Adaptive Adversary Emulation with

SANS Purple Team Summit

MITRE

System Owner/User Discovery (T1033)

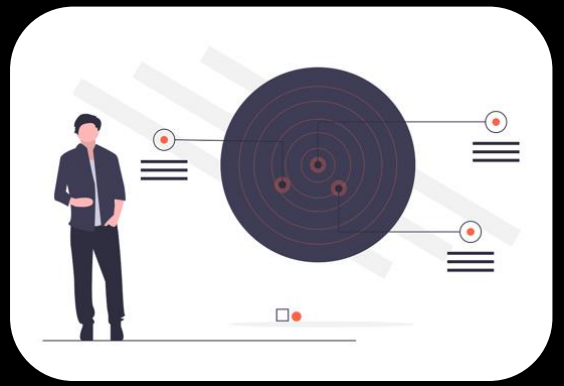
Timothy Schulz

Senior Cyber Adversarial Engineer

@teschulz

Adversary Emulation Researcher

Adversary Emulation: Why?



Result Prioritization

Verify Defenses

Identify Gaps

ATT&CK™

MITRE

Adversary Emulation: What?

Red Team

+ ATT&CK

Cyber Threat Intelligence (CTI)

“Threat Driven Red Teaming”

Adversary Emulation: CTI

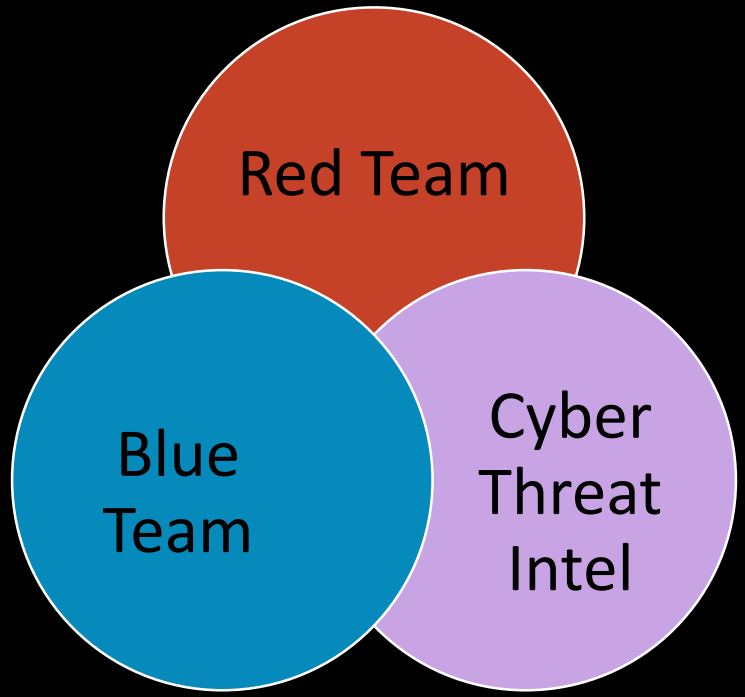
ATT&CK

Tactic: Discovery

Technique: System Owner/User Discovery

Procedure: whoami

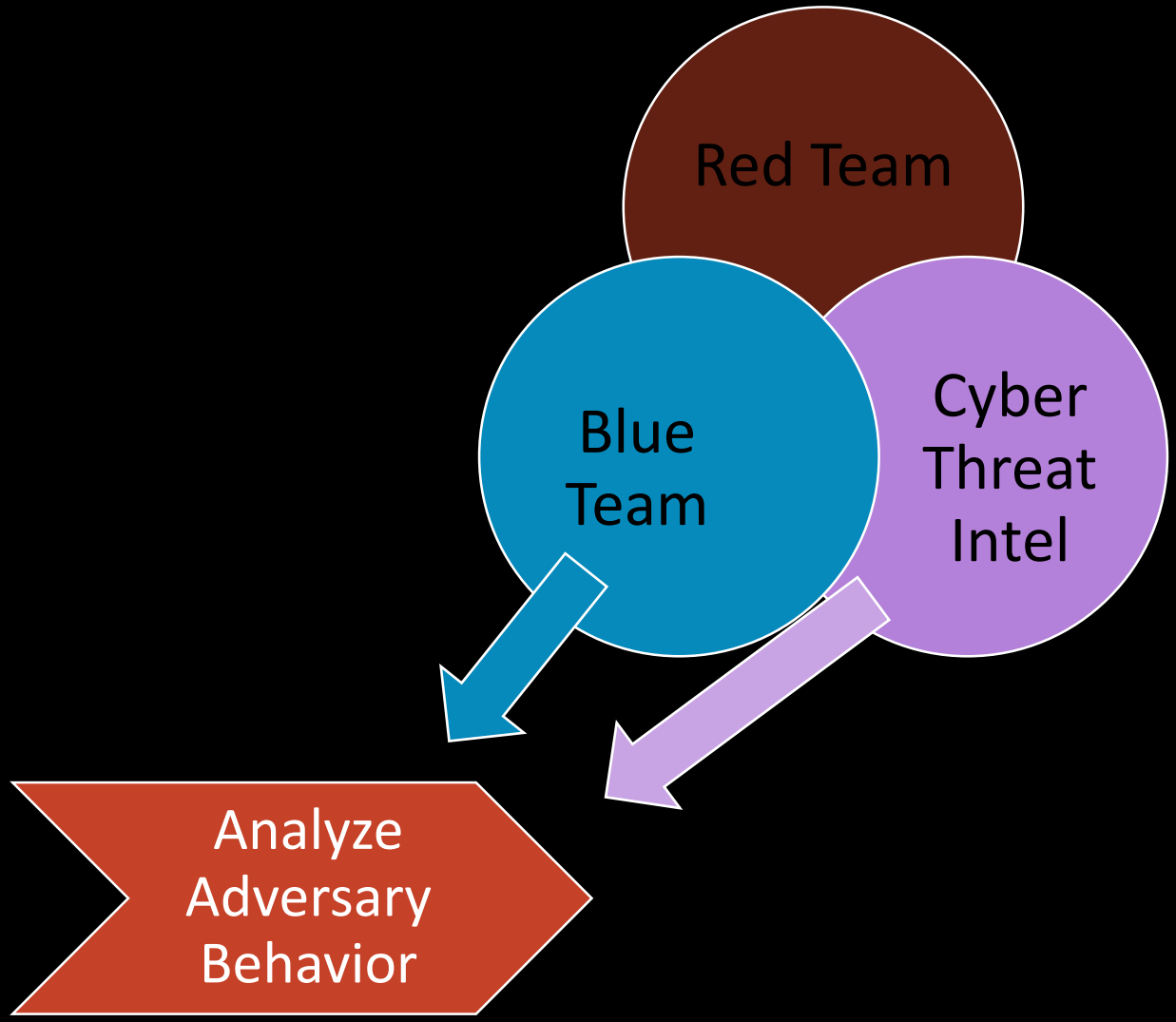
Adversary Emulation: Collaboration



