Creating a Risk Managed and Threat-Informed Cyber Defense Strategy

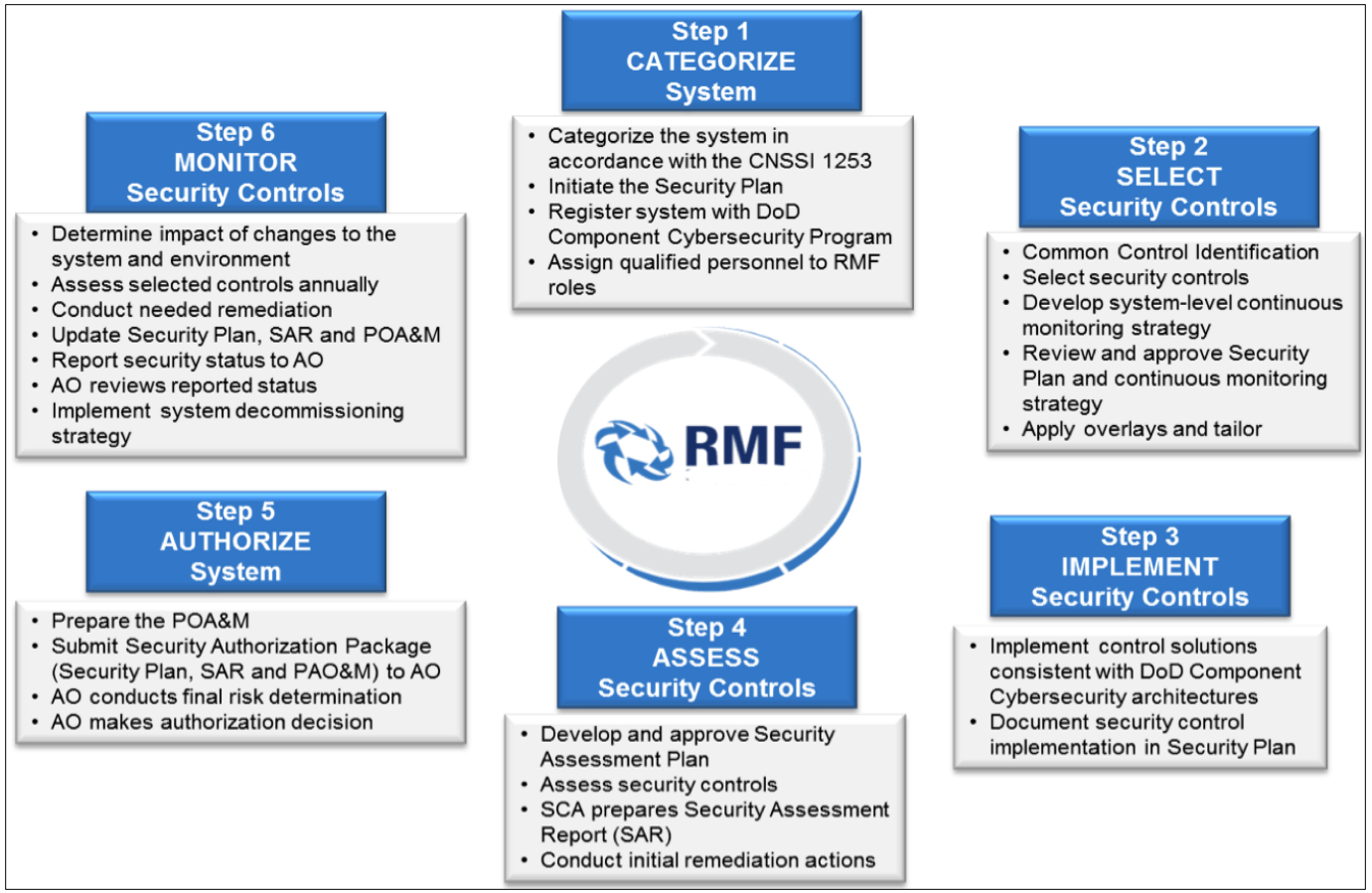
Micah VanFossen

Definitions

- **Risk Management** - The process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level
- **Risk Management Framework (RMF)** - A U.S. government framework designed to secure federal systems and manage the associated risks
- **Threat-Informed Defense (TID)** – Applying a deep understanding of adversary tradecraft and technology to protect against, detect, and mitigate cyber-attacks
- **Center for Threat-Informed Defense (CTID)** – A non-profit, privately funded research and development organization operated by MITRE Engenuity. Their goal is "to advance the state of the art and the state of the practice in threat-informed defense globally"
- **Adversary Emulation** - A type of red team engagement that models a known threat campaign to an organization by using threat intelligence to define what actions and behaviors the red team uses. Adversary emulators construct a scenario to test certain aspects of an adversary's TTPs
- **Security Controls** - A safeguard or countermeasure for an information system or organization designed to protect the confidentiality, integrity, and availability of its information and meet defined security requirements
- **Advanced Persistent Threat (APT)** - A well-funded and skilled group that is capable of gaining unauthorized access to systems and remaining undetected for extended amounts of time

