Inreat Modeling With ATT8CK

BSides Connecticut

Sept 21, 2024



Center for Threat Informed Defense

Your Gracious Hosts



Tyler Schechter Project Leader

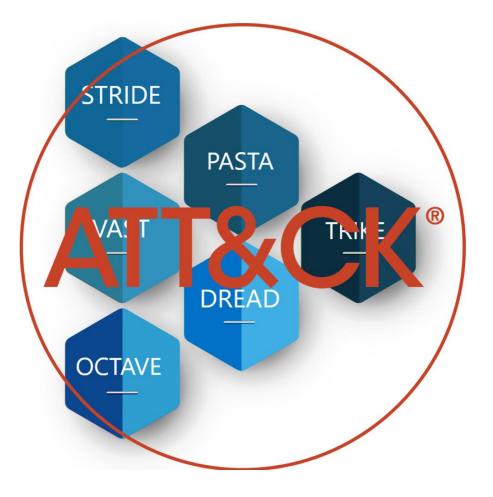


Ben Ballard Technical Leader



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.





- 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

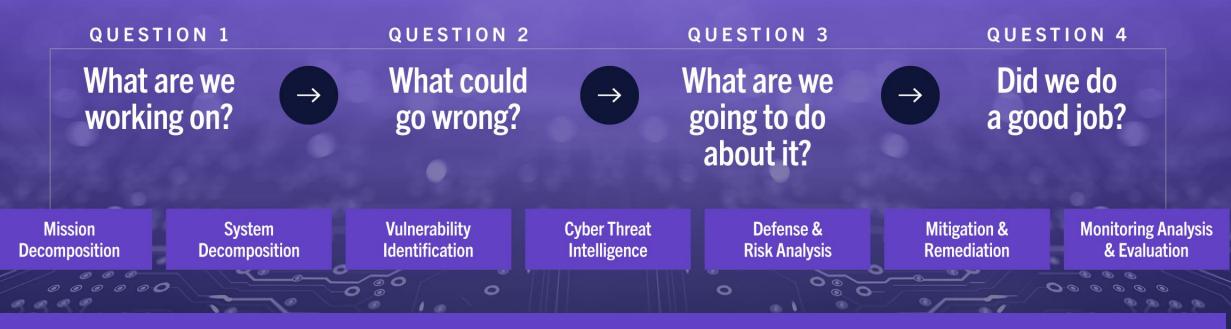


A Brief Overview of Threat Modeling



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

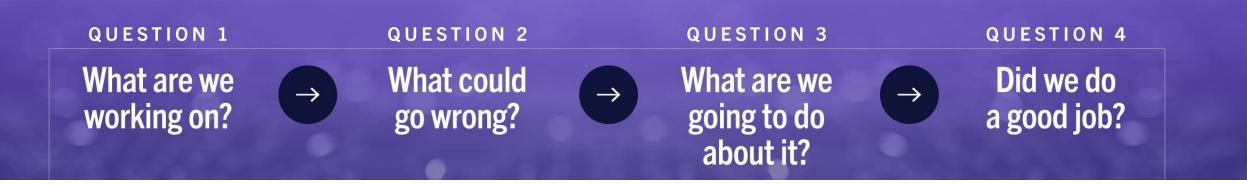


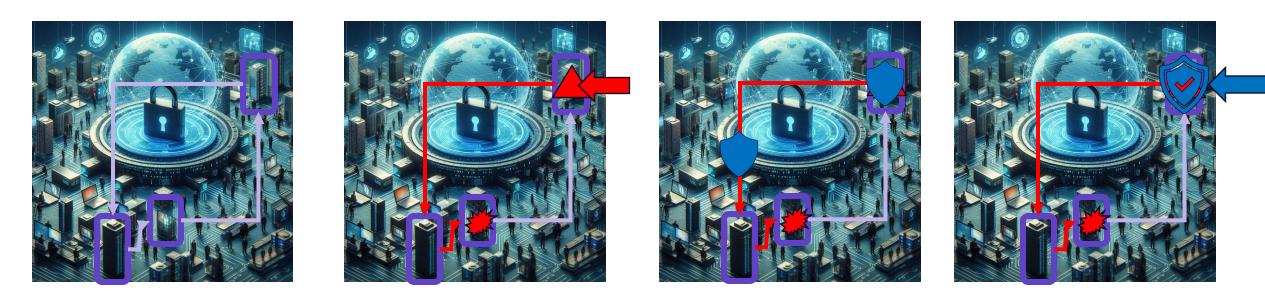
Organizations have **limited budgets** to protect their systems and data. We **threat model to help prioritize defensive investments** where they are needed most.



HOW:

Answer the 4 Questions!







A Brief Overview of ATT&CK



Center for Threat Informed Defense

ATT&CK®

ATT&CK is a **globallyaccessible** 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