ATT&CK™

MITRE

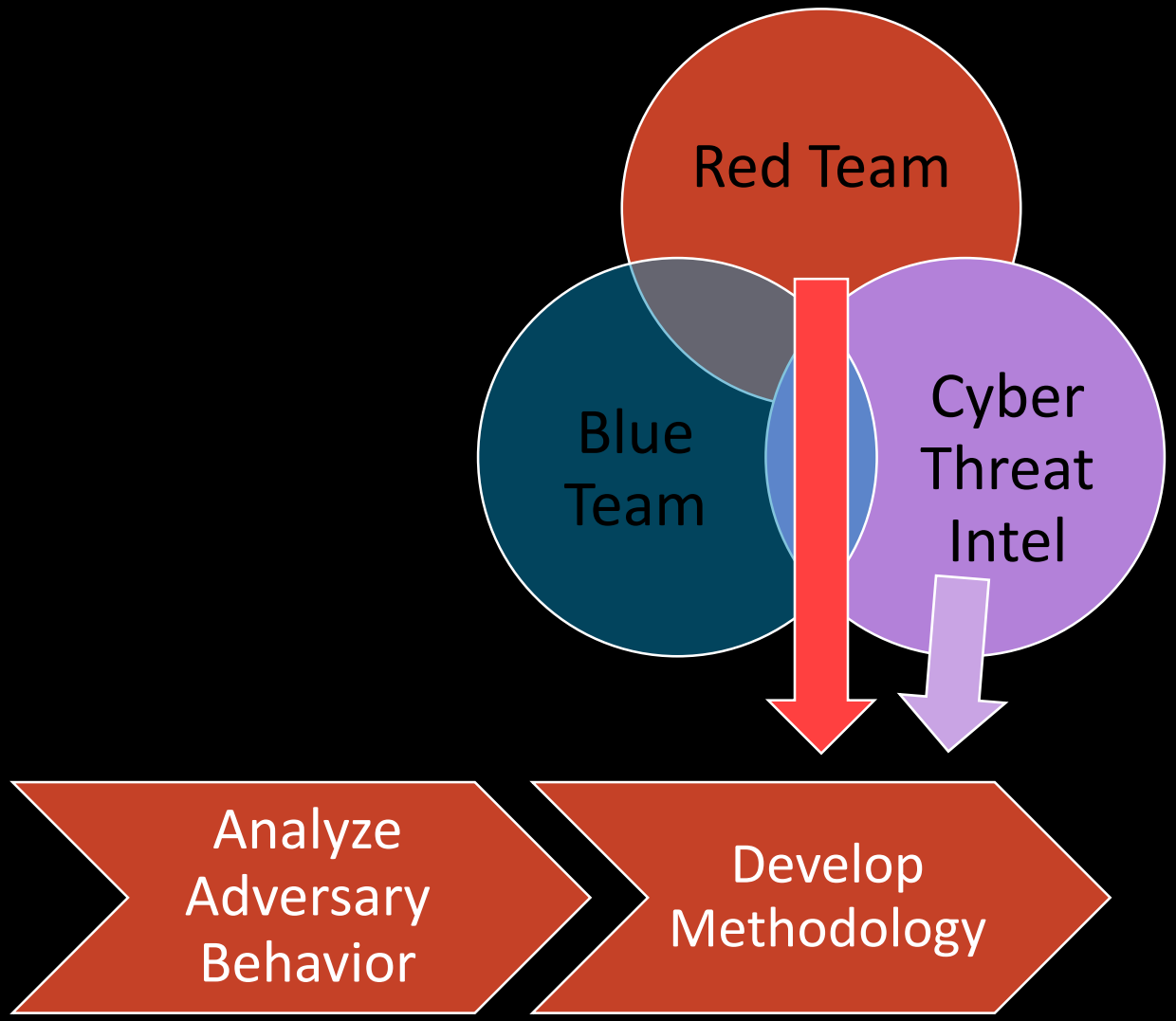
Adversary Emulation: Collaboration



ATT&CK™

MITRE

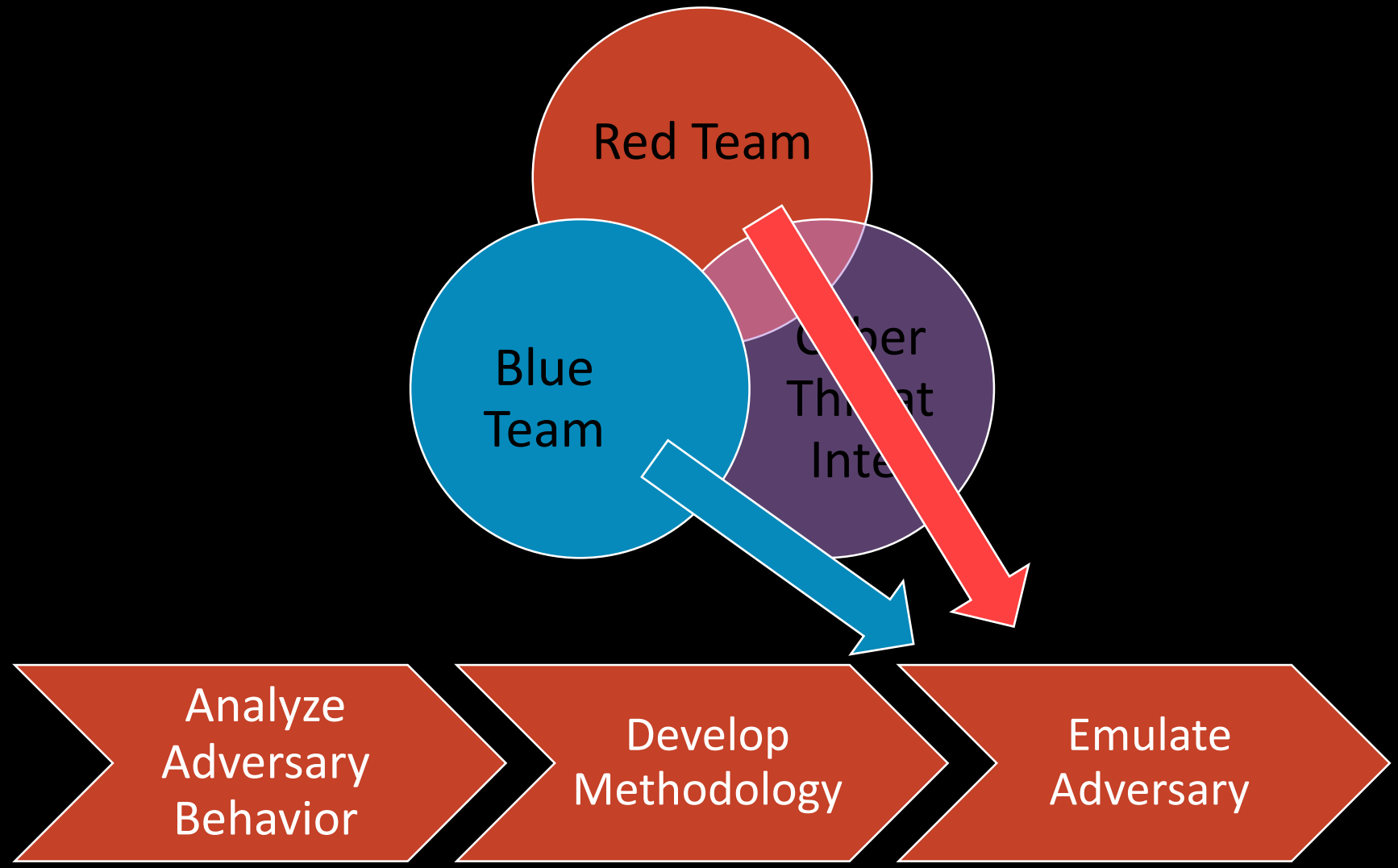
Adversary Emulation: Collaboration



ATT&CK™

MITRE

Adversary Emulation: Collaboration



ATT&CK™

MITRE

Challenges

- Adversary reporting and CTI is historic data

- Reports are ingested manually
- Old TTPs may not work in modern environment

Result: Bad Tests

1

VS

2

Red Team scoped to old CTI

Blue with modern EDR/NIDS

1. https://upload.wikimedia.org/wikipedia/commons/d/dc/Retrato_de_Julio_C%C3%A9sar_%2826724093101%29.jpg
2. https://www.indiastrategic.in/wp-content/uploads/2019/04/Spyder-SR_1-1024x681.jpg

