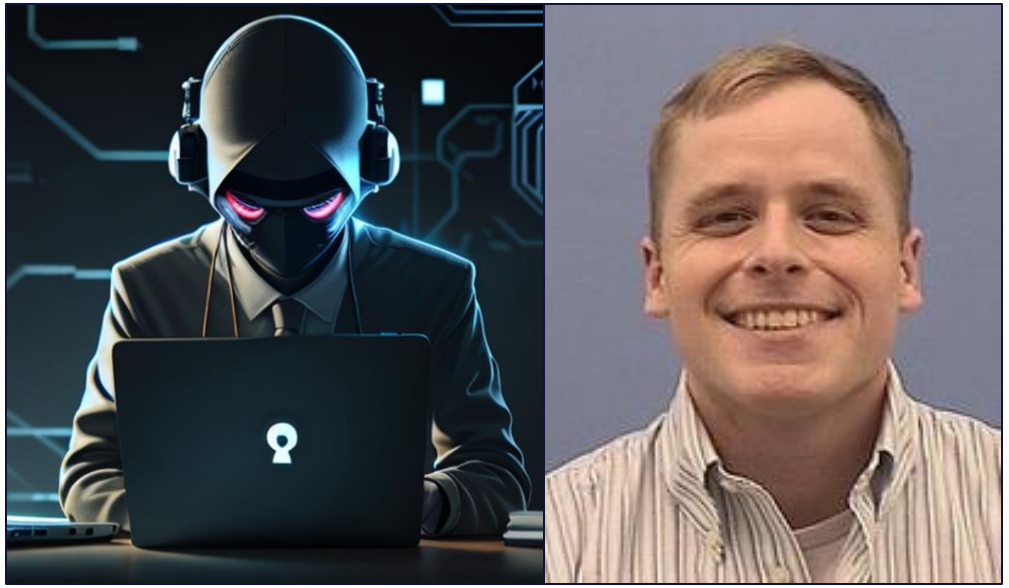
Threat Modeling With ATT&CK

BSides Connecticut

Sept 21, 2024

MITRE ENGENUITY | Center for Threat Informed Defense

Your Gracious Hosts



Tyler Schechter

Project Leader

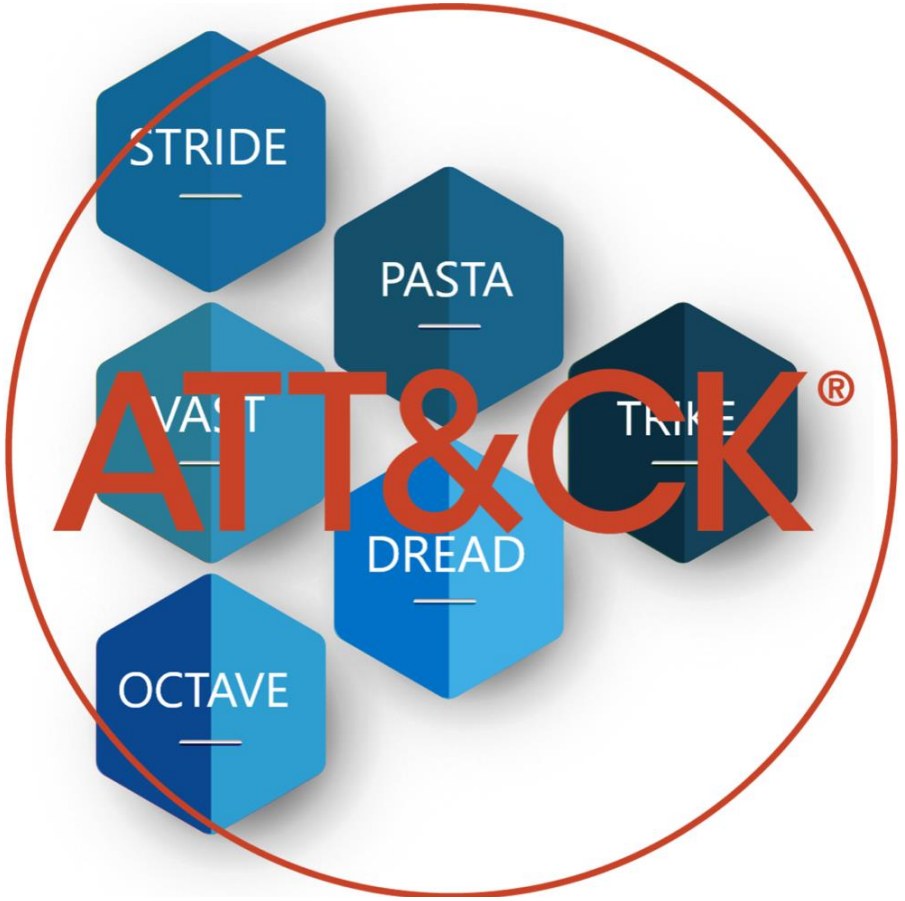
Ben Ballard

Technical Leader

How to go from Threat Model to Supermodel

- This is the first ever process to bridge the gap between industry-standard threat modeling methodologies and ATT&CK

- Organizations of any size or maturity level can use this step-by-step process to model threats to their own assets using their existing tools and cyber threat intelligence (CTI) data.



Workshop Agenda

- Intro to Threat Modeling: What is threat modeling?
- Intro to ATT&CK
- Intro to Threat Modeling with ATT&CK
- Introduction to AMPS
- Deep dive into each threat modeling step with practical hands-on experience in group and classroom setting
  - Question 1 – What am I working on?
  - Question 2 – What could go wrong?
  - Question 3 – What am I going to do about it?
  - Question 4 – Did I do a good job?

Total Expected Workshop Duration: 4 Hours (including bathroom breaks)

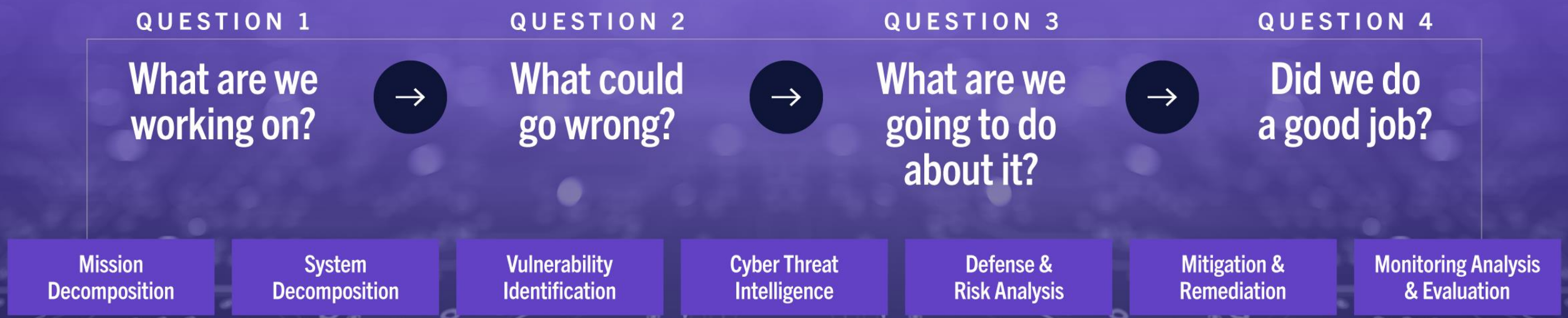
What you'll take away from today

- How to identify critical components in a system
- How to use Attack Trees
- How to identify threats to a system using ATT&CK
- How to mitigate threats to a system using ATT&CK

A Brief Overview of Threat Modeling

MITRE ENGENUITY™ | Center for Threat Informed Defense

WHAT: THREAT MODELING



A Process with Multiple Products

With ATT&CK®

WHY:

Threat Modeling enables analysts to focus on threats that are most concerning to their organization

Organizations have **limited budgets** to protect their systems and data. We **threat model to help prioritize defensive investments** where they are needed most.

HOW:

Answer the 4 Questions!

QUESTION 1
What are we working on?

→

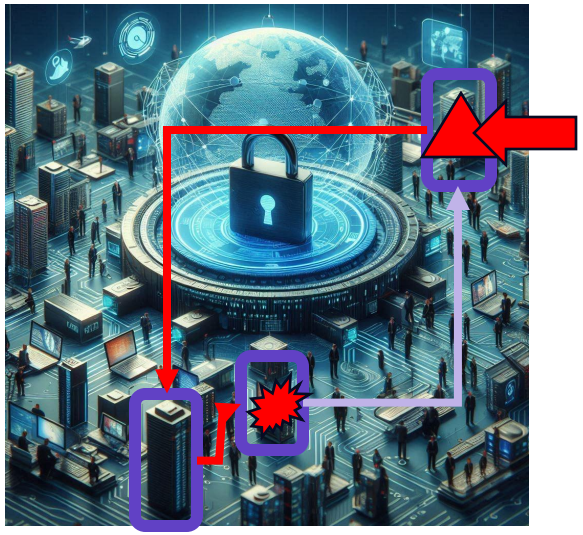
QUESTION 2
What could go wrong?

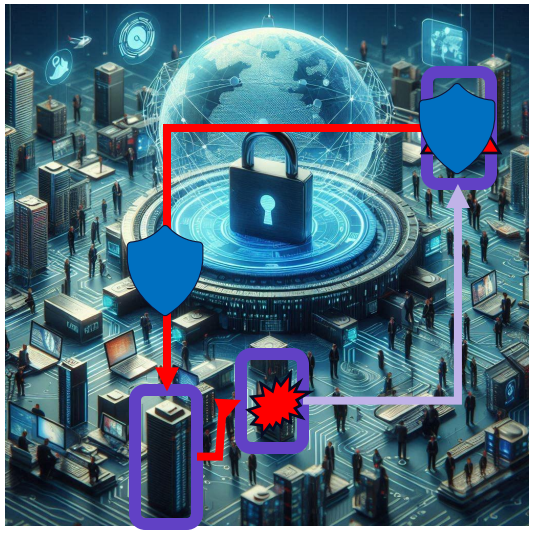
→

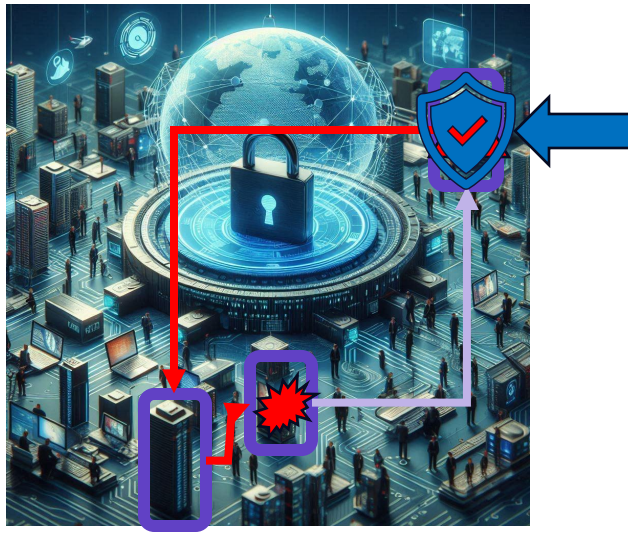
QUESTION 3
What are we going to do about it?

