Creating a Risk Managed and Threat-Informed Cyber Defense Strategy

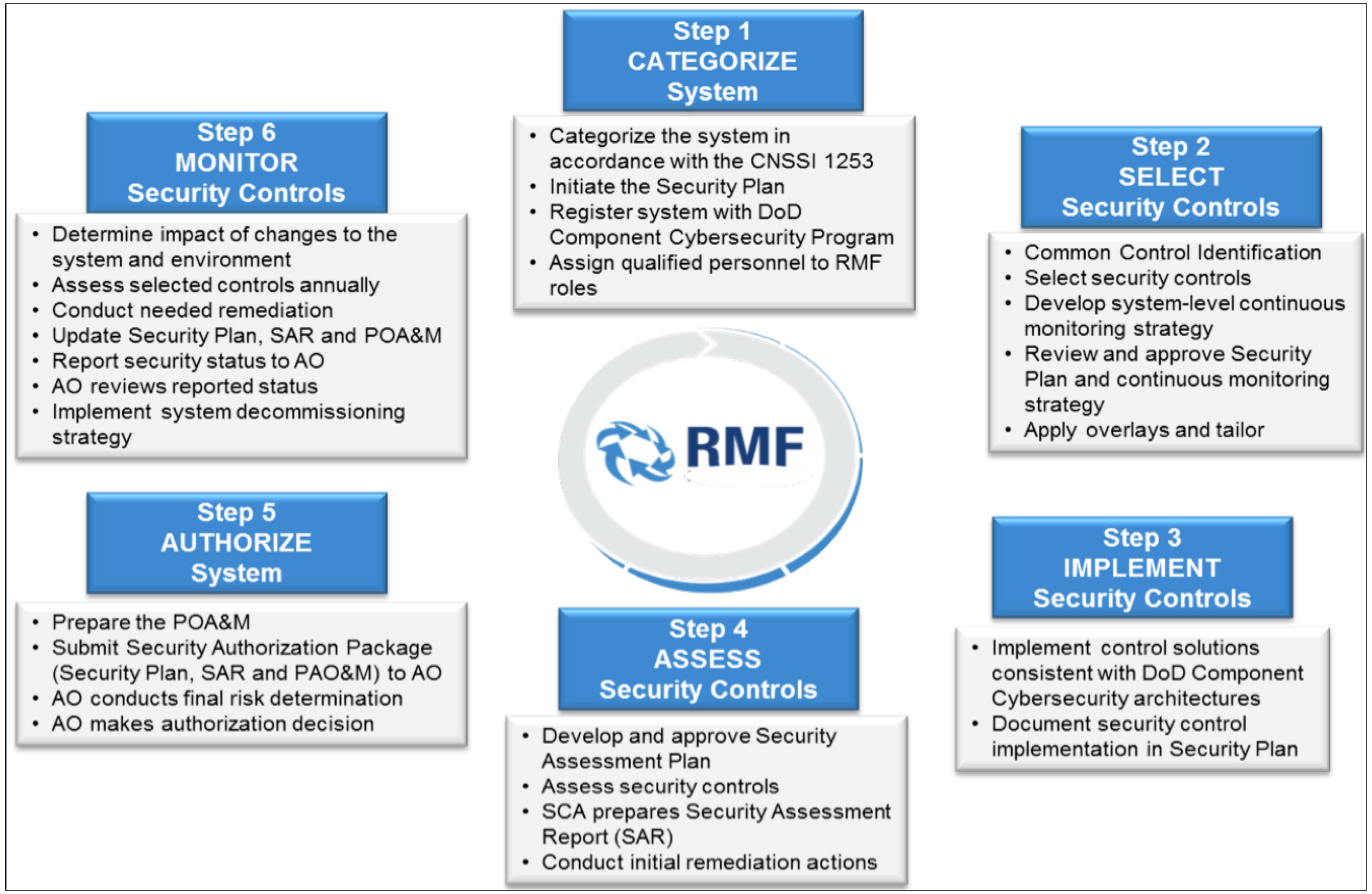
Micah VanFossen

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



Step 1 CATEGORIZE System

- Categorize the system in accordance with the CNSSI 1253
- Initiate the Security Plan
- Register system with DoD Component Cybersecurity Program
- Assign qualified personnel to RMF roles

Step 2 SELECT Security Controls

- Common Control Identification
- Select security controls
- Develop system-level continuous monitoring strategy
- Review and approve Security Plan and continuous monitoring strategy
- Apply overlays and tailor

Step 3 IMPLEMENT Security Controls

- Implement control solutions consistent with DoD Component Cybersecurity architectures
- Document security control implementation in Security Plan

Step 4 ASSESS Security Controls

- Develop and approve Security Assessment Plan
- Assess security controls
- SCA prepares Security Assessment Report (SAR)
- Conduct initial remediation actions

Step 5 AUTHORIZE System

- Prepare the POA&M
- Submit Security Authorization Package (Security Plan, SAR and PAO&M) to AO
- AO conducts final risk determination
- AO makes authorization decision

Step 6 MONITOR Security Controls

- Determine impact of changes to the system and environment
- Assess selected controls annually
- Conduct needed remediation
- Update Security Plan, SAR and POA&M
- Report security status to AO
- AO reviews reported status
- Implement system decommissioning strategy