Search Victim-Owned Websites	
🗮 Has sub-techniques	

RECONNAISSANCE

10 techniques

Active Scanning

Host Information

Gather Victim Identity

Gather Victim Network

Phishing for Information

Search Closed Sources

Search Open Technical Databases

Websites/Domains

Search Open

Gather Victim Org

Gather Victim

Information

nformation

Information

RESOURCE DEVELOPMENT

8 techniques

Acquire Infrastructure

Compromise Accounts

Establish Accounts

Obtain Capabilities

Develop Capabilities

Stage Capabilities

Acquire Access

Compromise Infrastructure

MITRE	ATT&CK [®]
Enterprise	Framework

INITIAL ACCESS

9 techniques

Valid Accounts

Replication Through

Trusted Relationship

Hardware Additions

Application

Phishing

Exploit Public-Facing

Supply Chain Compromise

External Remote Services

Drive-by Compromise

Removable Media

EXECUTION

14 techniques

Windows Management

Software Deployment Tools

Instrumentation

Shared Modules

User Execution

System Services

Execution

Interpreter

Native AP

Inter-Process

Command

Command

Communication

Deploy Container

Serverless Execution

Cloud Administration

Exploitation for Client

Command and Scripting

Container Administration

PERSISTENCE

19 techniques

Scheduled Task/Job

Account Manipulation

Create Account

Browser Extensions

Traffic Signaling

Server Software

Compromise Client

Implant Internal Image Modify Authentication Process

Software Binary

Component

Pre-OS Boot

BITS Jobs

External Remote Services

Office Application Startup

attack.mitre.org

chniques	42 techniques	17 techniques	31 techniques	9 techniques
≡	Modify Auther	itication Process =	System Service Discovery	Remote Services
counts	=	Networl	k Sniffing	Software Deployment Tools
ecution F l ow	=	OS Credential Dumping =	Application Window Discovery	Replication Through
≡	Direct Volume Access	Input Capture =	System Network =	Removable Media
=	Rootkit	Brute Force =	Configuration Discovery	Internal Spearphishing
=	Obfuscated Files = or Information	Two-Factor Authentication Interception	System Owner/User Discovery	Use Alternate Authentication Material
Process	Injection =	Exploitation for Credential Access	System Network Connections Discovery	Lateral Tool Transfer
Access Token	al obtion	Steal Web Session Cookie	Permission Groups =	Taint Shared Content
Abuse Elevation C		Unsecured Credentials =	Discovery	Exploitation of Remote Services
Domain Policy		Credentials from =	File and Directory Discovery	Remote Service Session
	Indicator Removal on Host 🛛 🗧	Password Stores	Peripheral Device	Hijacking
Privilege	Modify Registry	Steal or Forge Kerberos	Discovery	
	Trusted Developer Utilities = Proxy Execution	Tickets Forced Authentication	Network Share Discovery	
	Traffic Signaling	Steal Application	Password Policy Discovery	
	Signed Script Proxy	Access Token	Browser Information	
	Execution	Adversary-in-the-Middle =	Discovery	
	Rogue Domain Controller Indirect Command	Forge Web Credentials 🛛 😑	Virtualization/Sandbox Evasion	
	Execution	Multi-Factor Authentication	Cloud Service Dashboard	
	BITS Jobs	Request Generation	Software Discovery =	
	XSL Script Processing	Steal or Forge Authentication Certificates	Query Registry	
	Template Injection	Gertindates	Remote System Discovery	
	File and Directory Permissions Modification		Network Service Scanning	
	Virtualization/Sandbox		Process Discovery	
	Evasion Unused/Unsupported Cloud Regions	-	System Information Discovery	
	Use Alternate =	-	Account Discovery =	
	Authentication Material		System Time Discovery	
	Impair Defenses		Domain Trust Discovery	
	Hide Artifacts =		Cloud Service Discovery	
	Masquerading =		Container and Resource	
	Deobfuscate/Decode Files = or Information		Discovery Cloud Infrastructure	
	Signed Binary Proxy Execution		Discovery	
	Exploitation for Defense Evasion	-	System Location Discovery Cloud Storage Object	
	Execution Guardrails		Discovery Group Policy Discovery	
	Modify Cloud Compute	-	Debugger Evasion	
	Infrastructure Pre-OS Boot =	_	Device Driver Discovery	
	110 00 0000	-	,]
	Build Image on Host			
	Deploy Container	-		
	Modify System Image	-		
	Network Boundary Bridging	-		
	Weaken Encryption =	-		
	Reflective Code Loading	-		
	Debugger Evasion			
	Plist File Modification			

CREDENTIAL ACCESS

DISCOVERY

LATERAL MOVEMENT

PRIVILEGE ESCALATION

13 techniques

Valid Accounts

Boot or Logon Initialization Scripts

Create or Modify System Process

Event Triggered Execution

Boot or Logon Autostart Execution

Escape to Host

Escalation

Exploitation for Privilege

Hijack Execution Flow

DEFENSE EVASION

Browser Session Hijacking		Remote Access Software
Data from Information	Ξ	Dynamic Resolution 🛛 🗮
Repositories Adversary-in-the-Middle Archive Collected Data		Non-Standard Port
		Protocol Tunneling
		Encrypted Channel =
Data from Network Shared Drive		Non-Application Layer
Data from Cloud Storage Object		Protocol
Data from Configuration Repository	Ξ	