Risk Management Framework

- Developed by National Institute of Standards and Technology (800-37)
- United States federal government policy and standards to help secure information systems and DoD data
- 6 step lifecycle used to assess, authorize, and maintain accreditation for DoD systems (IS, IoT, OT/ICS, etc.)
- Integrates information security and risk management activities into system development, procurement, deployment, maintenance, and decommissioning
- Utilizes NIST 800-53 security controls



MITRE ATT&CK

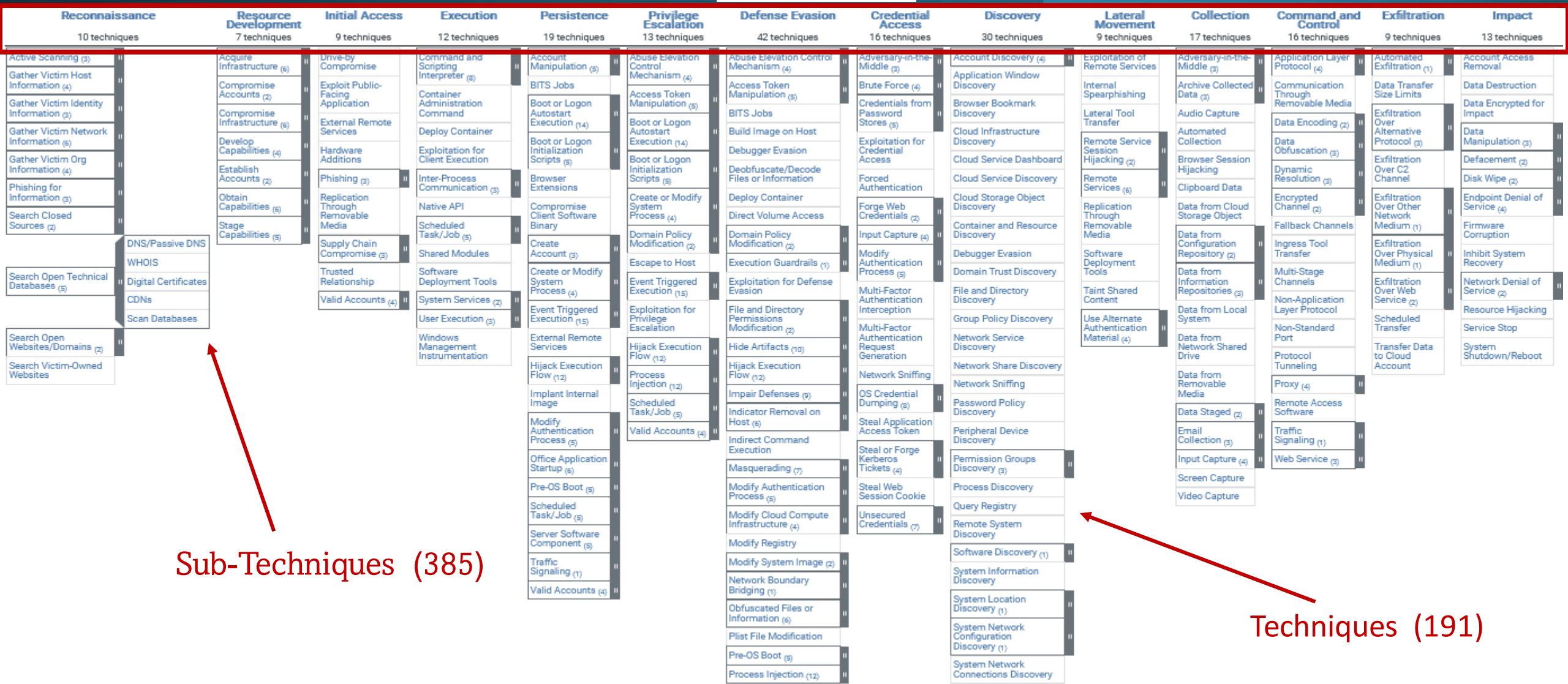
- A “knowledge base that outlines the real-world tactics and techniques used by cyber adversaries to help organizations across industries better understand threats and protect their critical systems” [1]
- Standardized threat behavior and offers information regarding specific APT groups, software/malware variants, the path of cyber attack kill chains, and much more
- ATT&CK framework currently supports matrices for Enterprise, ICS, and Mobile systems
- Consists of Tactics, Techniques, and Procedures (Sub-Techniques) - “TTPs”