Result: Bad Tests

1

VS

LOL

2

Red Team scoped to old CTI

Blue with modern EDR/NIDS

1. https://upload.wikimedia.org/wikipedia/commons/d/dc/Retrato_de_Julio_C%C3%A9sar_%2826724093101%29.jpg
2. https://www.indiastrategic.in/wp-content/uploads/2019/04/Spyder-SR_1-1024x681.jpg

Result: Bad Tests

1

VS

You belong in a museum!

2

Lessons learned?

Red Team scoped to old CTI

Blue with modern EDR/NIDS

1. https://upload.wikimedia.org/wikipedia/commons/d/dc/Retrato_de_Julio_C%C3%A9sar_%2826724093101%29.jpg
2. https://www.indiastrategic.in/wp-content/uploads/2019/04/Spyder-SR_1-1024x681.jpg

Solution: Even the odds

1,3

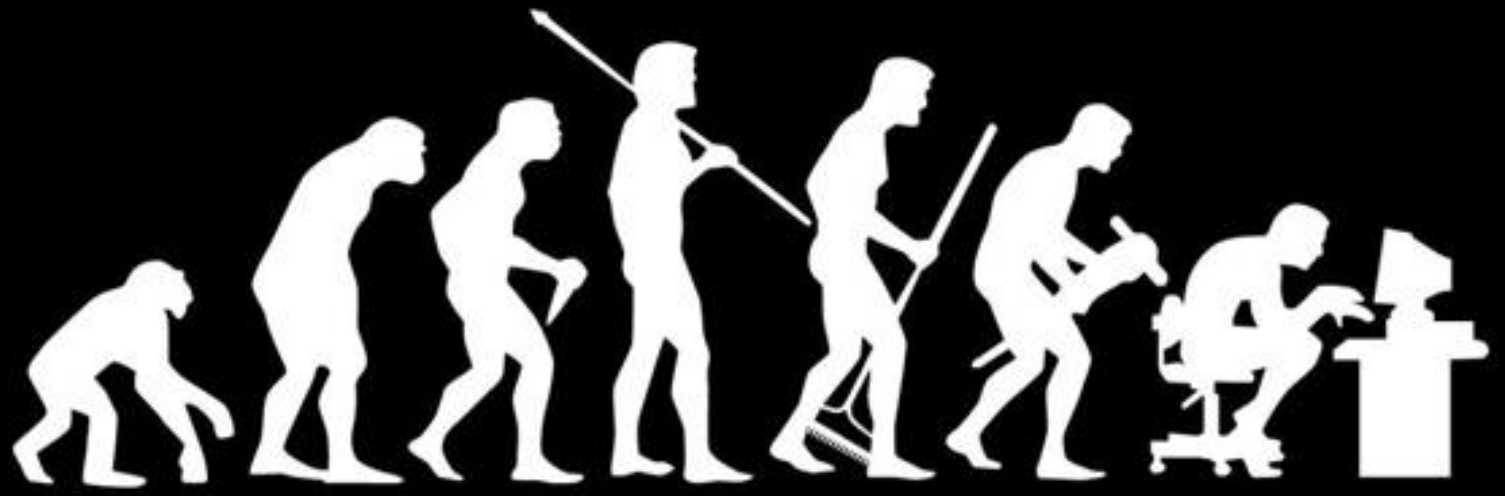
2

Adaptive Emulation

Modern EDR and NIDS

1. https://upload.wikimedia.org/wikipedia/commons/d/dc/Retrato_de_Julio_C%C3%A9sar_%2826724093101%29.jpg
2. https://www.indiastrategic.in/wp-content/uploads/2019/04/Spyder-SR_1-1024x681.jpg
3. https://images-na.ssl-images-amazon.com/images/I/61tcbl448lL._SY355_.jpg

How do we adapt?

