Counterintelligence in Red Teaming using MITRE ENGAGE in 15min

OWASP Meetup Frankfurt #51, Oct 27th 2021

Who am I

Johannes Schönborn

Penetration Testing since 2006
2016 Founded Exploit Labs
@johnny_sec, @xpltlabs

OWASP Frankfurt

ENISA’s Ad-Hoc Working Group on Cyber Threat Landscapes

johannes@exploitlabs.de

Who we are

APT “Happy Turtle”

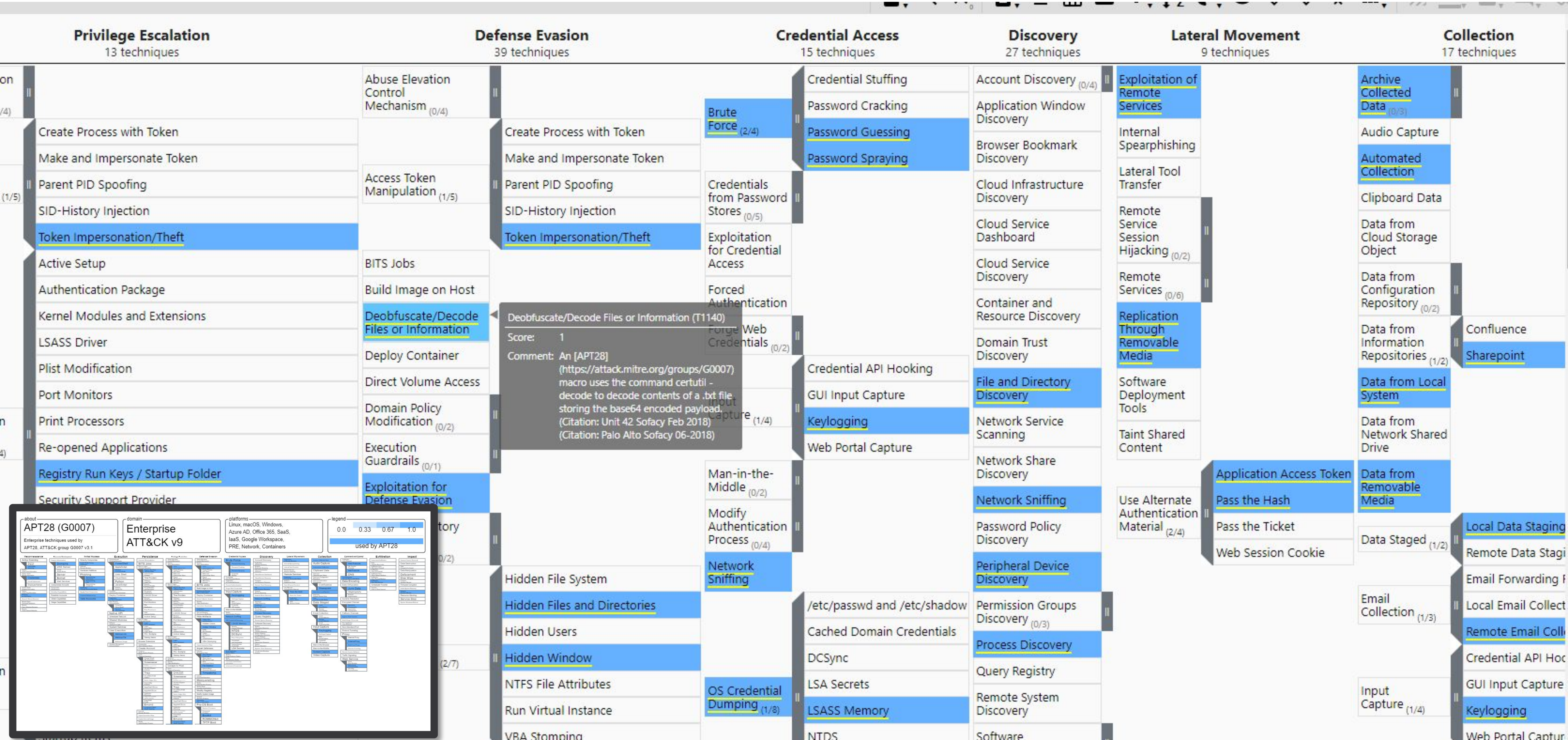
- Targets Power Plants PP
- Wants to disrupt
- Knows Robby is an OT Op
- Knows PP uses certain tech
- Knows PP uses cool WebApp OT