TTPs

- Tactics - The technical goals of an adversary
  - Why?
    - Examples: Reconnaissance, Initial Access, and Privilege Escalation
- Techniques - How those goals are achieved
  - How?
    - Examples: Phishing for Information (T1598), Scheduled Task/Job (T1053), and Data Encoding (T1132)
- Sub-Techniques (Procedures) - *Mostly* specific implementations of a technique
  - What?
    - Examples: Spear phishing link (T1598.003) and SSH (T1021.004)

ATT&CK Enterprise Matrix

Tactics (14)



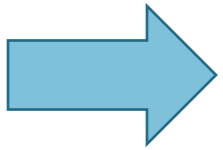
Sub-Techniques (385)

Techniques (191)

The Goal

Reactive/Compliance Driven

- Does only what is required and checks the boxes
- Attempts to protect against every threat (an unrealistic goal)
- Unsure if defenses will actually prevent attacks, and if they do, which attacks
- Focused on responding to incidents and preventing repeat attacks
- Defends against attacks that have already happened
- Stagnant and out of date



Risk & Threat-Informed

- Knows the org's threat profile and how to close gaps
- Implements controls that defend against known threats
- Achieves compliance with validated security against known threats
- Better overall security posture and effectiveness in stopping attacks
- Locates issues and reduces impacts *prior* to an attack
- Focused on prevention of attacks
- Moves with the pace of threats

Benefits of TID

- Threat-informed defense positions security goals and requirements with top risks and threats faced by an organization
- TID helps answer the questions:
  - What are adversaries doing?
  - How are they operating?
  - Can we detect them?
  - Can we stay one step ahead?
- To answer these questions, an organization needs:
  - Clear visibility into the effectiveness of their security controls
  - Knowledge of adversaries and attack methods
  - The ability to test defenses and take proactive action to any identified weaknesses in processes and tools