COLLECTION

17 techniques

Data from Local System

Data from Removable

Media

Input Capture

Data Staged

Creen Capture

Email Collection

Clipboard Data

Audio Capture

Video Capture

Automated Collection

COMMAND AND CONTROL

16 techniques

Data Obfuscation

Fallback Channels

Removable Media

Multi-Stage Channels

Ingress Tool Transfer

Web Service

Data Encoding

Traffic Signaling

Proxv

Application Layer Protoco

Communication Through

EXFILTRATION

9 techniques

Exfiltration Over Other Network Medium

Scheduled Transfer

Exfiltration Over

Exfiltration Over

Physical Medium

Exfiltration Over

Automated Exfiltration

Exfiltration Over Alternative Protocol

Transfer Data to Cloud Account

Web Service

C2 Channel

Data Transfer Size Limits

MPACT

13 techniques

Data Destruction

Service Stop

Defacement

Disk Wipe

Data Manipulation

Data Encrypted for Impact

Inhibit System Recovery

Firmware Corruption

Network Denial of Service

Endpoint Denial of Service

System Shutdown/Reboot

Account Access Removal

Resource Hijacking



	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	COMM
	Scheduled Task/Job	≡	Modify Authen	tication Process \equiv	System Service Discovery	Remote Services 📃	Data from Local System	Data Obfi
		Valid Accounts	=	Network	 Sniffing 	Software Deployment Tools	Data from Removable	Fallback (
		Hijack Execution Flow	=	OS Credential Dumping \equiv	Application Window Discovery	Replication Through	Media Input Capture =-	App l icatio
	TACTIC	M/by od	Voroorv	Input Capture =	System Network =	Removable Media	- Data Staged ≡	Proxy
=	IACIIC	: Why ad	versary	Brute Force \equiv	Configuration Discovery	Internal Spearphishing	- Screen Capture	Communi Removab
	ic norfor	ming acti		Two-Factor Authentication Interception	System Owner/User Discovery	Use Alternate Authentication Material	Email Collection =	Web Serv
	12 herror	miny acu	vity _	Exploitation for Credential Access	System Network Connections Discovery	Lateral Tool Transfer	Clipboard Data	Multi-Sta
/	ternal Remote Services	Access Token	Manipulation =	Steal Web Session Cookie	Permission Groups =	Taint Shared Content	Automated Collection	Ingress To
	fice Application Startup \equiv	Abuse Elevation C		Unsecured Credentials =	Discovery	Exploitation of Remote	Audio Capture	Data Enc
	eate Account 📃	Domain Policy		Credentials from	 File and Directory Discovery 	Services Remote Service Session =	Video Capture	Traffic Sig
_	owser Extensions	Escape to Host	Indicator Removal on Host =	Password Stores	Peripheral Device	Hijacking	Browser Session Hijacking	Remote A
	affic Signaling ≡ TS Jobs	Exploitation for Privilege Escalation	Modify Registry	Steal or Forge Kerberos ≡ Tickets	Discovery	_	Data from Information =	Dynamic
	rver Software =		Trusted Developer Utilities = Proxy Execution	Forced Authentication	Network Share Discovery	-	Repositories Adversary-in-the-Middle =	Non-Stan
	omponent		Traffic Signaling =	Steal Application	Password Policy Discovery	_	Archive Collected Data	Protocol 1
Pr	e-OS Boot 🛛 🗧		Signed Script Proxy Execution		Browser Information Discovery		Data from Network	Encrypted
	ompromise Client oftware Binary	-	Rogue Domain Controller	Adversary-in-the-Middle \equiv	Virtualization/Sandbox =	-	Shared Drive	Non-Appl
	iplant Internal Image	-	Indirect Command	Forge Web Credentials =	Evasion		Data from Cloud	Protocol
	adify Authontication	-	Execution	Multi-Factor Authentication	Cloud Service Dashboard		Storage ObjectData from Configuration	
		-	BITS Jobs XSL Script Processing	Request Generation Steal or Forge Authentication	Software Discovery =		Repository	
		-	Template Injection	Certificates	Query Registry	-		
			File and Directory =		Remote System Discovery	-		
		-	Permissions Modification	-	Network Service Scanning	_		
			Virtualization/Sandbox = Evasion		Process Discovery	_		
			Unused/Unsupported Cloud Regions		System Information Discovery			
		-	Use Alternate 📃 🚍	_	Account Discovery =			
		·	Authentication Material		System Time Discovery			
R)			Impair Defenses		Domain Trust Discovery			
			Hide Artifacts =	4	Cloud Service Discovery		UITY. Center for Threat	
© 2024 N	IITRE Engenuity, LLC. Approved for Public	Release. Document number CT0126	Masquerading =	-	Container and Resource			

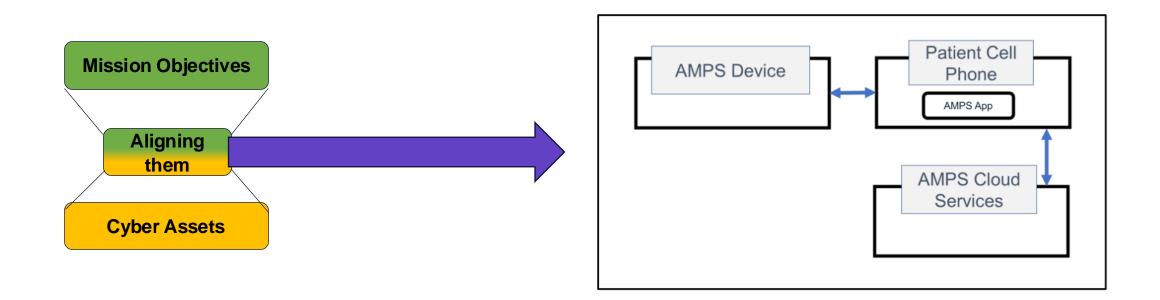
	PERSISTENCE 19 techniques	PRIVILEGE ESCALATION 13 techniques	DEFENSE EVASION 42 techniques	CREDENTIAL ACCESS 17 techniques	DISCOVERY 31 techniques	LATERAL MOVEMENT 9 techniques	COLLECTION 17 techniques	COMM
	Scheduled Task/Job	≡	Modify Authent	ication Process 🛛 🔳	System Service Discovery	Remote Services 🛛 🚍	Data from Local System	Data Obfi
		Valid Accounts	Ξ	Network	Sniffing	Software Deployment Tools	Data from Removable	Fallback (
		Hijack Execution Flow	=	OS Credential Dumping ≡	Application Window Discovery	Replication Through	Media Input Capture	App l icatio
	Boot or Logon Init	ialization Scripts 📃	Direct Volume Access	Input Capture =	System Network =	Removable Media	_ Data Staged	Proxy
=	Create or Modify	System Process =	Rootkit	Brute Force \blacksquare	Configuration Discovery	Internal Spearphishing	- Screen Capture	Communi Removabl
_	Event Trigger		Obfuscated Files \equiv	Two-Factor Authentication Interception	System Owner/User Discovery	Use Alternate = Authentication Material	Email Collection =	Web Servi
	Boot or Logon Aut	tostart Execution	or Information	Exploitation for	System Network	Lateral Tool Transfer	Clipboard Data	Multi-Sta
≡	Account Manipulation =	Process I		Credential Access	Connections Discovery	Taint Shared Content	Automated Collection	Ingress To
≡	External Remote Services Office Application Startup	Access Token		Steal Web Session Cookie	Permission Groups = Discovery	Exploitation of Remote	Audio Capture	Data Enco
	Office Application StartupImage: Create Account	Abuse Elevation Co Domain Policy		Unsecured Credentials =	File and Directory	Services	Video Canture	Traffic Sig
≡	Browser Extensions	Escape to Host	Indicator Romoval on Host =	Credentials from Password Stores	Discovery	Remote Service Session \equiv Hijacking	Browser Session Hijacking	Remote A
				Steal or Forge Kerberos 🛛 😑	Peripheral Device Discovery	Пјаски	Data from Information =	Dynamic I
	BILLUIN	IQUE: Ho	JW THE	Tickets	Network Share Discovery	-	Repositories	Non-Stan
	Se Co			Forced Authentication	Password Policy Discovery	-	Adversary-in-the-Middle =	Protocol T
	adversa	ry will ac	hieve	Steal Application Access Token	Browser Information	-	Archive Collected Data \equiv	Encrypted
				Adversary-in-the-Middle ≡	Discovery	-	Data from Network Shared Drive	Non-Appli
	their go			Forge Web Credentials =	Virtualization/Sandbox \equiv Evasion		Data from Cloud	Protocol
_		al		Multi-Factor Authentication	Cloud Service Dashboard	-	Storage Object	
	Mouny Authentication =	-	RILS JODS	Request Generation	Software Discovery =	-	Data from Configuration \equiv Repository	
		-	XSL Script Processing	Steal or Forge Authentication Certificates	Query Registry	-		
		-	Template Injection File and Directory =		Remote System Discovery	-		
			Permissions Modification		Network Service Scanning	-		
			Virtualization/Sandbox \equiv Evasion		Process Discovery	-		
		-	Unused/Unsupported		System Information	-		
		_	Cloud Regions		Discovery	-		
			Use Alternate \equiv Authentication Material		Account Discovery =	-		
R)		_	Impair Defenses		System Time Discovery	-		
		-	Hide Artifacts		Domain Trust Discovery		Center for Throat	
© 202	4 MITRE Engenuity, LLC. Approved for Public	Release. Document number CT0126	Masquerading =		Cloud Service Discovery		UITY. Center for Threat	
	5		Doobfucanto/Dooodo Eiloo		Container and Resource			