Agenda

1. How We Attack: MITRE ATT&CK
2. How Enterprises Can Defend: MITRE Engage
3. Adjusted Red Team Attack Playbooks
4. Key Takeaways

1. How We Attack: MITRE ATT&CK

1. How We Attack: MITRE ATT&CK



Privilege Escalation
13 techniques

- Create Process with Token
- Make and Impersonate Token
- Parent PID Spoofing
- SID-History Injection
- Token Impersonation/Theft
- Active Setup
- Authentication Package
- Kernel Modules and Extensions
- LSASS Driver
- Plist Modification
- Port Monitors
- Print Processors
- Re-opened Applications
- Registry Run Keys / Startup Folder
- Security Support Provider

Defense Evasion
39 techniques

- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (1/5)
  - Create Process with Token
  - Make and Impersonate Token
  - Parent PID Spoofing
  - SID-History Injection
  - Token Impersonation/Theft
- BITS Jobs
- Build Image on Host
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (0/2)
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion
- tory (0/2)
- (2/7)
  - Hidden File System
  - Hidden Files and Directories
  - Hidden Users
  - Hidden Window
  - NTFS File Attributes
  - Run Virtual Instance
  - VBA Stomping

Deobfuscate/Decode Files or Information (T1140)
Score: 1
Comment: An [APT28](https://attack.mitre.org/groups/G0007) macro uses the command certutil -decode to decode contents of a .txt file storing the base64 encoded payload.(Citation: Unit 42 Sofacy Feb 2018)(Citation: Palo Alto Sofacy 06-2018)

Credential Access
15 techniques

- Brute Force (2/4)
  - Credential Stuffing
  - Password Cracking
  - Password Guessing
  - Password Spraying
- Credentials from Password Stores (0/5)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (0/2)
- Input Capture (1/4)
  - Credential API Hooking
  - GUI Input Capture
  - Keylogging
  - Web Portal Capture
- Man-in-the-Middle (0/2)
- Modify Authentication Process (0/4)
- Network Sniffing
- OS Credential Dumping (1/8)
  - /etc/passwd and /etc/shadow
  - Cached Domain Credentials
  - DCSync
  - LSA Secrets
  - LSASS Memory
  - NTDS

Discovery
27 techniques

- Account Discovery (0/4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Container and Resource Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (0/3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software