→

QUESTION 4
Did we do a good job?







MITRE ENGENUITY™ | Center for Threat Informed Defense

A Brief Overview of ATT&CK

MITRE ENGENUITY™ | Center for Threat Informed Defense

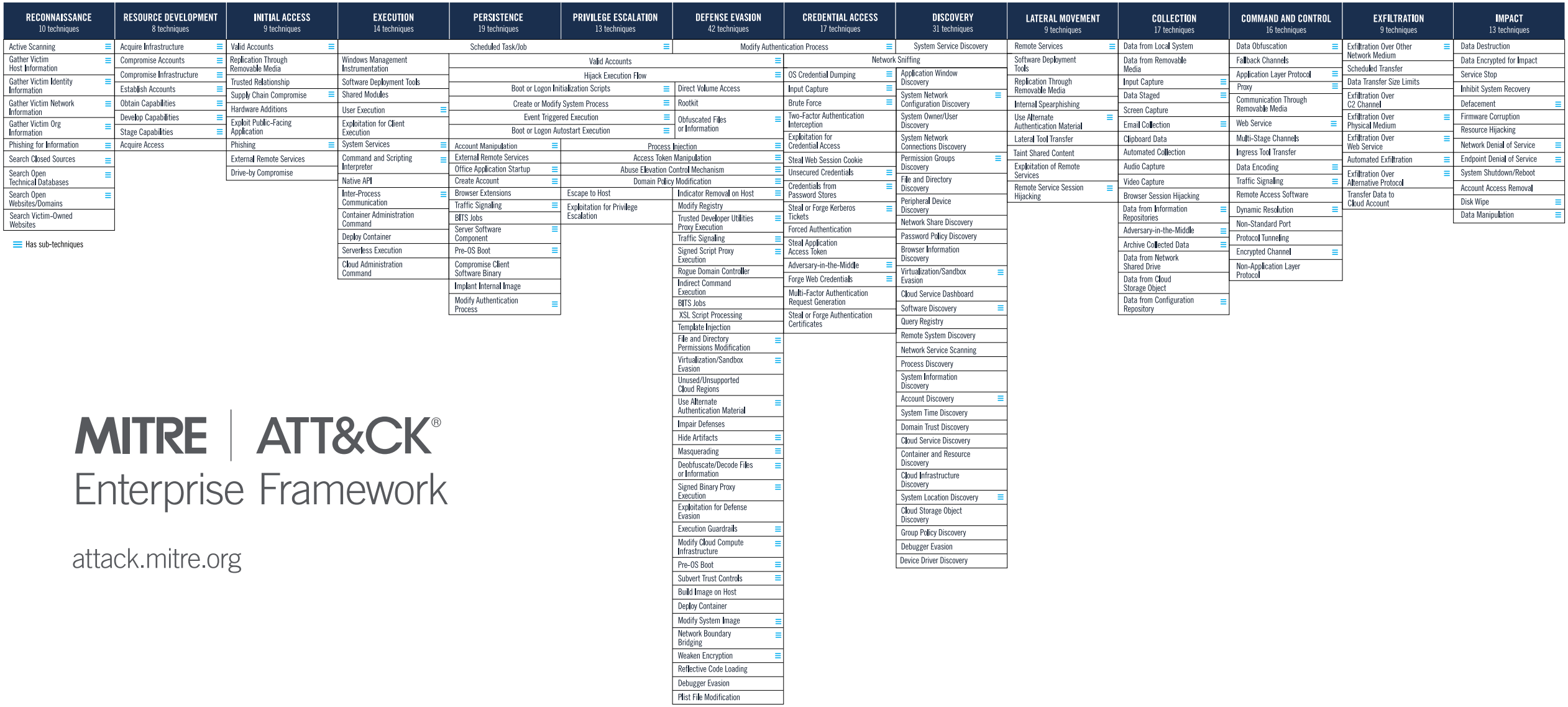
ATT&CK®

ATT&CK is a **globally-accessible** knowledge base of adversary tactics and techniques, developed by MITRE **based on real-world observations** of adversaries' operations.

ATT&CK is used by the cybersecurity community as a **common language** to describe adversary behavior.

attack.mitre.org

MITRE ENGENUITY | Center for Threat Informed Defense



MITRE | ATT&CK®

Enterprise Framework

attack.mitre.org

MITRE ENGENUITY™ | Center for Threat Informed Defense

TACTIC: Why adversary is performing activity

PERSISTENCE (19 techniques)	PRIVILEGE ESCALATION (13 techniques)	DEFENSE EVASION (42 techniques)	CREDENTIAL ACCESS (17 techniques)	DISCOVERY (31 techniques)	LATERAL MOVEMENT (9 techniques)	COLLECTION (17 techniques)	COMMA
Scheduled Task/Job		Modify Authentication Process		System Service Discovery	Remote Services	Data from Local System	Data Obfu
Valid Accounts			Network Sniffing		Software Deployment Tools	Data from Removable Media	Fallback C
Hijack Execution Flow			OS Credential Dumping	Application Window Discovery	Replication Through Removable Media	Input Capture	Applicatio
			Input Capture	System Network Configuration Discovery	Internal Spearphishing	Data Staged	Proxy
			Brute Force	System Owner/User Discovery	Use Alternate Authentication Material	Screen Capture	Communic Removabl
			Two-Factor Authentication Interception	System Network Connections Discovery	Lateral Tool Transfer	Email Collection	Web Servi
			Exploitation for Credential Access	Permission Groups Discovery	Taint Shared Content	Clipboard Data	Multi-Stag
			Steal Web Session Cookie	File and Directory Discovery	Exploitation of Remote Services	Automated Collection	Ingress To
External Remote Services	Access Token Manipulation		Unsecured Credentials	Peripheral Device Discovery	Remote Service Session Hijacking	Audio Capture	Data Encc
Office Application Startup	Abuse Elevation Control Mechanism		Credentials from Password Stores	Network Share Discovery		Video Capture	Traffic Sig
Create Account	Domain Policy Modification		Steal or Forge Kerberos Tickets	Password Policy Discovery		Browser Session Hijacking	Remote Ac
Browser Extensions	Escape to Host	Indicator Removal on Host	Forced Authentication	Browser Information Discovery		Data from Information Repositories	Dynamic F
Traffic Signaling	Exploitation for Privilege Escalation	Modify Registry	Steal Application Access Token	Virtualization/Sandbox Evasion		Adversary-in-the-Middle	Non-Stand
BITS Jobs		Trusted Developer Utilities Proxy Execution	Adversary-in-the-Middle	Cloud Service Dashboard		Archive Collected Data	Protocol T
Server Software Component		Traffic Signaling	Forge Web Credentials	Software Discovery		Data from Network Shared Drive	Encrypted
Pre-OS Boot		Signed Script Proxy Execution	Multi-Factor Authentication Request Generation	Query Registry		Data from Cloud Storage Object	Non-Appli Protocol
Compromise Client Software Binary		Rogue Domain Controller	Steal or Forge Authentication Certificates	Remote System Discovery		Data from Configuration Repository	
Implant Internal Image		Indirect Command Execution		Network Service Scanning			
Modify Authentication Process		BITS Jobs		Process Discovery			
		XSL Script Processing		System Information Discovery			
		Template Injection		Account Discovery			
		File and Directory Permissions Modification		System Time Discovery			
		Virtualization/Sandbox Evasion		Domain Trust Discovery			
		Unused/Unsupported Cloud Regions		Cloud Service Discovery			
		Use Alternate Authentication Material		Container and Resource Discovery			
		Impair Defenses					
		Hide Artifacts					
		Masquerading					
		Deobfuscate/Decode Files					

MITRE ENGENUITY | Center for Threat Informed Defense

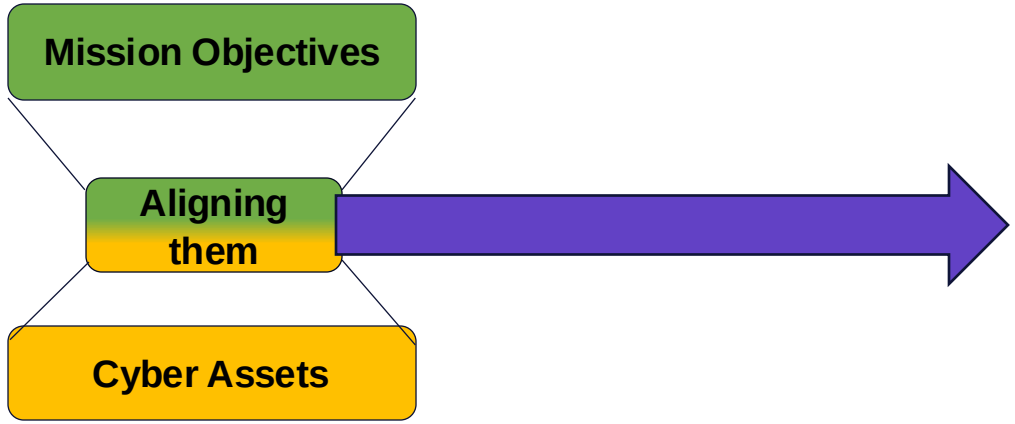
PERSISTENCE 19 techniques	PRIVILEGE ESCALATION 13 techniques	DEFENSE EVASION 42 techniques	CREDENTIAL ACCESS 17 techniques	DISCOVERY 31 techniques	LATERAL MOVEMENT 9 techniques	COLLECTION 17 techniques	COMMA
Scheduled Task/Job		Modify Authentication Process	Network Sniffing	System Service Discovery	Remote Services	Data from Local System	Data Obfu
Valid Accounts			OS Credential Dumping	Application Window Discovery	Software Deployment Tools	Data from Removable Media	Fallback C
Hijack Execution Flow			Input Capture	System Network Configuration Discovery	Replication Through Removable Media	Input Capture	Applicatio
Boot or Logon Initialization Scripts		Direct Volume Access	Brute Force	System Owner/User Discovery	Internal Spearphishing	Data Staged	Proxy
Create or Modify System Process		Rootkit	Two-Factor Authentication Interception	System Network Connections Discovery	Use Alternate Authentication Material	Screen Capture	Communic Removabl
Event Triggered Execution		Obfuscated Files or Information	Exploitation for Credential Access	Permission Groups Discovery	Lateral Tool Transfer	Email Collection	Web Servi
Boot or Logon Autostart Execution			Steal Web Session Cookie	File and Directory Discovery	Taint Shared Content	Clipboard Data	Multi-Stag
Account Manipulation	Process Injection		Unsecured Credentials	Peripheral Device Discovery	Exploitation of Remote Services	Automated Collection	Ingress To
External Remote Services	Access Token Manipulation		Credentials from Password Stores	Network Share Discovery	Remote Service Session Hijacking	Audio Capture	Data Encc
Office Application Startup	Abuse Elevation Control Mechanism		Steal or Forge Kerberos Tickets	Password Policy Discovery		Video Capture	Traffic Sig
Create Account	Domain Policy Modification		Forced Authentication	Browser Information Discovery		Browser Session Hijacking	Remote Ac
Browser Extensions	Escape to Host	Indicator Removal on Host	Steal Application Access Token	Virtualization/Sandbox Evasion		Data from Information Repositories	Dynamic R
Tra			Adversary-in-the-Middle	Cloud Service Dashboard		Adversary-in-the-Middle	Non-Stand
BI			Forge Web Credentials	Software Discovery		Archive Collected Data	Protocol T
Se Co			Multi-Factor Authentication Request Generation	Query Registry		Data from Network Shared Drive	Encrypted
Pr			Steal or Forge Authentication Certificates	Remote System Discovery		Data from Cloud Storage Object	Non-Appli Protocol
Co So				Network Service Scanning		Data from Configuration Repository	
Im				Process Discovery			
Modify Authentication Process		BITS Jobs		System Information Discovery			
		XSL Script Processing		Account Discovery			
		Template Injection		System Time Discovery			
		File and Directory Permissions Modification		Domain Trust Discovery			
		Virtualization/Sandbox Evasion		Cloud Service Discovery			
		Unused/Unsupported Cloud Regions		Container and Resource Discovery			
		Use Alternate Authentication Material					
		Impair Defenses					
		Hide Artifacts					
		Masquerading					
		Deobfuscate/Decode Files					

