From Walls to Webs:

Transforming Cyber Defense through Active Adversary Engagement with MITRE Engage

Presented By –

Jalaj Bhaskar @ CyberSangam
7th June 2025
Microsoft, Noida

$~ whoami

- Blue Teamer

Talks about Security Operations, Incident Response, Threat Hunting, Cloud Security, Security Engineering, or anything cyber security…

Rech out!!

- Telegram : @senditfast
- LinkedIn : linkedin.com/in/teamblue

Purpose of this presentation

- Understanding basics of MITRE Engage
- Need of Active adversary engagement
- Mitre Engage Matrix
- Bridge Mitre Engage and Mire Att&ck
- Getting started with tools
- Ethical and Strategic Challenges
- QnA

What is MITRE Engage ?

MITRE Engage is a framework that helps defenders **plan, implement, and evaluate**

Strategies for

Denial , Deception, and **adversary engagement**

✓Compliments Mitre Att&ck

✓Focusses on shaping **attacker's experience**

✓Helps defenders **Collect Intel** , **Slow attacks** and **gain advantage**

✓Supports **proactive, interactive defense** rather than passive detection

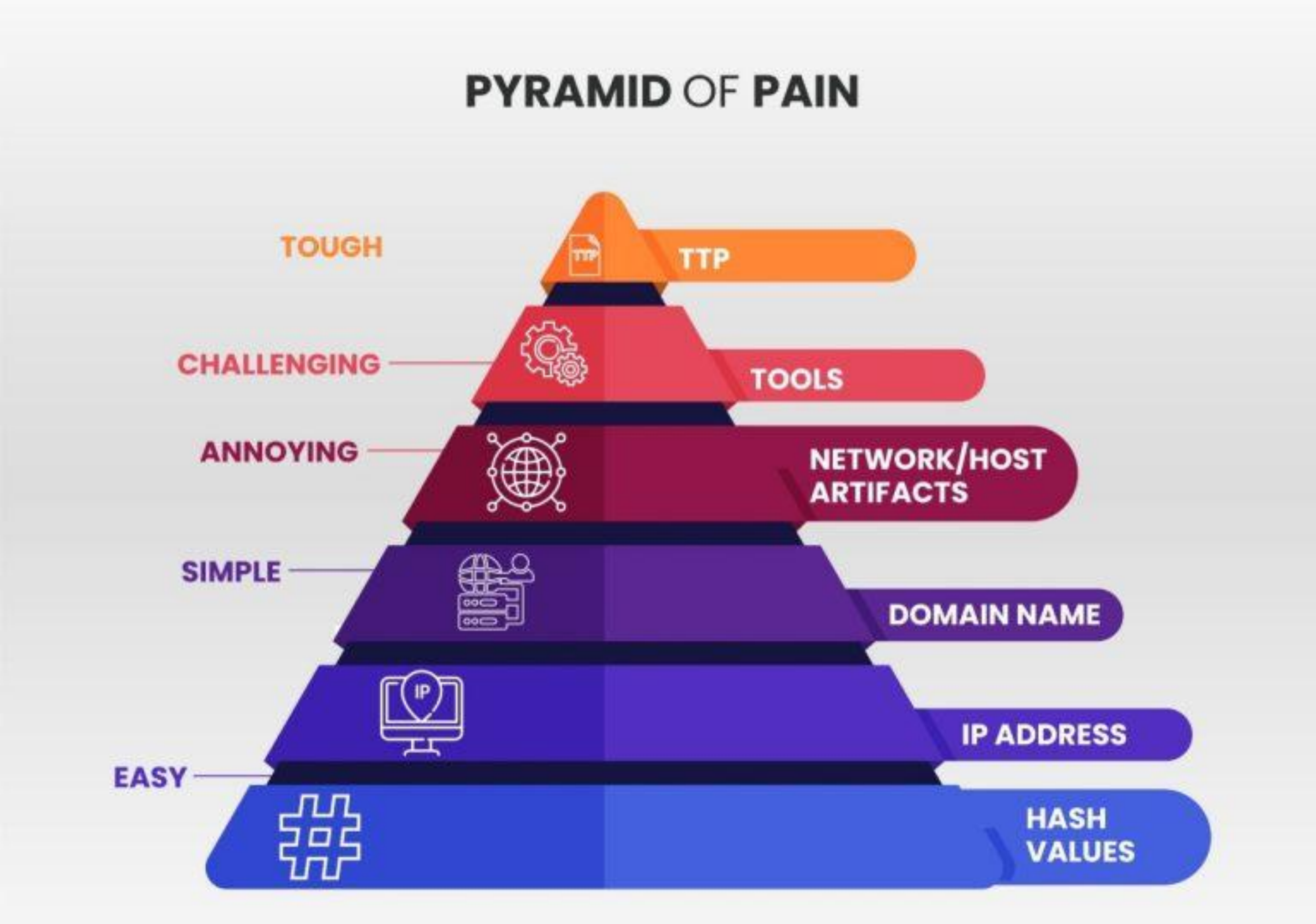
How does it compare with MITRE ATT&CK

	MITRE ATT&CK	MITRE Engage
Purpose	Describes adversary behaviour	Guides defender actions
Focus	Tactics, Techniques, and Procedures	Denial, Deception and Engagement
Use case	Threat Intel, Detection, threat modelling	Deception planning, adversary engagement
Perspective	Adversary-centric	Defender-centric
Outcome	Better detection and understanding	Better disruption and control

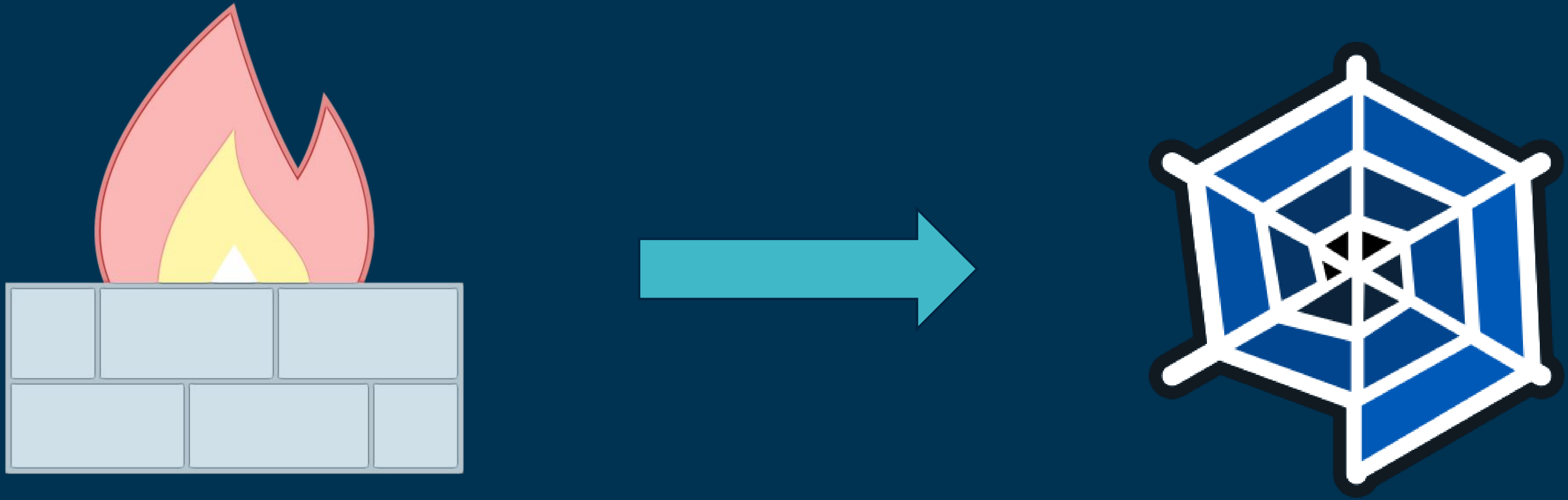
What do we gain from adversary engagement ?