MITRE ATT&CK

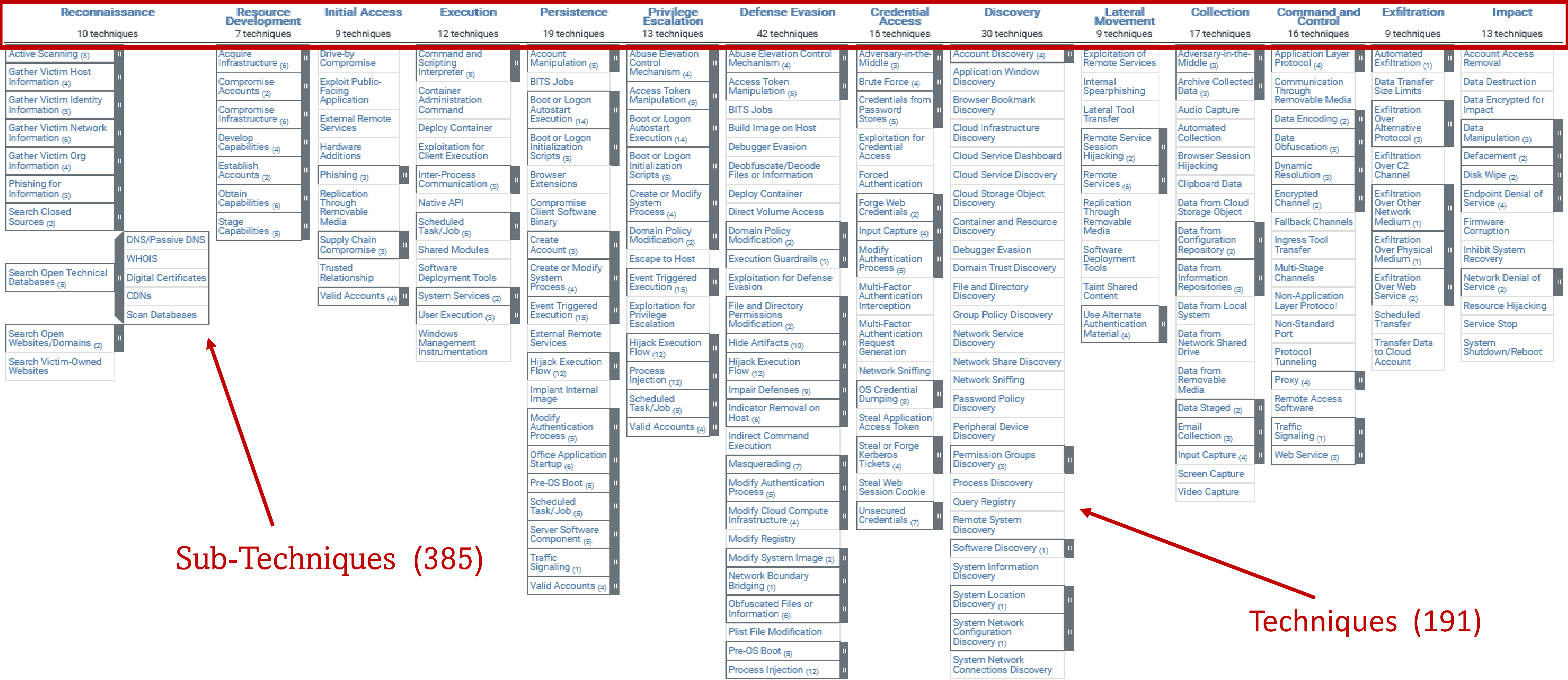
- ATT&CK - Adversarial Tactics, Techniques, and Common Knowledge
  - A “knowledge base that outlines the real-world tactics and techniques used by cyber adversaries to help organizations across industries better understand threats and protect their critical systems” [1]
- Standardized threat behavior 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)



Reconnaissance
10 techniques
- Active Scanning (3)
- Gather Victim Host Information (4)
- Gather Victim Identity Information (3)
- Gather Victim Network Information (6)
- Gather Victim Org Information (4)
- Phishing for Information (3)
- Search Closed Sources (2)
- Search Open Technical Databases (5)
  - DNS/Passive DNS
  - WHOIS
  - Digital Certificates
  - CDNs
  - Scan Databases
- Search Open Websites/Domains (2)
- Search Victim-Owned Websites

Resource Development
7 techniques
- Acquire Infrastructure (6)
- Compromise Accounts (2)
- Compromise Infrastructure (6)
- Develop Capabilities (4)
- Establish Accounts (2)
- Obtain Capabilities (6)
- Stage Capabilities (5)

Initial Access
9 techniques
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (3)
- Replication Through Removable Media
- Supply Chain Compromise (3)
- Trusted Relationship
- Valid Accounts (4)

Execution
12 techniques
- Command and Scripting Interpreter (8)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (3)
- Native API
- Scheduled Task/Job (5)
- Shared Modules
- Software Deployment Tools
- System Services (2)
- User Execution (3)
- Windows Management Instrumentation

Persistence
19 techniques
- Account Manipulation (5)
- BITS Jobs
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (3)
- Create or Modify System Process (4)
- Event Triggered Execution (15)
- External Remote Services
- Hijack Execution Flow (12)
- Implant Internal Image
- Modify Authentication Process (5)
- Office Application Startup (6)
- Pre-OS Boot (5)
- Scheduled Task/Job (5)
- Server Software Component (5)
- Traffic Signaling (1)
- Valid Accounts (4)

Privilege Escalation
13 techniques
- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Create or Modify System Process (4)
- Domain Policy Modification (2)
- Escape to Host
- Event Triggered Execution (15)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (12)
- Process Injection (12)
- Scheduled Task/Job (5)
- Valid Accounts (4)

Defense Evasion
42 techniques
- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (2)
- Execution Guardrails (1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (2)
- Hide Artifacts (10)
- Hijack Execution Flow (12)
- Impair Defenses (9)
- Indicator Removal on Host (6)
- Indirect Command Execution
- Masquerading (7)
- Modify Authentication Process (5)
- Modify Cloud Compute Infrastructure (4)
- Modify Registry
- Modify System Image (2)
- Network Boundary Bridging (1)
- Obfuscated Files or Information (6)
- Plist File Modification
- Pre-OS Boot (5)
- Process Injection (12)

Credential Access
16 techniques
- Adversary-in-the-Middle (3)
- Brute Force (4)
- Credentials from Password Stores (5)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (2)
- Input Capture (4)
- Modify Authentication Process (5)
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing
- OS Credential Dumping (8)
- Steal Application Access Token
- Steal or Forge Kerberos Tickets (4)
- Steal Web Session Cookie
- Unsecured Credentials (7)

Discovery
30 techniques
- Account Discovery (4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (1)
- System Information Discovery
- System Location Discovery (1)
- System Network Configuration Discovery (1)
- System Network Connections Discovery

Lateral Movement
9 techniques
- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (2)
- Remote Services (6)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (4)

Collection
17 techniques
- Adversary-in-the-Middle (3)
- Archive Collected Data (3)
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage Object
- Data from Configuration Repository (2)
- Data from Information Repositories (3)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (2)
- Email Collection (3)
- Input Capture (4)
- Screen Capture
- Video Capture