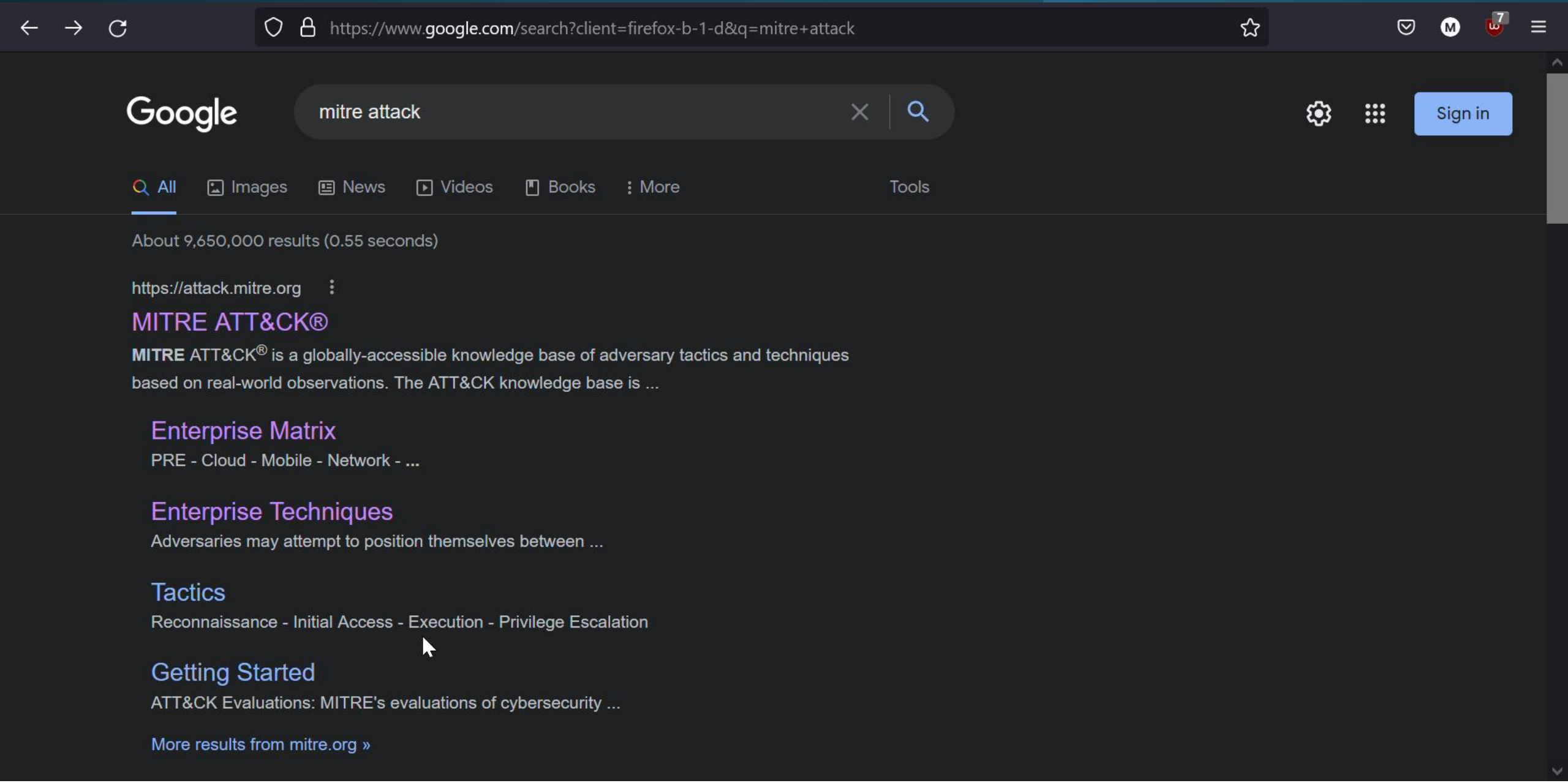
Free Tools

- The tools that will be covered briefly:
  1) ATT&CK Navigator
     - menuPass (APT 10) demo
  2) NIST 800-53 ATT&CK Navigator mapping layer
     - Review demo
  3) Top ATT&CK Techniques Calculator
     - Calculation demo
  4) CALDERA
     - Nothing, way too much involved, perform research on BAS tools

ATT&CK Navigator

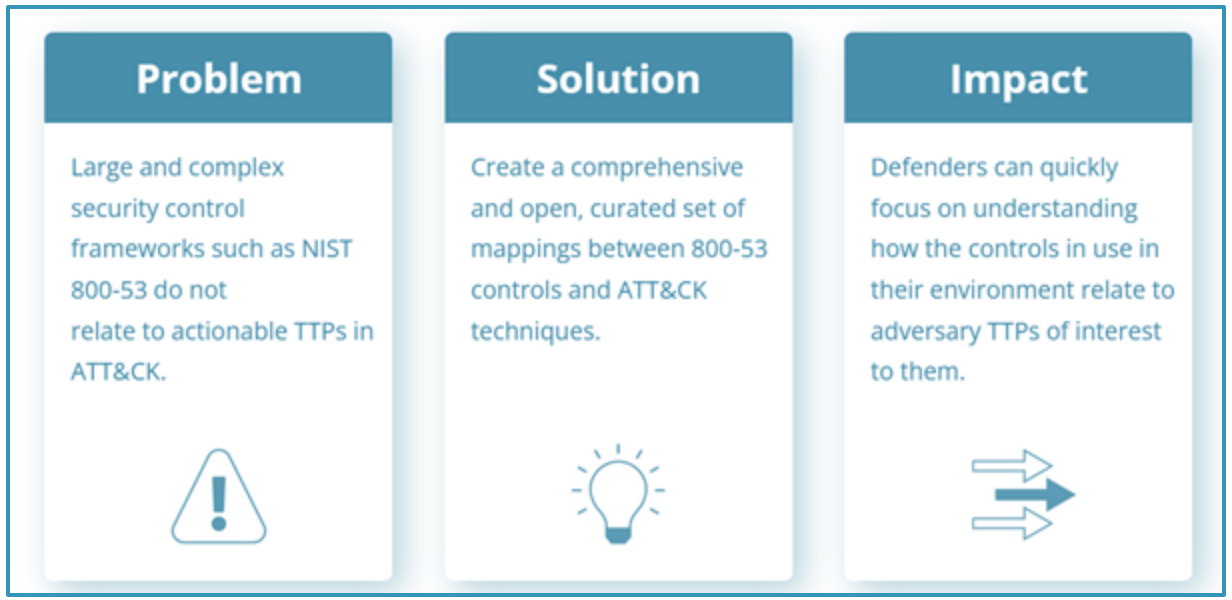
- Interactive web-based chart that allows for navigation and annotation of ATT&CK matrices
- Customize Navigator layers and utilize ones that have been created by others
- Provides ability to create heat maps, perform TTP identification, document the flow of a cyber-attack, etc.
  - Color coding, comments, assigning numerical values, identifying TTPs by APT, exporting results to Excel, and more
- Attack Navigator: https://mitre-attack.github.io/attack-navigator/