A Brief Overview of Threat Modeling With A 200



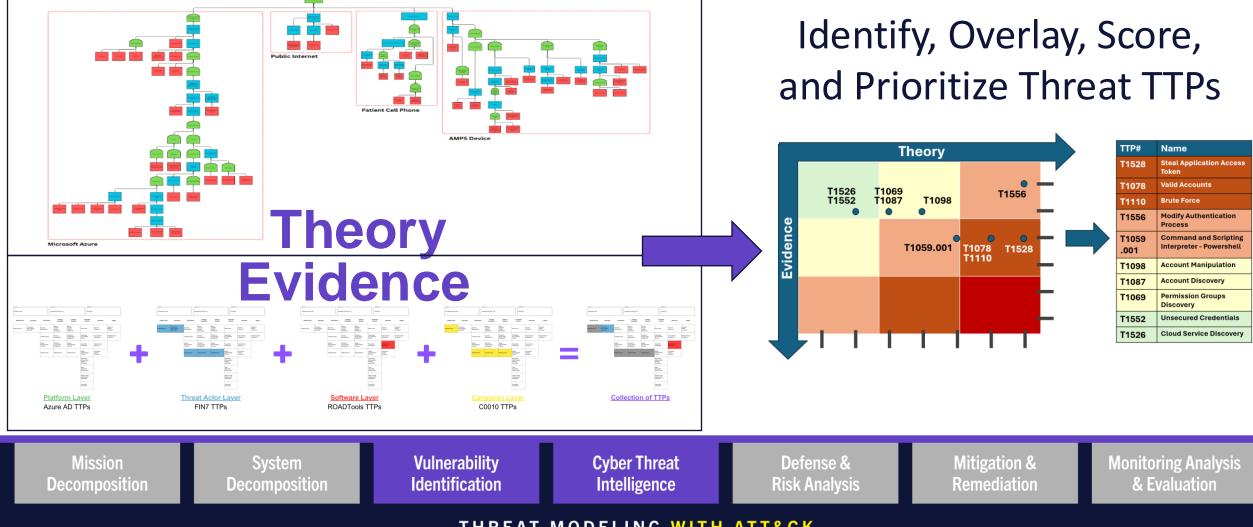
Center for Threat Informed Defense

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?





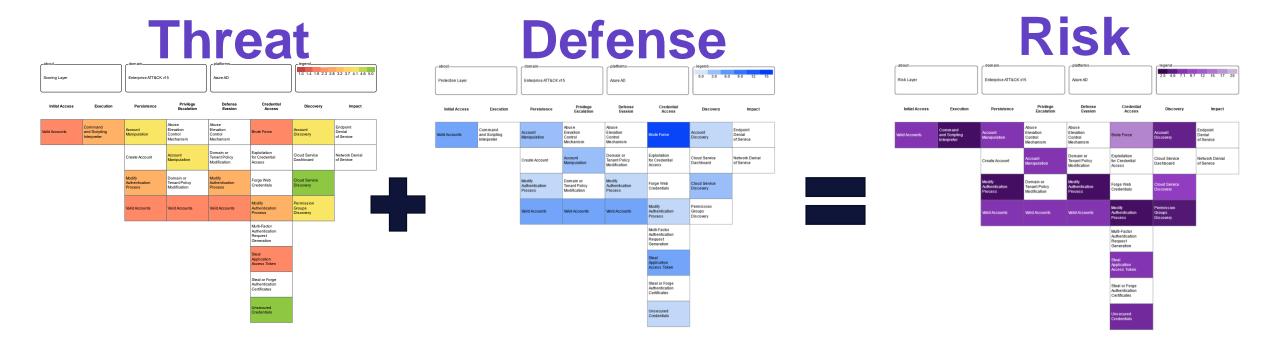
QUESTION 1	QUESTION 2	QUESTION 3	QUESTION 4
What are we working on?	What could go wrong?	What are we going to do about it?	Did we do a good job?



