Purple Teaming an Azure Environment

Content

09:00-09:15 Introductions

09:15-09:30 History of pen test, red team, and how we got to purple team

09:30-09:45 What is purple teaming ?

09:45-10:30 Activity - threat modelling sample organisations

10:30-11:00 Break

11:00-11:30 Threat actor emulation

11:30-12:30 Attack activity and discuss persistence

12:30-13:30 Lunch

13:30-14:30 Log Sources, SIEM, and Detection exercise

14:30-15:00 Continuous Improvement and Reporting

15:00-15:30 Break

15:30-16:00 Purple teaming for a state government

16:00 Open Discussion

Purple Teaming: How it all started?

- ❑ History of sysadmins
- ❑ Rise of Pentest as a service
- ❑ Evolution of Red teaming
- ❑ War stories

How did we get here?

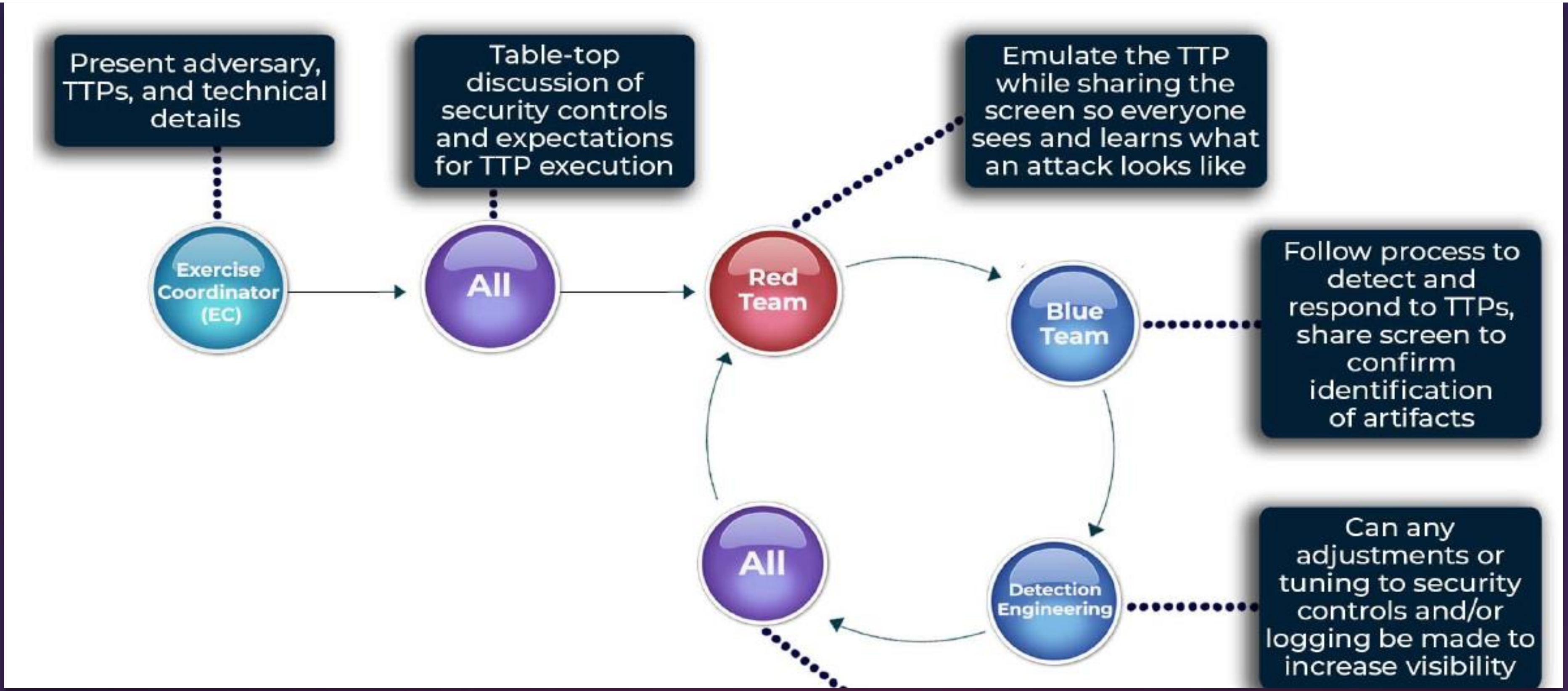
- Evolution of Pentesting over the years
- Quality of a pentest report is limited by the quality of the pentester
- Red team report may often be forgotten after a one-off engagement

Value Proposition

Who benefits from attack simulations?

What is Purple teaming?

- Benefits of a purple team exercise
  - Continuous improvement
  - Micro tests to focus on the outcome
  - Less planning, more time spent on execution
- Common approaches for Purple Teaming
- Industry frameworks - CORIE framework – targeted to Australian Financial Institutions (FIs)

