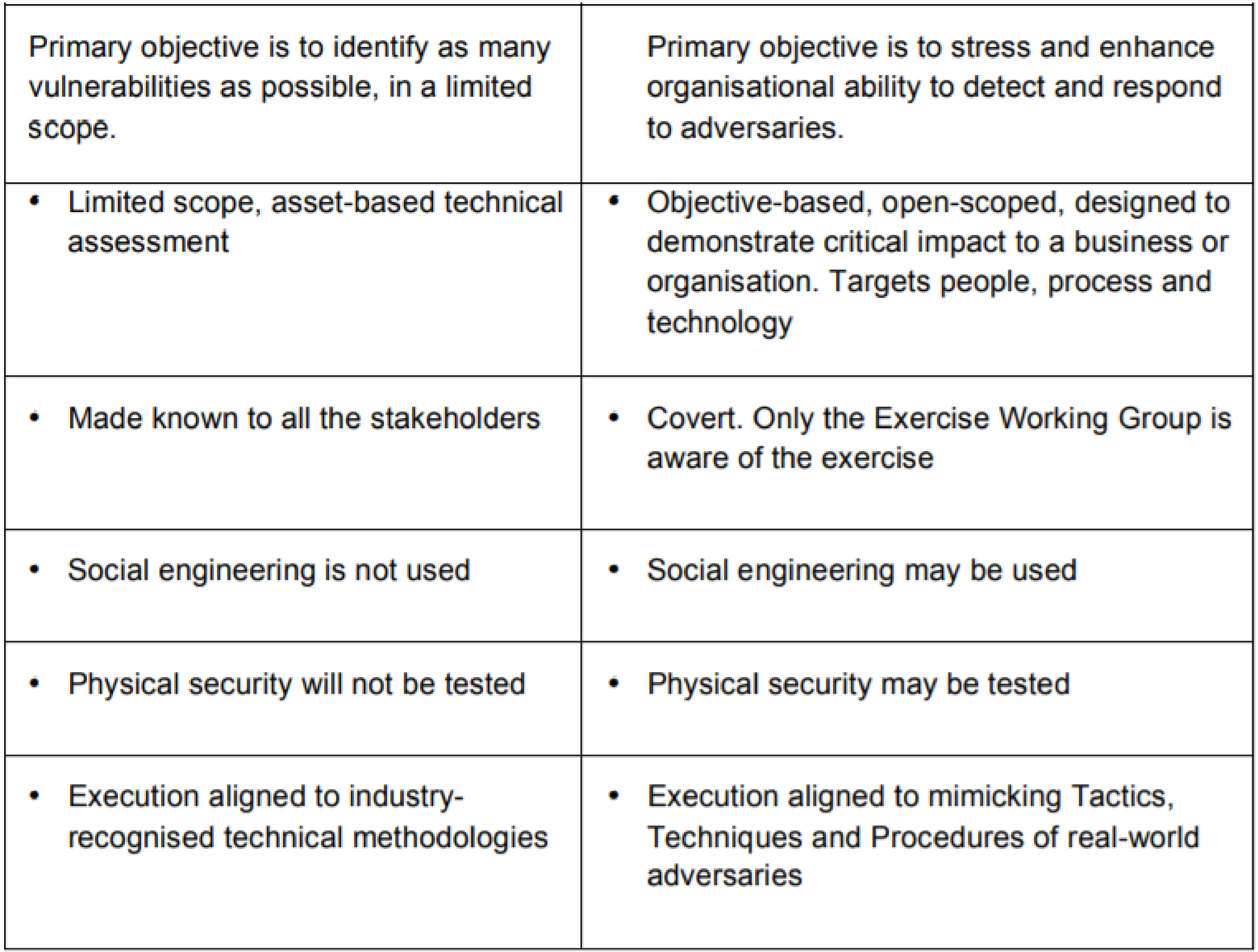
Threat Intelligence Based Red Teaming

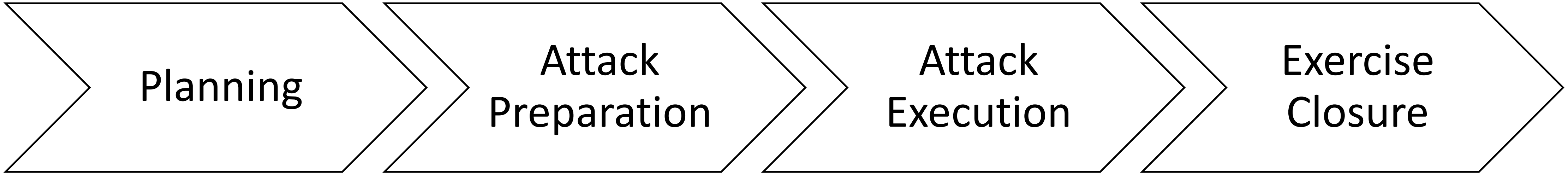
YYMTH

Traditional Penetration testing vs Red Teaming



Primary objective is to identify as many vulnerabilities as possible, in a limited scope.	Primary objective is to stress and enhance organisational ability to detect and respond to adversaries.
• Limited scope, asset-based technical assessment	• Objective-based, open-scoped, designed to demonstrate critical impact to a business or organisation. Targets people, process and technology
• Made known to all the stakeholders	• Covert. Only the Exercise Working Group is aware of the exercise
• Social engineering is not used	• Social engineering may be used