© 2024 MITRE Engenuity, LLC. Approved for Public Release. Document number CT0126

THREAT MODELING WITH ATT&CK

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?

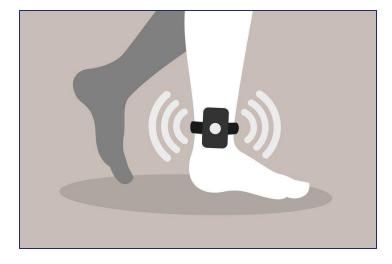




© 2024 MITRE Engenuity, LLC. Approved for Public Release. Document number CT0126

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?
System Improvement	nts		Secondary Review
Mission System Decomposition Decompositio		Threat Defense & igence Risk Analysis	Mitigation & RemediationMonitoring Analysis & Evaluation
© 2024 MITRE Engenuity, LLC. Approved for Public Release. Documen	THREAT MODELI	NG WITH ATT&CK	

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 <u>HERE</u>

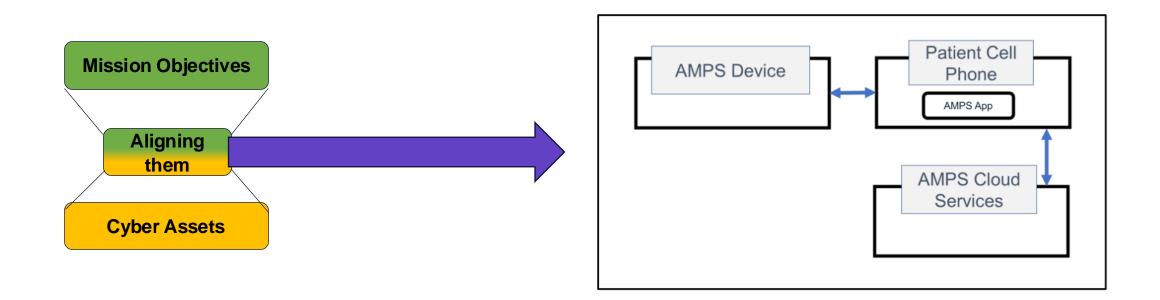
PLAYBOOK FOR THREAT MODELING MEDICAL DEVICES

November 30, 2021

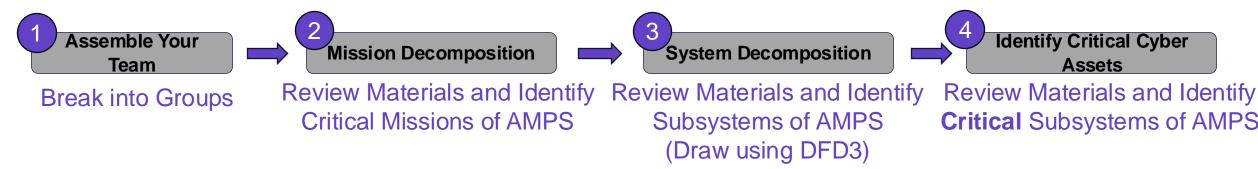




QUESTION 1	QUESTION 2	QUESTION 3	QUESTION 4
What are we working on?	What could go wrong?	What are we going to do about it?	Did we do a good job?

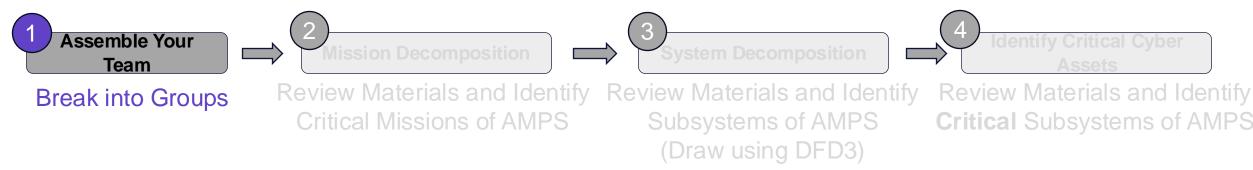








(5 Minutes)

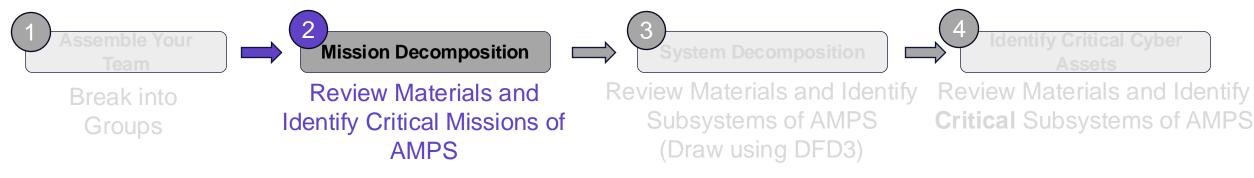


Group member roles:

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



(5 Minutes)

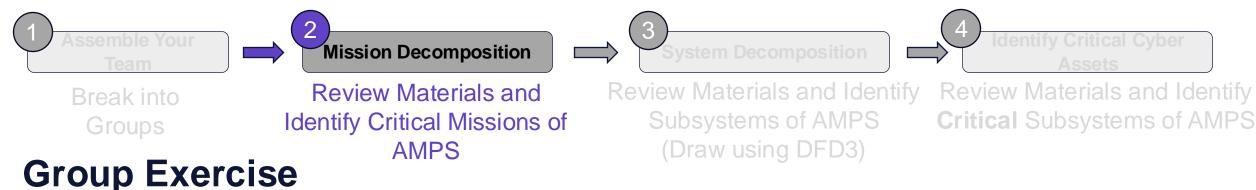


Class Exercise:

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



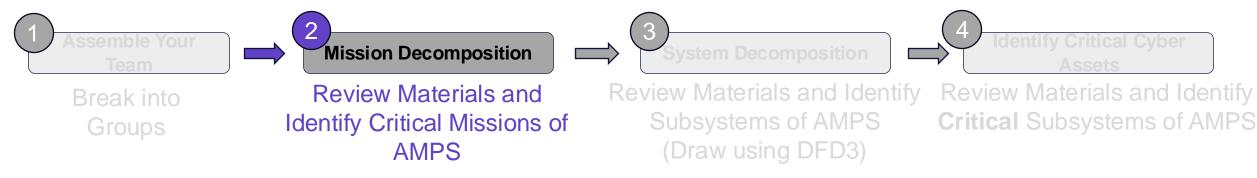
(20 Minutes)



Group member roles:

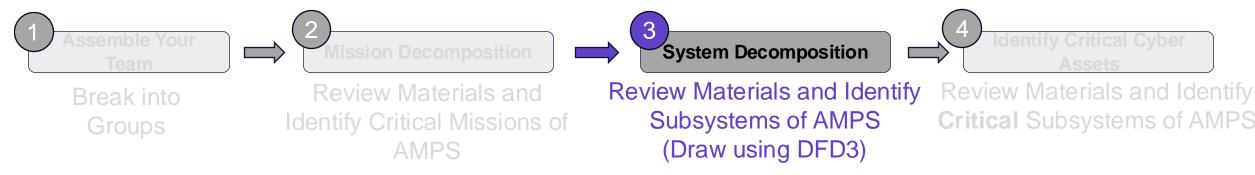
- All Discuss ideas as a team
- Scribe (need pen/paper or dry-erase board)
 - Capture team ideas and list the critical missions of this device
- **Researchers** (need access to internet or can use print-outs)
 - Read through materials in reference document under Mission Decomposition and discuss possible 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

(5 Minutes)



What are some critical missions we all identified?

(5 Minutes)

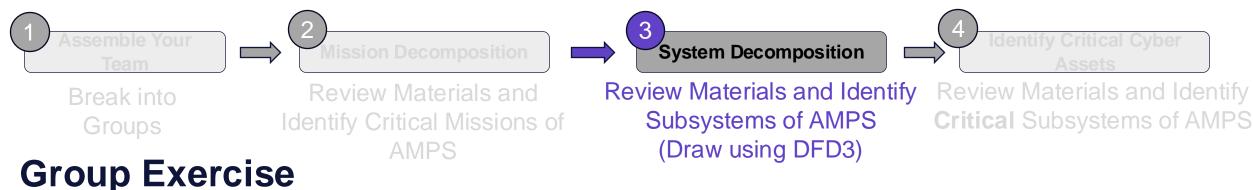


Class Exercise:

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



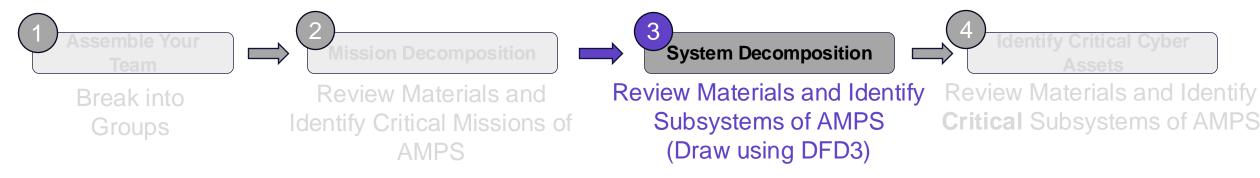
(20 Minutes)



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

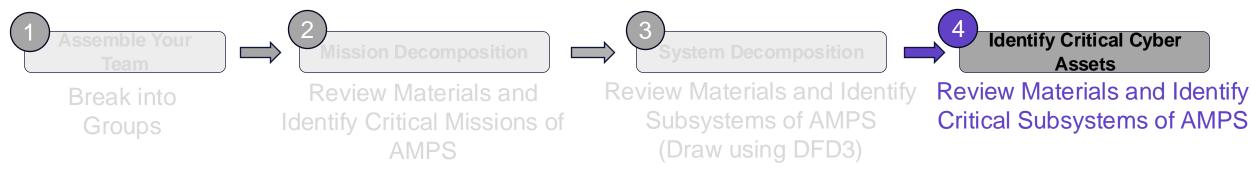
(10 Minutes)



What are some subsystems we all identified?



(10 Minutes)

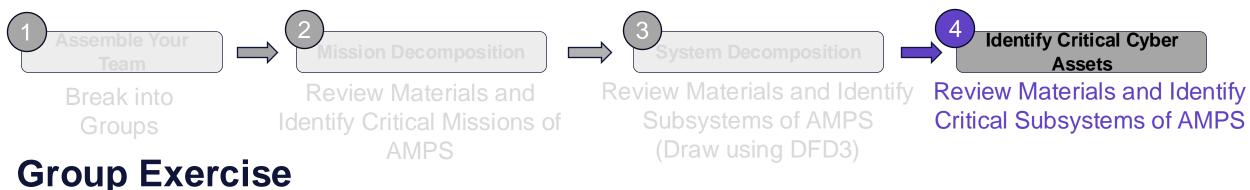


Class Exercise:

- 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?