Lateral Movement
9 techniques

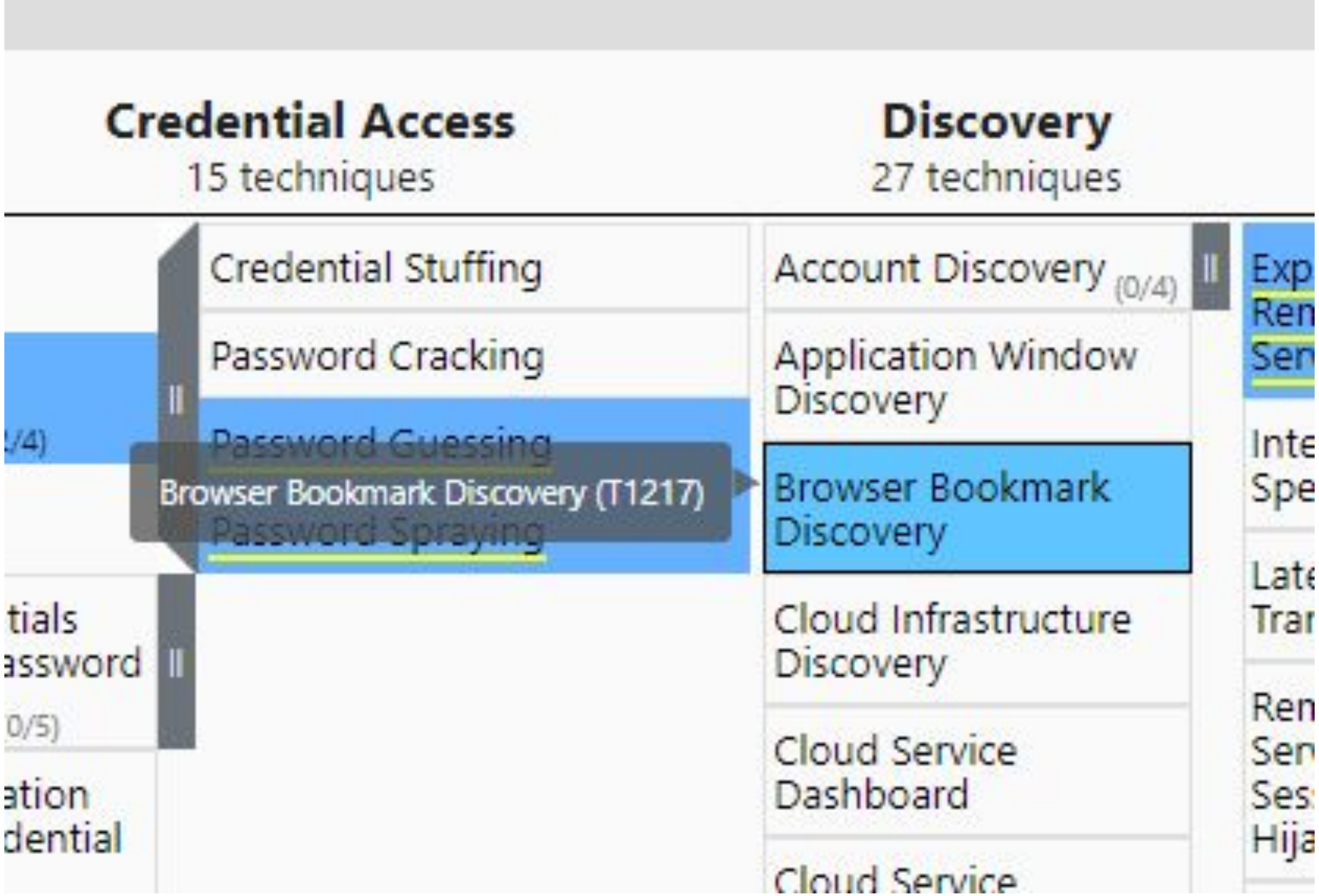
- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (0/2)
- Remote Services (0/6)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (2/4)
  - Application Access Token
  - Pass the Hash
  - Pass the Ticket
  - Web Session Cookie

Collection
17 techniques

- Archive Collected Data (0/3)
- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Cloud Storage Object
- Data from Configuration Repository (0/2)
- Data from Information Repositories (1/2)
  - Confluence
  - Sharepoint
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (1/2)
  - Local Data Staging
  - Remote Data Stagi
- Email Collection (1/3)
  - Email Forwarding R
  - Local Email Collect
  - Remote Email Coll
- Input Capture (1/4)
  - Credential API Hoo
  - GUI Input Capture
  - Keylogging
  - Web Portal Captur

about: APT28 (G0007)
Enterprise techniques used by APT28, ATT&CK group G0007 v3.1
domain: Enterprise ATT&CK v9
platforms: Linux, macOS, Windows, Azure AD, Office 365, SaaS, IaaS, Google Workspace, PRE, Network, Containers
legend: 0.0 0.33 0.67 1.0
used by APT28