menuPass Demo



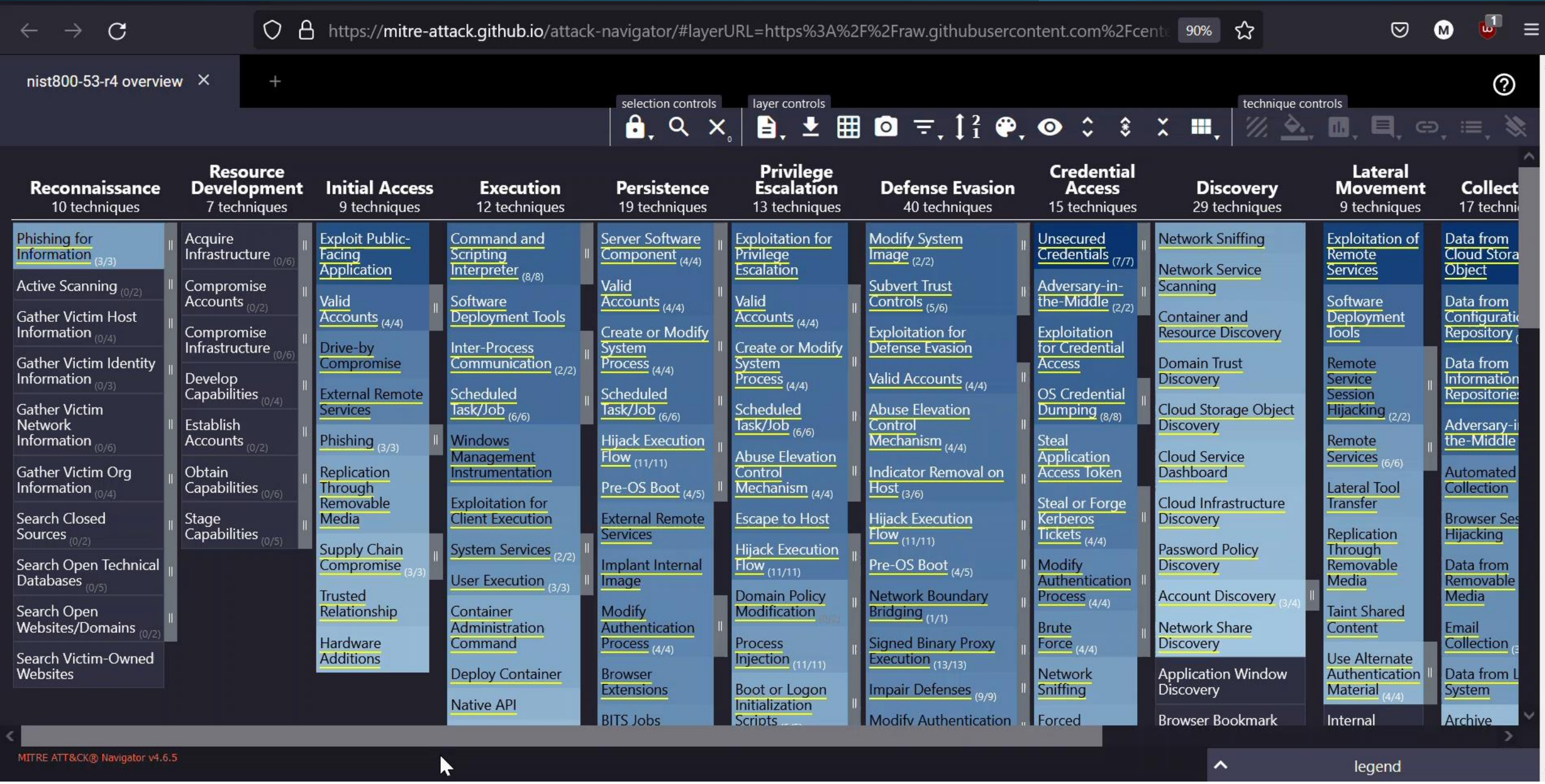
Navigator NIST 800-53 Mapping

- Difficult to identify overlap between security controls and actionable TTPs / threat group behaviors found in ATT&CK [2]
- CTID asked the question "how do we integrate the two?"