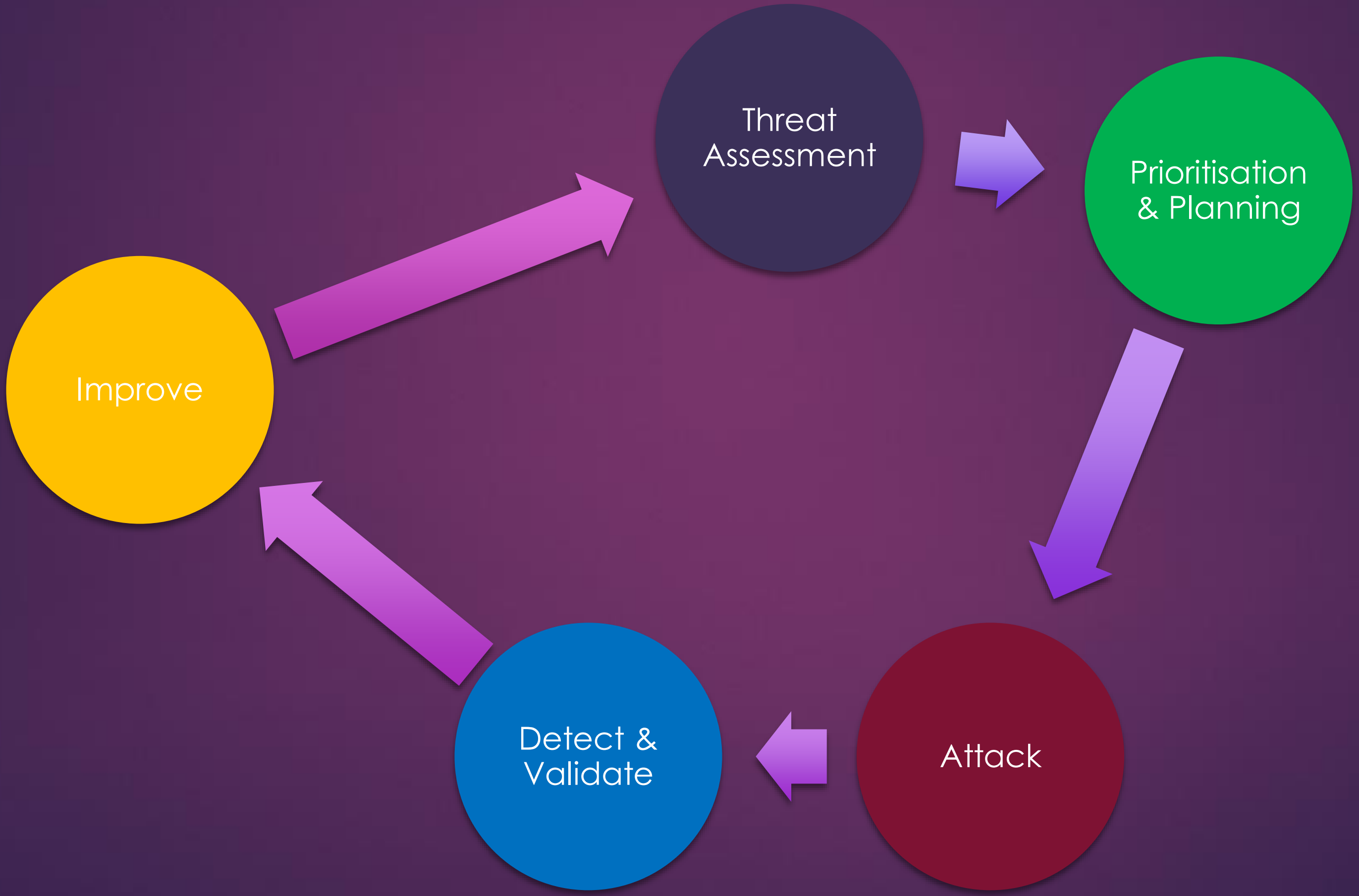


Present adversary, TTPs, and technical details
Table-top discussion of security controls and expectations for TTP execution
Emulate the TTP while sharing the screen so everyone sees and learns what an attack looks like
Exercise Coordinator (EC)
All
Red Team
Blue Team
Follow process to detect and respond to TTPs, share screen to confirm identification of artifacts
All
Detection Engineering
Can any adjustments or tuning to security controls and/or logging be made to increase visibility

Replay Adversary Attack Simulation (Purple Exercise)