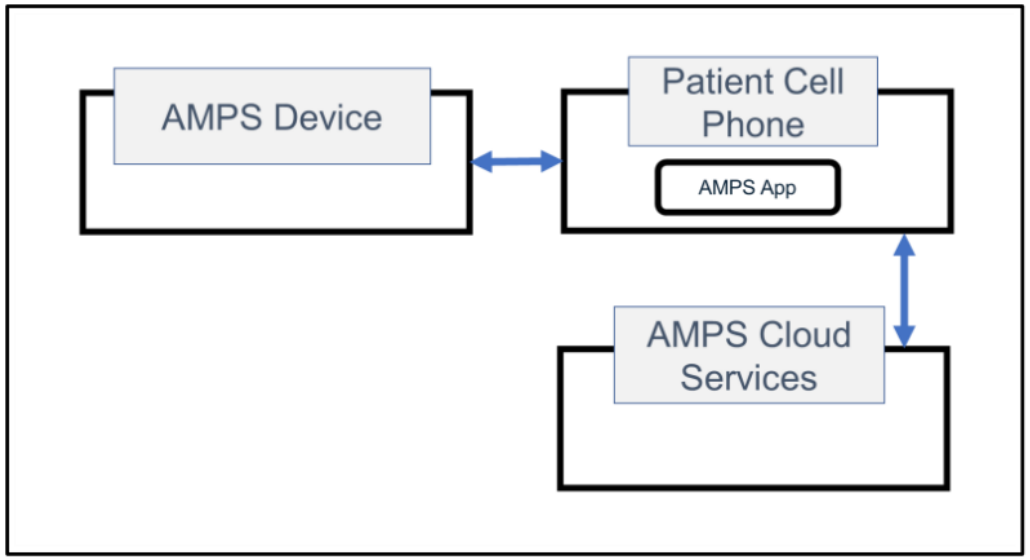
TECHNIQUE: How the adversary will achieve their goal

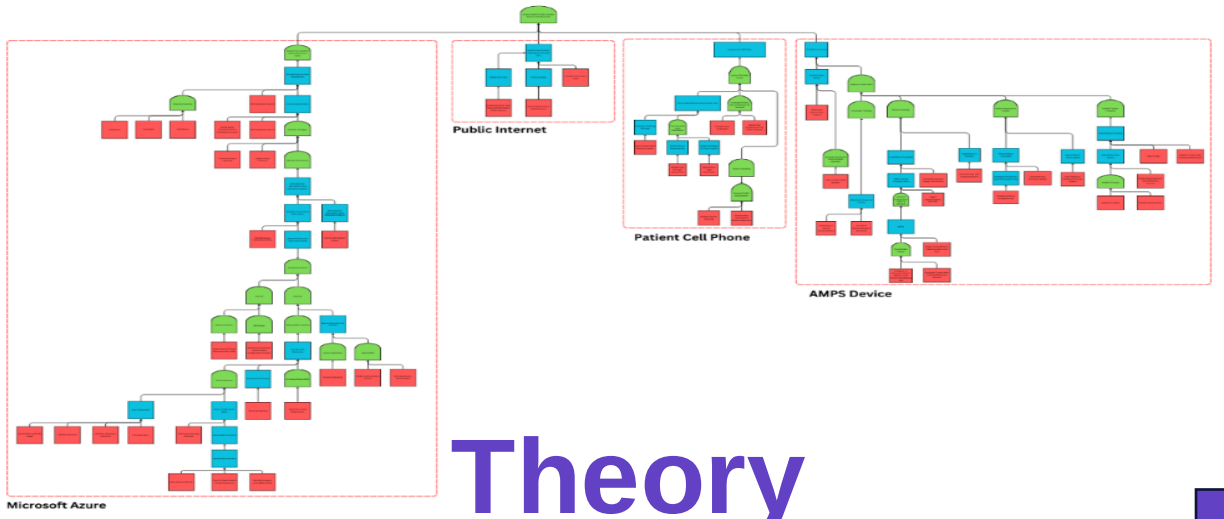
MITRE ENGENUITY | Center for Threat Informed Defense

A Brief Overview of Threat Modeling With ATT&CK

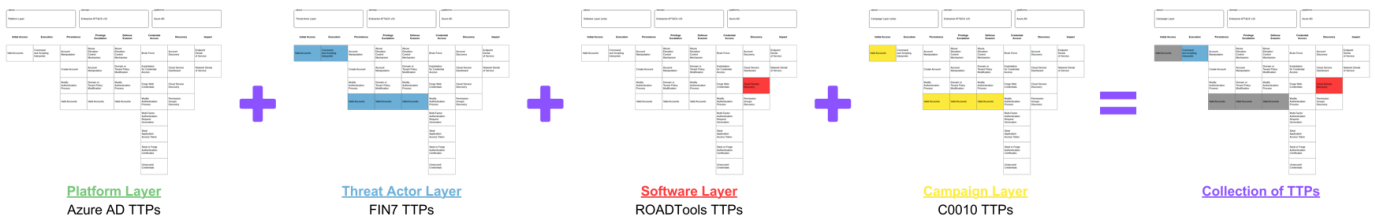
MITRE ENGENUITY™ | Center for Threat Informed Defense



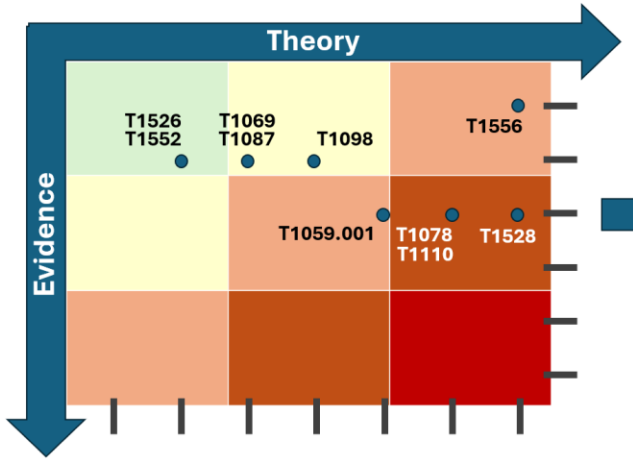




Theory
Evidence



Identify, Overlay, Score, and Prioritize Threat TTPs

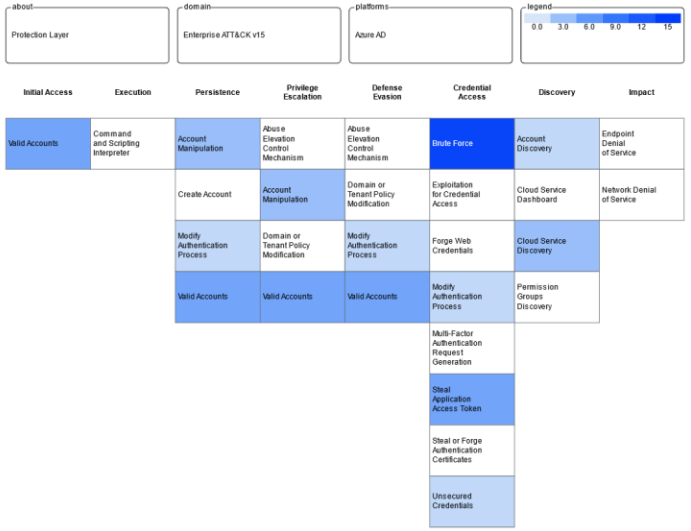


TTP#	Name
T1528	Steal Application Access Token
T1078	Valid Accounts
T1110	Brute Force
T1556	Modify Authentication Process
T1059 .001	Command and Scripting Interpreter - Powershell
T1098	Account Manipulation
T1087	Account Discovery
T1069	Permission Groups Discovery
T1552	Unsecured Credentials
T1526	Cloud Service Discovery

