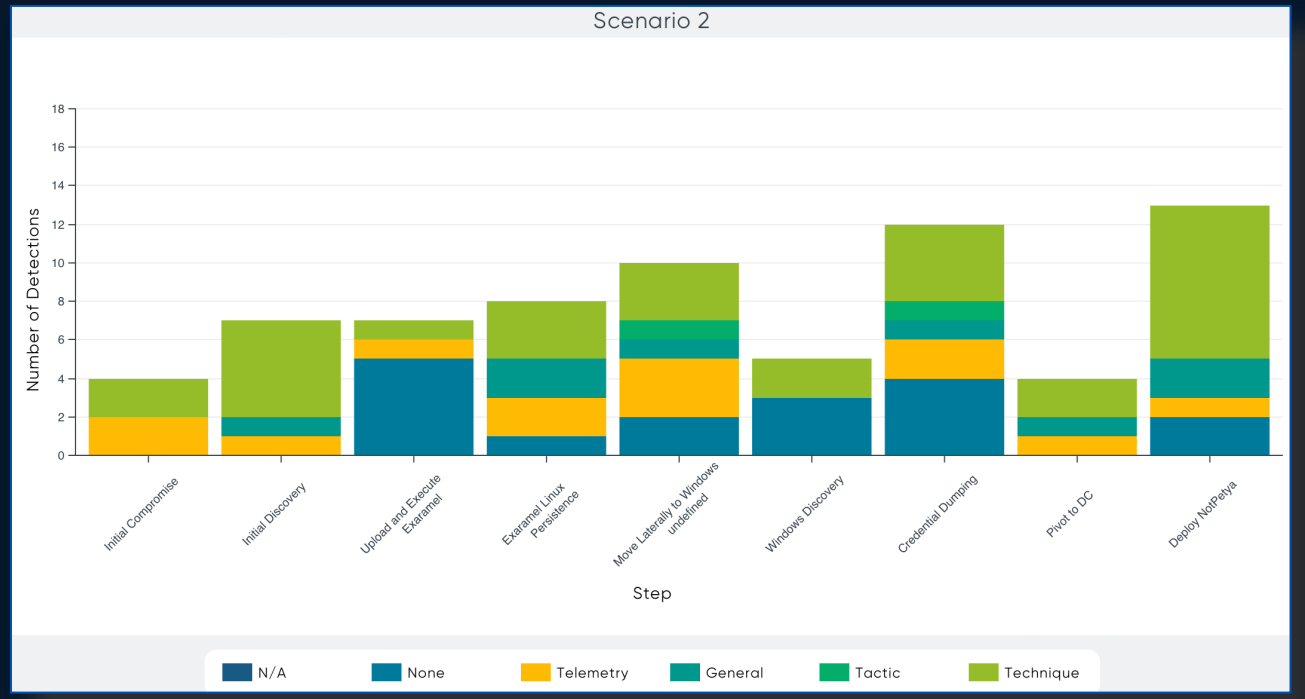
Building detections or engineering tools?
CAR and D3FEND extent ATT&CK into those realms

- Cyber Analytics Repository offers curated detections using SIEMs and related tools: https://car.mitre.org/analytics/by_technique
  - Psuedocode helpful for other products
  - Sigma project offers feed of supporting detections: https://github.com/SigmaHQ/sigma
- Engineering detection tools? D3FEND ties defensive tech to ATT&CK TTPs
  - https://d3fend.mitre.org/