Control Family	Mapped?
AC - Access Control	Yes
AT - Awareness and Training	No
AU - Audit and Accountability	No
CA - Security Assessment and Authorization	Yes
CM - Configuration Management	Yes
CP - Contingency Planning	Yes
IA - Identification and Authentication	Yes
IR - Incident Response	No
MA – Maintenance	No
MP - Media Protection	Yes
PE - Physical and Environmental Protection	No
PL – Planning	No
PM - Program Management	No
PS - Personnel Security	No
RA - Risk Assessment	Yes
SA - System and Services Acquisition	Yes
SC - System and Communications Protection	Yes
SI - System and Information Integrity	Yes

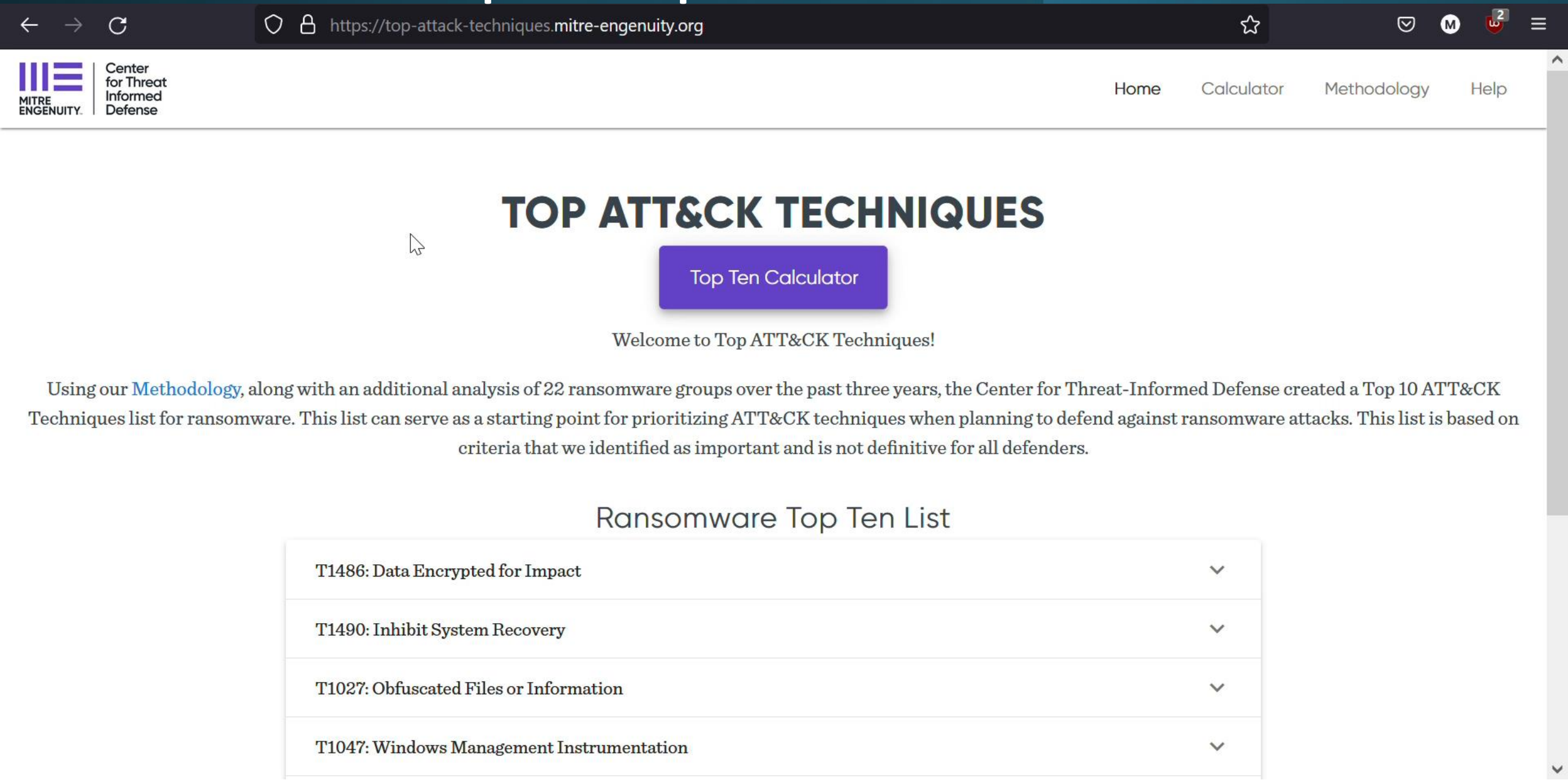
800-53 Navigator Layer Demo



Top Techniques Calculator

- Input data on current defenses and system environments, and then calculate an individualized listing of the top 10 techniques to address and focus on
- Calculation methodology is based on three components:
  - **Actionability**: The opportunity for a defender to detect or mitigate against each ATT&CK technique based on publicly available analytics and security controls
  - **Choke Point**: A specific technique where many other techniques converge or diverge, and where eliminating that specific technique would cause disruption to an adversary. One example is Process Injection (T1055). If T1055 is prevented from running and detected properly, an adversary would be unable to successfully evade detection or elevate privileges by injecting code into legitimate processes
  - **Prevalence**: The frequency of which an attacker uses a specific ATT&CK technique over a period of time