CORIE MODEL

Continuous Improvement



Threat Assessment

Prioritisation & Planning

Attack

Detect & Validate

Improve

Step 1 - Threat Assessment

Know which Threat Actors are likely to target your organisation

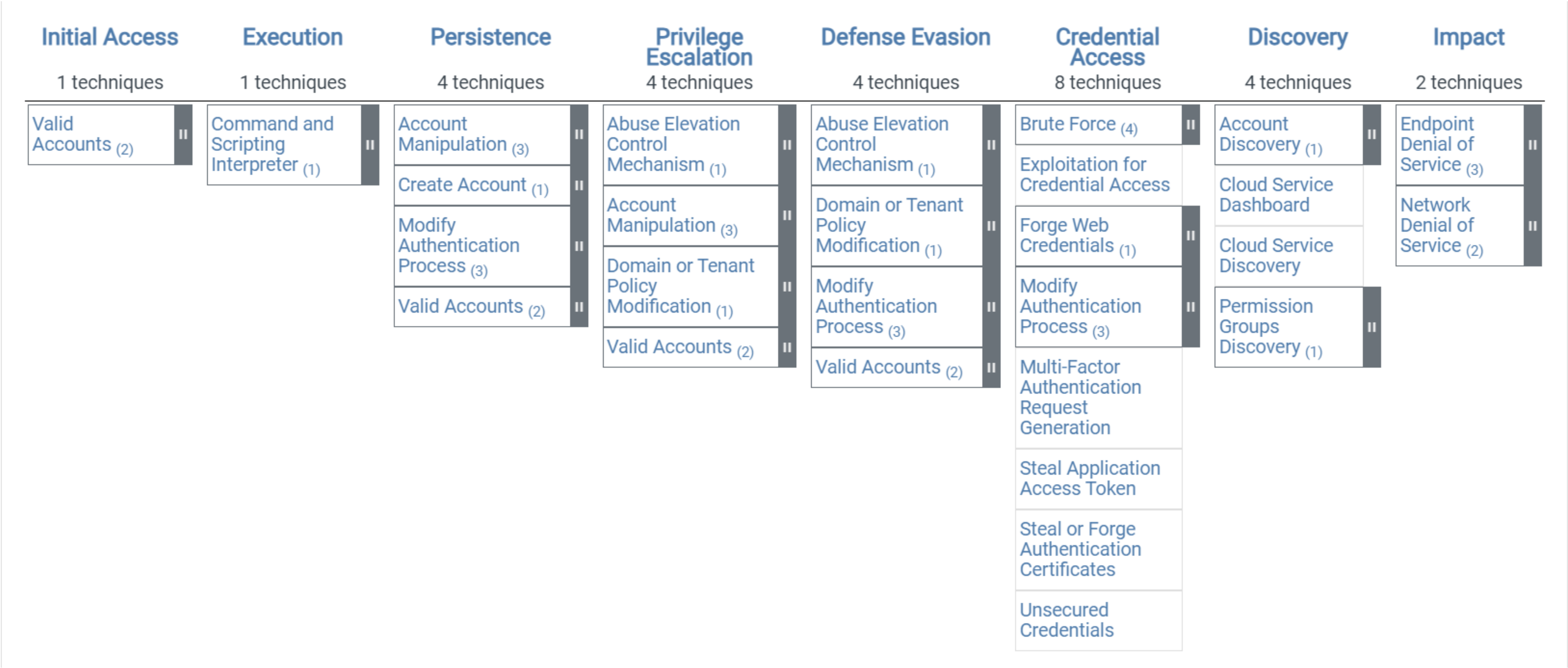
Know your crown jewels

Build a hypothesis of incident scenarios

- Know your processes and gaps
- Know user behaviour
- Know your supply chain behaviour, expect scenarios when they are breached

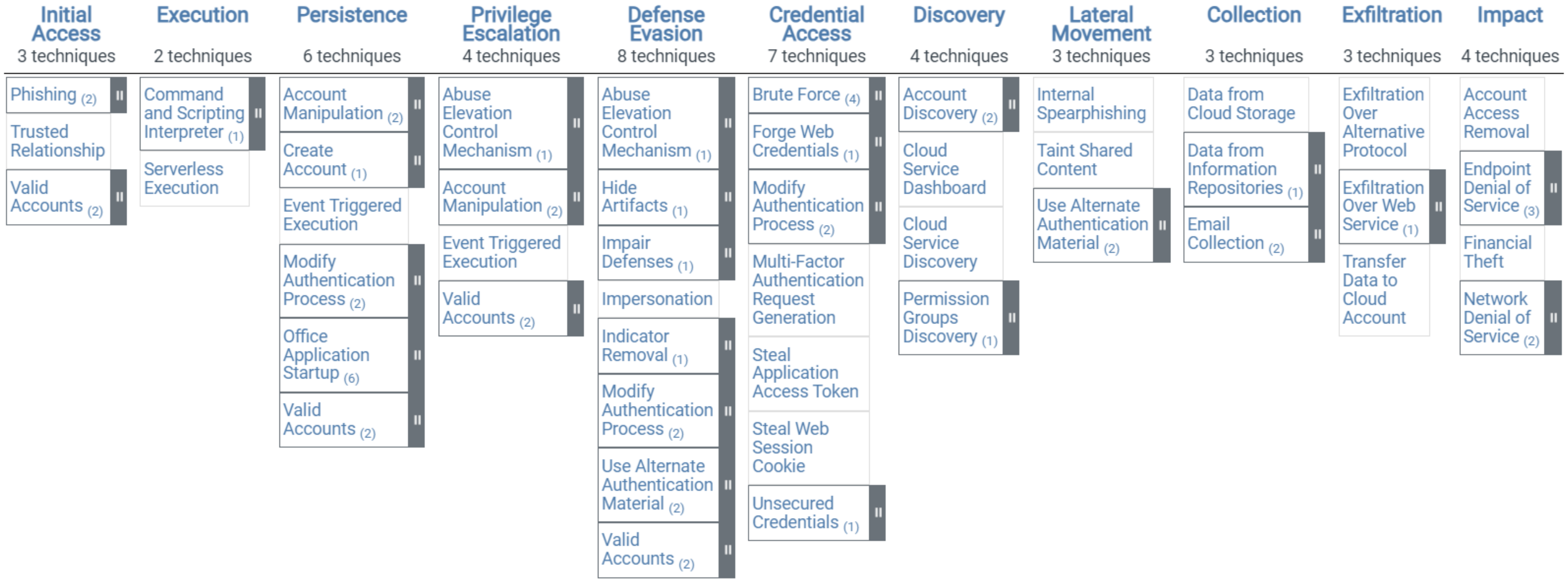
Activity 1: Threat Model common organisations

ATT&CK Framework: Azure AD (Entra ID)



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Impact
1 techniques	1 techniques	4 techniques	4 techniques	4 techniques	8 techniques	4 techniques	2 techniques
Valid Accounts (2)	Command and Scripting Interpreter (1)	Account Manipulation (3)	Abuse Elevation Control Mechanism (1)	Abuse Elevation Control Mechanism (1)	Brute Force (4)	Account Discovery (1)	Endpoint Denial of Service (3)
		Create Account (1)	Account Manipulation (3)	Domain or Tenant Policy Modification (1)	Exploitation for Credential Access	Cloud Service Dashboard	Network Denial of Service (2)
		Modify Authentication Process (3)	Domain or Tenant Policy Modification (1)	Modify Authentication Process (3)	Forge Web Credentials (1)	Cloud Service Discovery	
		Valid Accounts (2)	Valid Accounts (2)	Valid Accounts (2)	Modify Authentication Process (3)	Permission Groups Discovery (1)	
					Multi-Factor Authentication Request Generation		
					Steal Application Access Token		
					Steal or Forge Authentication Certificates		
					Unsecured Credentials		