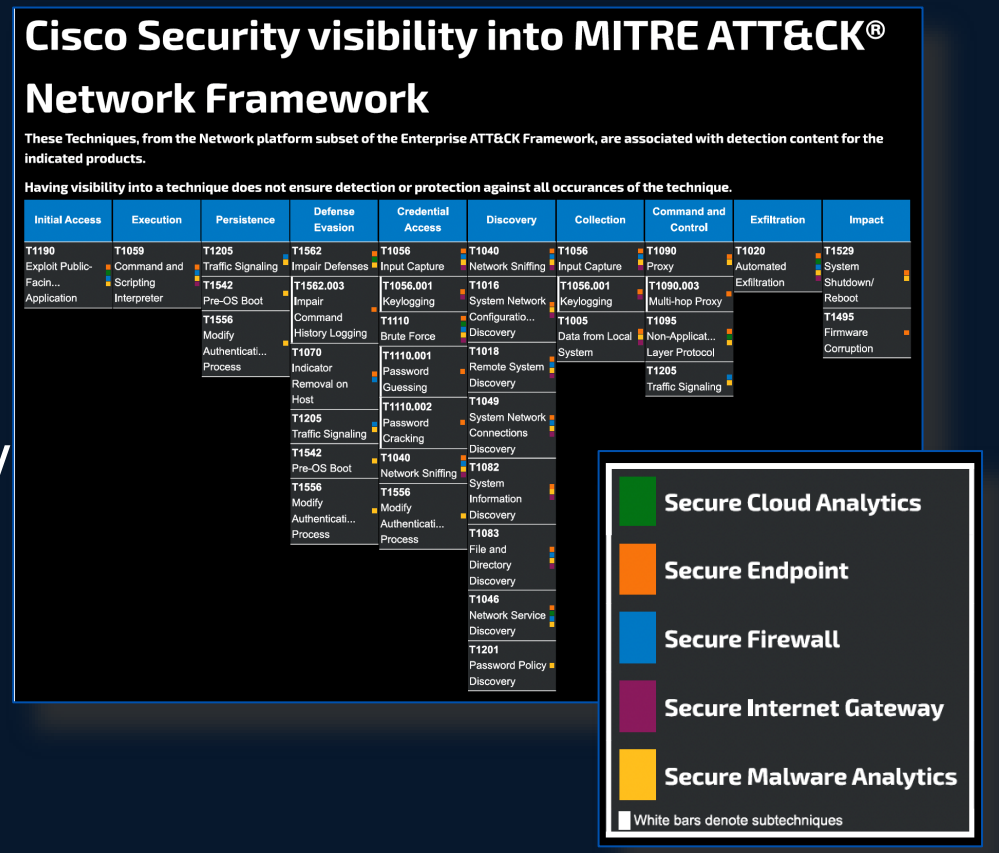
MITRE ATT&CK Evaluations

- Threat-informed evaluation of ability to detect or protect.
  - Adversary behavior in ATT&CK
  - Thoroughly & openly documented
  - Measurable/repeatable, constant eval of incremental improvements
- Latest round- Turla for 2022/2023
  - >EDR -submitted XDR-like offering
  - Cisco has had steady improvement with each iteration – drives our roadmaps!
- “not a competitive analysis”, “do not showcase scores, rankings, or ratings”
- Coverage != guarantees OR efficacy



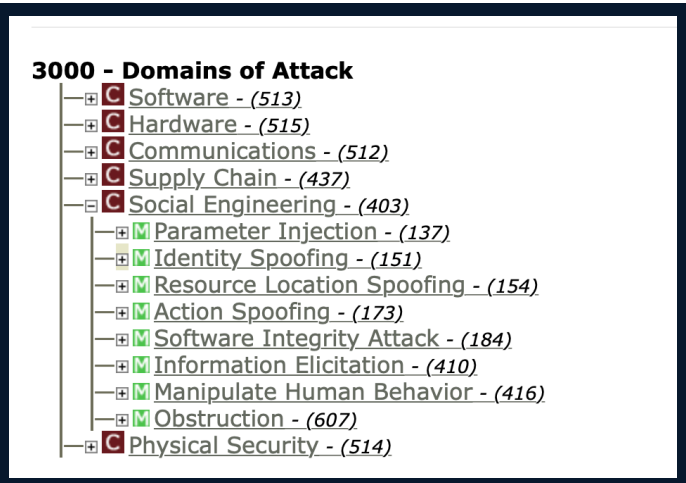
Marketing and Thought Leadership

- Customers increasingly evaluating ATT&CK Coverage
  - Most vendors (Cisco Included) offering matices
  - Built into tools like Cisco XDR
- Lots of FUD – be sure to know how they are establishing credit for coverage?
  - Cisco coverage assessed by analysis conducted by Cisco Talos
  - Even better? Verify using Emulation or BAS tools



CAPEC: Hyper-focused on app and web

Concentrate on the root of the problem to achieve security enlightenment



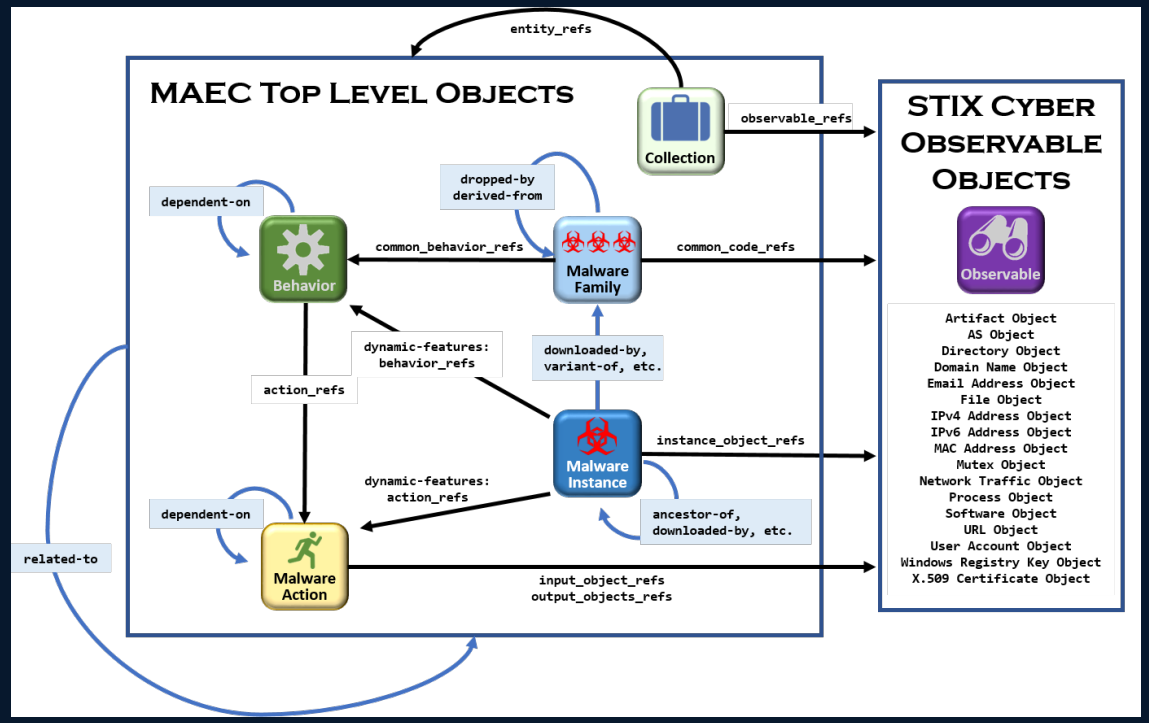
Common Attack Pattern Enumerations and Classifications (CAPEC)