• Physical security will not be tested	• Physical security may be tested
• Execution aligned to industry-recognised technical methodologies	• Execution aligned to mimicking Tactics, Techniques and Procedures of real-world adversaries

Threat Intelligence Based Red Teaming



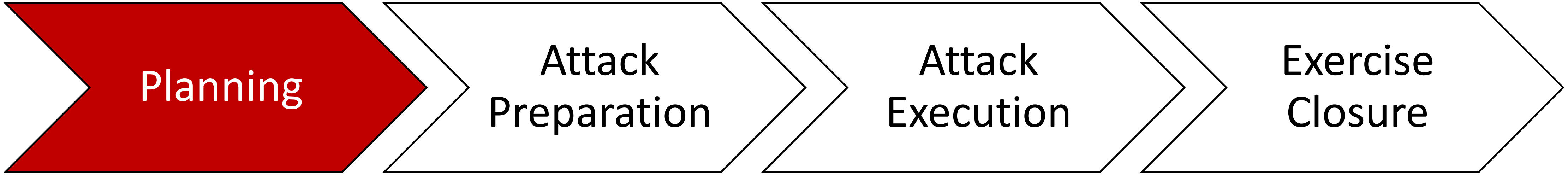
Planning

Attack Preparation

Attack Execution

Exercise Closure

Threat Intelligence Based Red Teaming



Planning

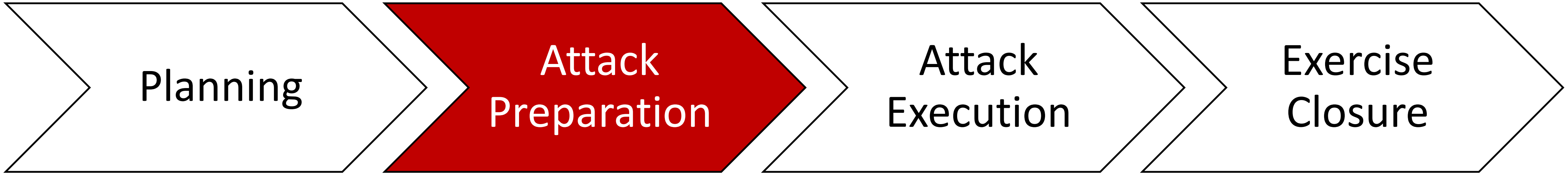
Attack Preparation

Attack Execution

Exercise Closure

- ✓ Define key exercise parameter
- ✓ Scope and duration
- ✓ Participation Model (Inhouse/Outsource)
- ✓ Exercise Working Group
- ✓ Escalation Process
- ✓ Budget
- ✓ Risk Management