ATT&CK Framework: Office365



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Impact
3 techniques	2 techniques	6 techniques	4 techniques	8 techniques	7 techniques	4 techniques	3 techniques	3 techniques	3 techniques	4 techniques
Phishing (2)	Command and Scripting Interpreter (1)	Account Manipulation (2)	Abuse Elevation Control Mechanism (1)	Abuse Elevation Control Mechanism (1)	Brute Force (4)	Account Discovery (2)	Internal Spearphishing	Data from Cloud Storage	Exfiltration Over Alternative Protocol	Account Access Removal
Trusted Relationship	Serverless Execution	Create Account (1)	Account Manipulation (2)	Hide Artifacts (1)	Forge Web Credentials (1)	Cloud Service Dashboard	Taint Shared Content	Data from Information Repositories (1)	Exfiltration Over Web Service (1)	Endpoint Denial of Service (3)
Valid Accounts (2)		Event Triggered Execution	Event Triggered Execution	Impair Defenses (1)	Modify Authentication Process (2)	Cloud Service Discovery	Use Alternate Authentication Material (2)	Email Collection (2)	Transfer Data to Cloud Account	Financial Theft
		Modify Authentication Process (2)	Valid Accounts (2)	Impersonation	Multi-Factor Authentication Request Generation	Permission Groups Discovery (1)				Network Denial of Service (2)
		Office Application Startup (6)		Indicator Removal (1)	Steal Application Access Token					
		Valid Accounts (2)		Modify Authentication Process (2)	Steal Web Session Cookie					
				Use Alternate Authentication Material (2)	Unsecured Credentials (1)					
				Valid Accounts (2)						

Discuss – Initial Access

Password Guessing Attacks

Password Spray

Credential Stuffing

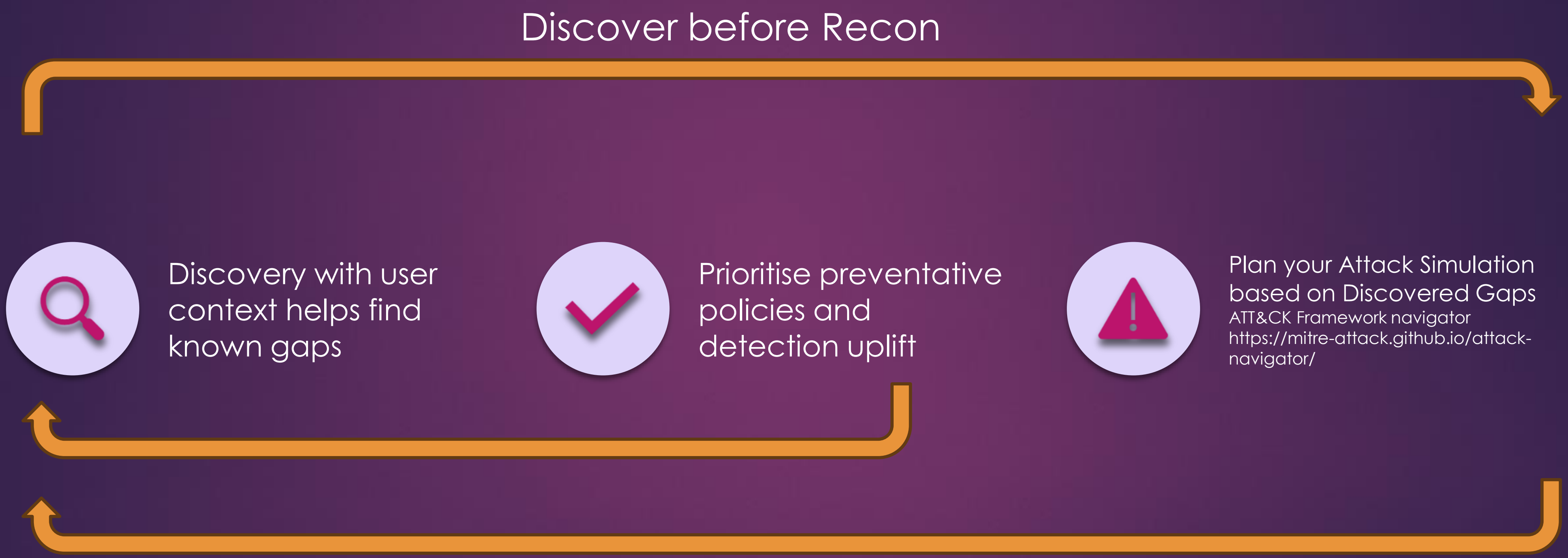
Importance of MFA

Conditional Access Policies

Protect / Detect / Respond

- Prevention is better than detection
- Know the behaviour of a prevention failure
- Build detections based on aggregation of behaviour
- Micro responses prevent bigger Incidents – co-relation vs isolation

Step 2: Prioritisation and Planning



Discover before Recon

Discovery with user context helps find known gaps

Prioritise preventative policies and detection uplift

Plan your Attack Simulation based on Discovered Gaps
ATT&CK Framework navigator
https://mitre-attack.github.io/attack-navigator/