- Catalogues attack patterns used in exploiting an application
  - SQL Injection, XSS, Hijacking, etc.
  - Includes supply chain & social engineering
- Useful when dealing with a web-facing customer or SaaS provider
- Compliments ATT&CK, neither is a subset of the other

Source: https://capec.mitre.org/index.html

MAEC:Malware what ATT&CK:Networks & devices

Concentrate on the root of the problem to achieve security enlightenment



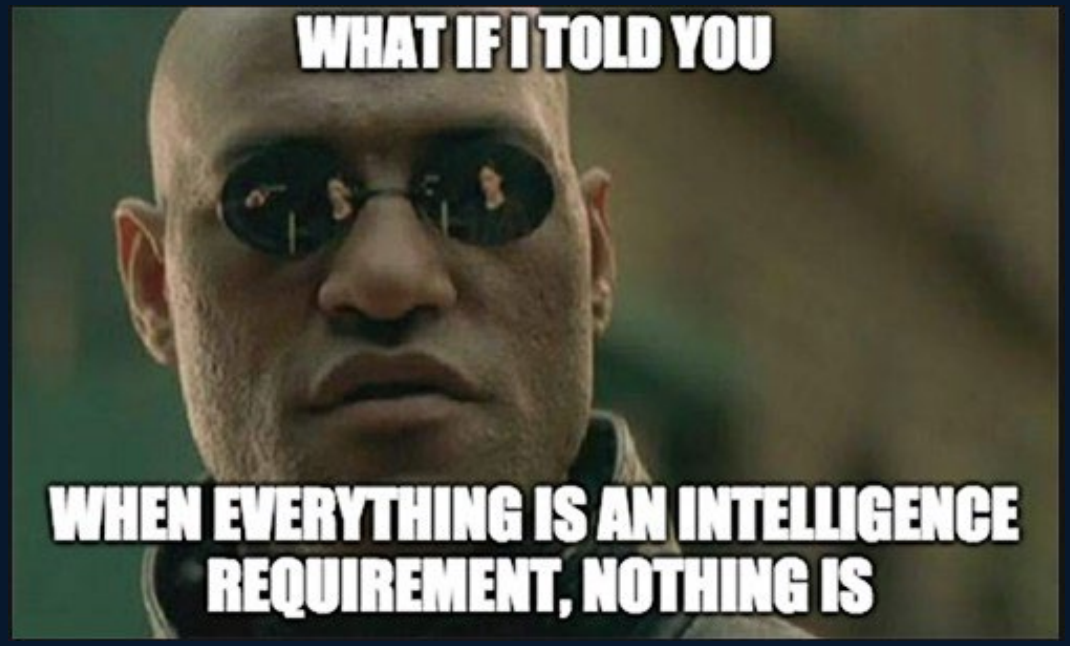
Source: http://maecproject.github.io

Malware Attribute Enumeration and Characterization (MAEC)

- Community-driven
- Catalogues malware attributes
  - Behaviour
  - Artifacts
  - Attack patterns
- Useful to malware researchers, IR teams and Cyber Threat Analysis

Use CTI to flip the script

Drowning in data, but starved for intel?