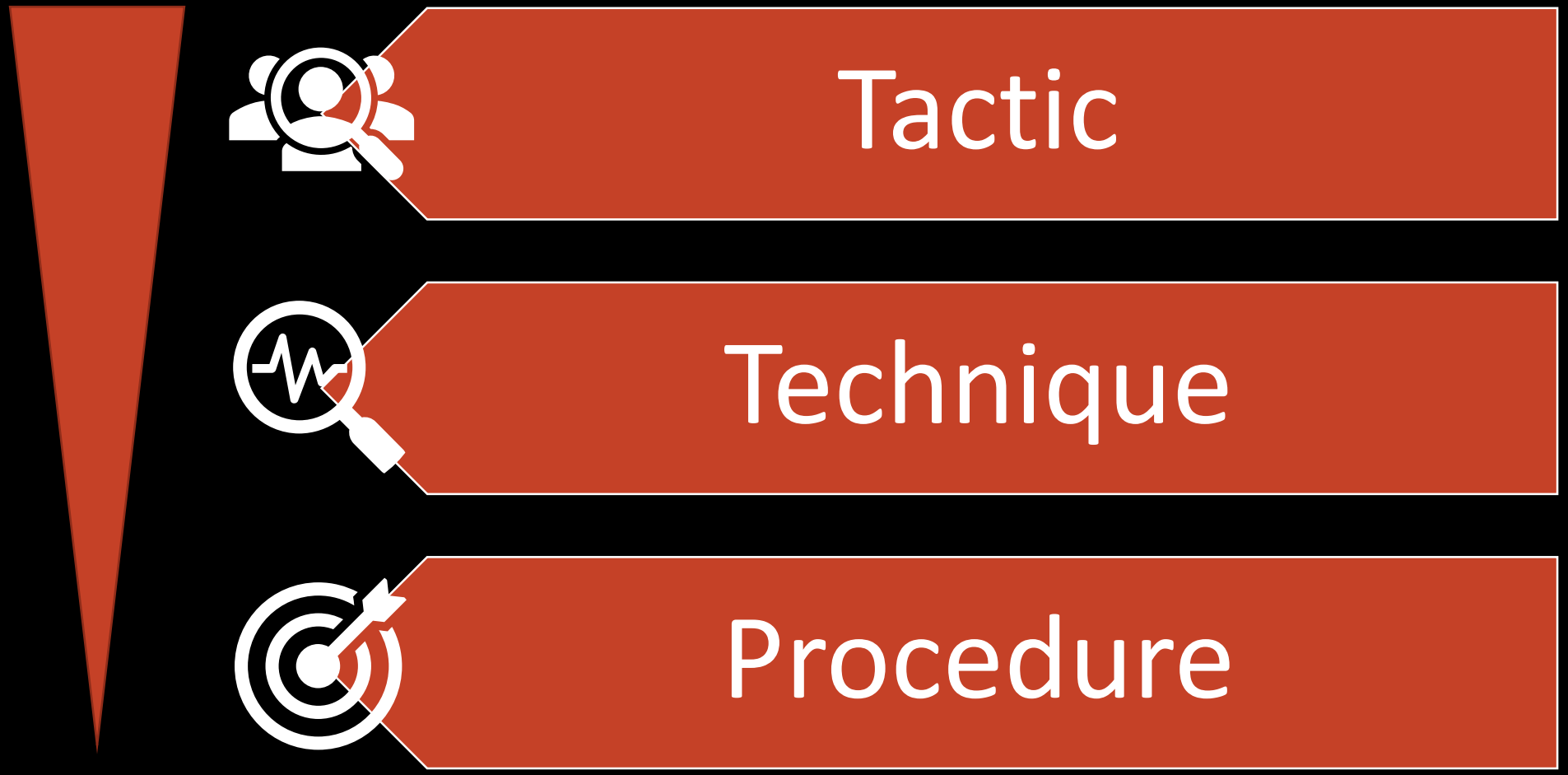


4

4. https://miro.medium.com/max/1200/1*XfjdqaabOCZj5CRb8QcmFg.jpeg

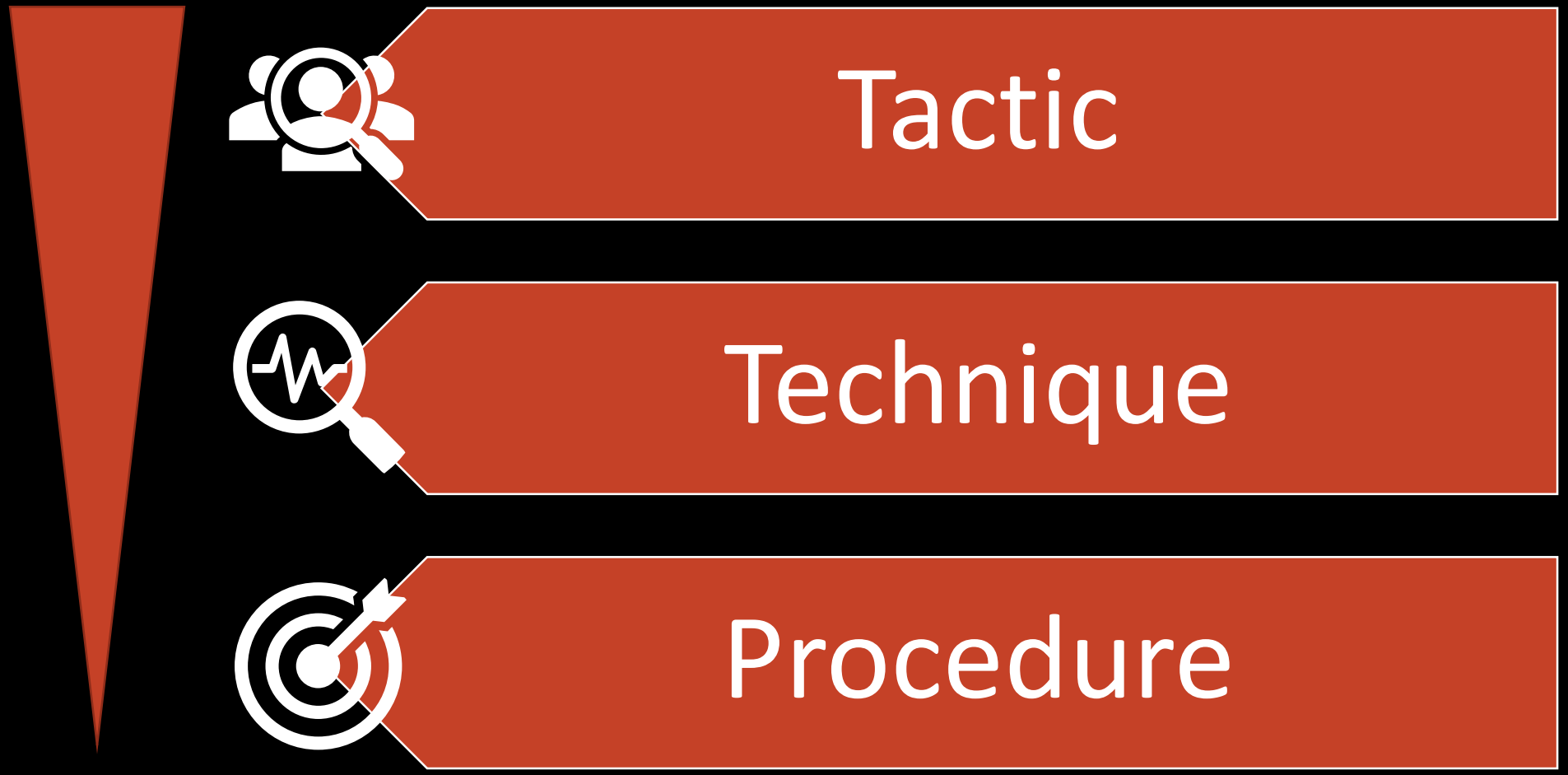