- Top techniques Calculator: https://top-attack-techniques.mitre-engenuity.org/calculator
  - Available as a web app or Excel file

Top Techniques Calculator Demo

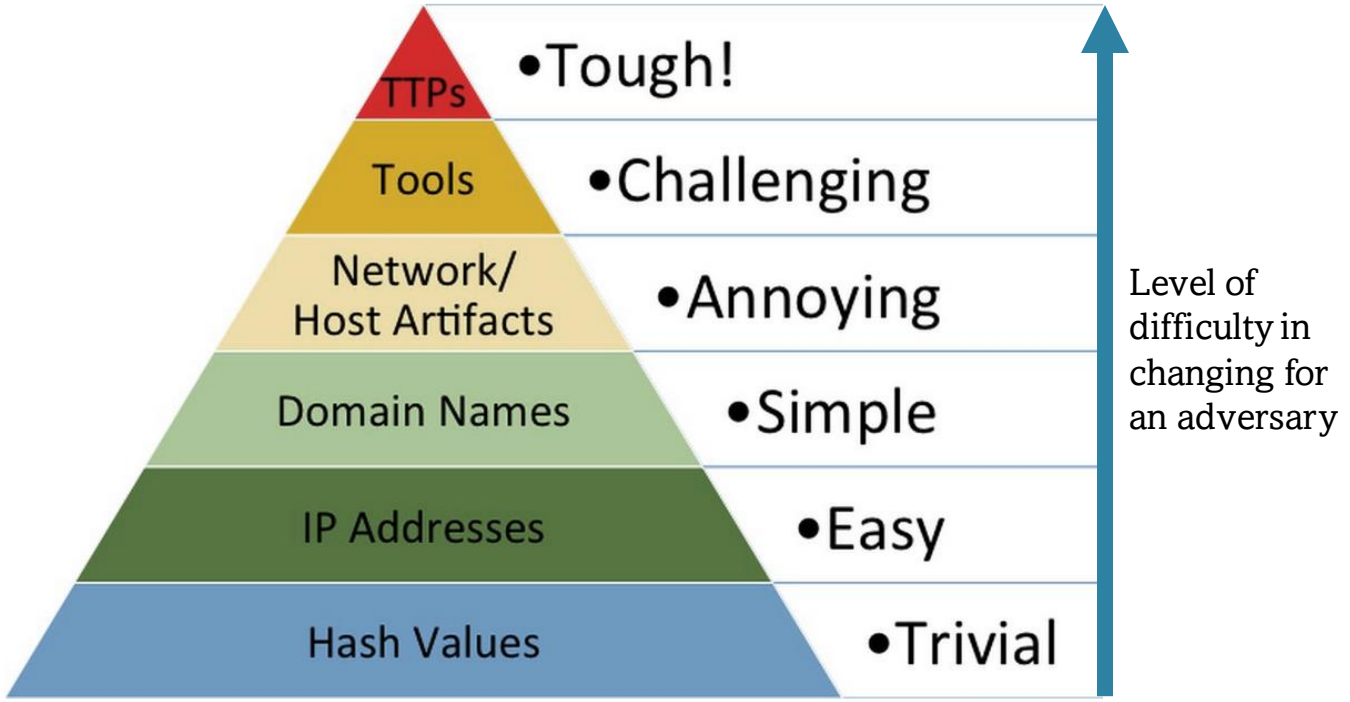


CALDERA

- *Adversary emulation:* the use of automated security assessments to validate that security controls are working as intended
  - Controls are worthless if they have not been tested against the actual attacks that they are supposed to protect from
- Goal: to save time and money by automating a cyber-attack in your environment
- "CALDERA leverages the ATT&CK model to identify and replicate adversary behaviors as if a real intrusion is occurring. This enables automated assessments of a network's susceptibility to adversary success, allowing organizations to see their networks through the eyes of an advanced persistent threat on-demand and to verify defenses and security configuration based upon known threat techniques." [3]
- Organizations can customize attacks or run through pre-created attack plans (menuPass plan)
- MITRE CALDERA: https://caldera.mitre.org/

Pyramid of Pain

- Many intrusion detection tools search for known threat indicators which change frequently, this leaves defenders guessing on response to active threats
- Shift from only the detection of static IOCs to the ability to detect and respond to adversary behaviors (TTPs), regardless of IP or hash
- When TTP patterns and actions are disrupted, threat actors have a much harder time continuing as normal, they must create entire new attack types, not just rename a file or change an IP



David J Bianco

Where to Start?