Command and Control
16 techniques
- Application Layer Protocol (4)
- Communication Through Removable Media
- Data Encoding (2)
- Data Obfuscation (3)
- Dynamic Resolution (3)
- Encrypted Channel (2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (4)
- Remote Access Software
- Traffic Signaling (1)
- Web Service (3)

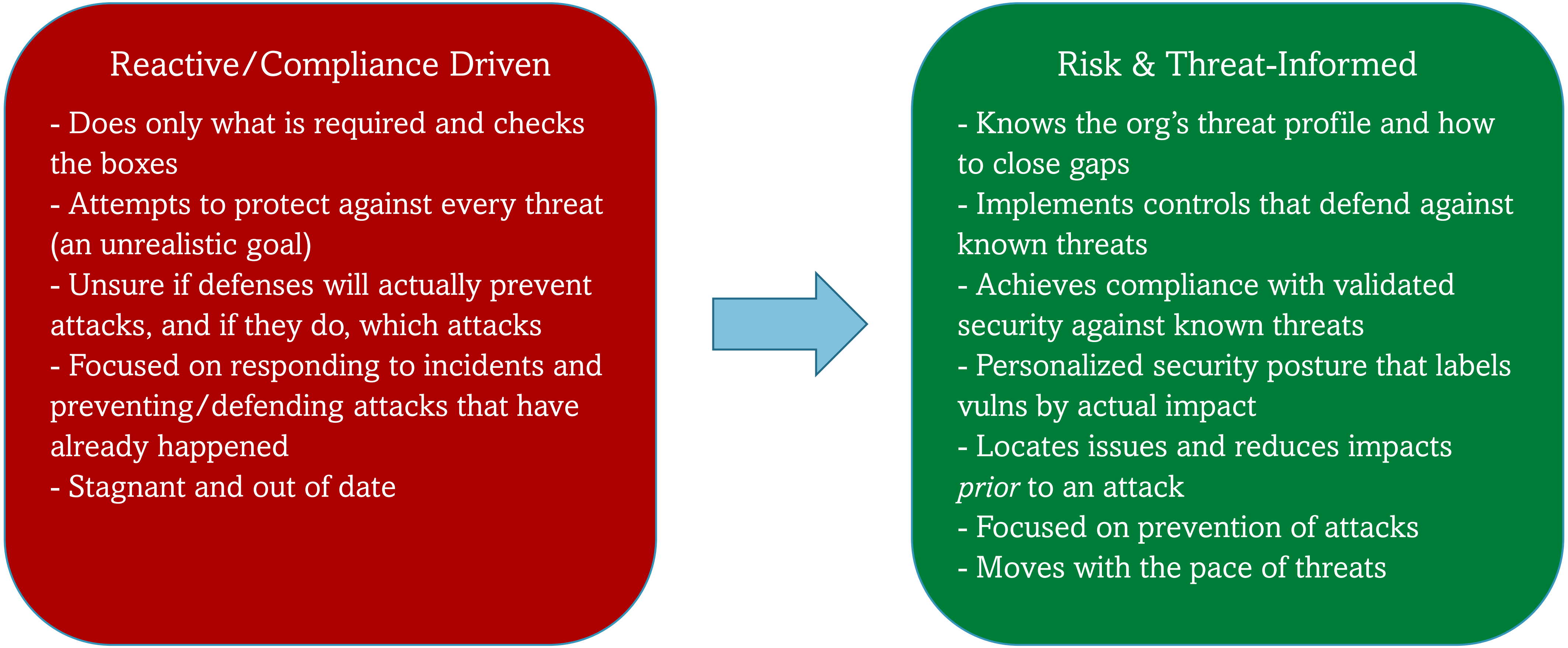
Exfiltration
9 techniques
- Automated Exfiltration (1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (1)
- Exfiltration Over Physical Medium (1)
- Exfiltration Over Web Service (2)
- Scheduled Transfer
- Transfer Data to Cloud Account

Impact
13 techniques
- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (3)
- Defacement (2)
- Disk Wipe (2)
- Endpoint Denial of Service (4)
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service (2)
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

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/defending 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
- Personalized security posture that labels vulns by actual impact
- 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