Solution: Variance in TTP

ATT&CK



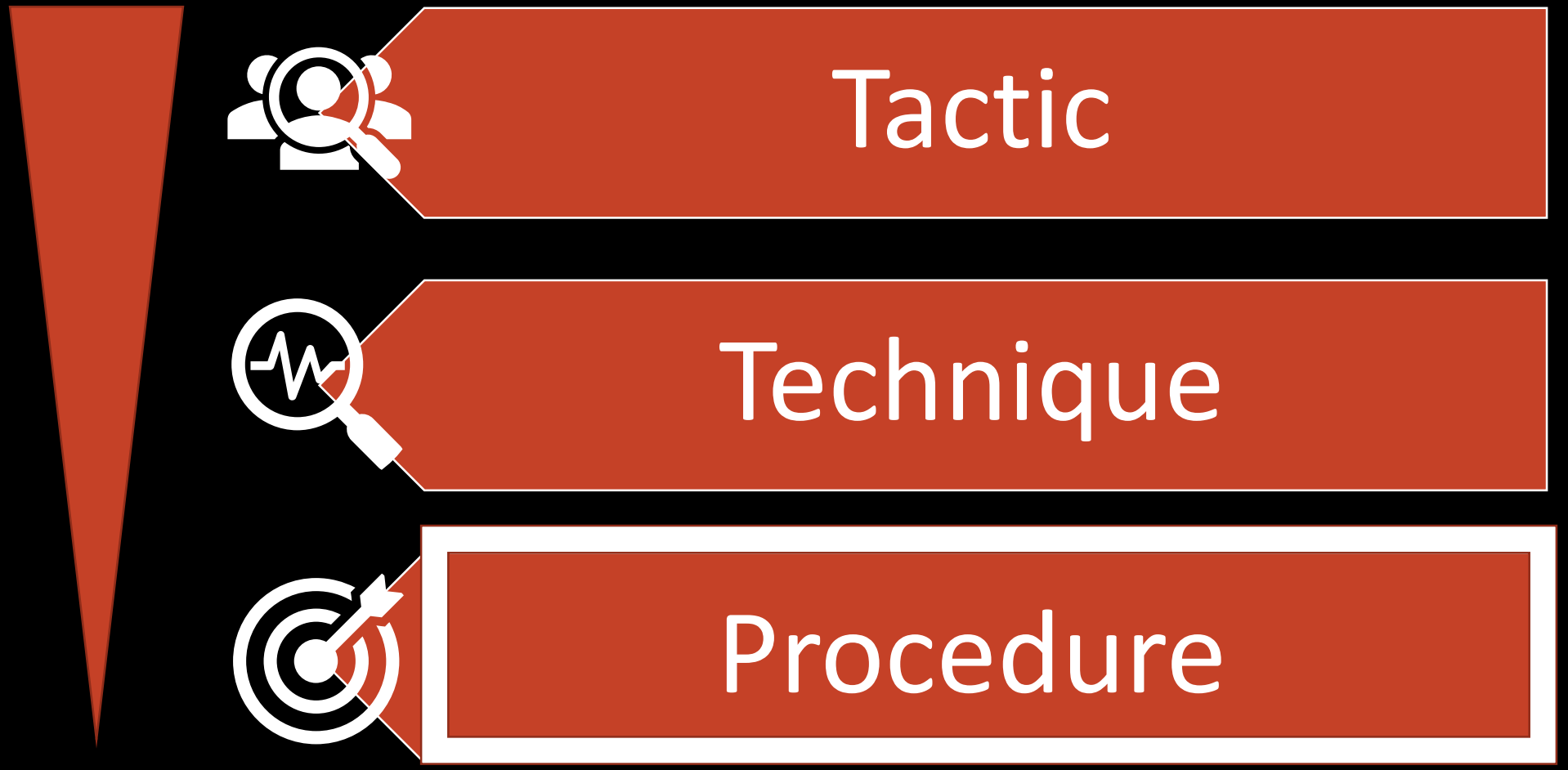
Solution: Variance in TTP

Deliberate ATT&CK