1. How We Attack: MITRE ATT&CK



Credential Access
15 techniques

Discovery
27 techniques

/4)

tials
assword
0/5)

ation
dential

Credential Stuffing

Password Cracking

Password Guessing

Browser Bookmark Discovery (T1217)

Password Spraying

Account Discovery (0/4)

Application Window Discovery

Browser Bookmark Discovery

Cloud Infrastructure Discovery

Cloud Service Dashboard

Cloud Service

Exp
Ren
Ser

Inte
Spe

Late
Trar

Ren
Ser
Ses
Hija

Browser bookmarks may also highlight additional targets after an adversary has access to valid credentials, especially Credentials In Files associated with logins cached by a browser.

1. How We Attack: MITRE ATT&CK

Playbook	T1217	Browser Bookmark Discovery
Goal	1. Enumerate local browsers 2. Extract history 3. Extract passwords from browser 4. Identify often used OT control interfaces 5. Identify how the operator authenticates i.e. via SSO or local credentials	
Method	SharpWeb, Browserloot.ps1 Metasploit: post/multi/gather/firefox_creds	
ATT&CK Defense	*"This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features."*	

1. How We Attack: MITRE ATT&CK

History:

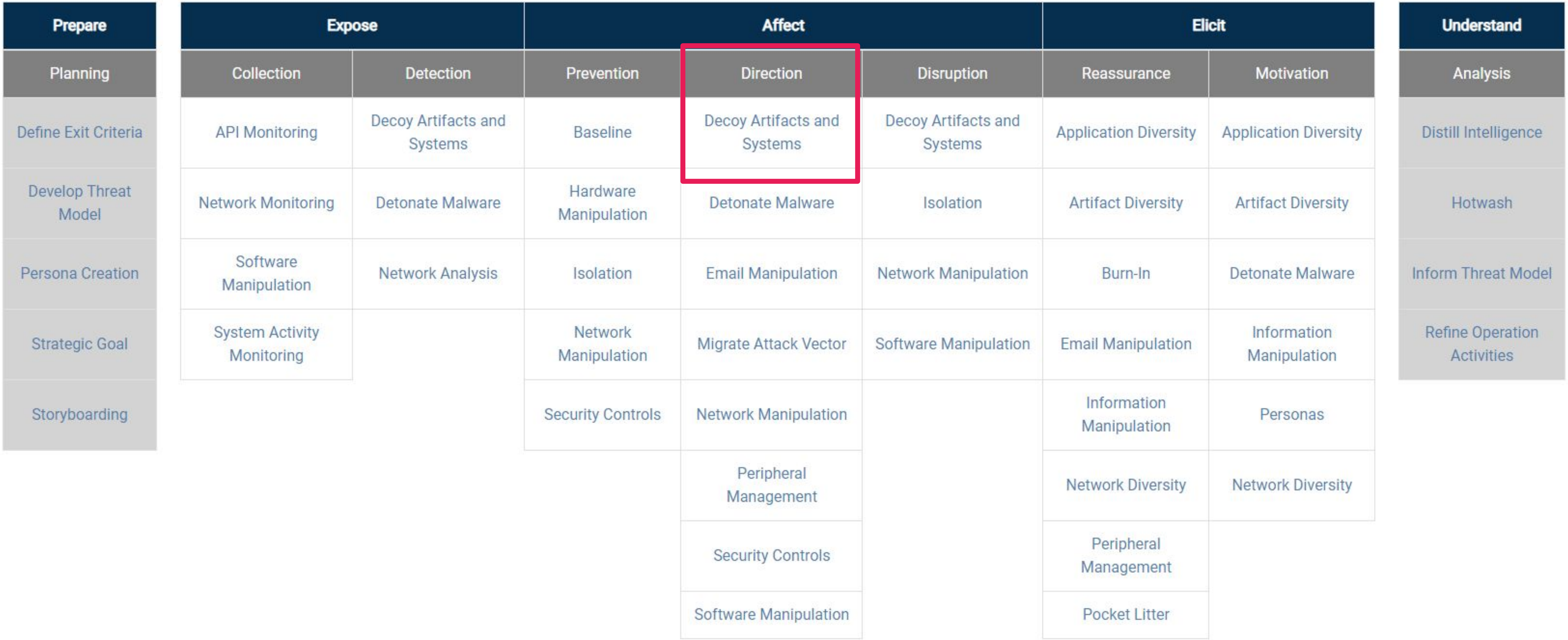
Heatingcontrols.kplant

Browser Credentials:

XN5896 / Nioij()/&*

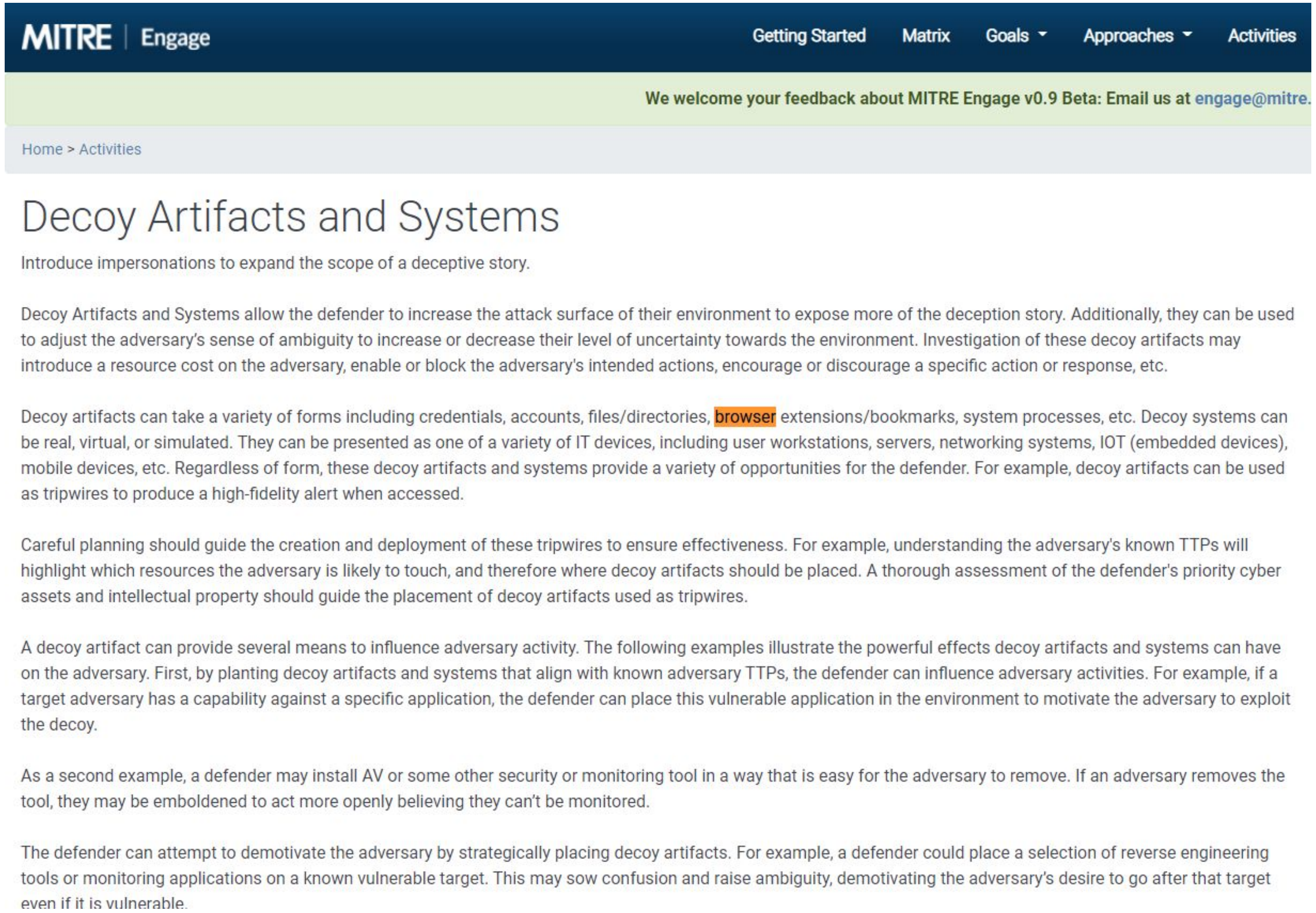
2. How Enterprises Can Defend: MITRE Engage