- 1st) Receive upper management support
  - This process will require culture and process changes, it needs to be supported from the top
- 2nd) Identify a team or individual to manage TID across the organization
  - This team needs to be given authority to make changes where necessary and shift the processes and tools that need to go or be changed
- 3rd) When working with RMF, incorporating threat knowledge should begin at step 2 (Select Controls) and continue throughout the life cycle of the system
  - When selecting controls, the organization should aim for controls to address both compliance requirements and adversary behavior
  - However, as adversaries change, so should defenses and controls, maintaining up-to-date knowledge is integral to a threat-informed cyber defense

Questions to Ask

- What threat actors commonly target my industry?
- What techniques are used by these groups?
- What controls do we currently have in place?
- What controls are we confident in and which ones are we less certain of their effectiveness?
- What are our crown jewels (business critical functions, information, and systems) that we must protect?

When RM and TID are combined

- When these two approaches are combined and used in conjunction, an organization can create a proactive, holistic, cyber defense strategy that:
    1. Knows the relevant risks and threats facing the organization
    2. Identifies what has been done to reduce risk and mitigate known threat actor behavior
    3. Verifies proper control implementation and coverage
    4. Maintains effective compliance and resiliency
    5. Can detect and protect against real-life attacks
    6. Puts the power back into the hands of the defenders

Summary

- Organizations need to personalize their defenses, the “stop everything” approach to cybersecurity is ineffective and leads to ad hoc defensive practices that only stop attacks that have already happened
- An organization that knows their defenses and knows their adversaries is much more likely to defend effectively against attacks
- The goal of a risk managed and threat-informed cyber defense strategy is to move from a compliance-driven approach that unrealistically attempts to defend against every threat + static IOCs, to an approach that knows specific adversaries and their TTPs/behaviors, and can prevent attacks by implementing and validating controls against those TTPs
- The NIST 800-53 Navigator layer, Top Techniques Calculator, and MITRE CALDERA tools assist with integrating MITRE ATT&CK and TID into RMF or other risk management frameworks

Resources and Helpful Links

- Links to the information and resources described earlier:
  - MITRE ATT&CK homepage: https://attack.mitre.org/
  - ATT&CK Navigator: https://mitre-attack.github.io/attack-navigator/
  - Top 10 Techniques Calculator: https://top-attack-techniques.mitre-engenuity.org/calculator
  - NIST 800-53 Mapping: https://ctid.mitre-engenuity.org/our-work/nist-800-53-control-mappings/
  - MITRE CALDERA: https://caldera.mitre.org/ and https://caldera.readthedocs.io/en/latest/
  - CALDERA Pathfinder (Adversary Emulation): https://github.com/mitre/caldera
  - Integrated vulnerability scanner with the CALDERA automated adversary emulation platform: https://github.com/center-for-threat-informed-defense/caldera_pathfinder
  - CALDERA Product Page: https://www.mitre.org/research/technology-transfer/open-source-software/caldera%E2%84%A2
  - menuPass Caldera profile: https://github.com/center-for-threat-informed-defense/adversary_emulation_library/blob/master/menuPass/Emulation_Plan/Scenario1.md
  - Azure, AWS, and GCP mappings: https://center-for-threat-informed-defense.github.io/security-stack-mappings/Azure/README.html and here https://github.com/center-for-threat-informed-defense/security-stack-mappings

References

- [1]: https://www.mitre.org/news/focal-points/threat-informed-defense
- [2]: https://mitre-attack.github.io/attack-navigator/#layerURL=https%3A%2F%2Fraw.githubusercontent.com%2Fcenter-for-threat-informed-defense%2Fattack-control-framework-mappings%2Fv1.5.0%2Fframeworks%2FATT%2526CK-v10.1%2Fnist800-53-r4%2Flayers%2Fnist800-53-r4-overview.json
- [3]: https://www.mitre.org/research/technology-transfer/open-source-software/caldera%E2%84%A2

GitHub (micahvan) – these slides will be shared in *Presentations* repository