- ✓ Attacker TTPs
- ✓ High Fidelity alerts
- ✓ Insider threat detection
- ✓ IoC in real time
- ✓ Attack path visibility
- ✓ Wasting attacker’s tim
- ✓ Operational disruption
- ✓ Attribution clues
- ✓ Behaviorral Intel
- ✓ Chasing ghosts: effect
- ✓ Building attacker profile
- ✓ Safe engagement sandbox

Disrupting the Adversary at their Weekest Point

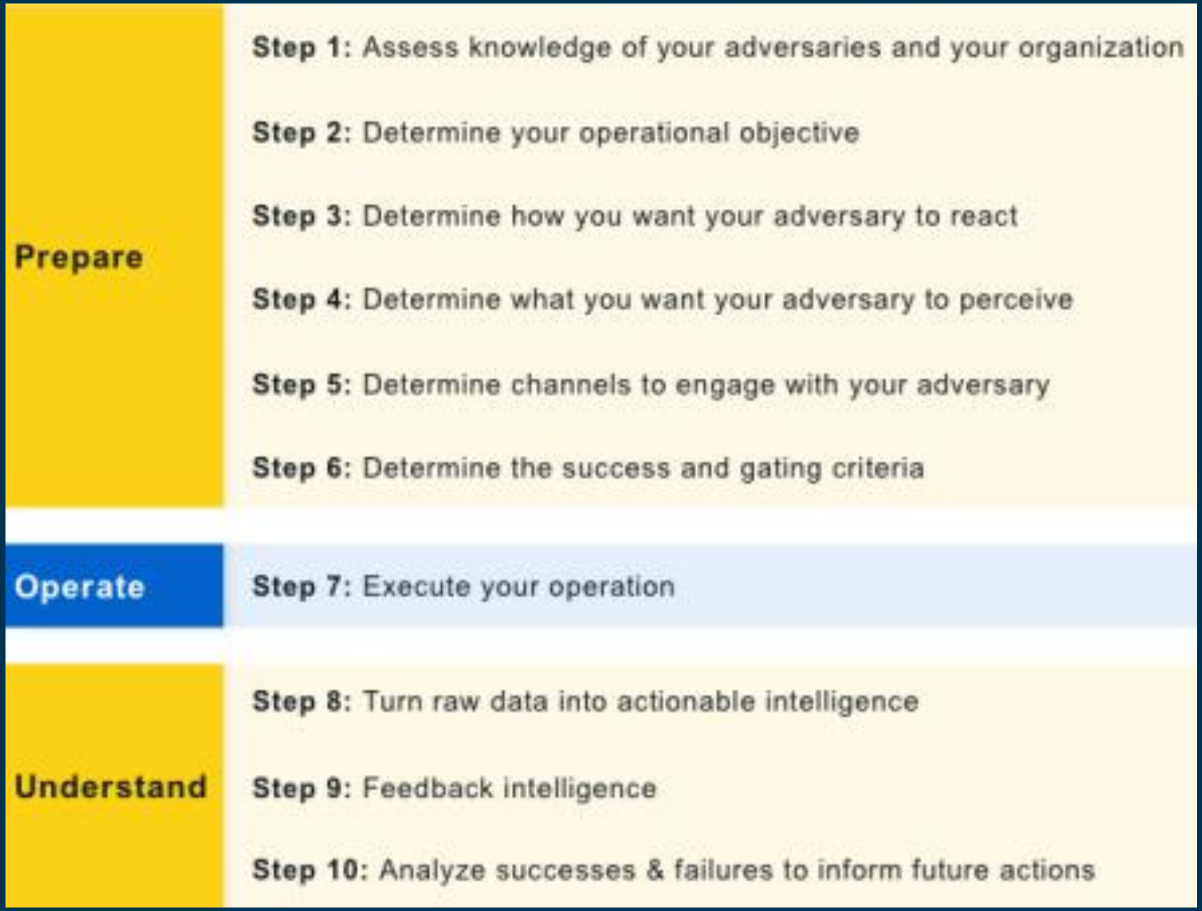


Not a Wall. A web.