2. How Enterprises Can Defend: MITRE Engage



Prepare	Expose		Affect			Elicit		Understand
Planning	Collection	Detection	Prevention	Direction	Disruption	Reassurance	Motivation	Analysis
Define Exit Criteria	API Monitoring	Decoy Artifacts and Systems	Baseline	Decoy Artifacts and Systems	Decoy Artifacts and Systems	Application Diversity	Application Diversity	Distill Intelligence
Develop Threat Model	Network Monitoring	Detonate Malware	Hardware Manipulation	Detonate Malware	Isolation	Artifact Diversity	Artifact Diversity	Hotwash
Persona Creation	Software Manipulation	Network Analysis	Isolation	Email Manipulation	Network Manipulation	Burn-In	Detonate Malware	Inform Threat Model
Strategic Goal	System Activity Monitoring		Network Manipulation	Migrate Attack Vector	Software Manipulation	Email Manipulation	Information Manipulation	Refine Operation Activities
Storyboarding			Security Controls	Network Manipulation		Information Manipulation	Personas	
				Peripheral Management		Network Diversity	Network Diversity	
				Security Controls		Peripheral Management		
				Software Manipulation		Pocket Litter		

2. How Enterprises Can Defend: MITRE Engage



We welcome your feedback about MITRE Engage v0.9 Beta: Email us at engage@mitre.

Home > Activities

Decoy Artifacts and Systems

Introduce impersonations to expand the scope of a deceptive story.

Decoy Artifacts and Systems allow the defender to increase the attack surface of their environment to expose more of the deception story. Additionally, they can be used to adjust the adversary's sense of ambiguity to increase or decrease their level of uncertainty towards the environment. Investigation of these decoy artifacts may introduce a resource cost on the adversary, enable or block the adversary's intended actions, encourage or discourage a specific action or response, etc.

Decoy artifacts can take a variety of forms including credentials, accounts, files/directories, browser extensions/bookmarks, system processes, etc. Decoy systems can be real, virtual, or simulated. They can be presented as one of a variety of IT devices, including user workstations, servers, networking systems, IOT (embedded devices), mobile devices, etc. Regardless of form, these decoy artifacts and systems provide a variety of opportunities for the defender. For example, decoy artifacts can be used as tripwires to produce a high-fidelity alert when accessed.

Careful planning should guide the creation and deployment of these tripwires to ensure effectiveness. For example, understanding the adversary's known TTPs will highlight which resources the adversary is likely to touch, and therefore where decoy artifacts should be placed. A thorough assessment of the defender's priority cyber assets and intellectual property should guide the placement of decoy artifacts used as tripwires.

A decoy artifact can provide several means to influence adversary activity. The following examples illustrate the powerful effects decoy artifacts and systems can have on the adversary. First, by planting decoy artifacts and systems that align with known adversary TTPs, the defender can influence adversary activities. For example, if a target adversary has a capability against a specific application, the defender can place this vulnerable application in the environment to motivate the adversary to exploit the decoy.

As a second example, a defender may install AV or some other security or monitoring tool in a way that is easy for the adversary to remove. If an adversary removes the tool, they may be emboldened to act more openly believing they can't be monitored.