Threat

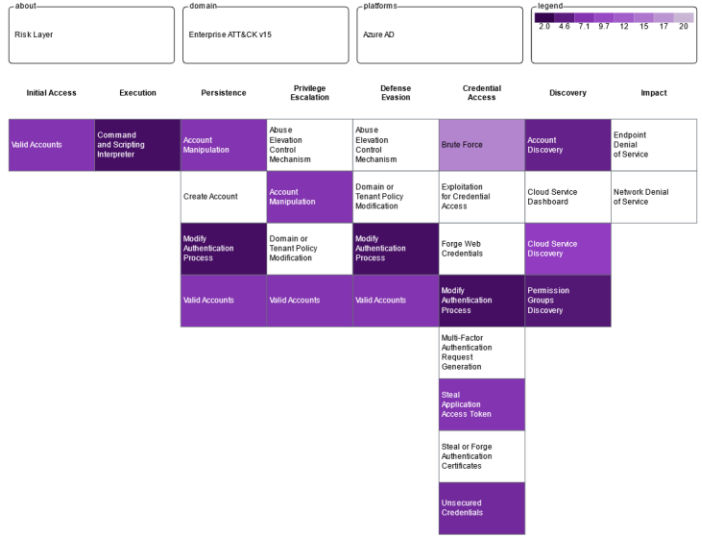
+

Defense

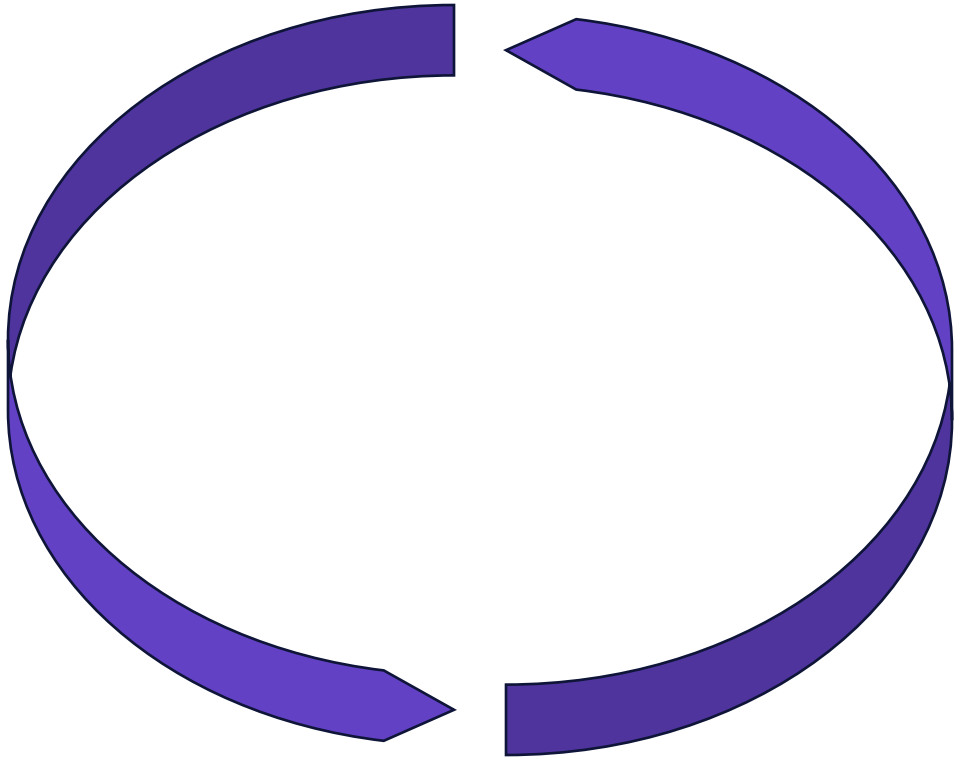


=

Risk

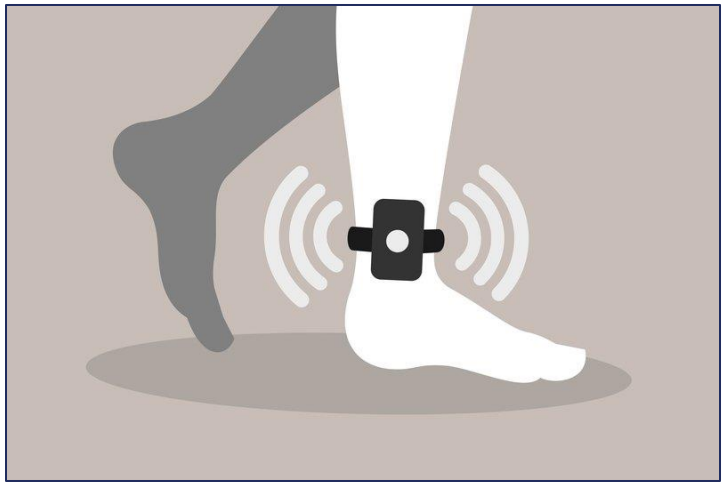


System Improvements

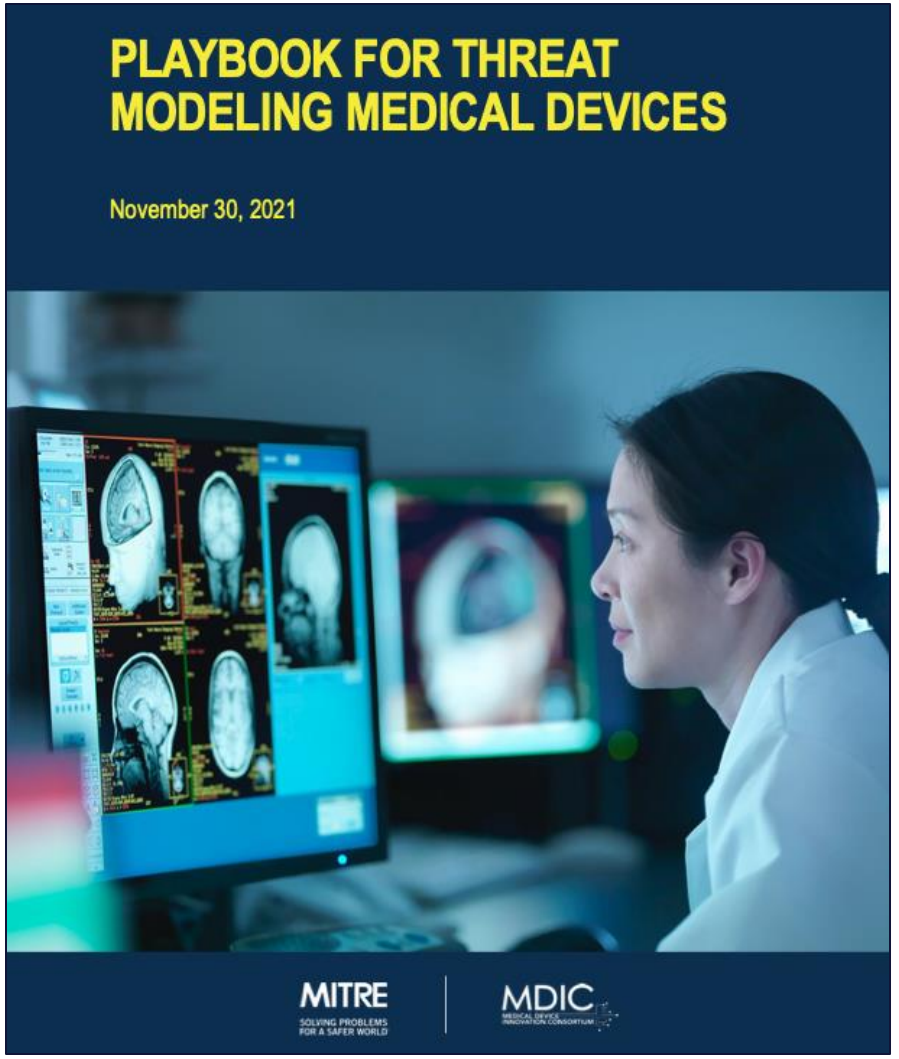


Secondary Review

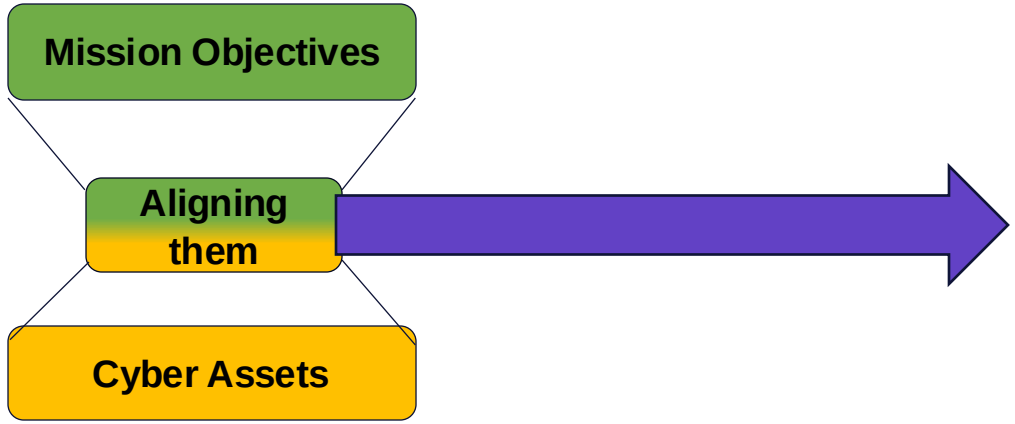
Today's Workshop = Threat Modeling this Device

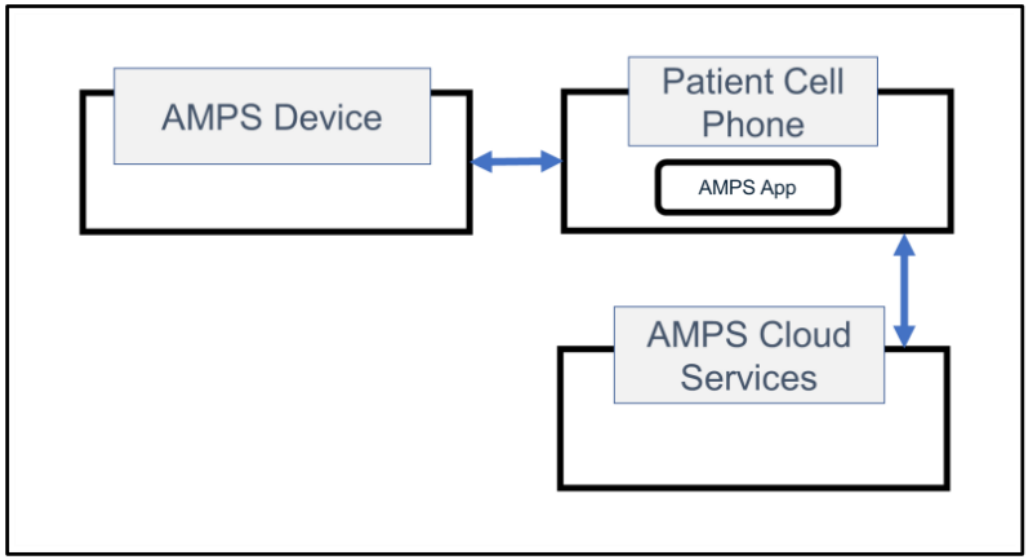


The **Ankle Monitor Predictor of Stroke (AMPS)**, device gives the wearer and their healthcare providers indications and warnings of a oncoming stroke. For more details, see HERE