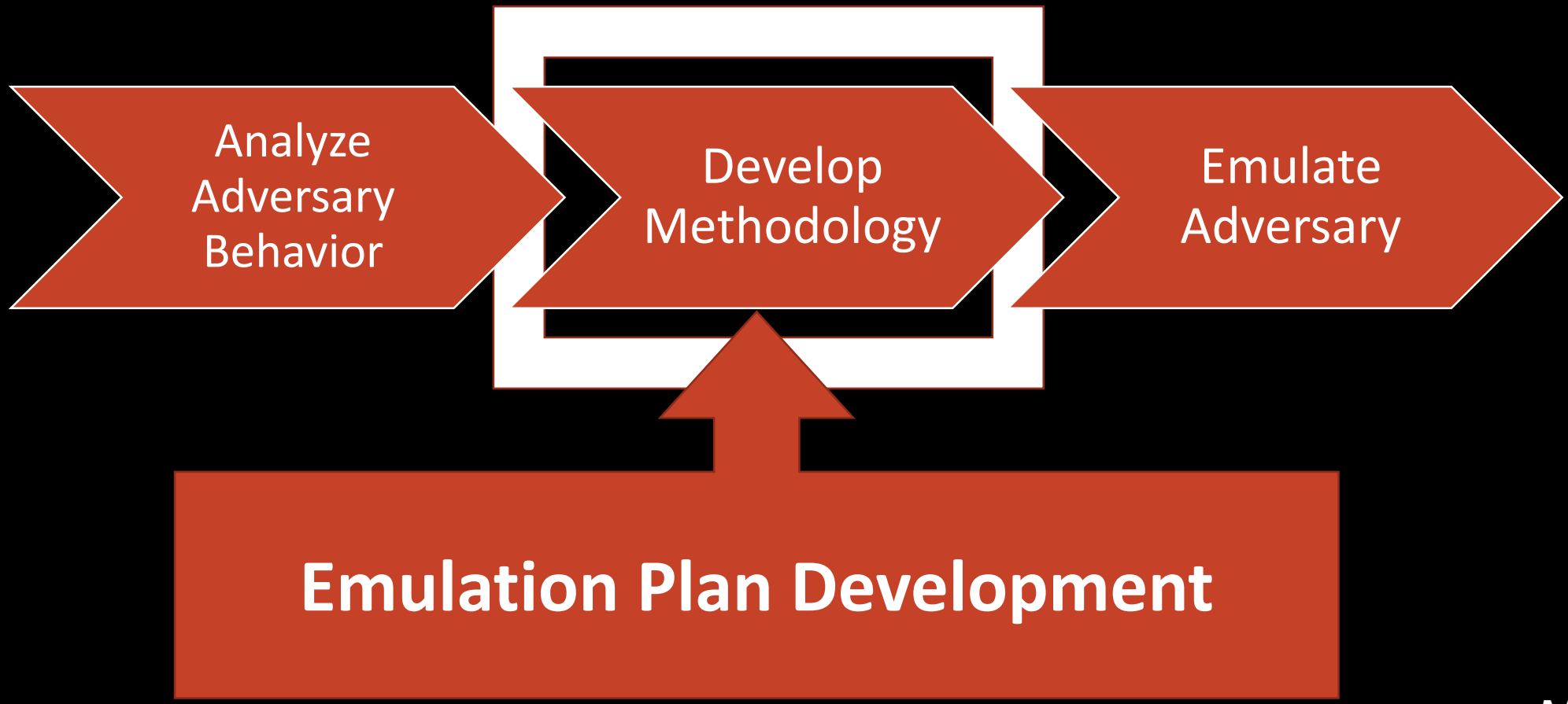


Solution: Variance in TTP

Deliberate ATT&CK



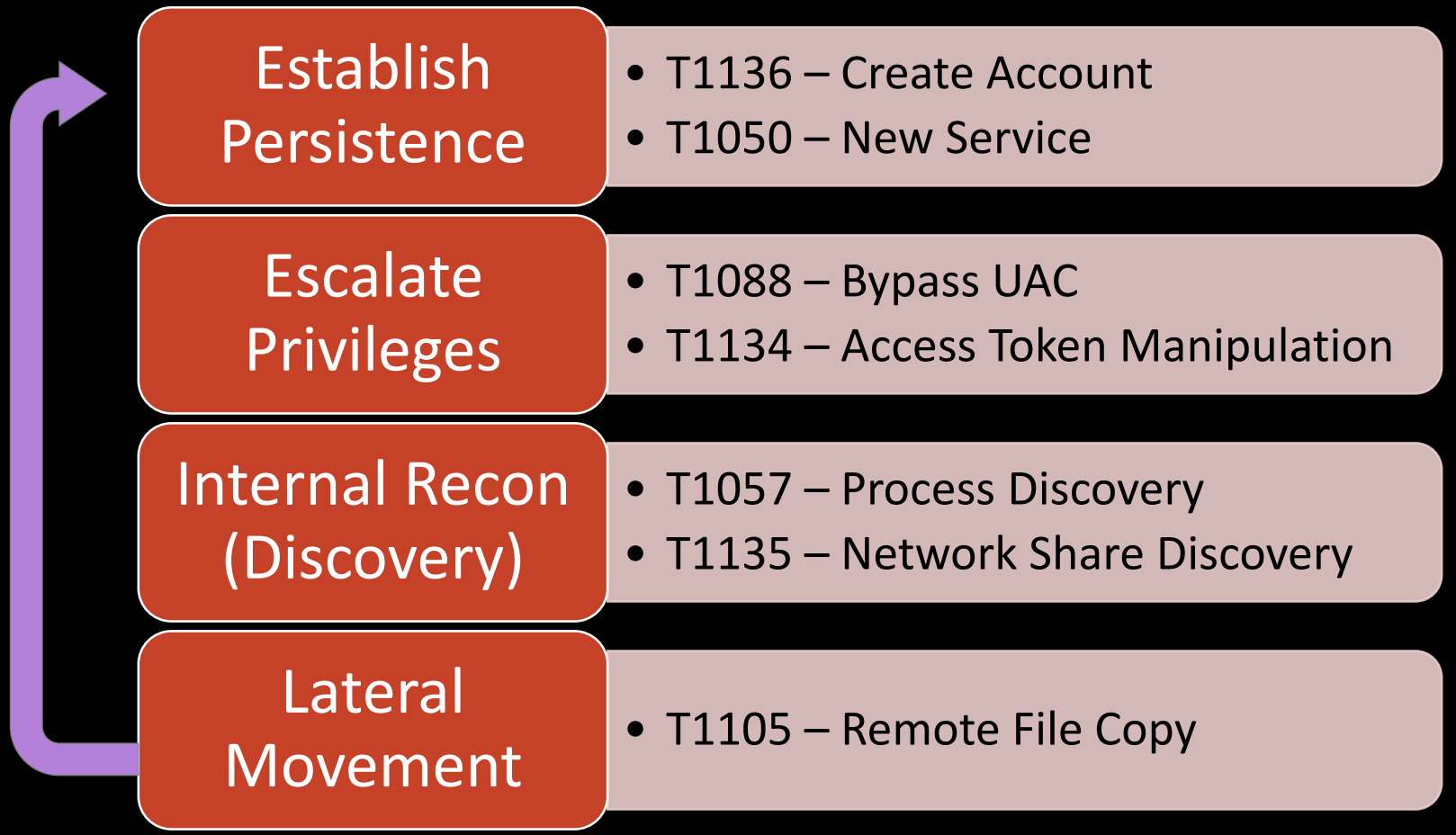
Adapt: Where?