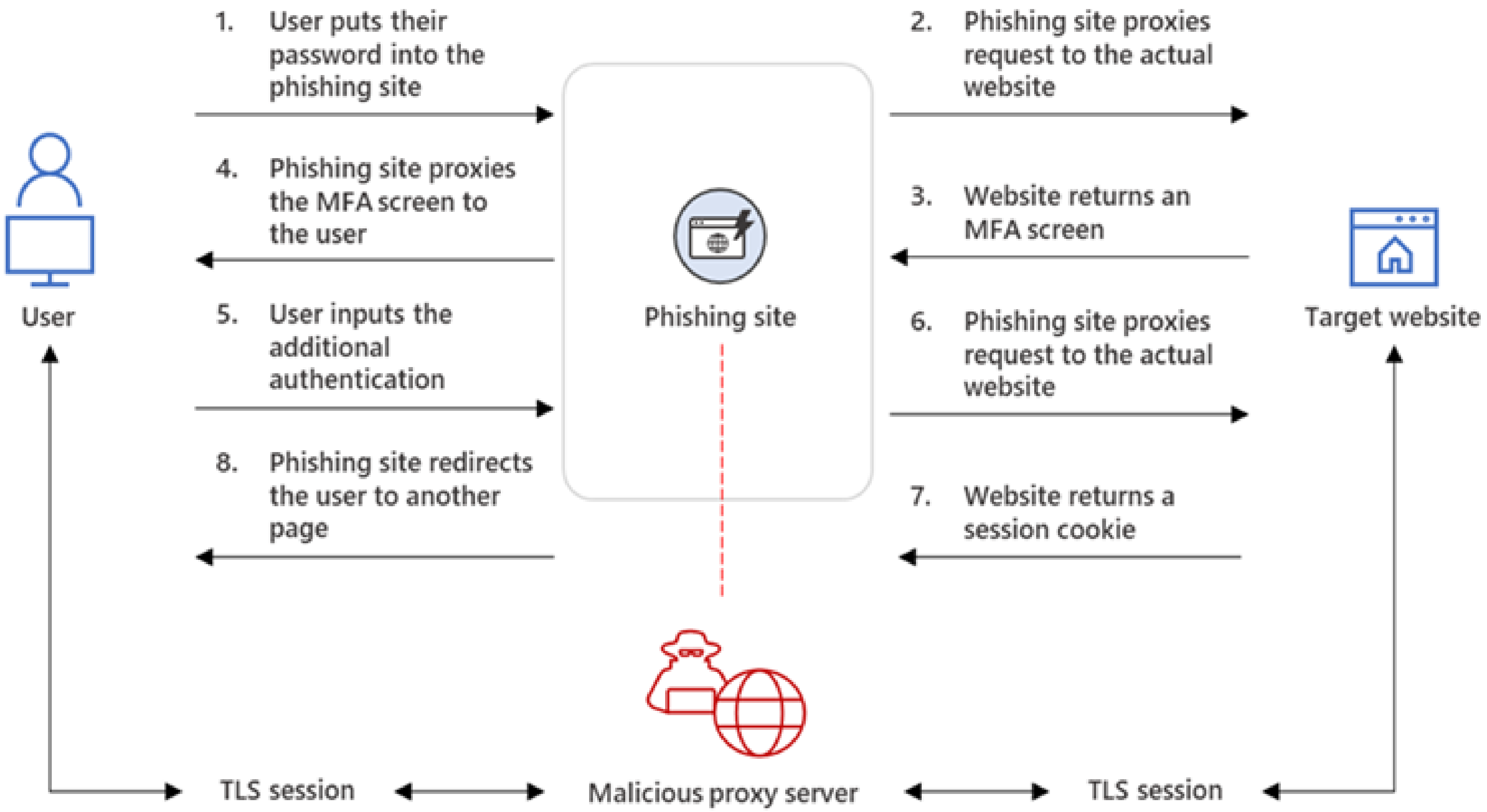
Step 3: Attack Emulation

- On-Prem moving to Azure
- Startup Organisation
- **Demo Attacks** – Recon and Initial Access – Password Spray
- https://portal.azure.com

Activity 2 – Persistence

- Security Monitoring team detects **Risky Sign-In** and will push activity “Revoke Sessions” and enforce MFA controls any minute. Find a way to maintain persistence in the tenant.
- With persistence achieved, find a way to read the document at sharepoint