MITRE Engage matrix

It is not an accident that engagement activities fall into the category with the least number of steps in the Process. While engagement activities often get the spotlight, the most important elements of any operation are the strategic actions taken to prepare for and understand the results of your operation

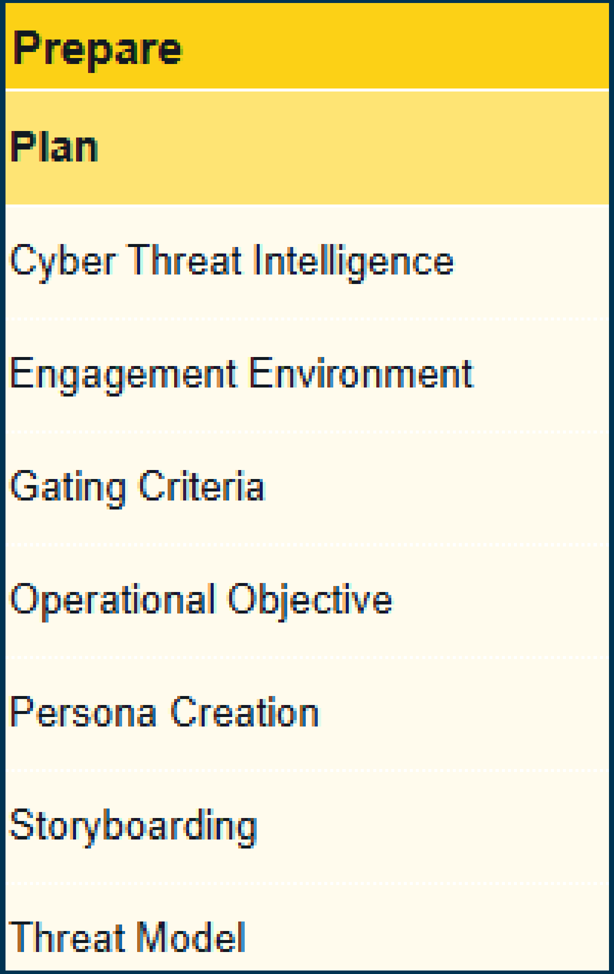


Prepare	**Step 1:** Assess knowledge of your adversaries and your organization
	Step 2: Determine your operational objective
	Step 3: Determine how you want your adversary to react
	Step 4: Determine what you want your adversary to perceive
	Step 5: Determine channels to engage with your adversary
	Step 6: Determine the success and gating criteria
Operate	**Step 7:** Execute your operation
Understand	**Step 8:** Turn raw data into actionable intelligence
	Step 9: Feedback intelligence
	Step 10: Analyze successes & failures to inform future actions