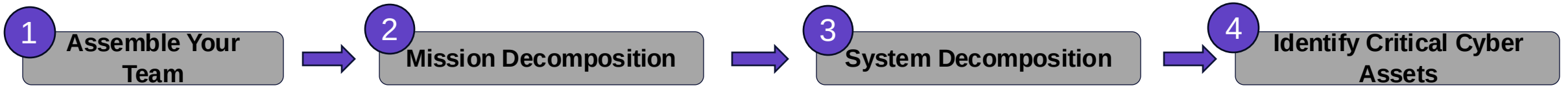


MITRE ENGENUITY | Center for Threat Informed Defense





Question 1: What Are We Working On?
Mission/system Decomposition and DFDs



Break into Groups

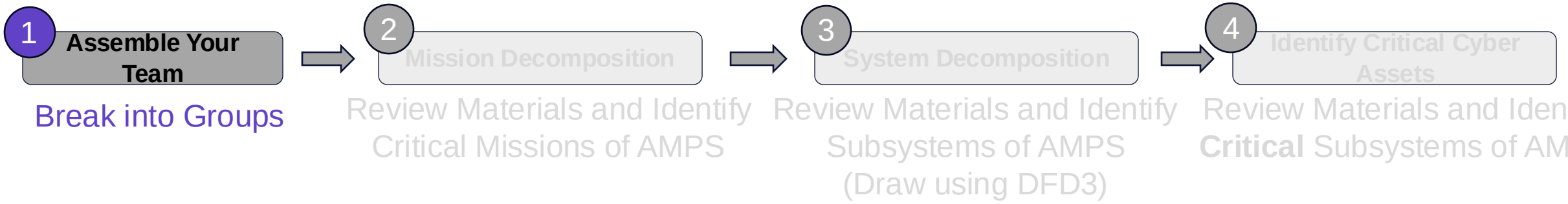
Review Materials and Identify Critical Missions of AMPS

Review Materials and Identify Subsystems of AMPS (Draw using DFD3)

Review Materials and Identify **Critical** Subsystems of AMPS

Question 1: What Are We Working On?
Mission/system Decomposition and DFDs

(5 Minutes)

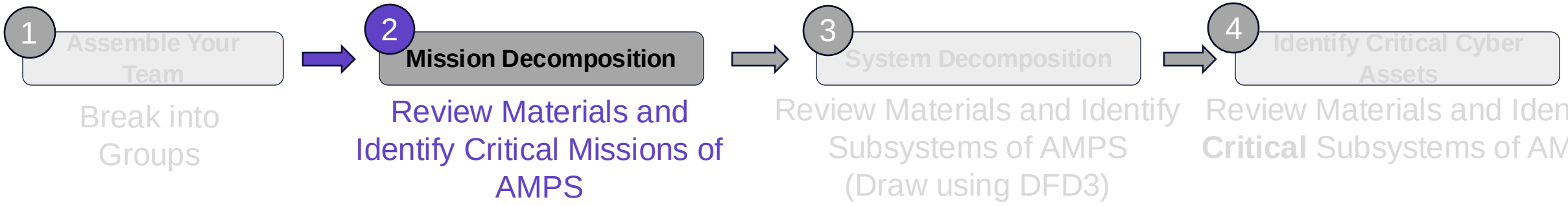


Group member roles:

- Scribe (need pen/paper or dry-erase board)
- Researchers (need access to internet or can use printouts)

Question 1: What Are We Working On?
Mission/system Decomposition and DFDs

(5 Minutes)

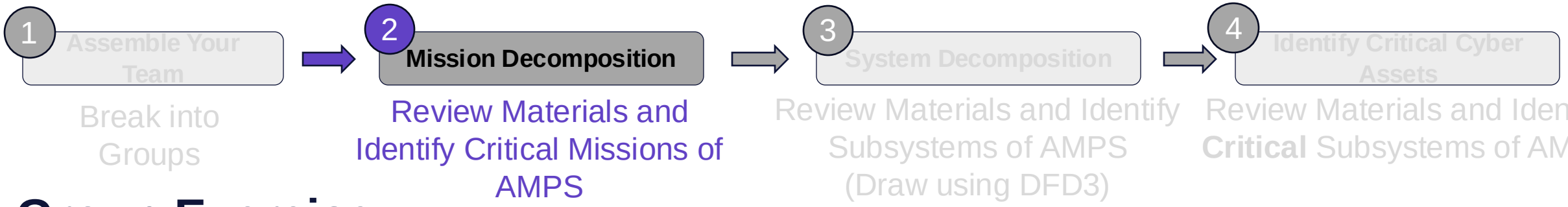


Class Exercise:

- What are some critical missions of this classroom?
  - What does it need to be able to do?

Question 1: What Are We Working On?
Mission/system Decomposition and DFDs

(20 Minutes)



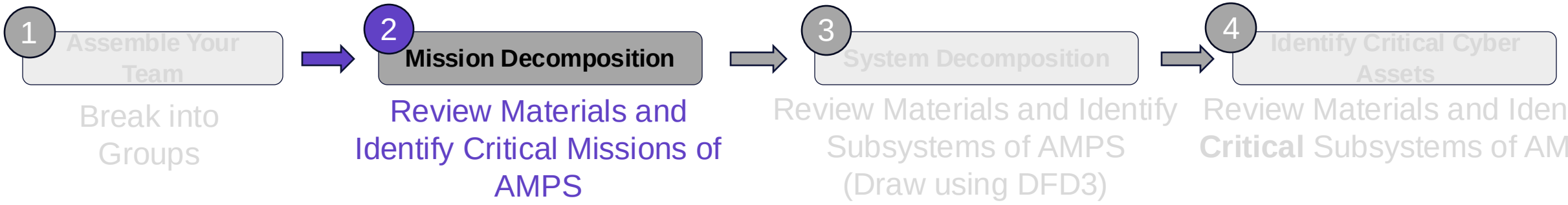
Group Exercise

Group member roles:

- **All** – Discuss ideas as a team
- **Scribe** (need pen/paper or dry-erase board)
  - Capture team ideas and list the critical missions of this device
- **Researchers** (need access to internet or can use print-outs)
  - Read through materials in reference document under Mission Decomposition and discuss possible critical missions of AMPS. Focus on below 3 sections:
    - The Ankle Monitor Predictor of Stroke System
    - AMPS Core Use Case
    - AMPS Core Technology
- **Pick someone to explain your ideas once complete**

Question 1: What Are We Working On?
Mission/system Decomposition and DFDs

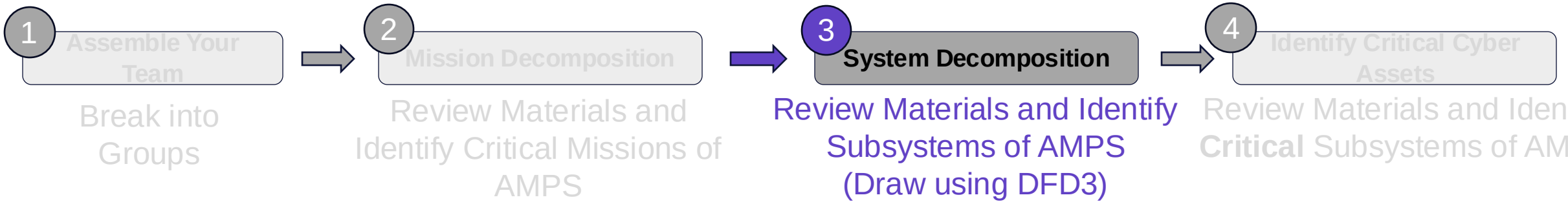
(5 Minutes)



What are some critical missions we all identified?

Question 1: What Are We Working On?
Mission/system Decomposition and DFDs

(5 Minutes)

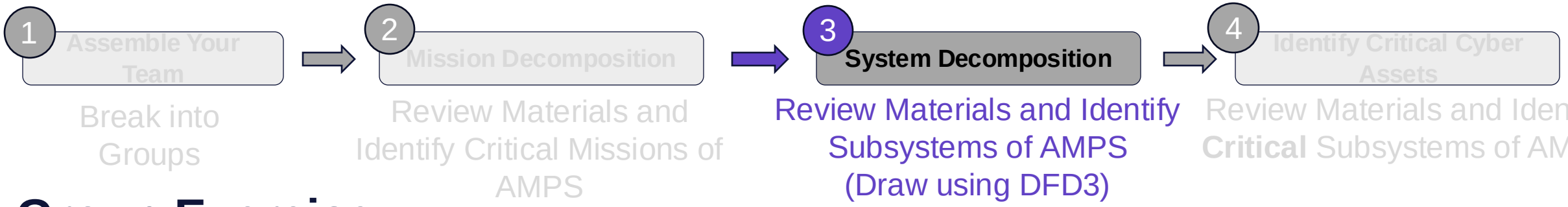


Class Exercise:

- What are some subsystems within this classroom?
  - What things make up the classroom?

Question 1: What Are We Working On?
Mission/system Decomposition and DFDs

(20 Minutes)



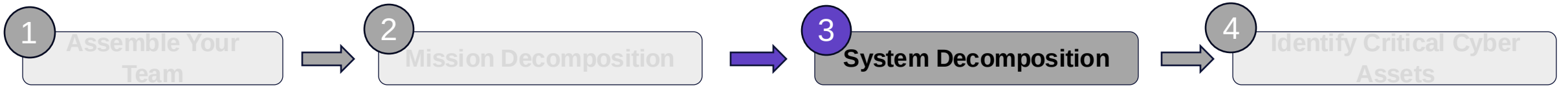
Group Exercise

Group member roles:

- **All** – Discuss ideas as a team
- **Scribe** (need pen/paper or dry-erase board)
  - Capture team ideas using DFD3 on page 5&6 - draw the AMPS subsystems
- **Researchers** (use print-outs)
  - Read through the reference materials under System Decomposition and discuss possible subsystems of AMPS. Focus on below 3 sections:
    - AMPS device
    - Patient App
    - AMPS Cloud Service
- **Pick someone to explain your diagram once complete**

Question 1: What Are We Working On?
Mission/system Decomposition and DFDs

(10 Minutes)



Break into Groups

Review Materials and Identify Critical Missions of AMPS

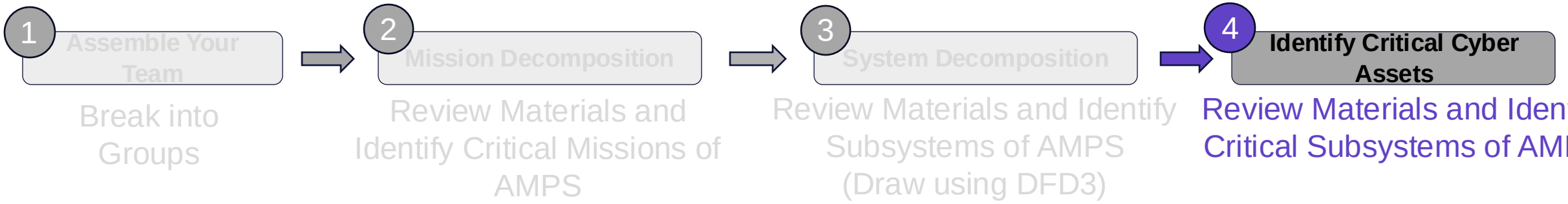
Review Materials and Identify Subsystems of AMPS (Draw using DFD3)

Review Materials and Identify **Critical** Subsystems of AMPS

What are some subsystems we all identified?