The defender can attempt to demotivate the adversary by strategically placing decoy artifacts. For example, a defender could place a selection of reverse engineering tools or monitoring applications on a known vulnerable target. This may sow confusion and raise ambiguity, demotivating the adversary's desire to go after that target even if it is vulnerable.

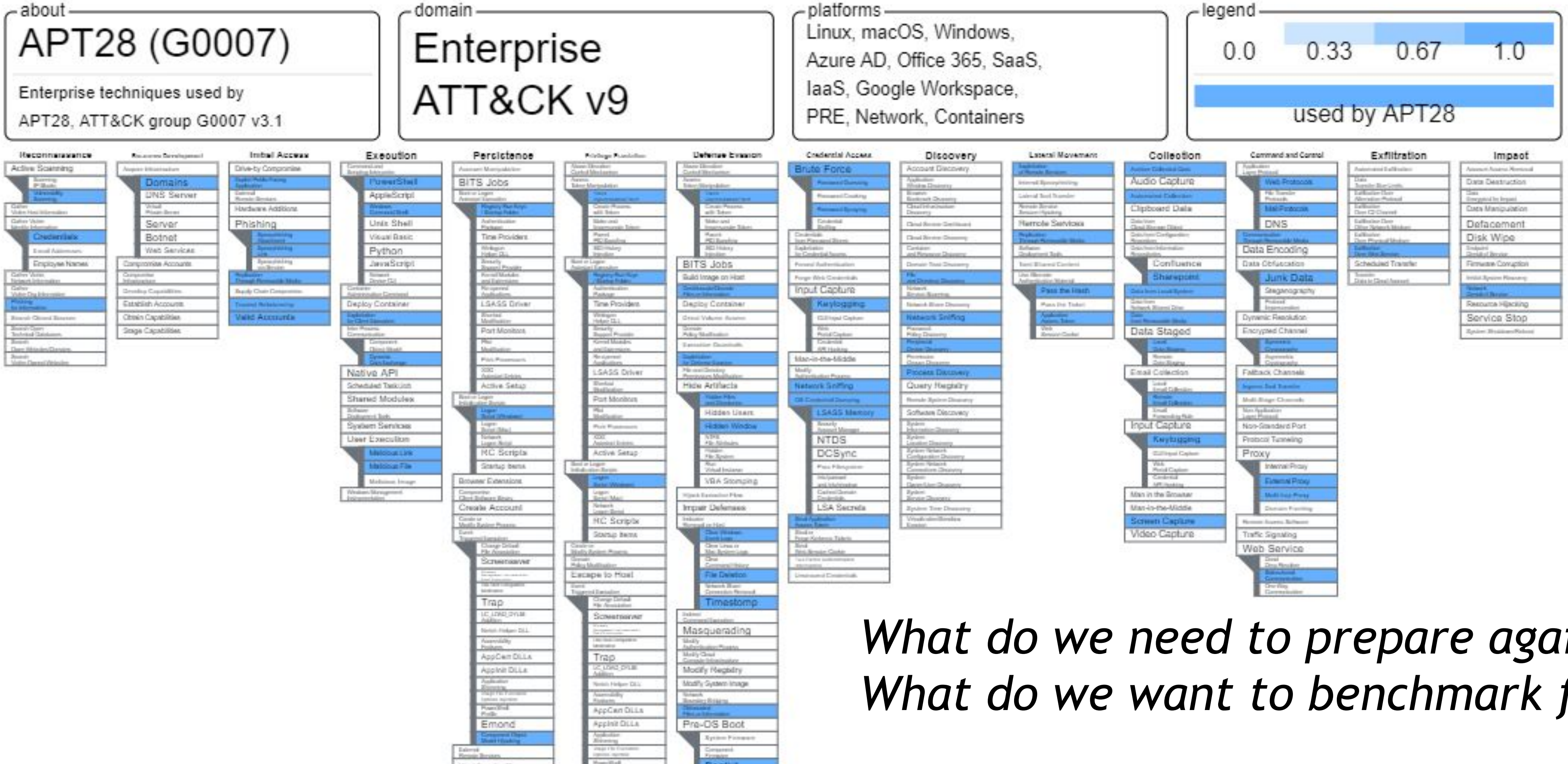
Decoy artifacts can take a variety of forms including credentials, accounts, files/directories, browser extensions/bookmarks, system processes, etc. Decoy systems can be real, virtual, or simulated.