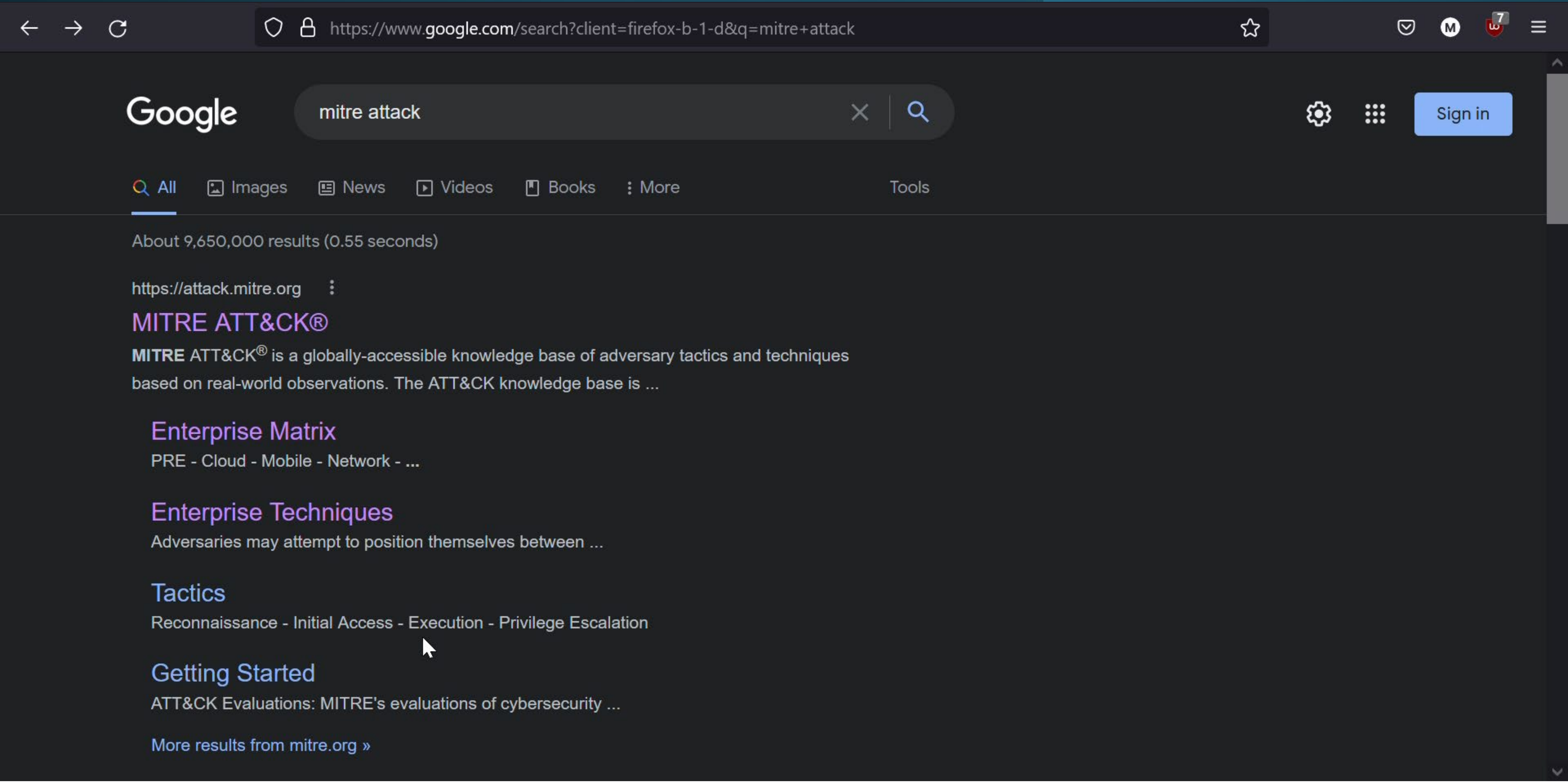
Free Tools

- 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
     - Short Operation demo

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



https://www.google.com/search?client=firefox-b-1-d&q=mitre+attack
Google
mitre attack
Sign in
All
Images
News
Videos
Books
More
Tools

About 9,650,000 results (0.55 seconds)

https://attack.mitre.org

MITRE ATT&CK®

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

Enterprise Matrix

PRE - Cloud - Mobile - Network - ...

Enterprise Techniques

Adversaries may attempt to position themselves between ...

Tactics

Reconnaissance - Initial Access - Execution - Privilege Escalation

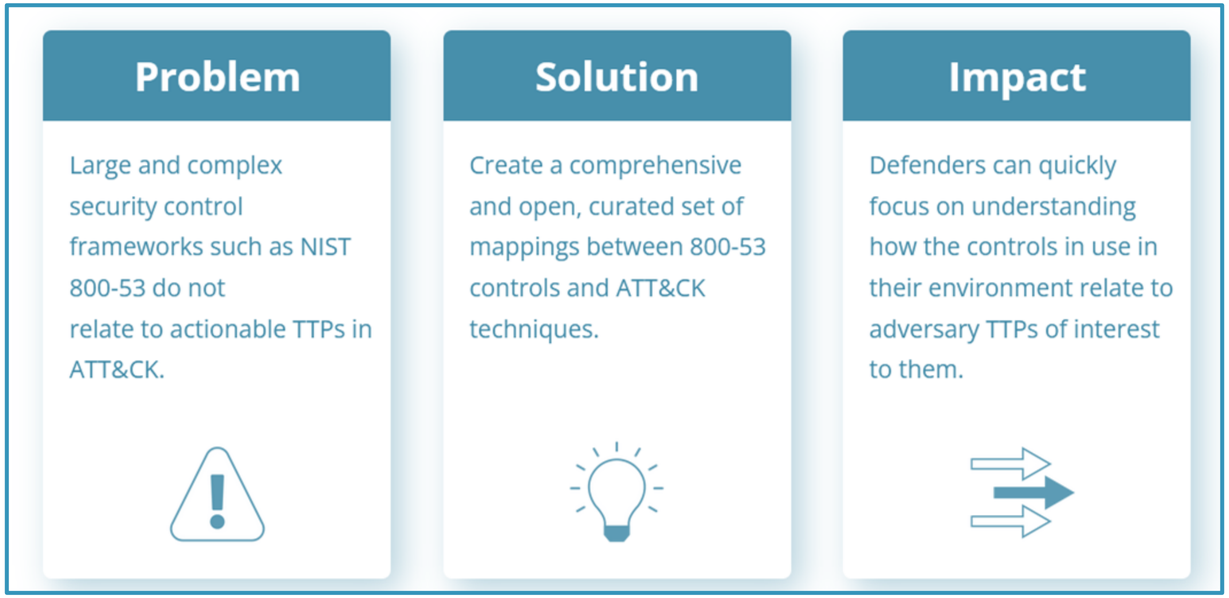
Getting Started

ATT&CK Evaluations: MITRE's evaluations of cybersecurity ...

More results from mitre.org »

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?”



Problem

Large and complex security control frameworks such as NIST 800-53 do not relate to actionable TTPs in ATT&CK.