Question 1: What Are We Working On?
Mission/system Decomposition and DFDs

(10 Minutes)

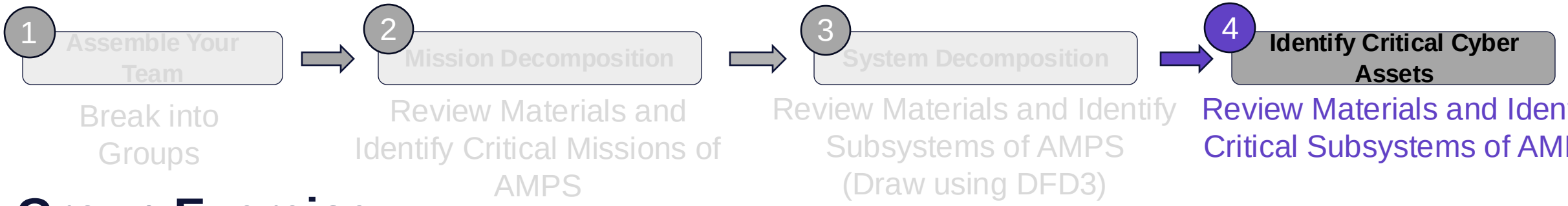


Class Exercise:

- What subsystems enable the classroom to achieve its missions?
  - What things that make up the classroom, also enable it to do what it needs to do?

Question 1: What Are We Working On?
Mission/system Decomposition and DFDs

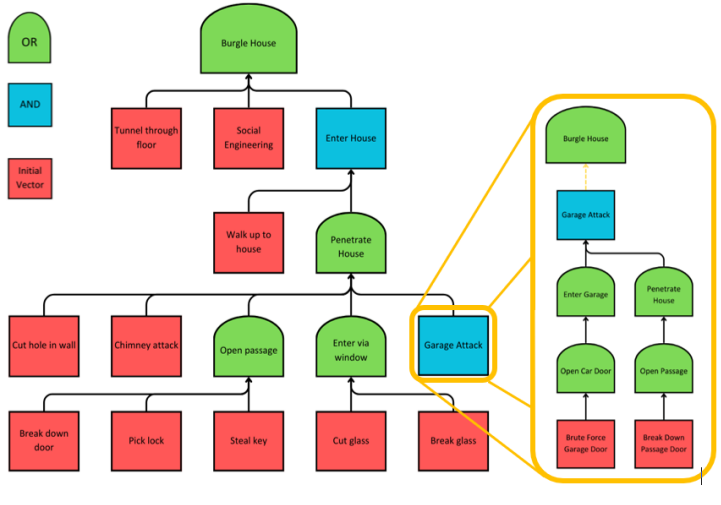
(30 Minutes)

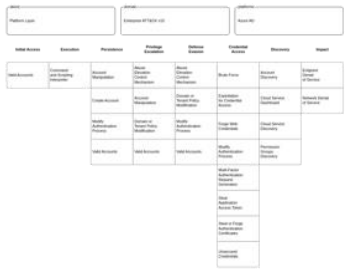


Group Exercise

Group member roles:

- **All** – Discuss ideas as a team
- **Scribe** (need pen/paper or dry-erase board)
  - Capture team ideas by notating which subsystems enable critical missions
- **Researchers** (use print-outs)
  - Review the team's previous mission and system decomposition products and discuss which of the AMPS subsystems are most critical (support the most missions).
- **Pick someone to explain your choices once complete**



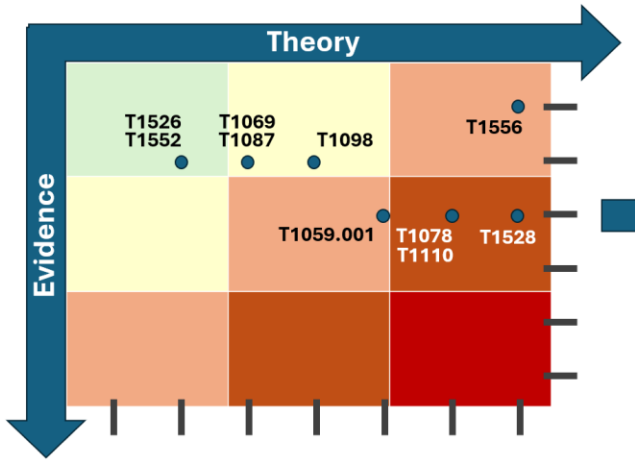


Platform Layer

Azure AD TTPs

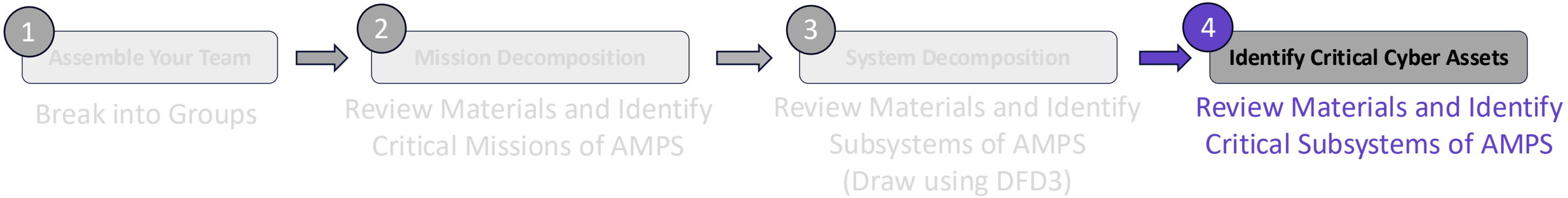
Theory
Evidence

Identify, Overlay, Score, and Prioritize Threat TTPs



TTP#	Name
T1528	Steal Application Access Token
T1078	Valid Accounts
T1110	Brute Force
T1556	Modify Authentication Process
T1059 .001	Command and Scripting Interpreter - Powershell
T1098	Account Manipulation
T1087	Account Discovery
T1069	Permission Groups Discovery
T1552	Unsecured Credentials
T1526	Cloud Service Discovery

At the end of Question 1 we have critical subsystems/components identified



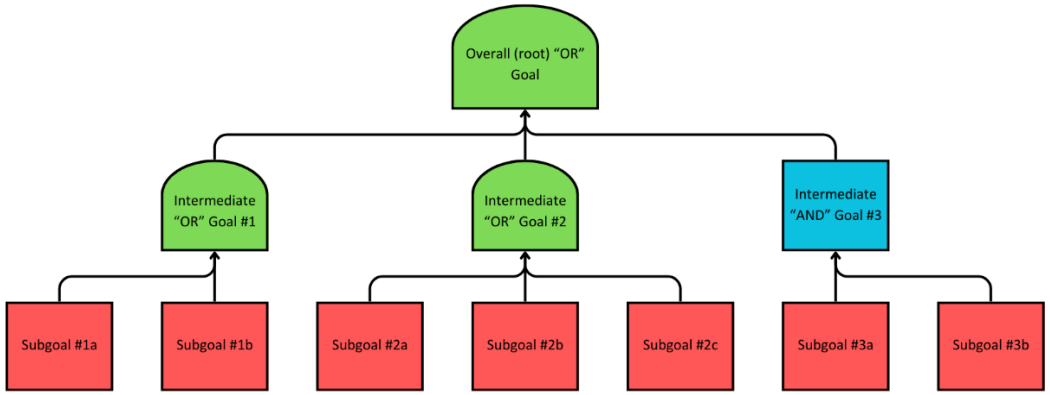
In Questions 2, we need to identify what could go wrong with these critical subsystems/components

Question 2: What could go wrong?
A good way to theorize threats to a system is to use a methodology called Attack Trees

(5 Minutes)

- An attack tree is a threat modeling technique that maps vectors an adversary can use to exploit a target.

- The arrow-shaped OR nodes within the tree represent goals that can be achieved by any of the goals below them (here, Intermediate Goal 1 OR 2 OR 3).
- The flat bottom AND nodes, similarly, are fulfilled by the goals listed beneath them. All these goals (here, Subgoal 3a AND Subgoal 3b) must be fulfilled to progress.
- The square subgoals represent the actions that must be taken to achieve their final goal.

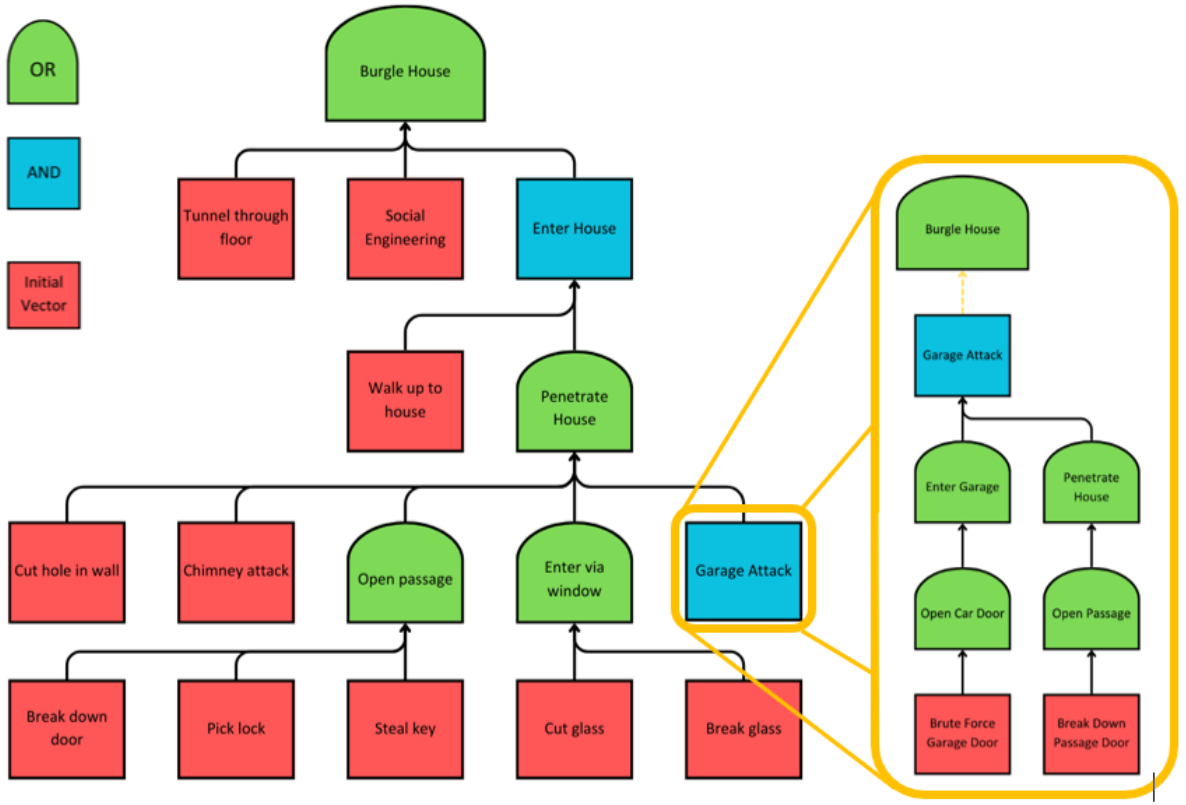


MITRE ENGENUITY | Center for Threat Informed Defense

Question 2: What could go wrong?
A good way to theorize threats to a system is to use a methodology called Attack Trees