MITRE Engage matrix

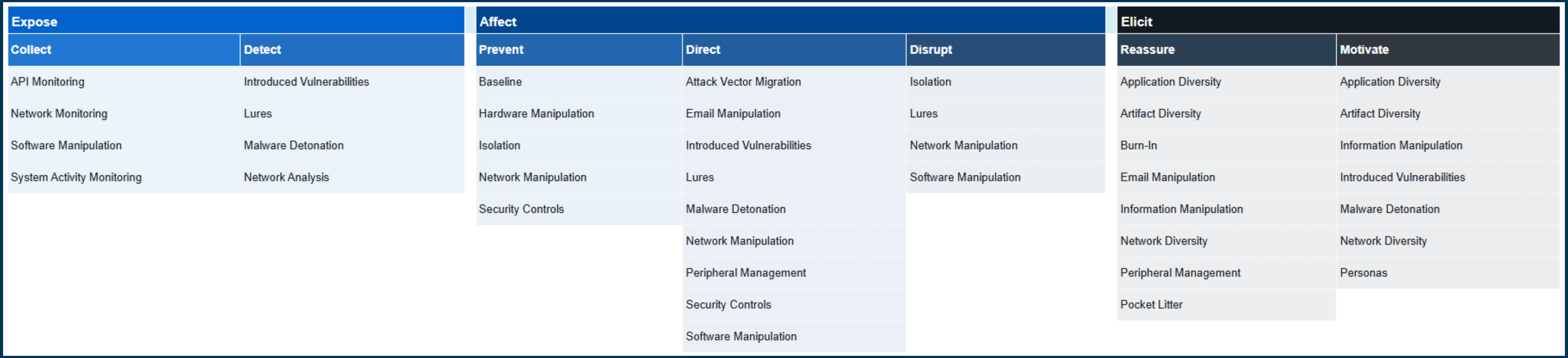
Prepare	Expose		Affect			Elicit		Understand
Plan	**Collect**	**Detect**	**Prevent**	**Direct**	**Disrupt**	**Reassure**	**Motivate**	**Analyze**
Cyber Threat Intelligence	API Monitoring	Introduced Vulnerabilities	Baseline	Attack Vector Migration	Isolation	Application Diversity	Application Diversity	After-Action Review
Engagement Environment	Network Monitoring	Lures	Hardware Manipulation	Email Manipulation	Lures	Artifact Diversity	Artifact Diversity	Cyber Threat Intelligence
Gating Criteria	Software Manipulation	Malware Detonation	Isolation	Introduced Vulnerabilities	Network Manipulation	Burn-In	Information Manipulation	Threat Model
Operational Objective	System Activity Monitoring	Network Analysis	Network Manipulation	Lures	Software Manipulation	Email Manipulation	Introduced Vulnerabilities	
Persona Creation			Security Controls	Malware Detonation		Information Manipulation	Malware Detonation	
Storyboarding				Network Manipulation		Network Diversity	Network Diversity	
Threat Model				Peripheral Management		Peripheral Management	Personas	
				Security Controls		Pocket Litter		
				Software Manipulation				

MITRE Engage : Prepare phase



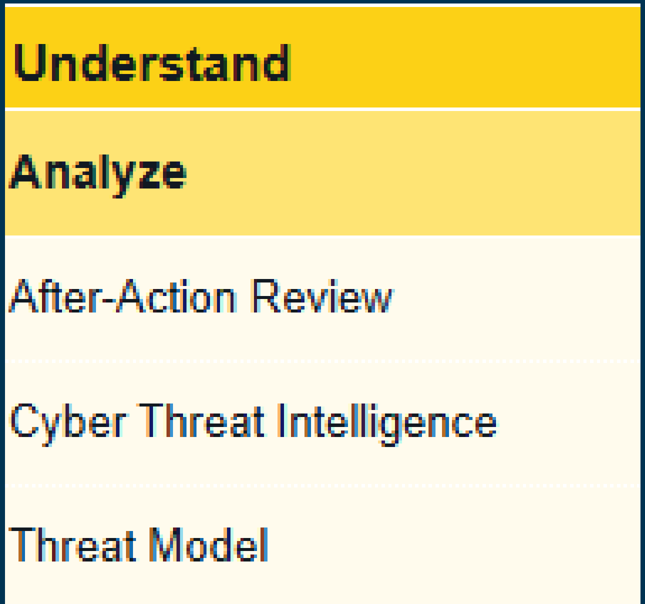
Prepare
Plan
Cyber Threat Intelligence
Engagement Environment
Gating Criteria
Operational Objective
Persona Creation
Storyboarding
Threat Model