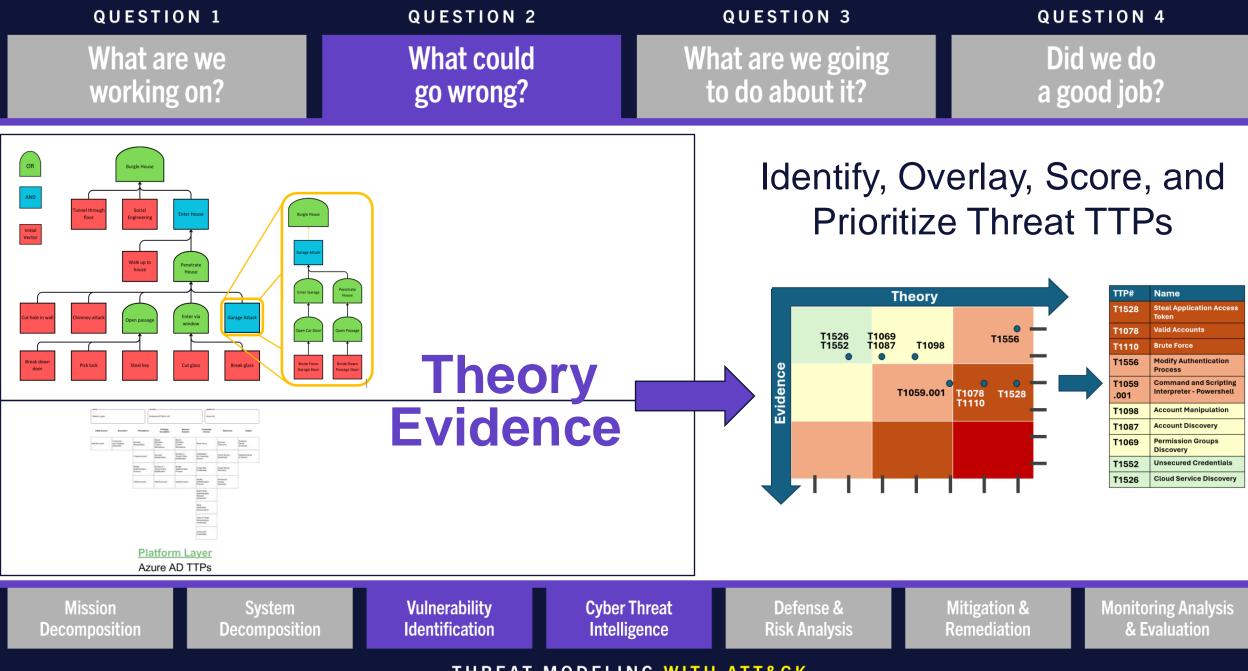
(30 Minutes)



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

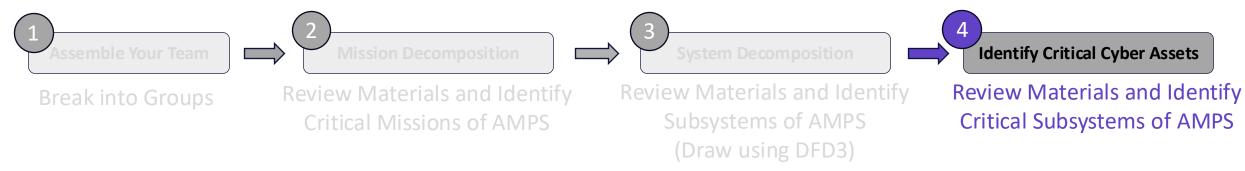




© 2024 MITRE Engenuity, LLC. Approved for Public Release. Document number CT0126

THREAT MODELING WITH ATT&CK

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

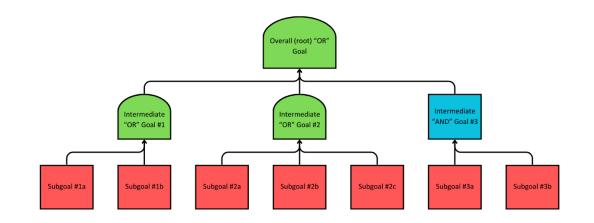


In Questions 2, we need to identify what could go wrong with these critical subsystems/components



Question 2: What could go wrong?(5 Minutes)A good way to theorize threats to a system is to use amethodology called Attack Trees

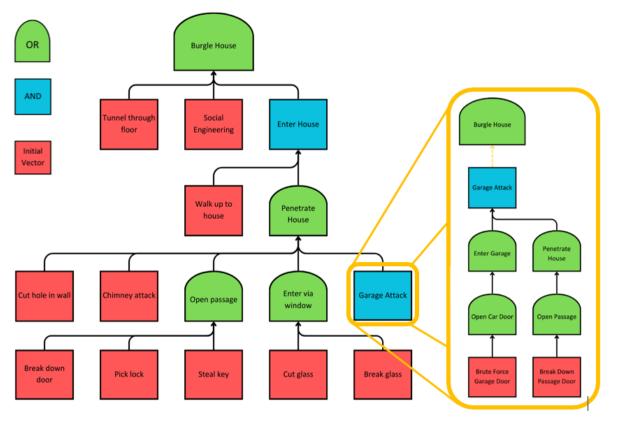
- An attack tree is a threat modeling technique that maps vectors an adversary can use to exploit a target.
- The arrow-shaped OR nodes within the tree represent goals that can be achieved by any of the goals below them (here, Intermediate Goal 1 OR 2 OR 3).
- The flat bottom AND nodes, similarly, are 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.



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

• 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.