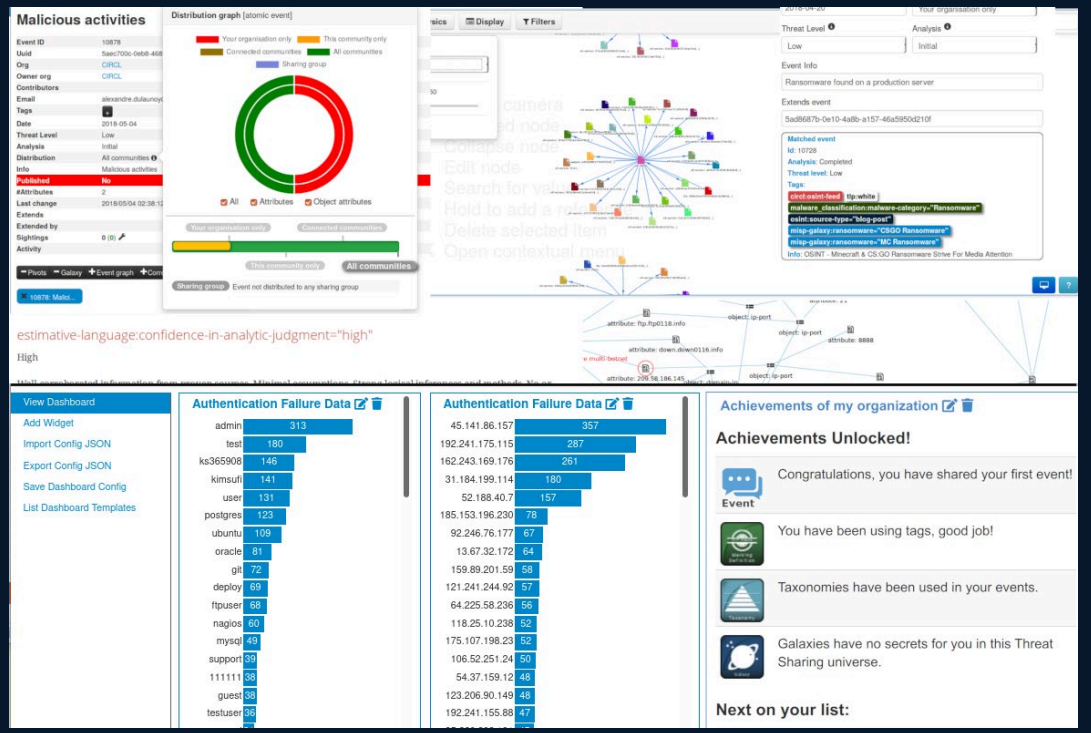
- Balance detection & protection/prevention – hard to defend what you cannot see!
- Start slow w/ 1 or 2 feeds - Weigh & continuously re-evaluate as you mature
- Add only as need is identified and the IR/TH activities can make use of it
- Use ATT&CK threat picture & Risk Management to tune needs and ID gaps
- Peer and learn from your human network – helps ID most impactful sources and methods
- Let the experts worry about attribution – focus on actionable intel!

Evolution of the Threat Intelligence Platform

- Most orgs started with a SIEM (Security Incident & Event Manager)
  - correlated all logs (bounded by $)
  - Internal context only – blind to global trending
  - Detached from response, offered little/no confidence rating or weighting
- Along came SOAR
  - Melded detections in SIEM with context-aware automated response
  - Started to see threat feeds, but erratic at best
  - Blended internal & external data- difficult to compare the two domains
- SIEM, SOAR and XDR can consume CTI, but wouldn't it be nice to curate it? → TIP was born!

What is a TIP?

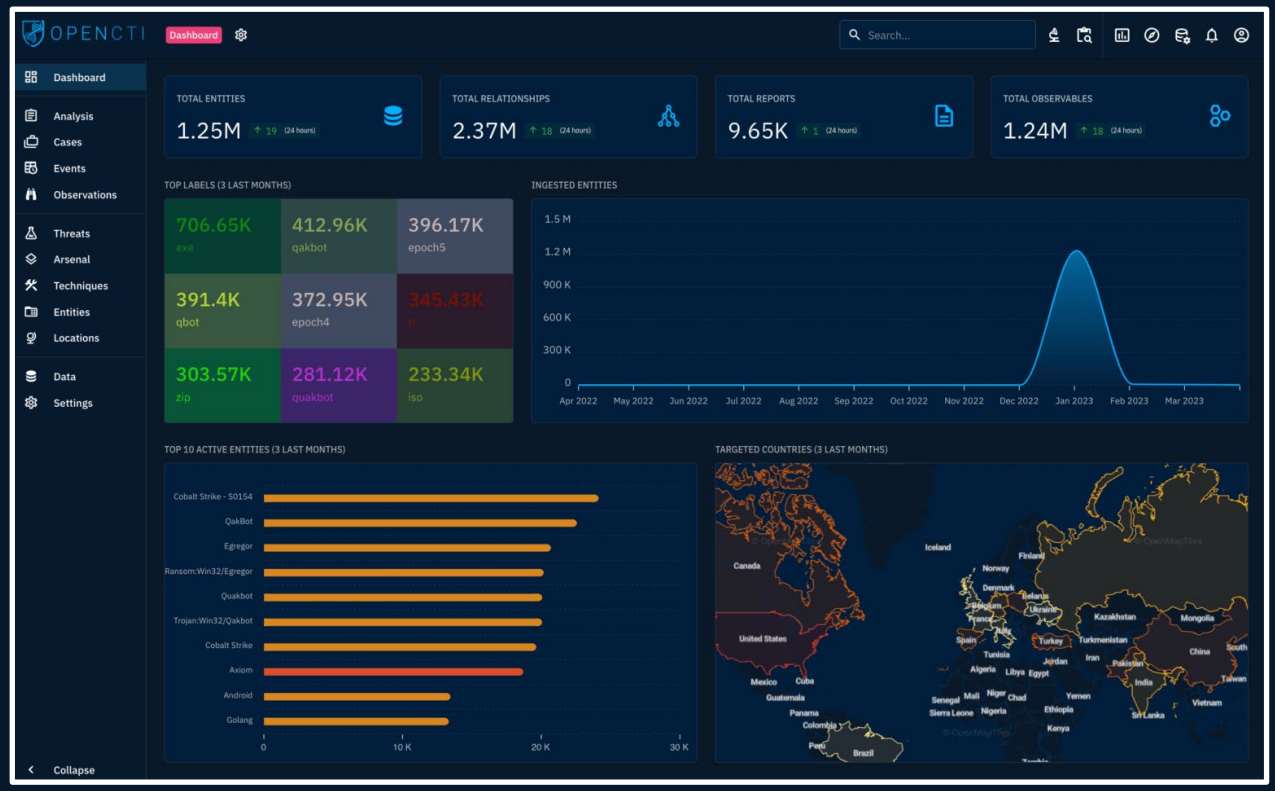
- TIPs process multiple CTI sources for:
  - Global context: identify trending TTPs, offer reputation
  - Internal context: posture, infrastructure capabilities, behavior, actions/responses
  - External + Internal: guidance to SecOps + enrichment for automation.
- TIP is emerging tech
  - Commercial and Open Source viable
  - Largely API driven
  - Integrates with SIEM/SOAR/XDR, GRC, Digital Risk Protection (DRP), and Ticketing systems.