3. Adjusted Red Team Attack Playbooks

3. Adjusted Red Team Attack Playbooks

https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcQtks9MCB6oj3vdueBR1fPGOUj6D00yAFqjnQ&usqp=CAU

3. Adjusted Red Team Attack Playbooks



about

APT28 (G0007)

Enterprise techniques used by APT28, ATT&CK group G0007 v3.1

domain

Enterprise ATT&CK v9

platforms

Linux, macOS, Windows, Azure AD, Office 365, SaaS, IaaS, Google Workspace, PRE, Network, Containers

legend

0.0	0.33	0.67	1.0

🟦 used by APT28

What do we need to prepare against?
What do we want to benchmark for?

3. Adjusted Red Team Attack Playbooks

Playbook	T1217	Browser Bookmark Discovery
Goal	1. Enumerate local browsers 2. Extract history 3. Extract passwords from browser 4. Identify often used OT control interfaces 5. Identify how the operator authenticates i.e. via SSO or local credentials Do not engage before: Compare browsing history between browsers to identify honeypot URLs, i.e. a browser that only surfs to two, three high impact websites is suspicious Compare credentials from browsers against standard credentials: If they seem very different it could be a honeypot	
Method	SharpWeb, Browserloot.ps1 Metasploit: post/multi/gather/firefox_creds	
ATT&CK Defense	This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.	
Engage	Decoy artifacts can take a variety of forms including credentials, accounts, files/directories, browser extensions/bookmarks, system processes, etc.	

3. Adjusted Red Team Attack Playbooks

History:

Heatingcontrols.kplant

Browser Credentials:

XN5896 / Nioij()/&*

History:

maintainance.kplant

Browser Credentials:

Kplant\Johnny.s / Start2021!

4. Key Takeaways

4. Key Takeaways

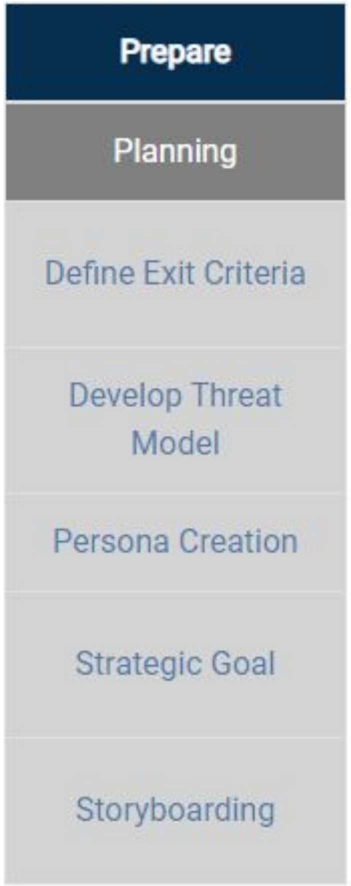
Use MITRE Engage to augment your Red Teaming TTPs

Understand the options the Blue Team has to defend, i.e. if a single security control is not available, it does not mean there is not defense in place

Identify Engage controls in place to derive further controls: If they have honeypot credentials in the browser, what about Active Directory?

Align your results

We are now able to better advise on remediations by citing MITRE Engage and how it would have impacted the engagement



[BlackHills: OPSEC Fundamentals for Remote Red Teams]

[X33fCon: OPSEC Obsessed]

[CYBV436 Counter Cyber Threat Intelligence]

Questions?

johannes@exploitlabs.de