Question 2: What could go wrong?(5 Minutes)A good way to theorize threats to a system is to use amethodology called Attack Trees

• 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 <u>Attack Trees</u>

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 <u>Attack Trees</u>

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/





(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



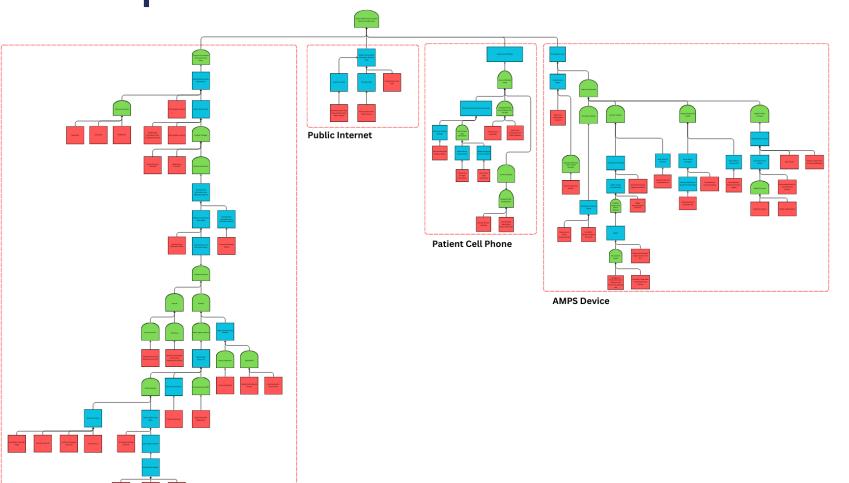
Question 2: What could go wrong?

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



Microsoft Azure

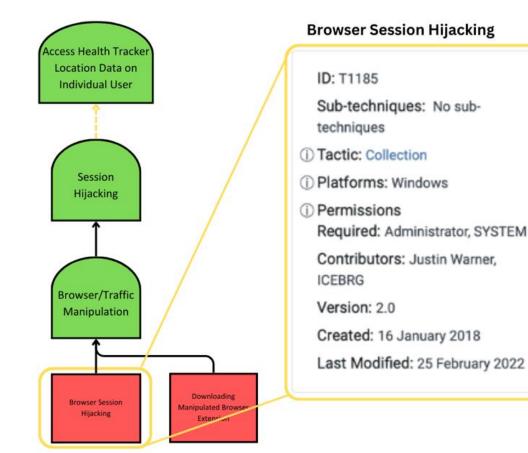


Question 2: What could go wrong? Translating Attack Tree Nodes into ATT&CK TTPs

- 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





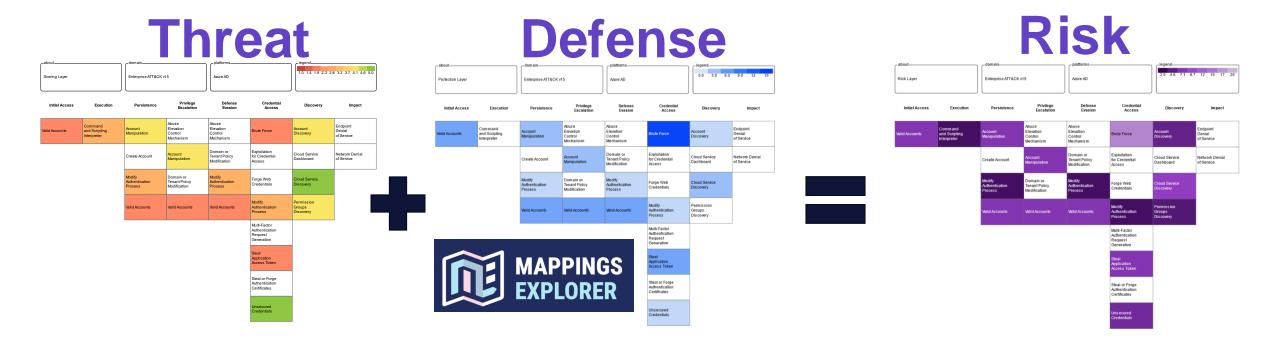
(10 min)

10min Bathroom/Stretch Break



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?





© 2024 MITRE Engenuity, LLC. Approved for Public Release. Document number CT0126

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/





QUESTIC)N 1	QUESTION 2		QUESTION 3	QUI	QUESTION 4	
What are working		What could go wrong?		nat are we going o do about it?		Did we do a good job?	
Syster Improv	n /ement	S			Seco	ondary ew	
Mission Decomposition	System Decomposition	Vulnerability Identification	Cyber Threat Intelligence	Defense & Risk Analysis	Mitigation & Remediation	Monitoring Analysis & Evaluation	

THREAT MODELING WITH ATT&CK



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.

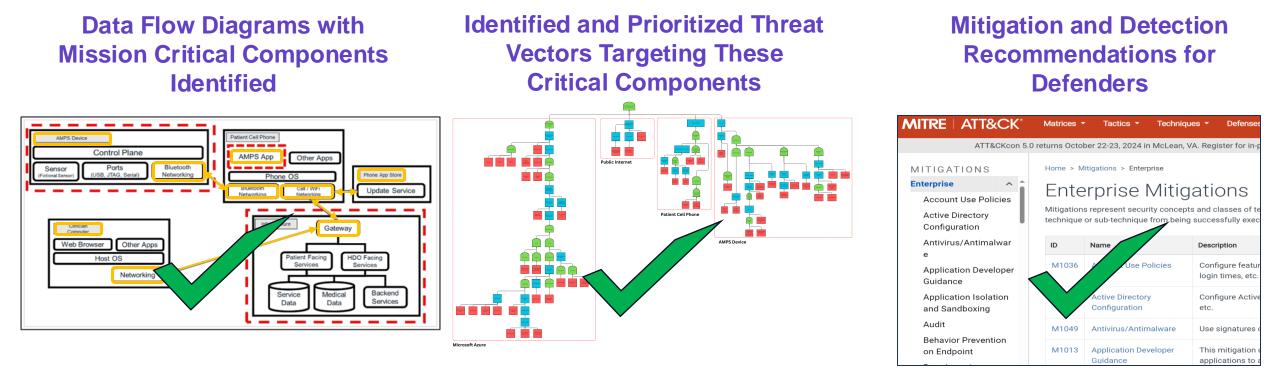
The best way to ensure your assessments stay up to date is to periodically review your system for new threats.

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





Thanks for attending!

We'll stick around for any questions you may have

https://ctid.io/our-work