ATT&CK™

MITRE

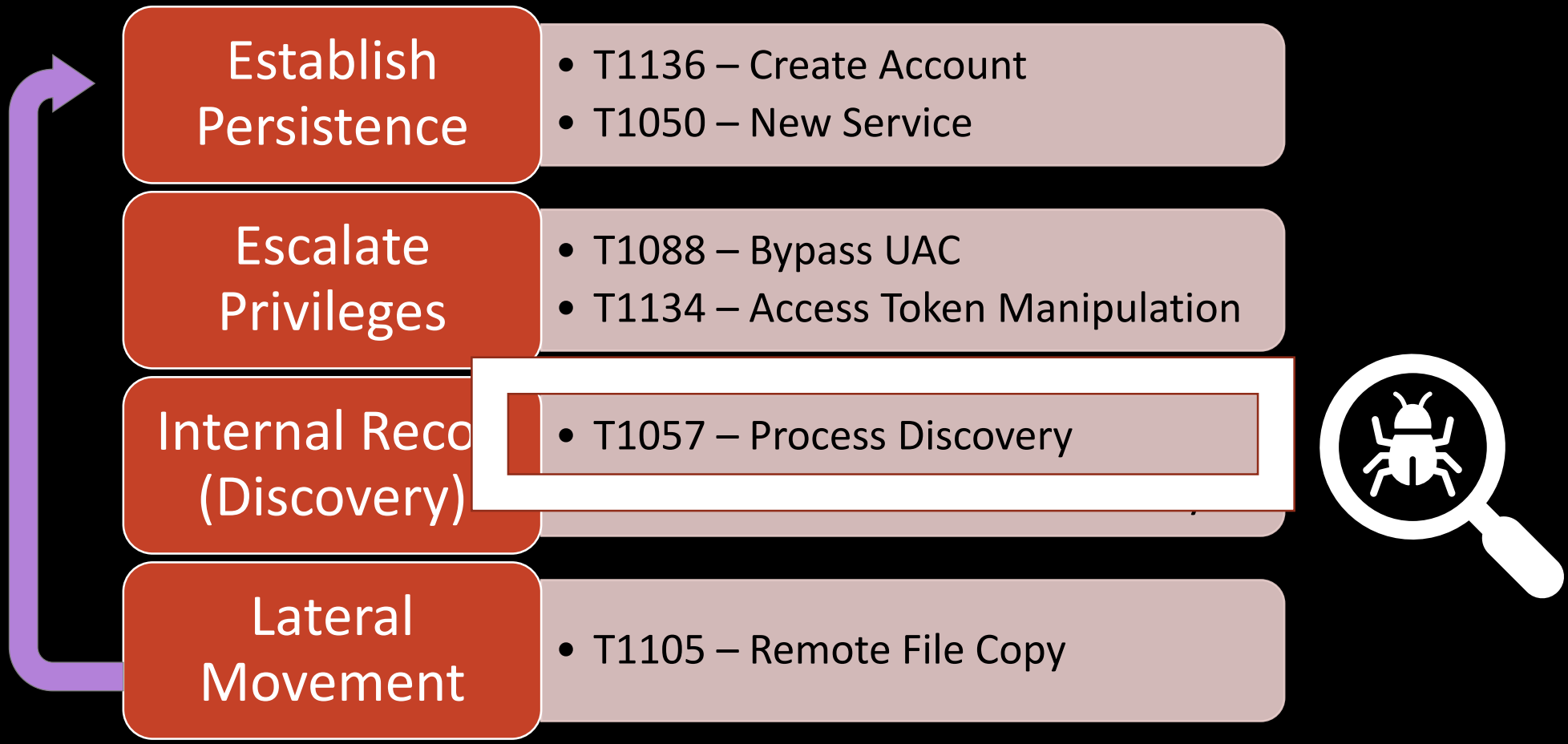
Adapt: Example Emulation Plan



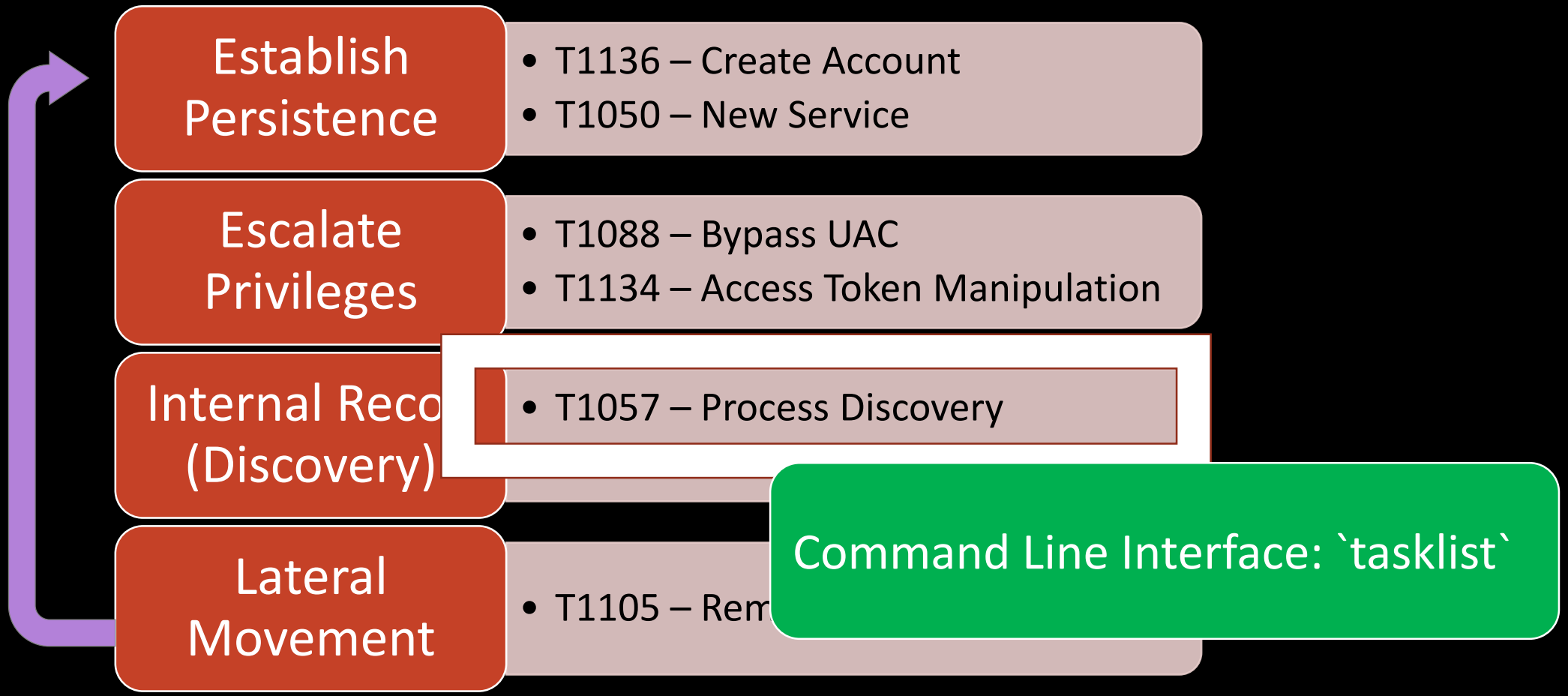
ATT&CK™

MITRE

Adapt: Example Emulation Plan

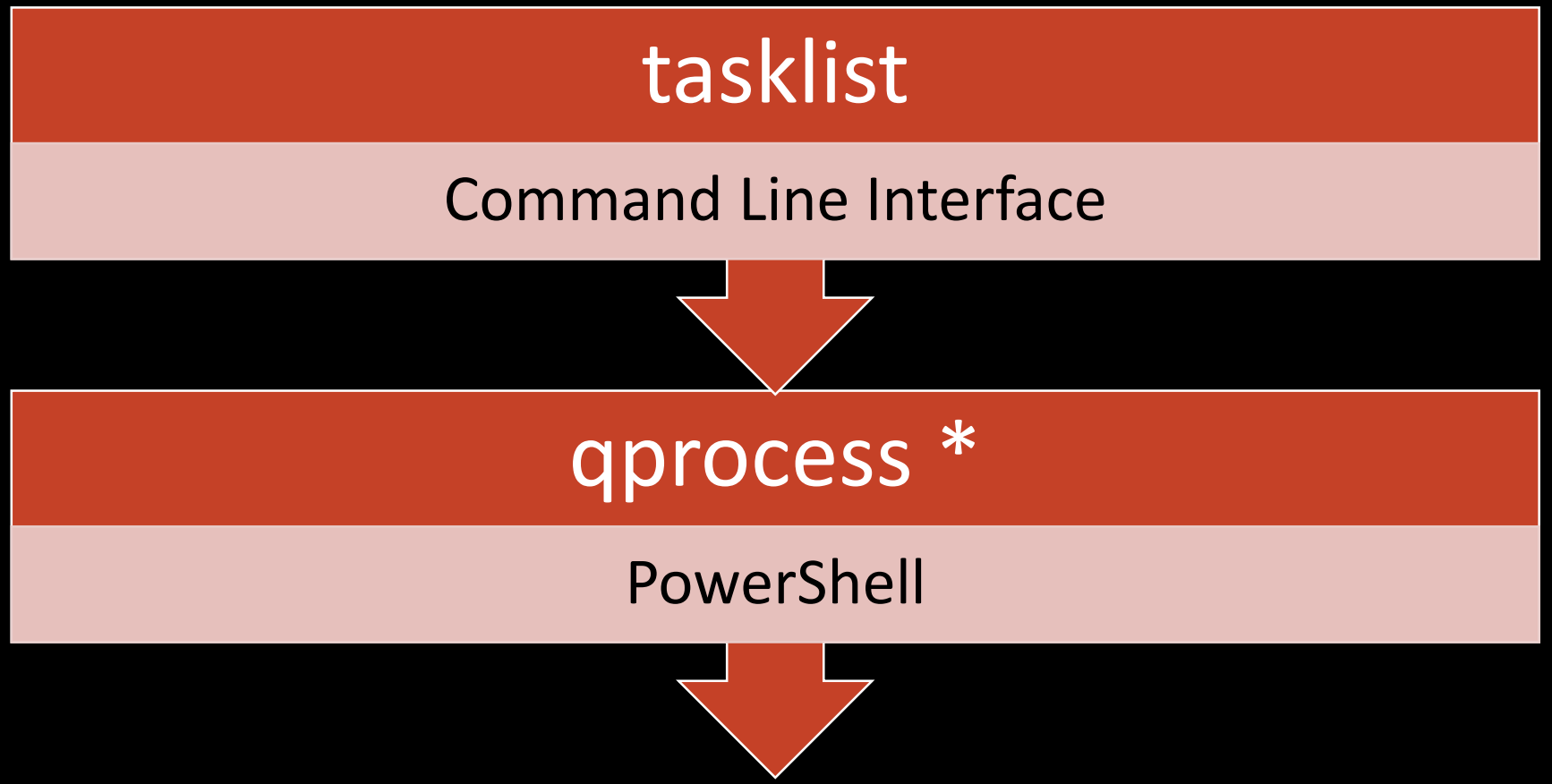


Adapt: Example Emulation Plan