Examples

- Threat Quotient
- ThreatConnect
- Seclytics (Augur)
- Recorded Future
- Intsights
- AlienVault
- Cisco Tools (partial but growing):
  - Cisco Threat Intelligence Director (CTID)
  - SecureX

- MISP (https://www.misp-project.org)
- OpenCTI (https://www.opencti.io/en/)
- Intel Owl (https://intelowlproject.github.io)



Strategies for Fusing and Using TI

Keep your Threat Picture up to date!

- Join associations & subscribe to relevant IOC feeds:
  - Join your (Information Sharing and Analysis Center) ISAC: https://www.nationalisacs.org/member-isacs-3
  - STIX/TAXXI feeds and API gateways to provide real-time updates
  - Leverages everyone else's sensors to inform defense
- Make use of free API-based tools for enrichment
  - Newer approach – STIX/TAXII still prevalent but API == more surgical use
  - Examples: AlienVault OTX feeds, VirusTotal, Spamhaus Project, Google Safe Browsing
  - Integrate with wherever you need enrichment (SIEM, TIP, XDR, FW –look for most likely place for fusion to occur)

Try a CTI Cycle out!

Most follow a 6-step process

1. Planning & Prerequisites – what do we (all) need to see?
2. Collection – how do we see it?
3. Processing – how can we make it useful?
4. Analysis – what does it mean?
5. Dissemination – who needs to know what?
6. Feedback – did it help? Was it worth it?

Great Write-up: https://www.splunk.com/en_us/blog/learn/what-is-cyber-threat-intelligence.html

Where else can we gather CTI?

- Use your vendors!
  - Cisco Talos and competitors offer threat feeds – much of the value of subscriptions
- Join associations & subscribe to relevant IOC feeds:
  - https://www.nationalisacs.org
  - Often include domains, IPs, hashes in STIX/TAXXI feeds/formats
  - Leverages everyone else's sensors to inform defense
- Make use of free API-based tools for enrichment
  - Newer approach – STIX/TAXII still prevalent but API offers more surgical use
  - AlienVault OTX feeds, VirusTotal, Spamhaus Project, Google Safe Browsing
  - Integrate with wherever you need enrichment (SIEM, TIP, XDR, FW –look for most likely place for fusion to occur)

Drowning in data, but starved for intel?