MITRE Engage : Operate



Expose		Affect			Elicit	
Collect	Detect	Prevent	Direct	Disrupt	Reassure	Motivate
API Monitoring	Introduced Vulnerabilities	Baseline	Attack Vector Migration	Isolation	Application Diversity	Application Diversity
Network Monitoring	Lures	Hardware Manipulation	Email Manipulation	Lures	Artifact Diversity	Artifact Diversity
Software Manipulation	Malware Detonation	Isolation	Introduced Vulnerabilities	Network Manipulation	Burn-In	Information Manipulation
System Activity Monitoring	Network Analysis	Network Manipulation	Lures	Software Manipulation	Email Manipulation	Introduced Vulnerabilities
		Security Controls	Malware Detonation		Information Manipulation	Malware Detonation
			Network Manipulation		Network Diversity	Network Diversity
			Peripheral Management		Peripheral Management	Personas
			Security Controls		Pocket Litter	
			Software Manipulation			

MITRE Engage : Understand



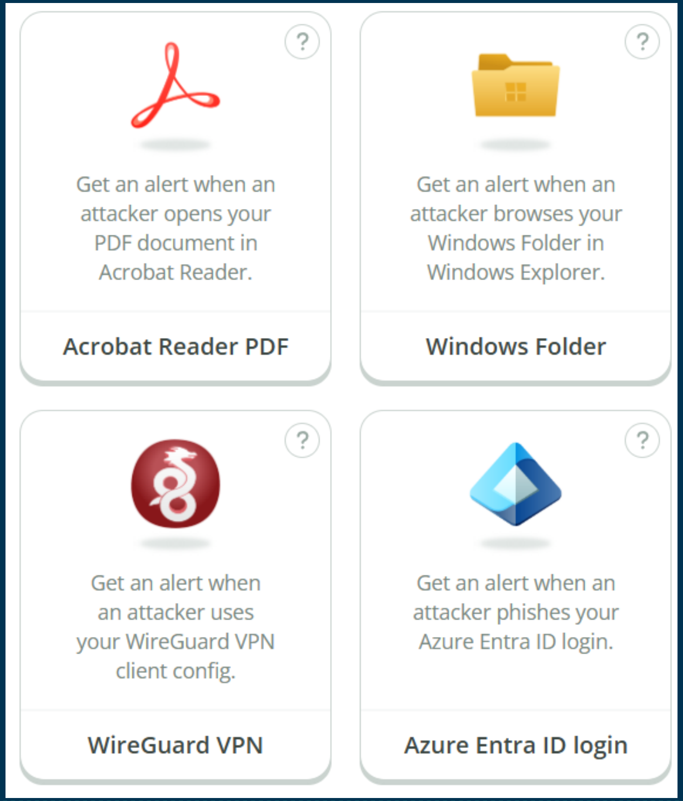
Understand
Analyze
After-Action Review
Cyber Threat Intelligence
Threat Model

Mapping MITRE Att&ck to MITRE Engage

-	ATT&CK Technique	Adversary Vulnerability	Engagement Activity
Ex	When adversaries perform specific actions	Their actions leave vulnerabilities	That the defender can take advantage of for defensive purpose
1	Remote System Discovery (T1018)	Adversaries reveal their reconnaissance behavior and interest in specific systems	Deploy deceptive system artifacts to mislead adversaries and track their movements
2	Process Injection (T1055)	Attackers rely on injecting malicious code into legitimate processes	Attackers rely on injecting malicious code into legitimate processes
3	Data Encrypted for Impact (T1486)	Attackers expose their encryption methods and reliance on specific algorithms	Introduce deceptive files that trigger alerts when accessed, helping defenders detect ransomware behavior
4	Exploitation for Privilege Escalation (T1068)	Attackers reveal their dependency on unpatched vulnerabilities	Deploy controlled vulnerabilities that allow defenders to observe attacker behavior without real risk
5	Command and Scripting Interpreter (T1059)	Attackers rely on scripting languages for automation and persistence	Introduce deceptive scripts that log attacker interactions and provide intelligence on their tactics

Getting started …. Prebuilt tools -

Canary Tokens (https://www.canarytokens.org/)



Get an alert when an attacker opens your PDF document in Acrobat Reader.

Acrobat Reader PDF

Get an alert when an attacker browses your Windows Folder in Windows Explorer.

Windows Folder

Get an alert when an attacker uses your WireGuard VPN client config.