AiTM phishing



1. User puts their password into the phishing site

2. Phishing site proxies request to the actual website

3. Website returns an MFA screen

4. Phishing site proxies the MFA screen to the user

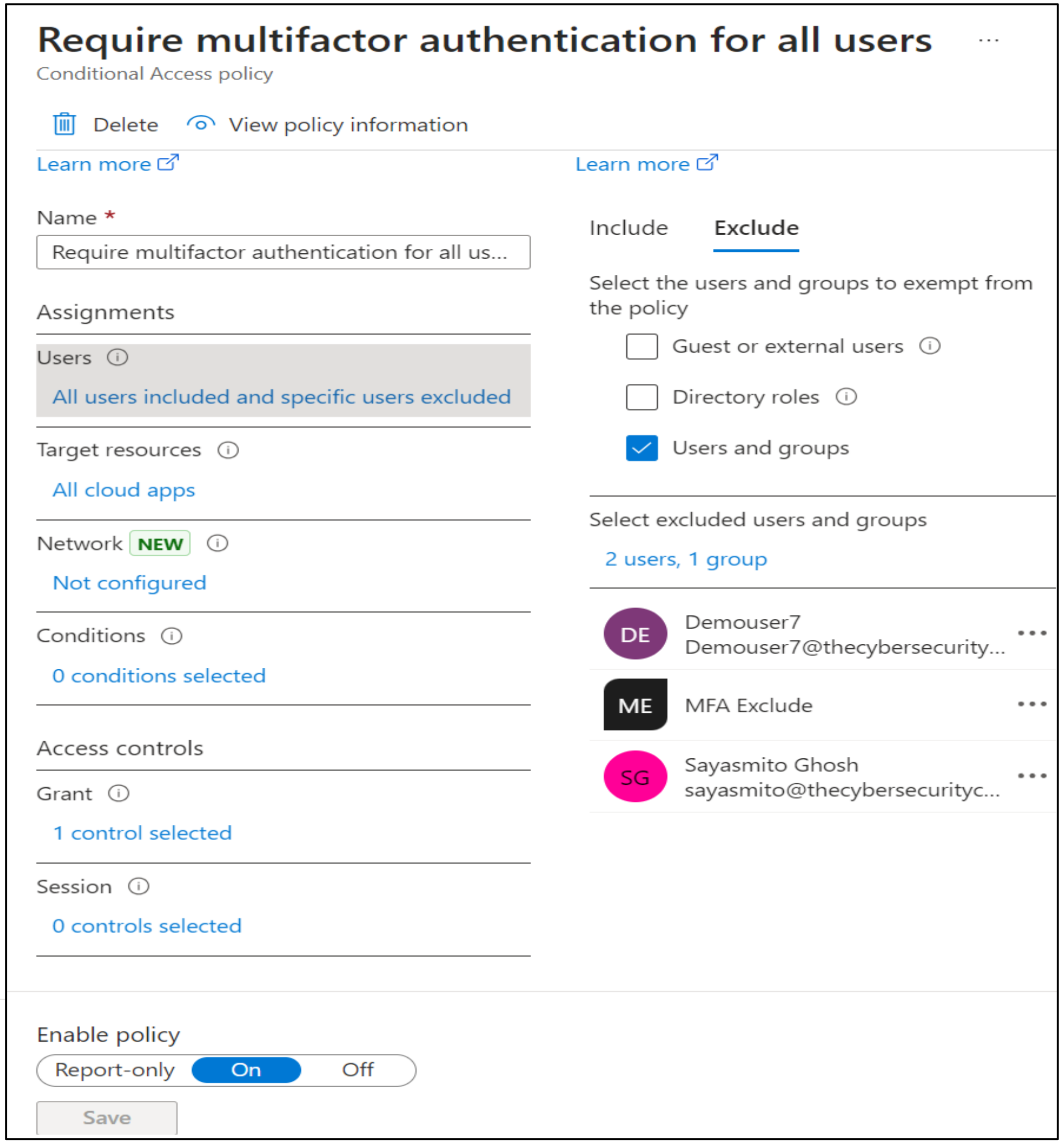
5. User inputs the additional authentication

6. Phishing site proxies request to the actual website

7. Website returns a session cookie

8. Phishing site redirects the user to another page

Conditional Access Policies – Example MFA Policy



Require multifactor authentication for all users

Conditional Access policy

Learn more

Name *

Require multifactor authentication for all us...

Assignments

Users ⓘ

All users included and specific users excluded

Target resources ⓘ

All cloud apps

Network NEW ⓘ

Not configured

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

1 control selected

Session ⓘ

0 controls selected

Learn more

Include Exclude

Select the users and groups to exempt from the policy

☐ Guest or external users ⓘ

☐ Directory roles ⓘ

☑ Users and groups

Select excluded users and groups

2 users, 1 group

DE Demouser7
Demouser7@thecybersecurity... •••

ME MFA Exclude •••

SG Sayasmito Ghosh
sayasmito@thecybersecurityc... •••

Enable policy

Report-only [✓ On] Off

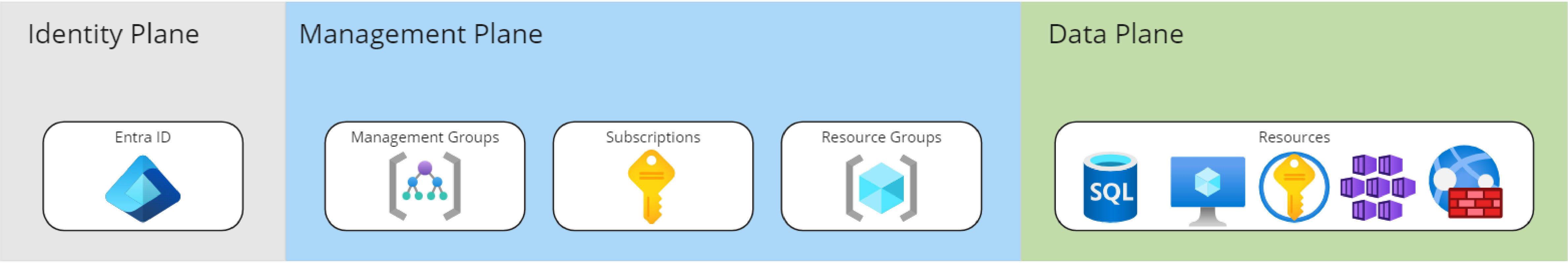
Detection and Response

- The Defender's role
- Key data sources for Azure
- Hands-on exercise and open discussions
- Optimizing detections
- Evaluating threat response processes

The Defender’s Role

- Identify control gaps and validate assumptions
- Test and validate detection and response capability
- Continuous improvement

Azure Data Sources



Identity Plane

Entra ID

Management Plane

Management Groups

Subscriptions

Resource Groups

Data Plane

Resources

Activity: Finding Evil

- https://t.ly/ua5pS

Discussion

- Observations
- Ideas or strategies to implement to mitigate risks

Optimizing detections

- Categorizing security events in the alerting pipeline
- Correlation-based alerts based on attack paths
- Risk-Based Alerting