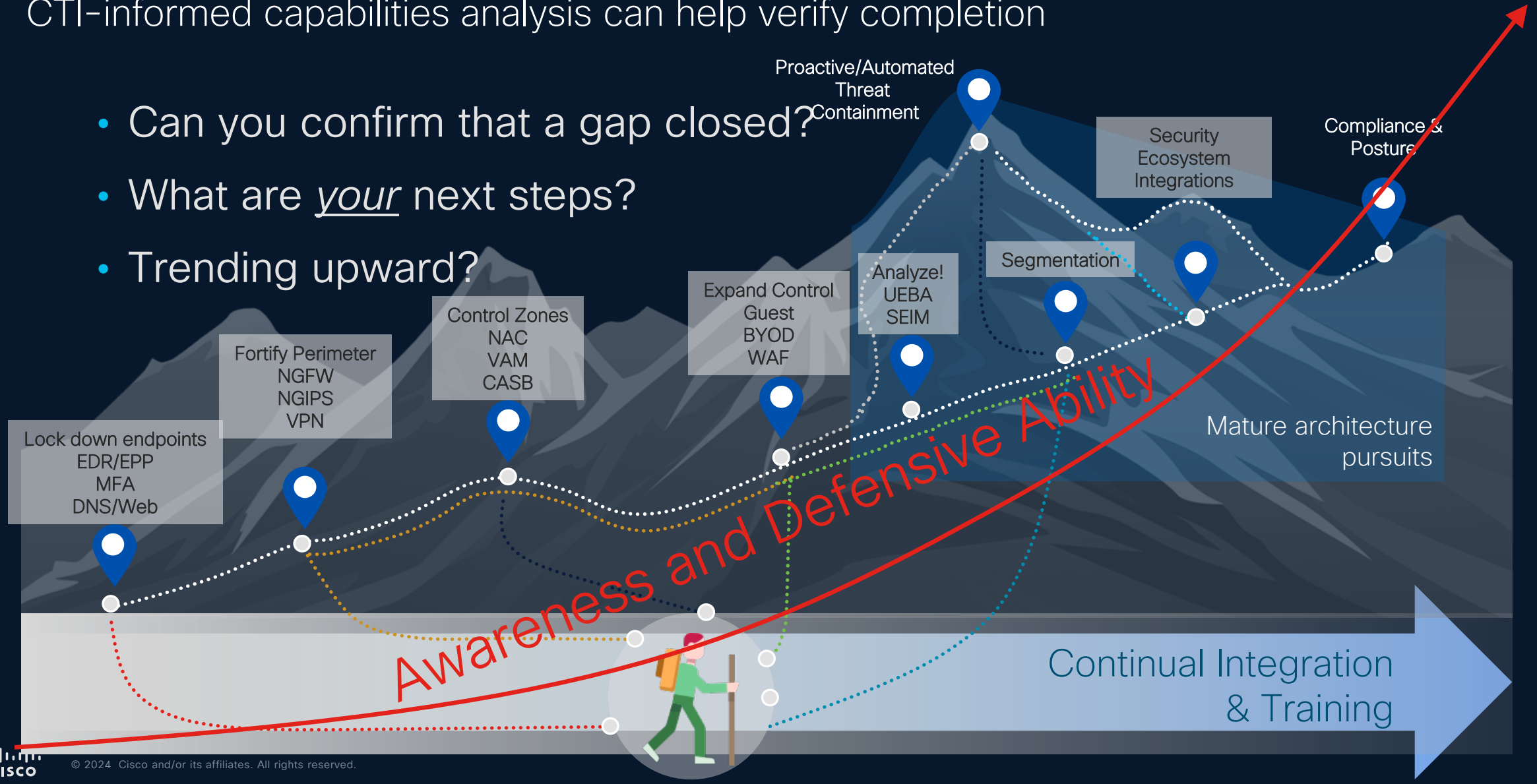
- Take it slow and start with 1 or 2 feeds
- Add only as value is identified and the IR/TH activities can make use of it
- Weigh and continuously re-evaluate as you mature
- Use ATT&CK threat picture and Risk Management process to help tune needs and ID gaps
- Peer and learn from your network – helps ID most impactful sources and methods
- Let the experts worry about attribution – focus on actionable intel!

Conclusion

Security maturity is a journey

CTI-informed capabilities analysis can help verify completion

- Can you confirm that a gap closed?
- What are *your* next steps?
- Trending upward?