Solution

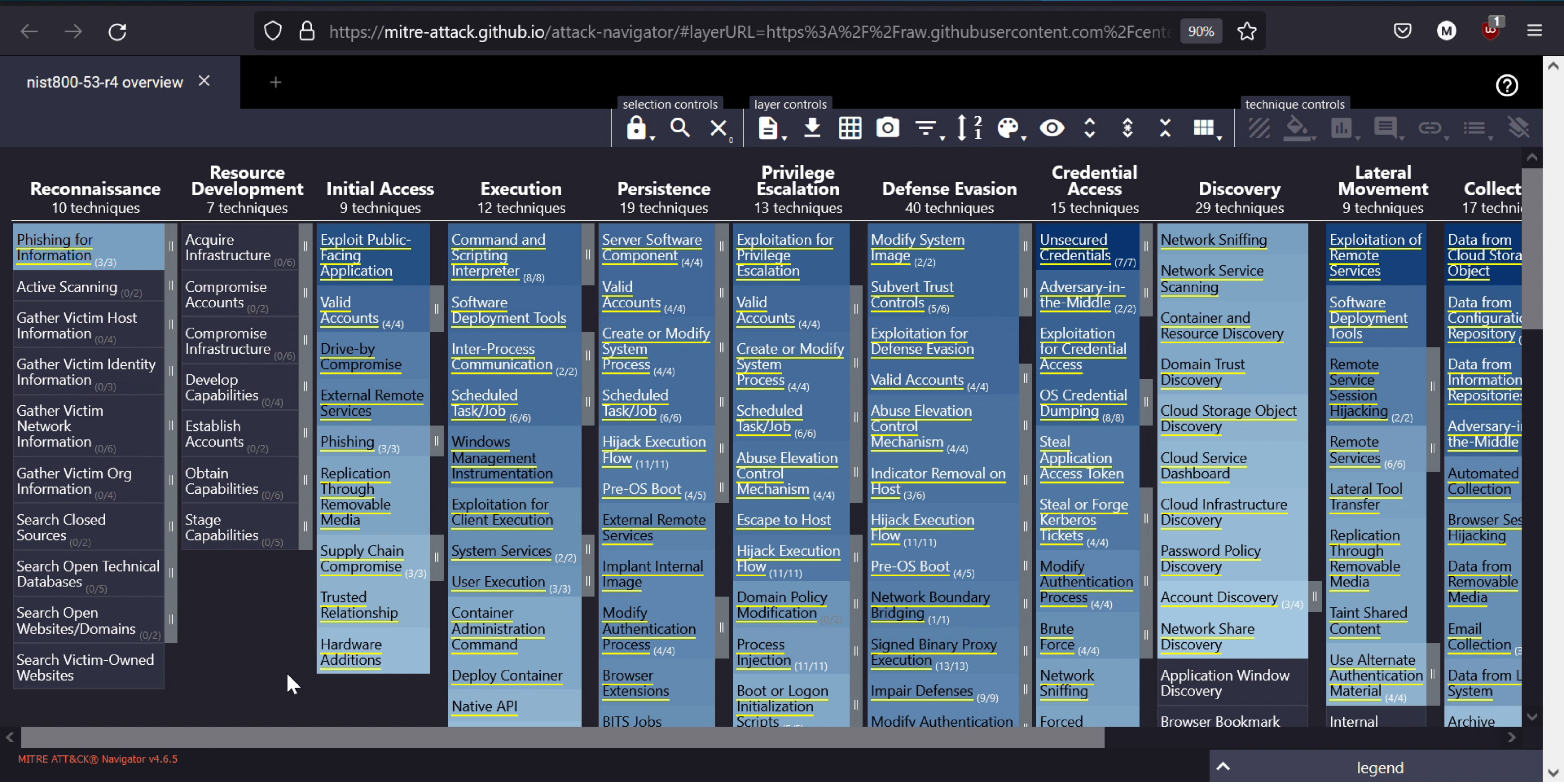
Create a comprehensive and open, curated set of mappings between 800-53 controls and ATT&CK techniques.

Impact

Defenders can quickly focus on understanding how the controls in use in their environment relate to adversary TTPs of interest to them.

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


https://mitre-attack.github.io/attack-navigator/#layerURL=https%3A%2F%2Fraw.githubusercontent.com%2Fcent
90%
nist800-53-r4 overview
selection controls
layer controls
technique controls
MITRE ATT&CK® Navigator v4.6.5
legend

Reconnaissance 10 techniques
- Phishing for Information (3/3)
- Active Scanning (0/2)
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (0/3)
- Gather Victim Network Information (0/6)
- Gather Victim Org Information (0/4)
- Search Closed Sources (0/2)
- Search Open Technical Databases (0/5)
- Search Open Websites/Domains (0/2)
- Search Victim-Owned Websites

Resource Development 7 techniques
- Acquire Infrastructure (0/6)
- Compromise Accounts (0/2)
- Compromise Infrastructure (0/6)
- Develop Capabilities (0/4)
- Establish Accounts (0/2)
- Obtain Capabilities (0/6)
- Stage Capabilities (0/5)

Initial Access 9 techniques
- Exploit Public-Facing Application
- Valid Accounts (4/4)
- Drive-by Compromise
- External Remote Services
- Phishing (3/3)
- Replication Through Removable Media
- Supply Chain Compromise (3/3)
- Trusted Relationship
- Hardware Additions

Execution 12 techniques
- Command and Scripting Interpreter (8/8)
- Software Deployment Tools
- Inter-Process Communication (2/2)
- Scheduled Task/Job (6/6)
- Windows Management Instrumentation
- Exploitation for Client Execution
- System Services (2/2)
- User Execution (3/3)
- Container Administration Command
- Deploy Container
- Native API

Persistence 19 techniques
- Server Software Component (4/4)
- Valid Accounts (4/4)
- Create or Modify System Process (4/4)
- Scheduled Task/Job (6/6)
- Hijack Execution Flow (11/11)
- Pre-OS Boot (4/5)
- External Remote Services
- Implant Internal Image
- Modify Authentication Process (4/4)
- Browser Extensions
- BITS Jobs

Privilege Escalation 13 techniques
- Exploitation for Privilege Escalation
- Valid Accounts (4/4)
- Create or Modify System Process (4/4)
- Scheduled Task/Job (6/6)
- Abuse Elevation Control Mechanism (4/4)
- Escape to Host
- Hijack Execution Flow (11/11)
- Domain Policy Modification (0/2)
- Process Injection (11/11)
- Boot or Logon Initialization Scripts

Defense Evasion 40 techniques
- Modify System Image (2/2)
- Subvert Trust Controls (5/6)
- Exploitation for Defense Evasion
- Valid Accounts (4/4)
- Abuse Elevation Control Mechanism (4/4)
- Indicator Removal on Host (3/6)
- Hijack Execution Flow (11/11)
- Pre-OS Boot (4/5)
- Network Boundary Bridging (1/1)
- Signed Binary Proxy Execution (13/13)
- Impair Defenses (9/9)
- Modify Authentication

Credential Access 15 techniques
- Unsecured Credentials (7/7)
- Adversary-in-the-Middle (2/2)
- Exploitation for Credential Access
- OS Credential Dumping (8/8)
- Steal Application Access Token
- Steal or Forge Kerberos Tickets (4/4)
- Modify Authentication Process (4/4)
- Brute Force (4/4)
- Network Sniffing
- Forced