Threat Intelligence Based Red Teaming



Planning

Attack Preparation

Attack Execution

Exercise Closure

✓ Critical function identification

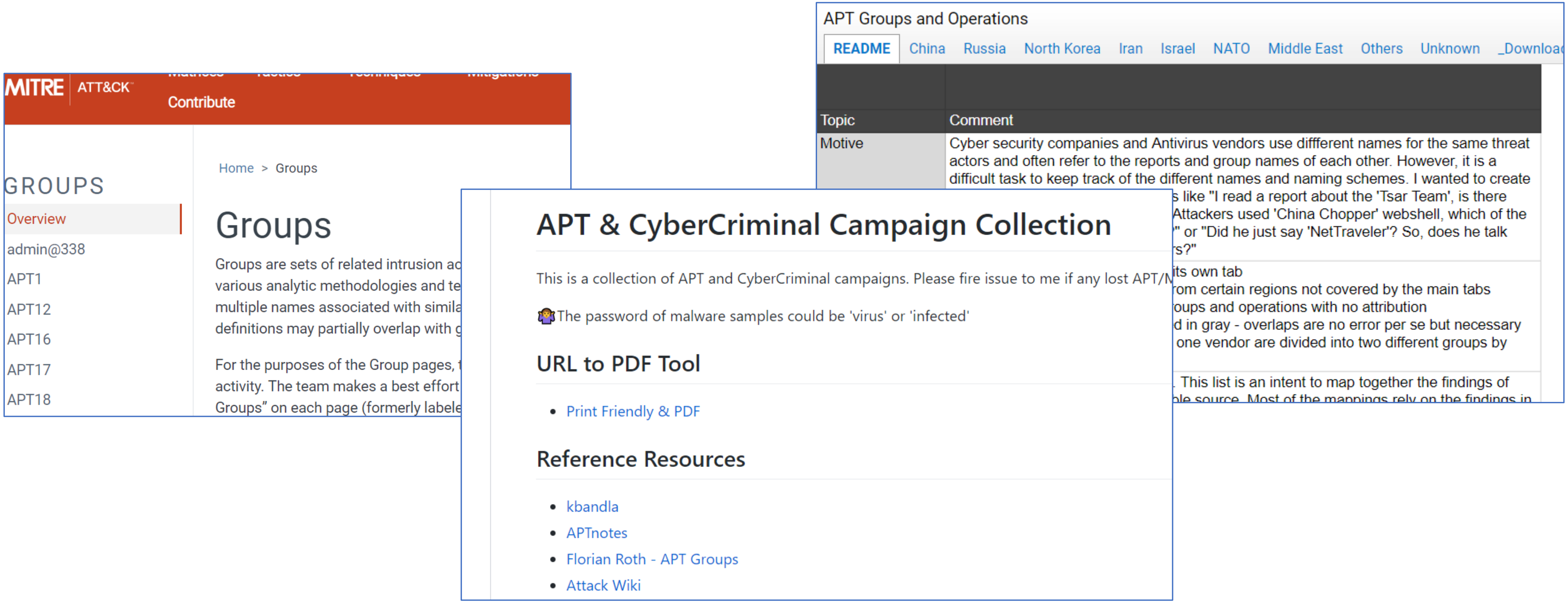
✓ Threat modelling (Targeted Threat Intell)

✓ Recon / OSINT

✓ Attack Scenario Creation

Threat Intelligence Based Red Teaming

- Targeted Threat Intelligence
  - Collect (Threat Intell Feeds/Platform, Public Reports, …)



Groups

Groups are sets of related intrusion ac
various analytic methodologies and te
multiple names associated with simila
definitions may partially overlap with g

For the purposes of the Group pages, t
activity. The team makes a best effort
Groups" on each page (formerly labele

APT Groups and Operations

Topic	Comment
Motive	Cyber security companies and Antivirus vendors use diffferent names for the same threat actors and often refer to the reports and group names of each other. However, it is a difficult task to keep track of the different names and naming schemes. I wanted to create

s like "I read a report about the 'Tsar Team', is there
Attackers used 'China Chopper' webshell, which of the
" or "Did he just say 'NetTraveler'? So, does he talk
rs?"

its own tab
rom certain regions not covered by the main tabs
oups and operations with no attribution
d in gray - overlaps are no error per se but necessary
one vendor are divided into two different groups by

. This list is an intent to map together the findings of
ble source. Most of the mappings rely on the findings in

APT & CyberCriminal Campaign Collection

This is a collection of APT and CyberCriminal campaigns. Please fire issue to me if any lost APT/M

🤷The password of malware samples could be 'virus' or 'infected'