Next steps for ATT&CK-ing your foes

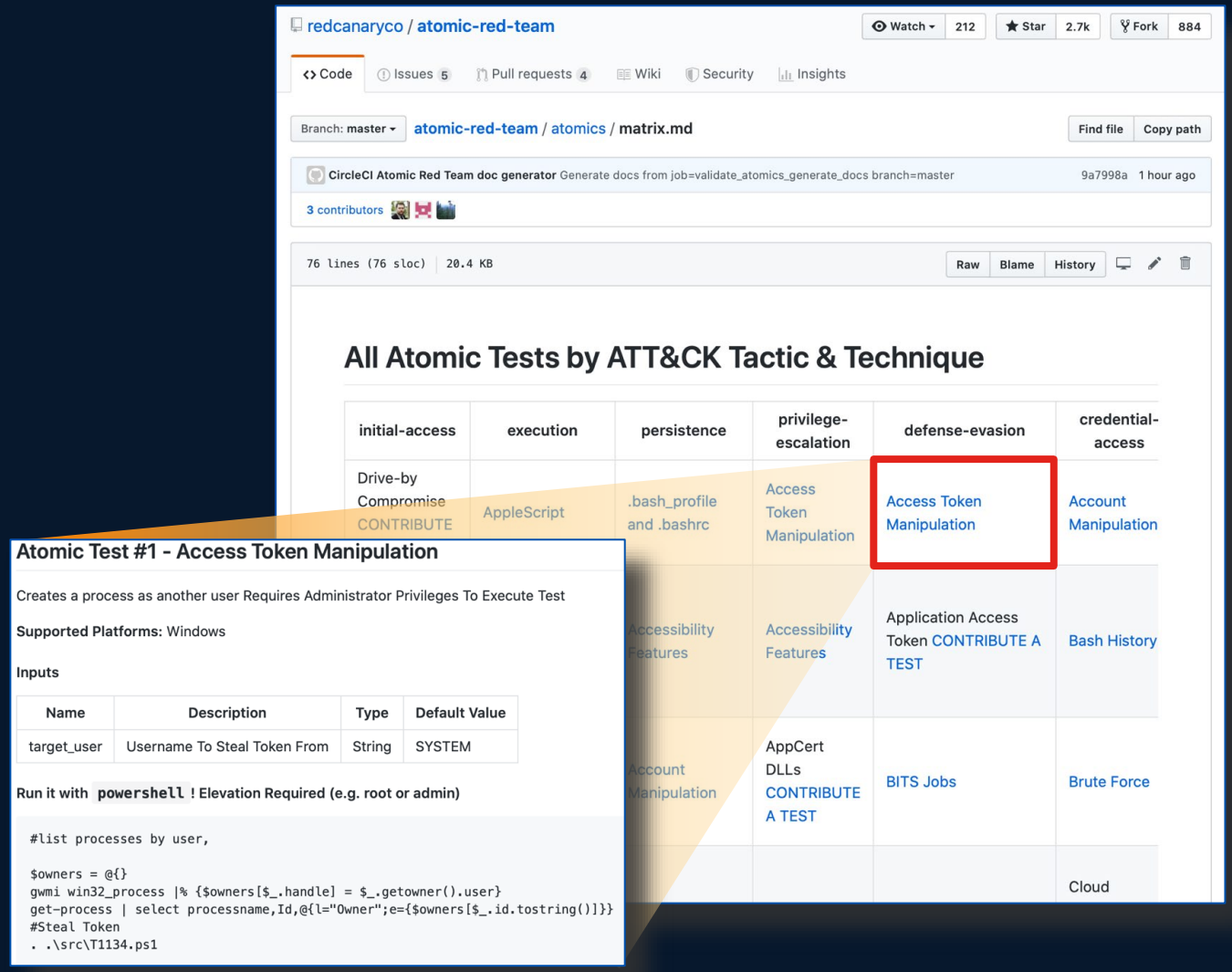
Collect and parse logs and pull data

- Grab your SIEM, XDR, or TIP and integrate!
- Infrastructure logging is good, but Sysmon (Windows) & Syslog (others) essential for internal context:
  - Help building secure Windows environment - Detection Lab: https://github.com/clong/DetectionLab
  - Starter Sysmon file by SwiftOnSecurity: https://github.com/SwiftOnSecurity/sysmon-config
- Apply automated logging parsers and scripts for ATT&CK-based detection
  - Event Query Language (EQL): https://eqllib.readthedocs.io/en/latest/analytics.html
  - Sigma: https://github.com/Neo23x0/sigma
- Implement in stages
  - Pick a detection, focus, type and start there, expand with success
  - Don’t try to ”boil the ocean”

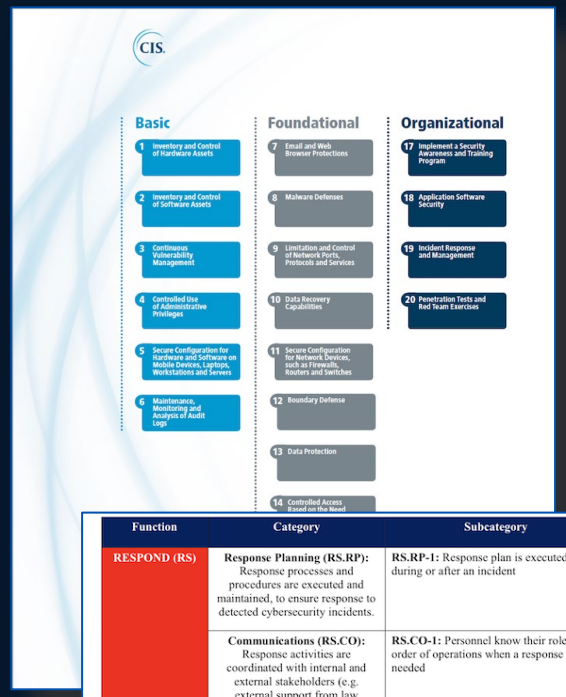
Next steps for ATT&CK-ing your foes

Use guides like Atomic Red Team or Caldera to simulate attacks & verify your coverage

- Open-source tests by Red Canary
  - https://atomicredteam.io/testing
- Emulate using the MITRE CALDERA project:
  - https://github.com/mitre/caldera
  - Check out my demo video using Caldera here: https://youtu.be/wXLwPWHdBLU



Other tools can assist in structuring your CTI process, gap analysis, etc.



Function	Category	Subcategory	Informative References
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	**RS.RP-1:** Response plan is executed during or after an incident	**CIS CSC** 19 **COBIT 5** APO12.06, BAI01.10 **ISA 62443-2-1:2009** 4.3.4.5.1 **ISO/IEC 27001:2013** A.16.1.5 **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	**CIS CSC** 19 **COBIT 5** EDM03.02, APO01.02, APO12.03 **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, A.16.1.1 **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8
		RS.CO-2: Incidents are reported consistent with established criteria	**CIS CSC** 19 **COBIT 5** DSS01.03 **ISA 62443-2-1:2009** 4.3.4.5.5 **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8
		RS.CO-3: Information is shared consistent with response plans	**CIS CSC** 19 **COBIT 5** DSS03.04 **ISA 62443-2-1:2009** 4.3.4.5.2 **ISO/IEC 27001:2013** A.16.1.2, Clause 7.4, Clause 16.1.2 **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	**CIS CSC** 19 **COBIT 5** DSS03.04

- CIS Controls:
  - Threat-focused guidance we should ALL heed
  - https://www.cisecurity.org/controls/

- NIST Cybersecurity Framework:
  - Outcome-focused framework based on stakeholders, functions, and resources
  - https://www.nist.gov/cyberframework

So what have we learned?