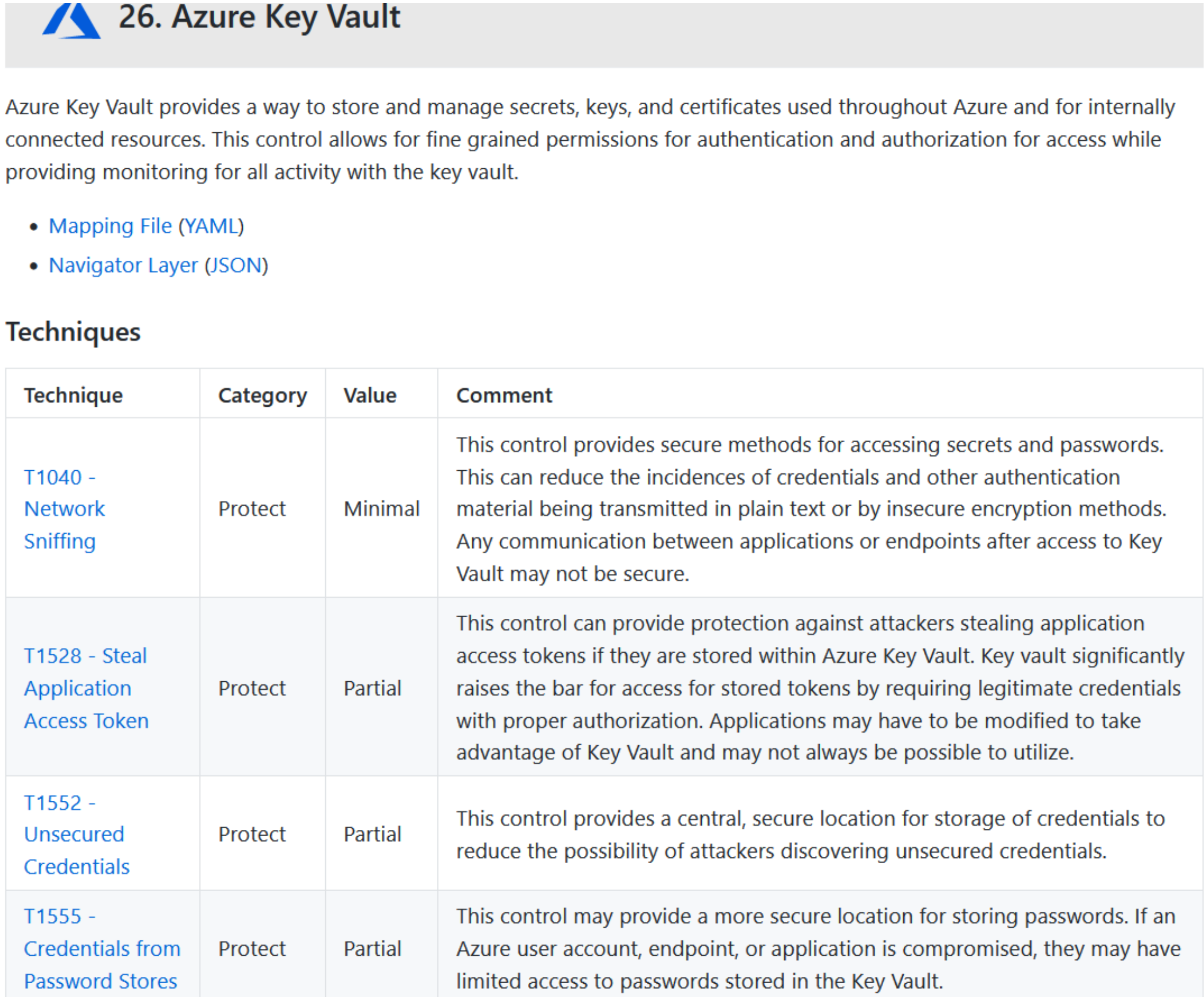
Discovery 29 techniques
- Network Sniffing
- Network Service Scanning
- Container and Resource Discovery
- Domain Trust Discovery
- Cloud Storage Object Discovery
- Cloud Service Dashboard
- Cloud Infrastructure Discovery
- Password Policy Discovery
- Account Discovery (3/4)
- Network Share Discovery
- Application Window Discovery
- Browser Bookmark

Lateral Movement 9 techniques
- Exploitation of Remote Services
- Software Deployment Tools
- Remote Service Session Hijacking (2/2)
- Remote Services (6/6)
- Lateral Tool Transfer
- Replication Through Removable Media
- Taint Shared Content
- Use Alternate Authentication Material (4/4)
- Internal

Collect 17 techni
- Data from Cloud Stora Object
- Data from Configurati Repository (
- Data from Information Repositorie
- Adversary-i the-Middle
- Automated Collection
- Browser Ses Hijacking
- Data from Removable Media
- Email Collection (3
- Data from L System
- Archive

More Control to TTP Mappings

- Mappings for cloud security:
  - Microsoft Azure
  - Amazon Web Services
  - Google Cloud Platform



26. Azure Key Vault

Azure Key Vault provides a way to store and manage secrets, keys, and certificates used throughout Azure and for internally connected resources. This control allows for fine grained permissions for authentication and authorization for access while providing monitoring for all activity with the key vault.