- An attack tree is a threat modeling technique that maps vectors an adversary can use to exploit a target.

The example on the right is a simple attack tree illustrating how a burglar might break into a house.



MITRE ENGENUITY | Center for Threat Informed Defense

Question 2: What could go wrong?
A good way to theorize threats to a system is to use a methodology called Attack Trees

(5 Minutes)

- An attack tree is a threat modeling technique that maps vectors an adversary can use to exploit a target.

Class Exercise:

- A student has a quiz today that they didn't study for. They want to delay the quiz so they have more time to study. **Using an Attack Tree, describe how a bad student would stop this classroom from functioning (without getting arrested).**

Question 2: What could go wrong?
A good way to theorize threats to a system is to use a methodology called Attack Trees

(30min)

Using your same teams as before, construct an attack tree against AMPS. Assume an attacker's **goal is to access a particular users health data recorded by AMPS**. How might they do this?

Group Exercise

Group member roles:

- **All** – Discuss ideas as a team
- **Scribe** (need pen/paper or dry-erase board)
  - Capture team ideas by drawing an Attack Tree
- **Threat Analysts** (use print-outs)
  - Review threat research done against similar systems to the AMPS
  - Starting with the goal above, work backwards identifying which subsystems and components might need to be accesses to facilitate the attacker's goal. Don't worry about identifying the means/tools an attacker uses, just focus on the lateral movement across the system and possible initial access vectors.
- **Pick someone to explain your choices once complete**

Question 2: What could go wrong?
A good way to theorize threats to a system is to use a methodology called Attack Trees

(10 min)

Using your same teams as before, construct an attack tree against AMPS. Assume an attacker's **goal is to access a particular users health data recorded by AMPS**. How might they do this?

What are some common attack vectors we all identified?

(10 min)

Question 2: What could go wrong?

Now that we have a theory-based attack tree, lets look up some evidence-based threats using Cyber Threat Intelligence (CTI)

ATT&CK CTI Research Demo
Follow along here:

https://attack.mitre.org/

https://mitre-attack.github.io/attack-navigator/

MITRE ENGENUITY | Center for Threat Informed Defense

(30 min)

Question 2: What could go wrong?

Now that we have a theory-based attack tree, lets look up some evidence-based threats using Cyber Threat Intelligence (CTI)

Group Exercise

Group member roles:

- **All** – Discuss ideas as a team
- **Scribe** (need pen/paper or dry-erase board)
  - Capture team ideas by adding any new evidence-based threat vectors to the tree or notating which existing threat vectors have been confirmed in CTI reports (exist in ATT&CK)
- **Threat Analysts** (Open ATT&CK Navigator on your laptops) **https://mitre-attack.github.io/attack-navigator/**
  - Open an ATT&CK Enterprise layer
  - Down select tactics/techniques based on those used against a particular AMPS platform (maybe Azure?)
  - Compare these tactics/techniques to your attack tree
- **Pick someone to explain your choices once complete**

(10 min)

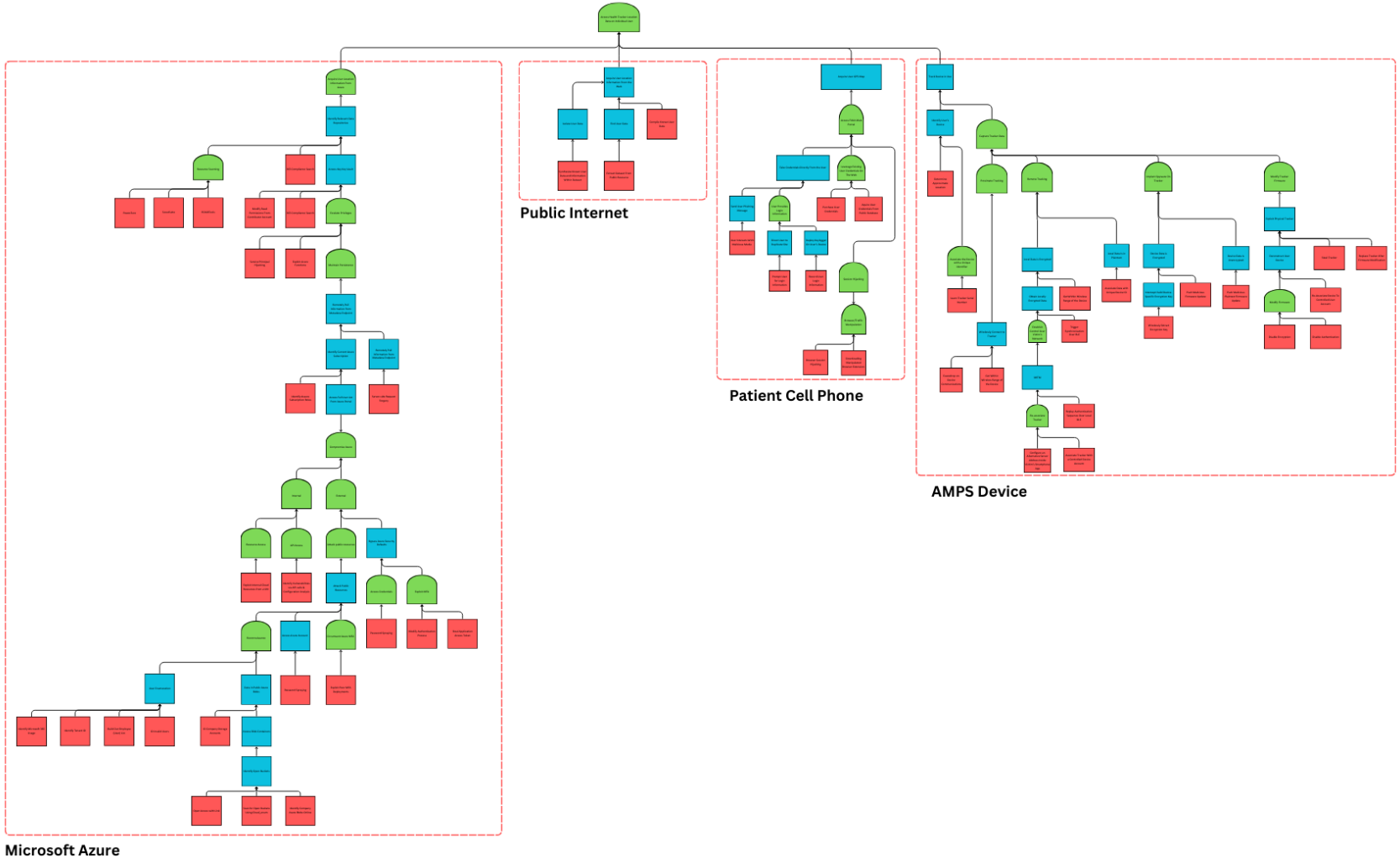
Question 2: What could go wrong?

Now that we have a theory-based attack tree, lets look up some evidence-based threats using Cyber Threat Intelligence (CTI)

What are some common attack vectors we all identified?

Question 2: What could go wrong?

Example of a completed attack tree



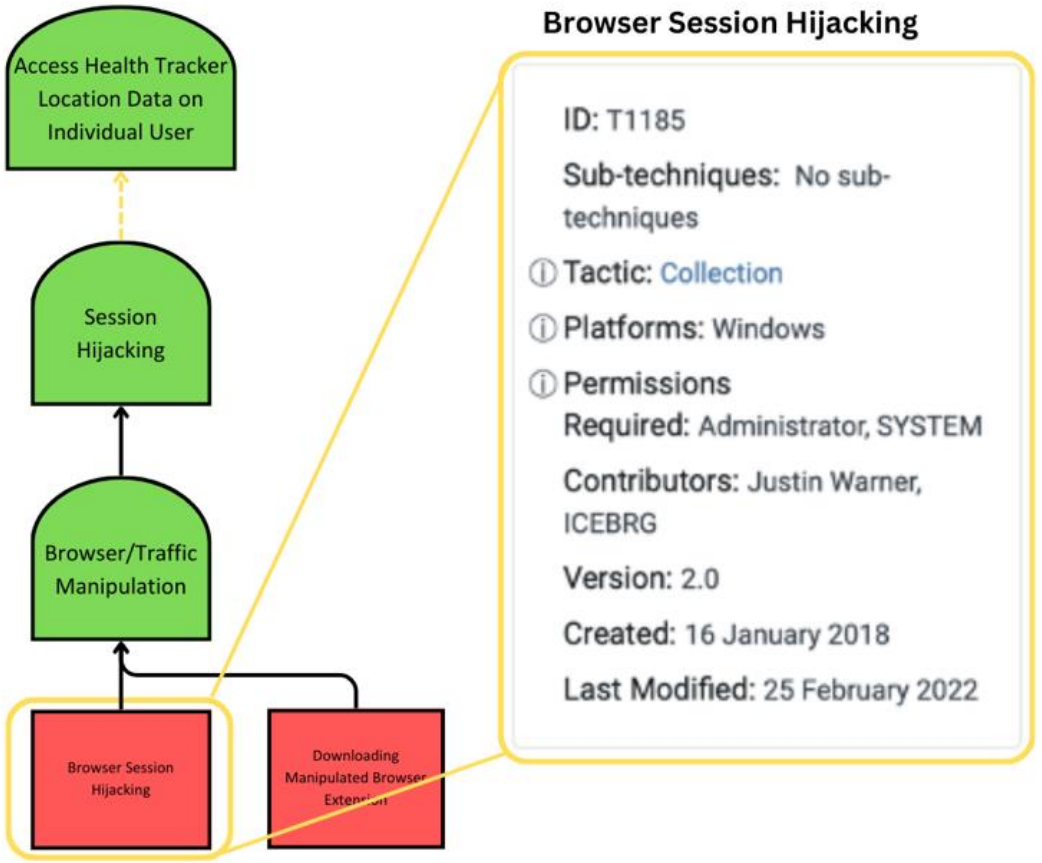
Question 2: What could go wrong?
Translating Attack Tree Nodes into ATT&CK TTPs

(10 min)

- This step is essentially the manual translation of your attack tree vectors into ATT&CK TTPs
- We do this so that we correlate necessary defensive measures to each. ATT&CK provides detection and mitigation recommendations for each adversarial TTP.