URL to PDF Tool

- Print Friendly & PDF

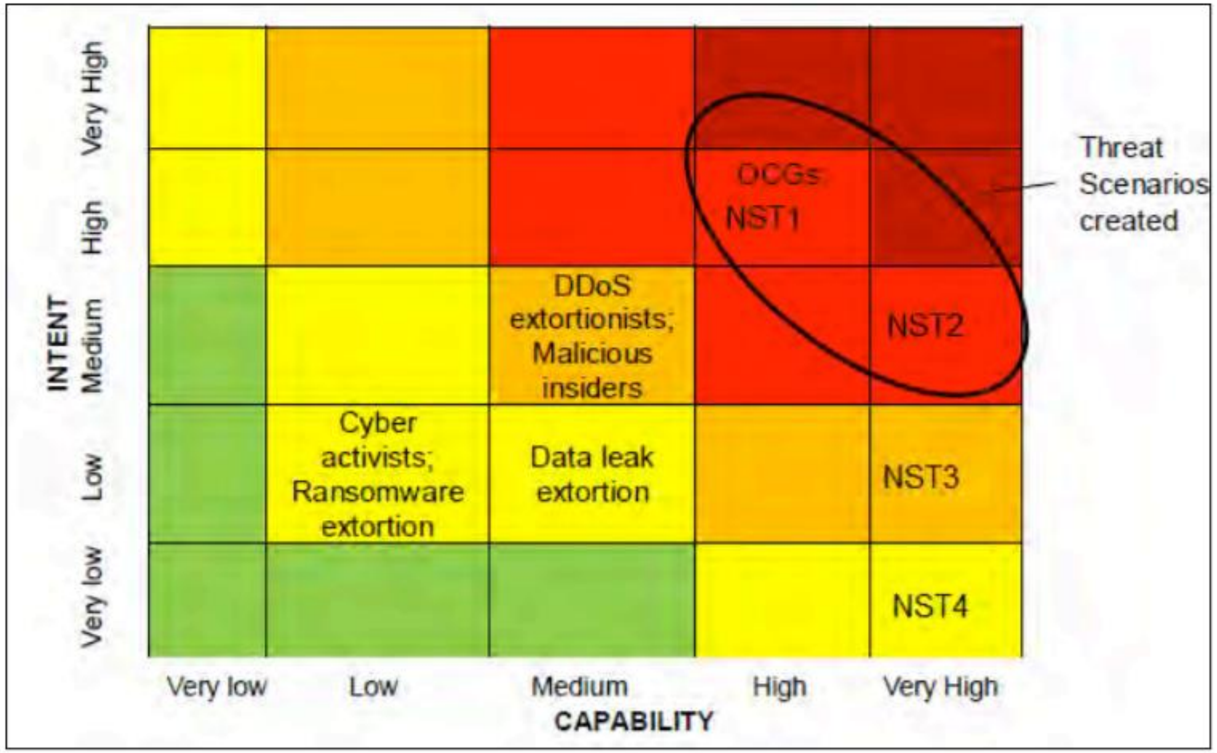
Reference Resources

- kbandla
- APTnotes
- Florian Roth - APT Groups
- Attack Wiki

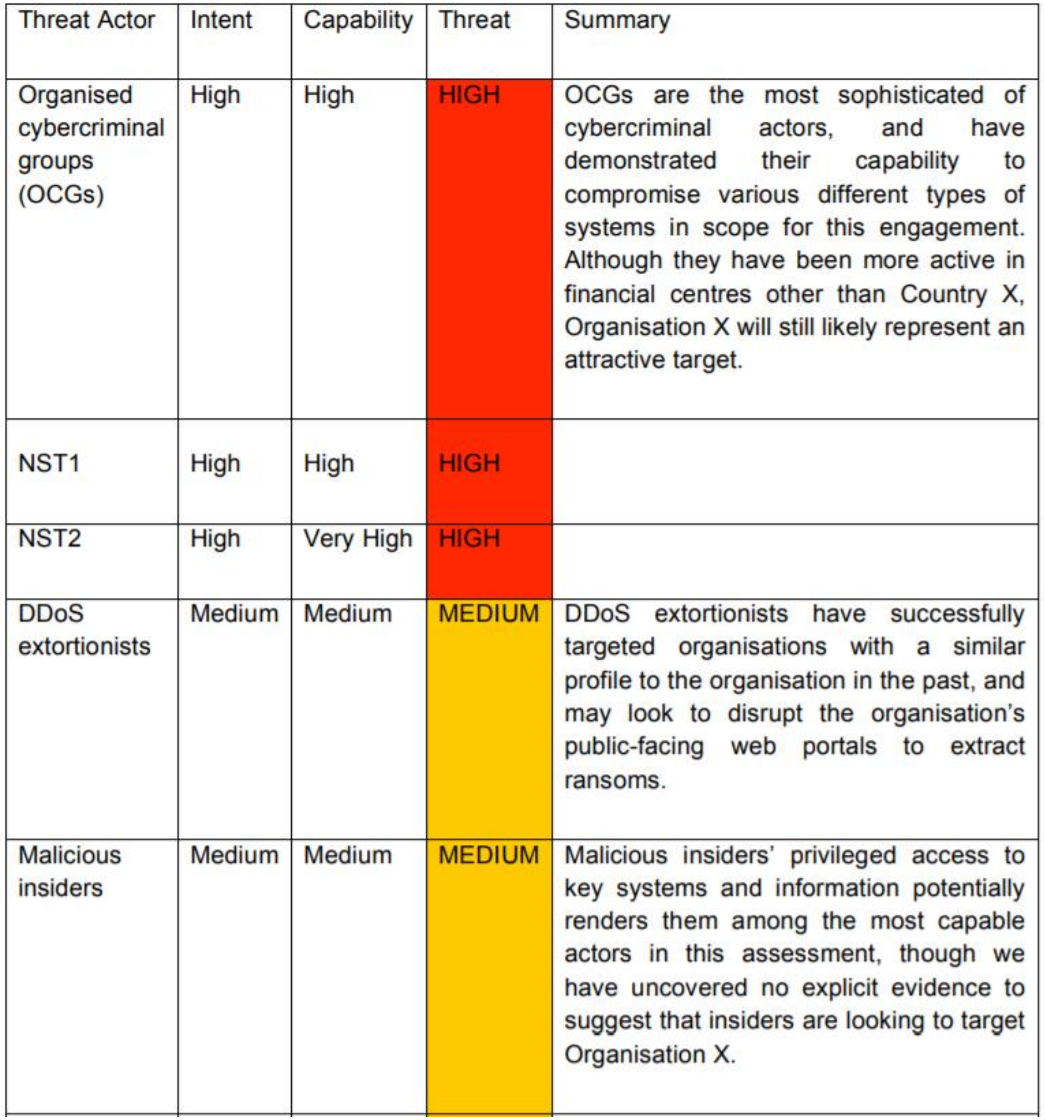
Threat Intelligence Based Red Teaming

- Targeted Threat Intelligence

Threat matrix sample

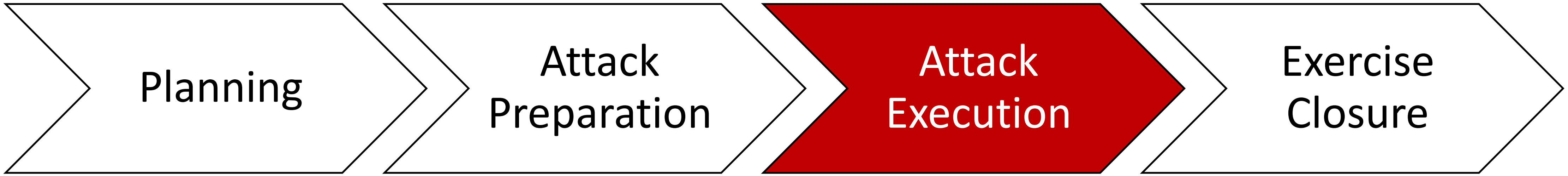


Threat Summary Table Sample



Threat Actor	Intent	Capability	Threat	Summary
Organised cybercriminal groups (OCGs)	High	High	HIGH	OCGs are the most sophisticated of cybercriminal actors, and have demonstrated their capability to compromise various different types of systems in scope for this engagement. Although they have been more active in financial centres other than Country X, Organisation X will still likely represent an attractive target.
NST1	High	High	HIGH	
NST2	High	Very High	HIGH	
DDoS extortionists	Medium	Medium	MEDIUM	DDoS extortionists have successfully targeted organisations with a similar profile to the organisation in the past, and may look to disrupt the organisation's public-facing web portals to extract ransoms.
Malicious insiders	Medium	Medium	MEDIUM	Malicious insiders' privileged access to key systems and information potentially renders them among the most capable actors in this assessment, though we have uncovered no explicit evidence to suggest that insiders are looking to target Organisation X.