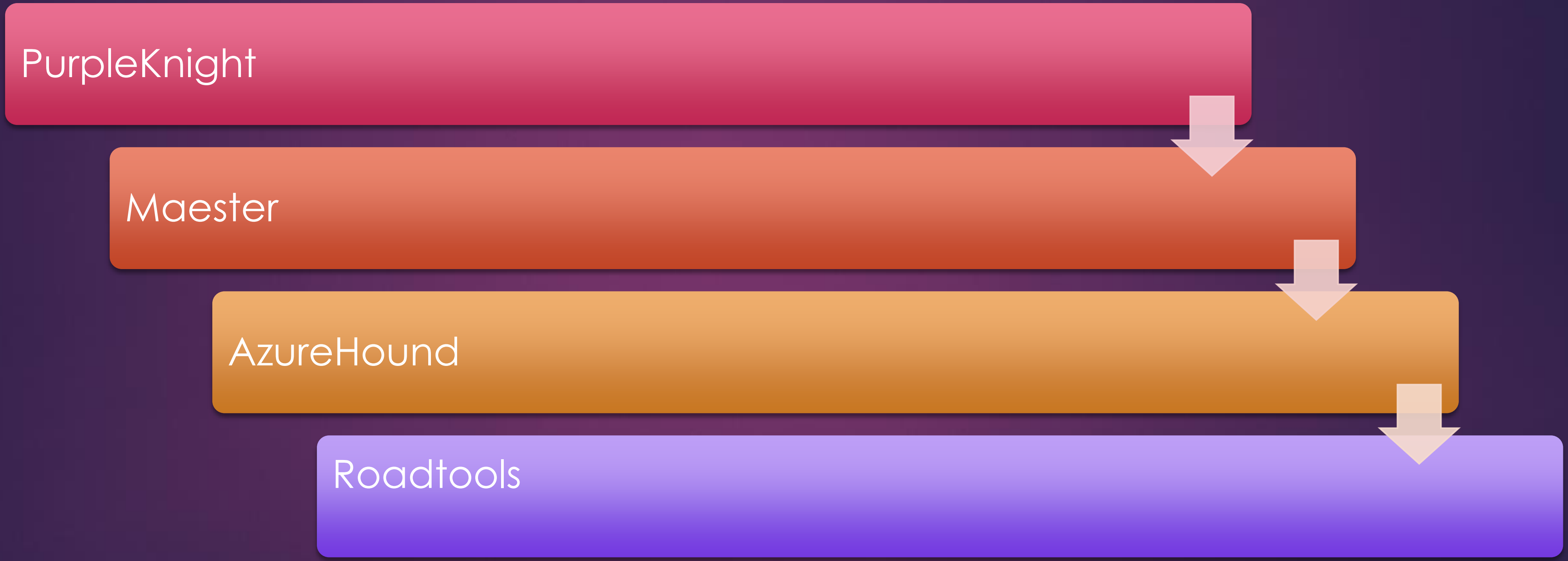
Response Processes

- Evaluate incident handling by analysts / incident responders.
- Identify blockers and dependencies
- Standard operating procedures and playbooks
- 1-10-60 Challenge