- ATT&CK can help us assess our threat picture and coverage gaps!
  - TTPs provide insight into adversarial behavior == know thy enemy!
- OUR threat picture can help focus CTI efforts and security strategies
  - Helps identity high ROI investments (people, process, technology)
  - Collecting a little of the right intel beats drowning in too much of the wrong data
- Whether using a SIEM, XDR, or dedicated TIP, CTI can quickly enhance your security efficacy
- Open-Source efforts from MITRE and others can help you test those defenses or learn about the adversaries
  - MITRE Caldera project as an automated framework
  - Atomic Red Team offering the tests we invoked in Caldera

What next? Baby steps!

Build the habit – a little better every day is worth it

- Iterate
  - Repeat cycle and track improvement
  - Add APTs/threats as time permits
  - Continually test to validate progress
- Leverage tools that better support the SOC and engineering together!
- Educate and communicate across functions with Risk and ATT&CK
- Compel your partners and vendors to do the same

Additional ATT&CK-related resources

Blogs & References

- MITRE's own ATT&CK materials are hard to beat: https://attack.mitre.org
- Getting Started Guide – useful for all 4 use cases: https://attack.mitre.org/resources/getting-started/
- Best blog on Medium: https://medium.com/mitre-attack/
- Pyramid of Pain: https://globalsecuresolutions.com/the-pyramid-of-pain/
- Orbital for ATT&CK: https://blogs.cisco.com/security/finding-the-malicious-needle-in-your-endpoint-haystacks
- Threat Grid use of ATT&CK TTPs in reports: https://blogs.cisco.com/security/black-hat-usa-2018-attck-in-the-noc
- MITRE ATT&CK Ecosystem Rosetta Stone: https://github.com/mjmcphee/attack-rosetta
- Demoed APTs and coverage matrices for this session: https://github.com/mjmcphee/clapjc24_attack

Additional ATT&CK-related resources

Complimentary MITRE efforts

- Center for Threat-Informed Defense (CTID): group in MITRE Engenuity, leads ATT&CK, D3FEND, and related
  - https://ctid.mitre-engenuity.org
- D3FEND: counter ATT&CKs TTPs by detailing how one can harden, detect, isolate, deceive, or evict the threat
  - https://d3fend.mitre.org
- Cyber Analytics Repository (CAR): validated analytical recipes for tools like Splunk, Elastic, etc. help detect TTPs in use
  - https://car.mitre.org/
- ATT&CK Flow – a tool to assist in linking TTPs into an adversary's behavior (alchemy ;))
  - https://center-for-threat-informed-defense.github.io/attack-flow/
- ATT&CK Powered Suit: Browser plugin to link and research TTPs
  - https://mitre-engenuity.org/cybersecurity/center-for-threat-informed-defense/attack-powered-suit/
- Common Attack Pattern Enumeration and Classification (CAPEC): Like ATT&CK, but focused on applications
  - https://capec.mitre.org/

Additional ATT&CK-related resources

Software tools

- MITRE Caldera: provides a browser-driven automated emulation platform to test against ATT&CK TTPs for endpoints (Linux, Mac, Windows)
  - Main project website: https://caldera.mitre.org/
  - Awesome tutorial by Mohammed Alshaboti : https://medium.com/@alshaboti/getting-started-with-mitre-caldera-offensive-and-defensive-training-3ca9f693e0d7
- MITRE's ATT&CK Workbench: allows orgs to maintain a local repo of their own ATT&CK data and keep it in synch with global feeds
  - https://ctid.mitre-engenuity.org/our-work/attack-workbench/
- Red Canary's Atomic Red Team: https://atomicredteam.io
- D3TTECT: https://github.com/rabobank-cdc/DeTTECT/wiki

Additional CTI-related resources

Blogs & References

- CIS Critical Security Controls, OS Benchmarks & Hardened Images a fantastic resource: https://www.cisecurity.org/cybersecurity-tools/
- OWASP Secure Software Development Lifecycle Project: https://www.owasp.org/index.php/OWASP_Secure_Software_Development_Lifecycle_Project
- UK National Cyber Security Centre: https://www.ncsc.gov.uk/section/advice-guidance/all-topics
- NIST Cybersecurity Framework: https://www.nist.gov/cyberframework
- US-CERT Resources: https://www.us-cert.gov/resources
- CREST Resource page: https://www.crest-approved.org/knowledge-sharing/index.html
- SANS Cyber Defense Reading Room: https://cyber-defense.sans.org/resources/whitepapers


CISCO


CISCO