Example

- We determined one approach an attacker could use to access user data via the AMPS was by accessing the user's web portal.
- We determined that one potential vector for gaining access to the user's portal was by stealing their log-in credentials.
- We understood this could be done through a web browser but don't know much more.
- **Go to ATT&CK webpage and search "Browser" in the search bar – "Browser Session Hijacking" comes up as the appropriate TTP**



MITRE ENGENUITY | Center for Threat Informed Defense


10min Bathroom/Stretch Break
MITRE ENGENUITY
Center for Threat Informed Defense

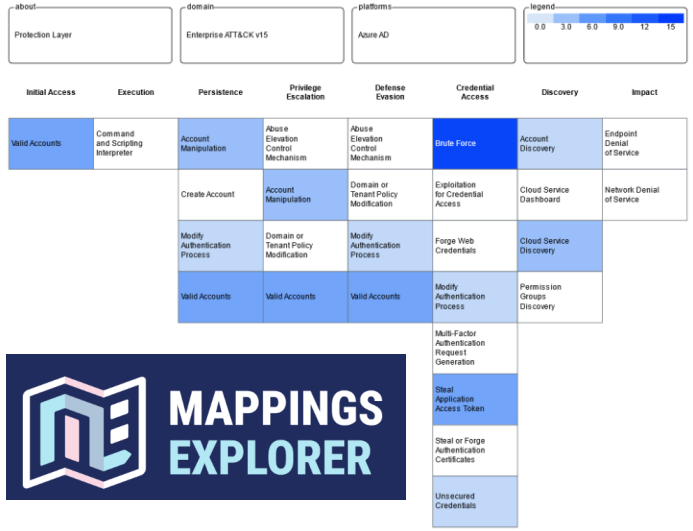
QUESTION 1 | QUESTION 2 | QUESTION 3 | QUESTION 4

What are we working on? | What could go wrong? | **What are we going to do about it?** | Did we do a good job?

Threat

+

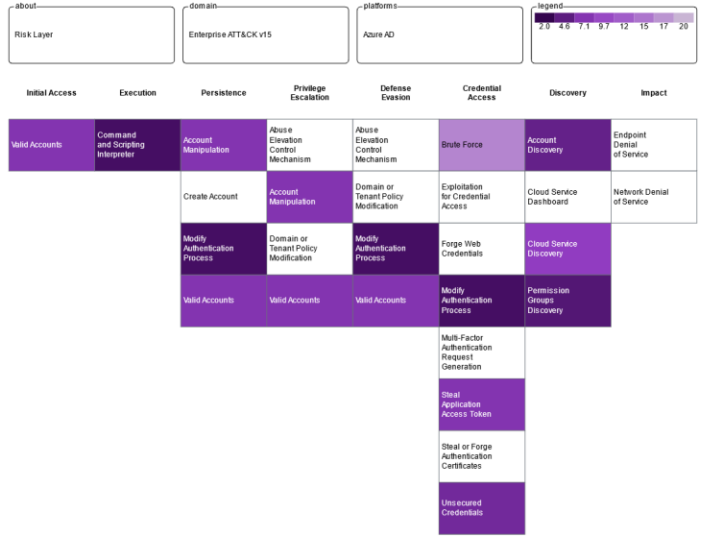
Defense



MAPPINGS EXPLORER

=

Risk



Mission Decomposition | System Decomposition | Vulnerability Identification | Cyber Threat Intelligence | **Defense & Risk Analysis** | Mitigation & Remediation | Monitoring Analysis & Evaluation

(10 min)

Question 3: What are we going to do about it?

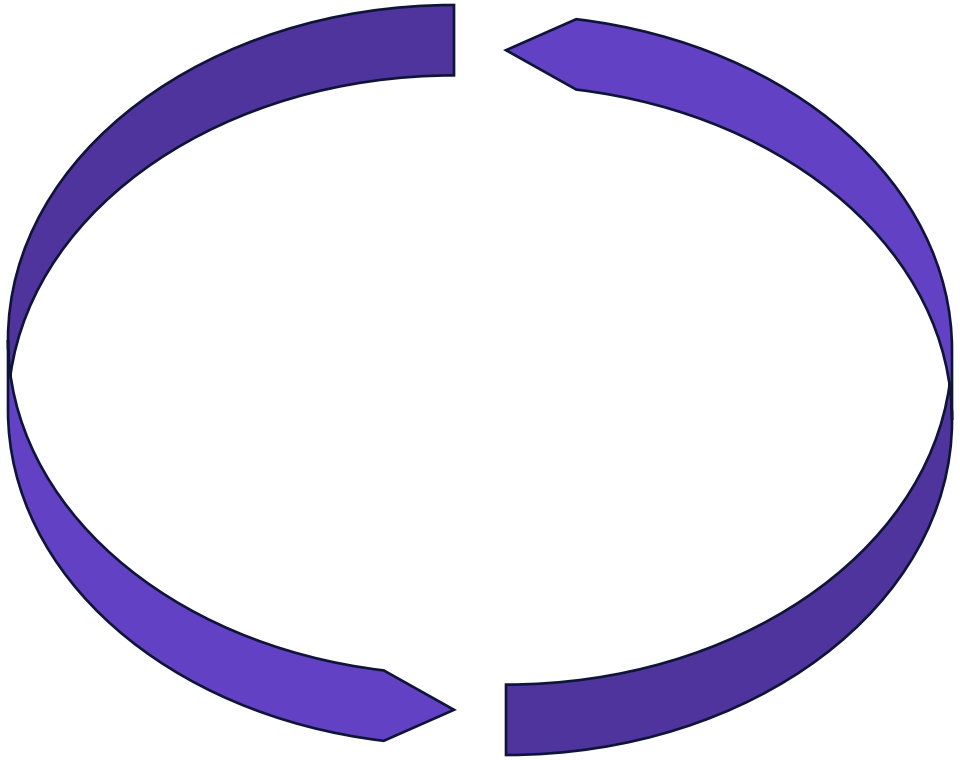
Now that we have our threat TTPs identified, we can start to look for defensive measures we can take to detect or mitigate them.

ATT&CK Detections/Mitigations Demo

Follow along here:

https://attack.mitre.org/

System Improvements



Secondary Review

(5 min)

Question 4: Did we do a good job?

At this phase of the game, you've applied some of these defensive measures and now you want to ensure these models stay up to date.

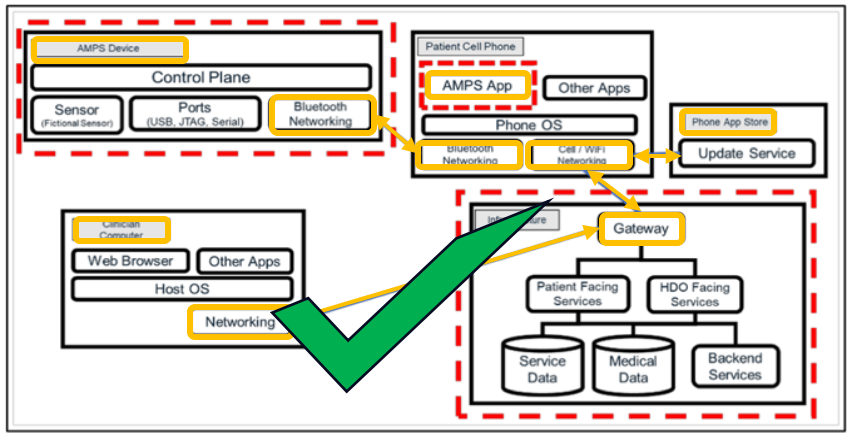
The best way to ensure your assessments stay up to date is to periodically review your system for new threats.

Also stay up to date on new detections and mitigations against the threats you've identified by periodically reviewing each TTP online.

For security teams with the appropriate amount of funding, a great next step might be to validate that your systems are performing the defensive measures you've recommended. This can be done via Red Team testing particular TTPs. A great tool for this is CALDERA.

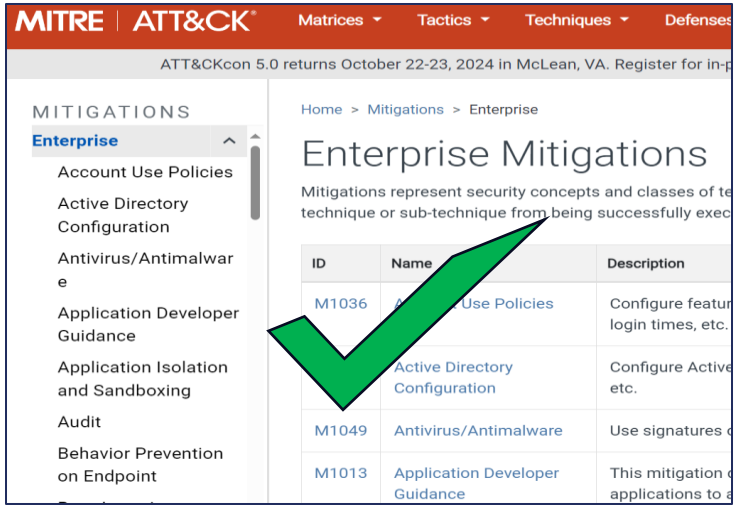
Final Products from Threat Modeling with ATT&CK

Data Flow Diagrams with Mission Critical Components Identified



Identified and Prioritized Threat Vectors Targeting These Critical Components

Mitigation and Detection Recommendations for Defenders



MITRE ENGENUITY | Center for Threat Informed Defense

That’s a wrap folks! You made it!!

Thanks for attending!

We’ll stick around for any questions you may have

https://ctid.io/our-work

MITRE ENGENUITY | Center for Threat Informed Defense