Purpleteam cheatsheet

https://t.ly/_odhp

Continuous Discovery Tools



PurpleKnight

Maester

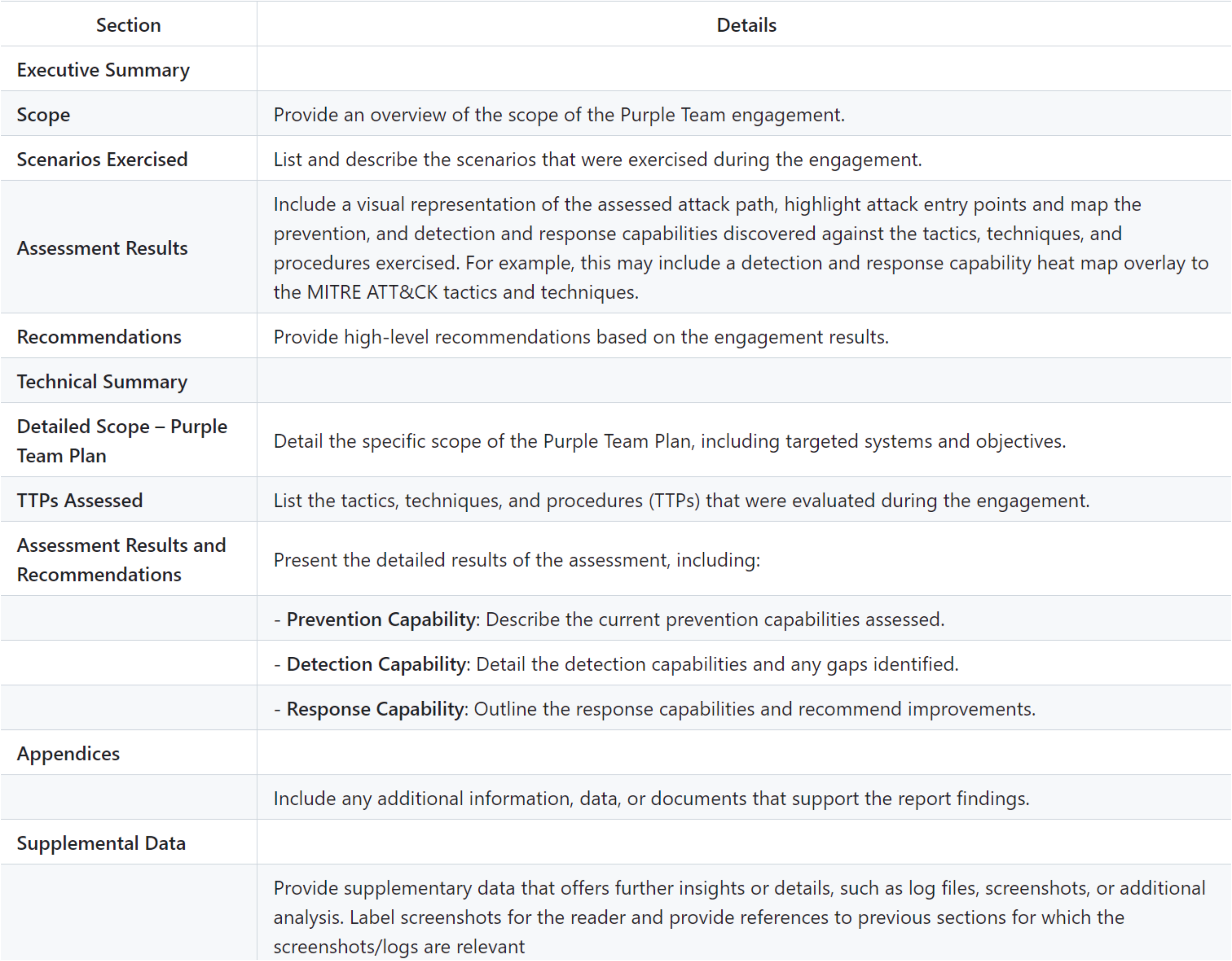
AzureHound

Roadtools

Sentinel security coverage by the MITRE ATT&CK® framework

- https://learn.microsoft.com/en-us/azure/sentinel/mitre-coverage

Reports

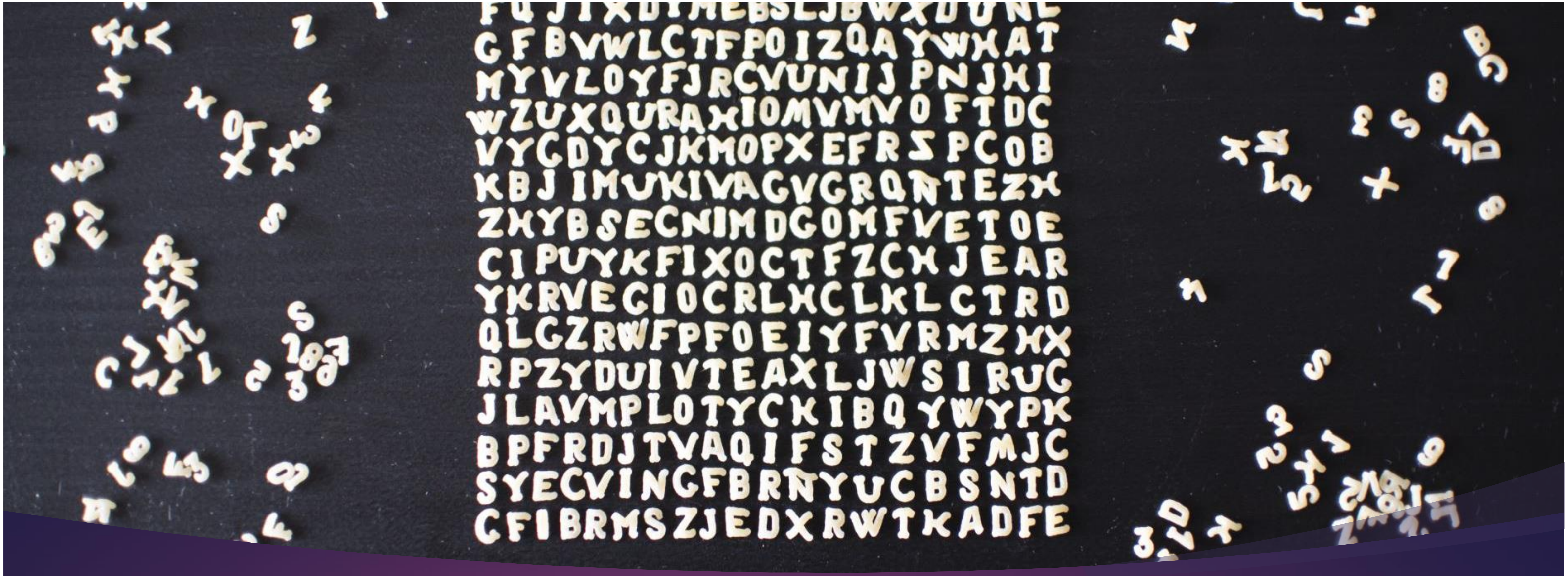


Section	Details
Executive Summary	
Scope	Provide an overview of the scope of the Purple Team engagement.
Scenarios Exercised	List and describe the scenarios that were exercised during the engagement.
Assessment Results	Include a visual representation of the assessed attack path, highlight attack entry points and map the prevention, and detection and response capabilities discovered against the tactics, techniques, and procedures exercised. For example, this may include a detection and response capability heat map overlay to the MITRE ATT&CK tactics and techniques.
Recommendations	Provide high-level recommendations based on the engagement results.
Technical Summary	
Detailed Scope – Purple Team Plan	Detail the specific scope of the Purple Team Plan, including targeted systems and objectives.
TTPs Assessed	List the tactics, techniques, and procedures (TTPs) that were evaluated during the engagement.
Assessment Results and Recommendations	Present the detailed results of the assessment, including:
	- **Prevention Capability**: Describe the current prevention capabilities assessed.
	- **Detection Capability**: Detail the detection capabilities and any gaps identified.
	- **Response Capability**: Outline the response capabilities and recommend improvements.
Appendices	
	Include any additional information, data, or documents that support the report findings.
Supplemental Data	
	Provide supplementary data that offers further insights or details, such as log files, screenshots, or additional analysis. Label screenshots for the reader and provide references to previous sections for which the screenshots/logs are relevant

Thought exercise – Purple Teaming a State Government

- what would be some Crown Jewels?
- What does Initial Access look like?

Open Discussions and Questions



Feedback QR Code