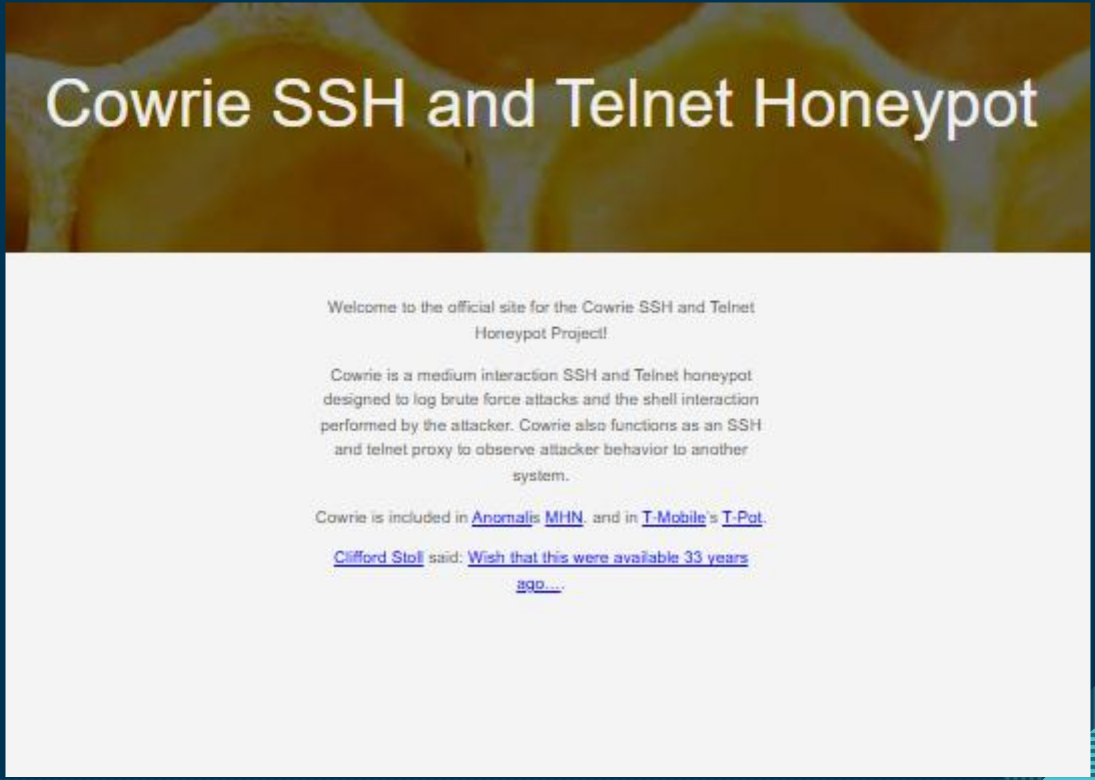
WireGuard VPN

Get an alert when an attacker phishes your Azure Entra ID login.

Azure Entra ID login

Honeypots

(https://github.com/cowrie/cowrie)



Cowrie SSH and Telnet Honeypot

Welcome to the official site for the Cowrie SSH and Telnet Honeypot Project!

Cowrie is a medium interaction SSH and Telnet honeypot designed to log brute force attacks and the shell interaction performed by the attacker. Cowrie also functions as an SSH and telnet proxy to observe attacker behavior to another system.

Cowrie is included in Anomalis MHN, and in T-Mobile's T-Pot.

Clifford Stoll said: Wish that this were available 33 years ago….

Deployment Demo

Case Study

> MITRE Engage isn’t about waiting for attackers – it’s about making battlefield yours, one deception at a time..

Thanks for following along, any questions ?

Scan for reading links and ppt –

- Mitre engage website
- Engage Matrix
- Mitre engage tools
- Engage 10 step process
- Engage Handbook
- BHIS- pay-what-you-can : Active defence and deception
- Youtube video sources– 1 , 2
- Medium sources – 1 , 2 , 3