Threat Intelligence Based Red Teaming

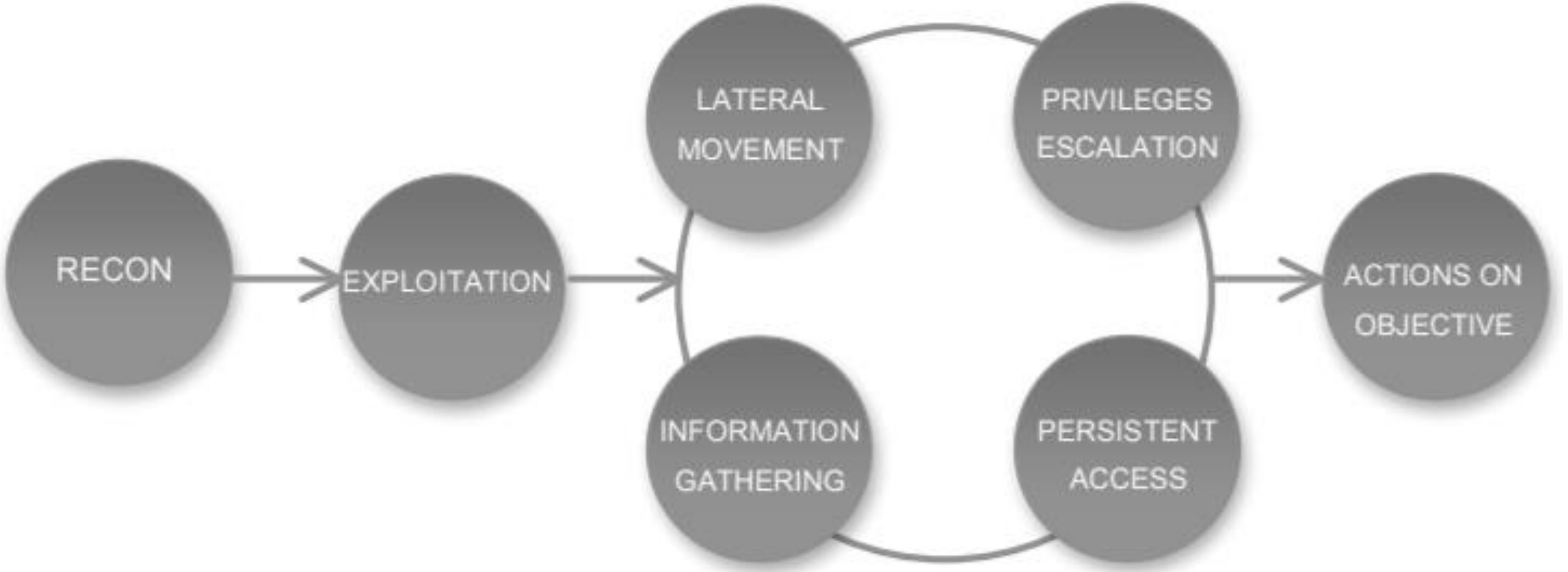


Planning

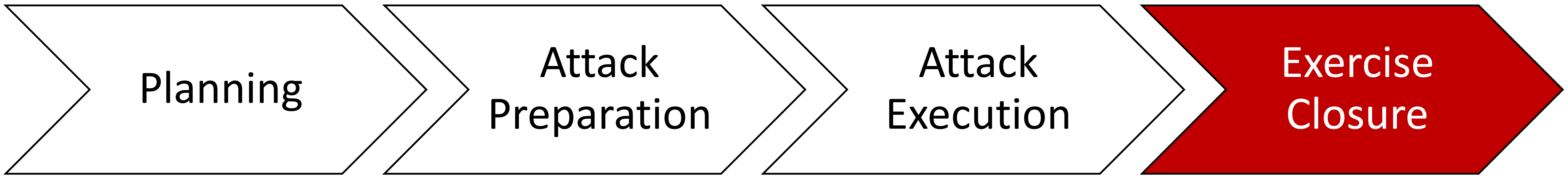
Attack Preparation

Attack Execution

Exercise Closure



Threat Intelligence Based Red Teaming



Planning

Attack Preparation

Attack Execution

Exercise Closure

- ✓ Clean up / revert and remediation
- ✓ Defence Report
- ✓ Attack/defence replay
- ✓ Final report and recommendation

Red Teaming Guideline

- CBEST:

https://www.bankofengland.co.uk/financial-stability/financial-sector-continuity

- TIBER-EU:

https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf

- iCAST:

http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-andcircular/2016/20161221e1.pdf

- AASE

https://abs.org.sg/docs/library/abs-red-team-adversarial-attack-simulation-exercises-guidelines-v1-06766a69f299c69658b7dff00006ed795.pdf

Automated Attack Simulation

- Infection monkey
- Red canary
- Metta
- APT Simulator
- Red Team Automation
- CALDERA
- Invoke-Adversary

Full list : http://pentestit.com/adversary-emulation-tools-list/

Thank you

- Q & A