- Mapping File (YAML)
- Navigator Layer (JSON)

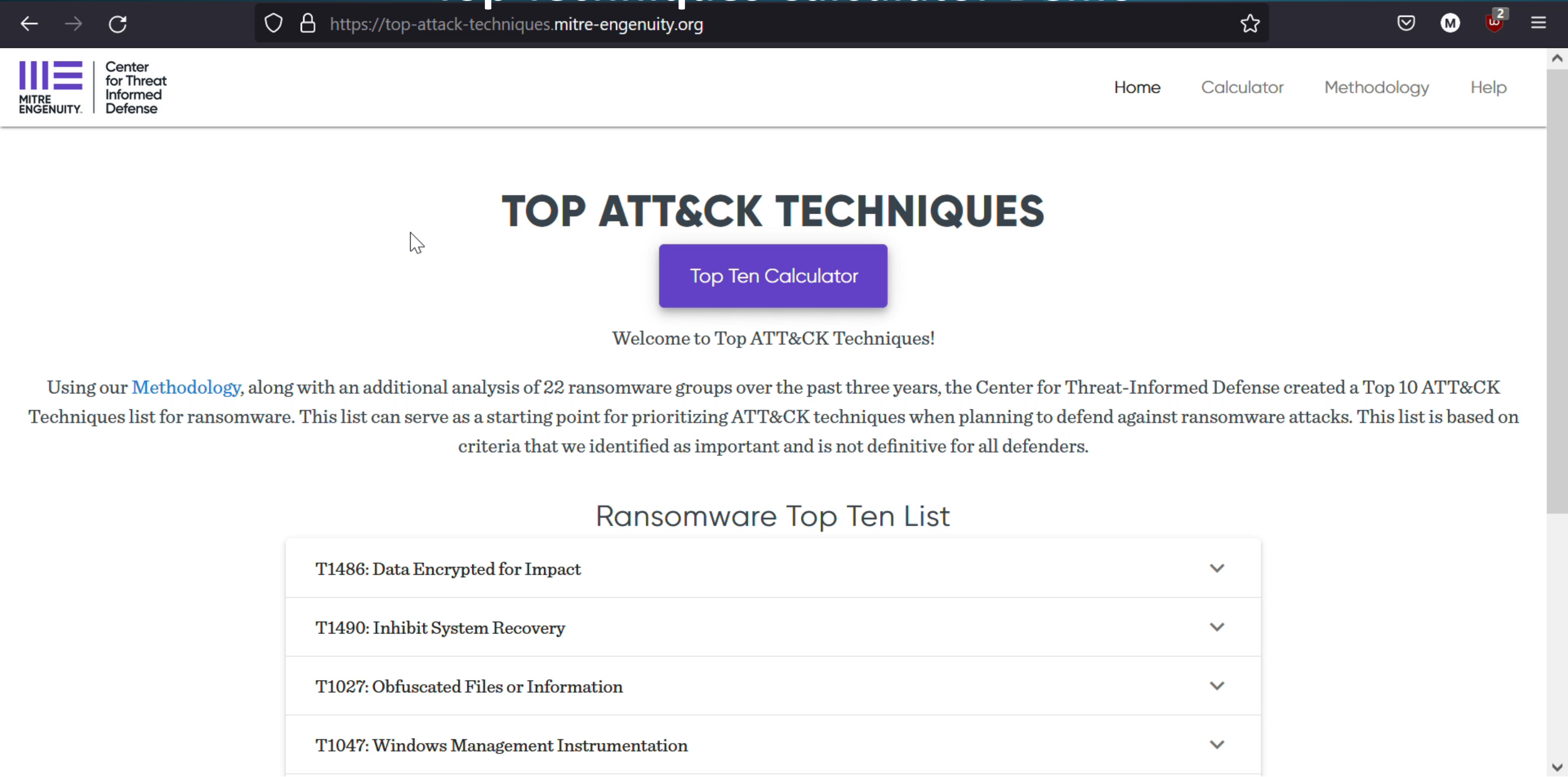
Techniques

Technique	Category	Value	Comment
T1040 - Network Sniffing	Protect	Minimal	This control provides secure methods for accessing secrets and passwords. This can reduce the incidences of credentials and other authentication material being transmitted in plain text or by insecure encryption methods. Any communication between applications or endpoints after access to Key Vault may not be secure.
T1528 - Steal Application Access Token	Protect	Partial	This control can provide protection against attackers stealing application access tokens if they are stored within Azure Key Vault. Key vault significantly raises the bar for access for stored tokens by requiring legitimate credentials with proper authorization. Applications may have to be modified to take advantage of Key Vault and may not always be possible to utilize.
T1552 - Unsecured Credentials	Protect	Partial	This control provides a central, secure location for storage of credentials to reduce the possibility of attackers discovering unsecured credentials.
T1555 - Credentials from Password Stores	Protect	Partial	This control may provide a more secure location for storing passwords. If an Azure user account, endpoint, or application is compromised, they may have limited access to passwords stored in the Key Vault.

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


https://top-attack-techniques.mitre-engenuity.org
MITRE ENGENUITY
Center for Threat Informed Defense
Home
Calculator
Methodology
Help
Top Ten Calculator

TOP ATT&CK TECHNIQUES

Welcome to Top ATT&CK Techniques!

Using our Methodology, along with an additional analysis of 22 ransomware groups over the past three years, the Center for Threat-Informed Defense created a Top 10 ATT&CK Techniques list for ransomware. This list can serve as a starting point for prioritizing ATT&CK techniques when planning to defend against ransomware attacks. This list is based on criteria that we identified as important and is not definitive for all defenders.

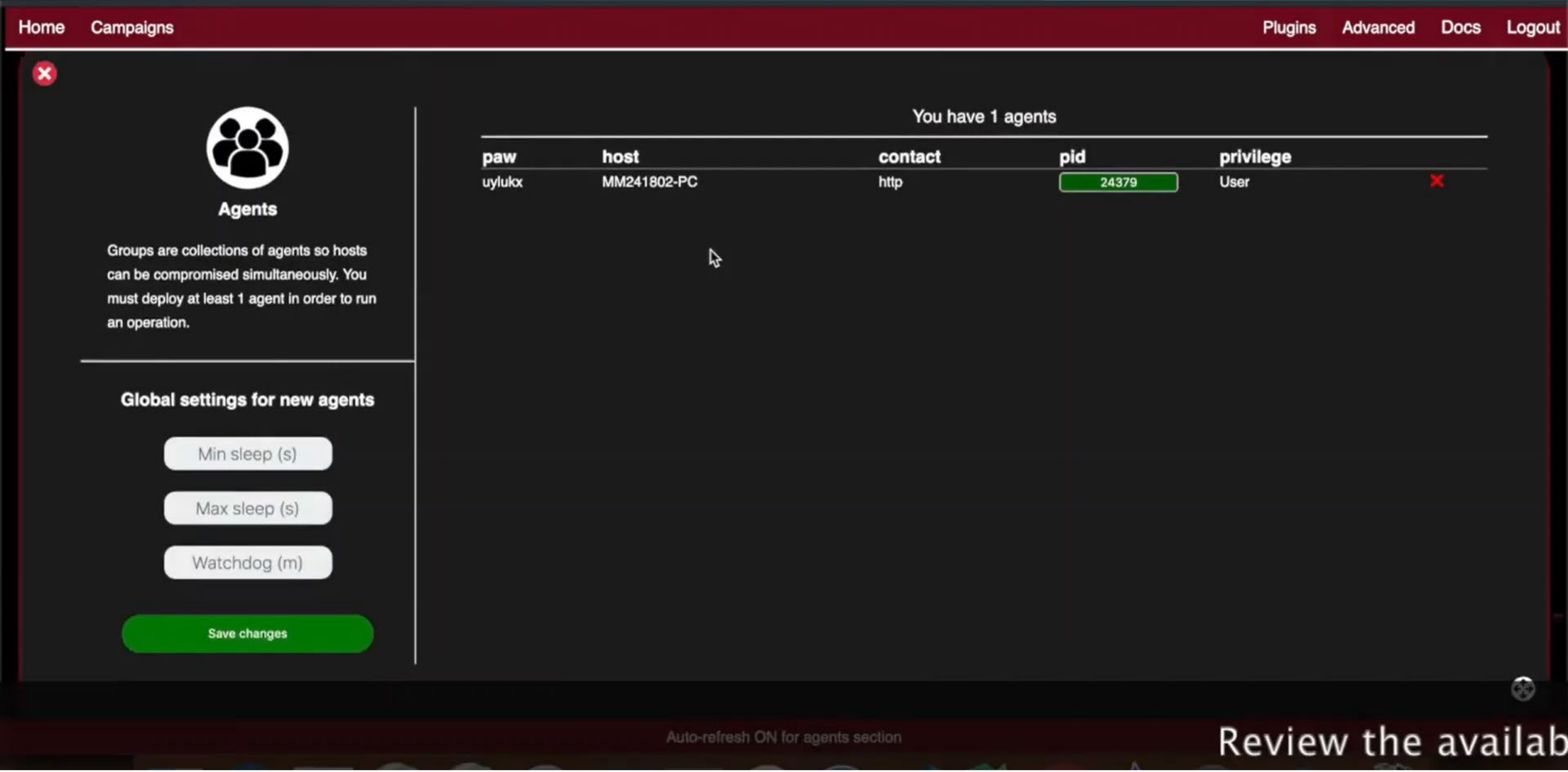
Ransomware Top Ten List

- T1486: Data Encrypted for Impact
- T1490: Inhibit System Recovery
- T1027: Obfuscated Files or Information
- T1047: Windows Management Instrumentation

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 operations (menuPass plan)
- Install plugins for added functionality (Pathfinder from CTID)
- MITRE CALDERA: https://caldera.mitre.org/

CALDERA Operation Demo [4]


Home
Campaigns
Plugins
Advanced
Docs
Logout
Agents
Min sleep (s)
Max sleep (s)
Watchdog (m)
Save changes

Groups are collections of agents so hosts can be compromised simultaneously. You must deploy at least 1 agent in order to run an operation.

Global settings for new agents

You have 1 agents

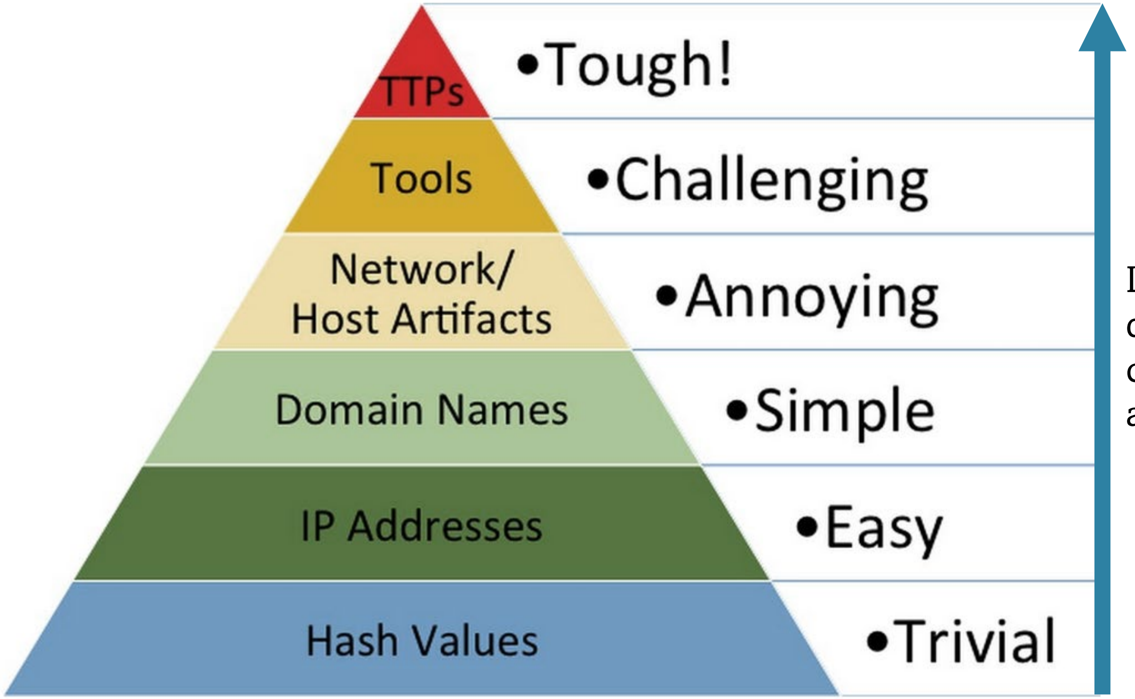
paw	host	contact	pid	privilege
uylukx	MM241802-PC	http	24379	User

Auto-refresh ON for agents section

Review the availab

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


TTPs
•Tough!
Tools
•Challenging
Network/ Host Artifacts
•Annoying
Domain Names
•Simple
IP Addresses
•Easy
Hash Values
•Trivial

Level of difficulty in changing for an adversary

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 (Download): 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
  - Pathfinder Info Page: https://medium.com/mitre-engenuity/caldera-pathfinder-7564e63f3082
  - 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
- [4]: https://www.youtube.com/watch?v=_mVGjqu03fg

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