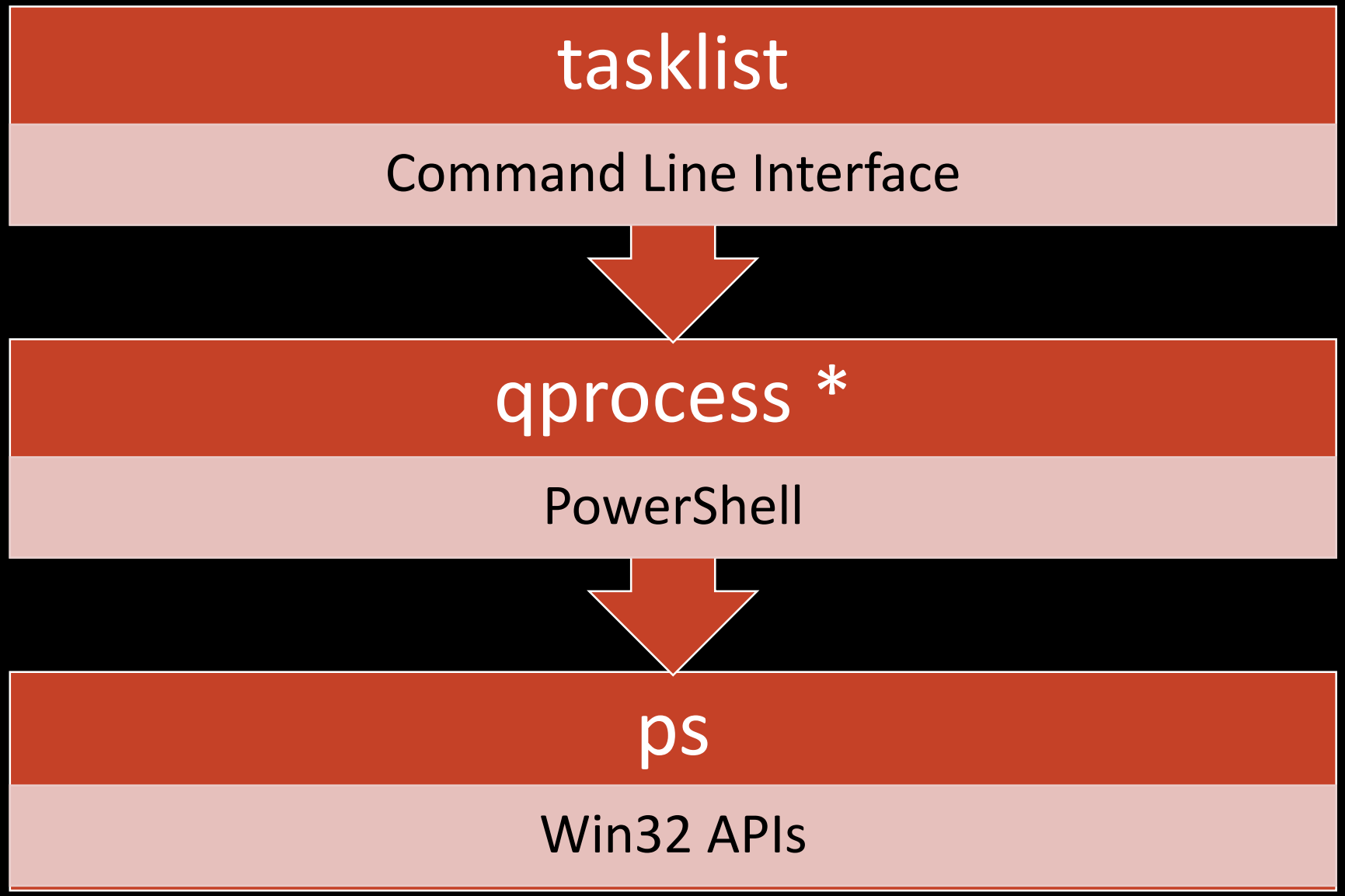


Adapt: Process Discovery (T1057)

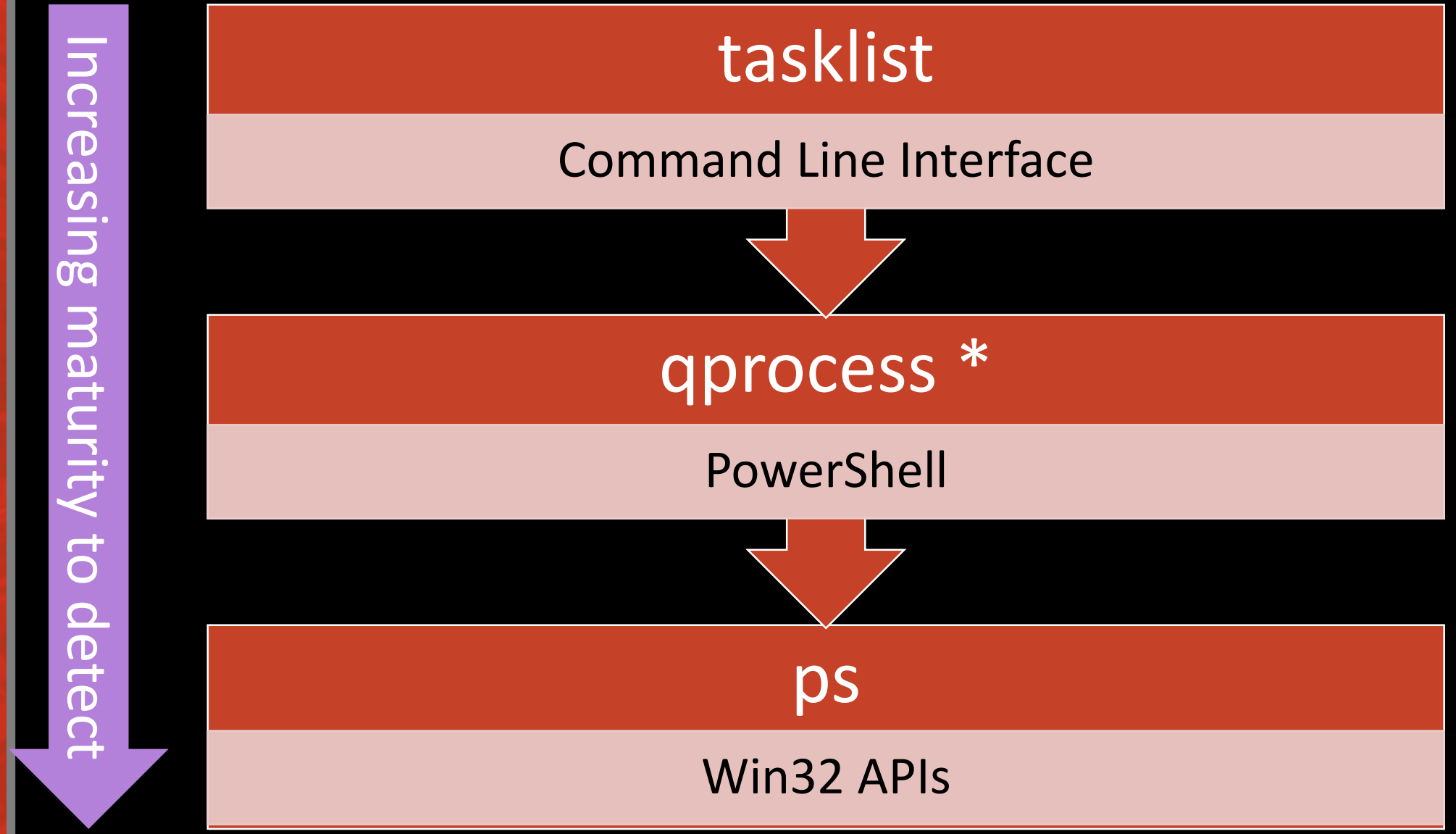
Adapt: Process Discovery (T1057)



Adapt: Process Discovery (T1057)



Adapt: Process Discovery (T1057)

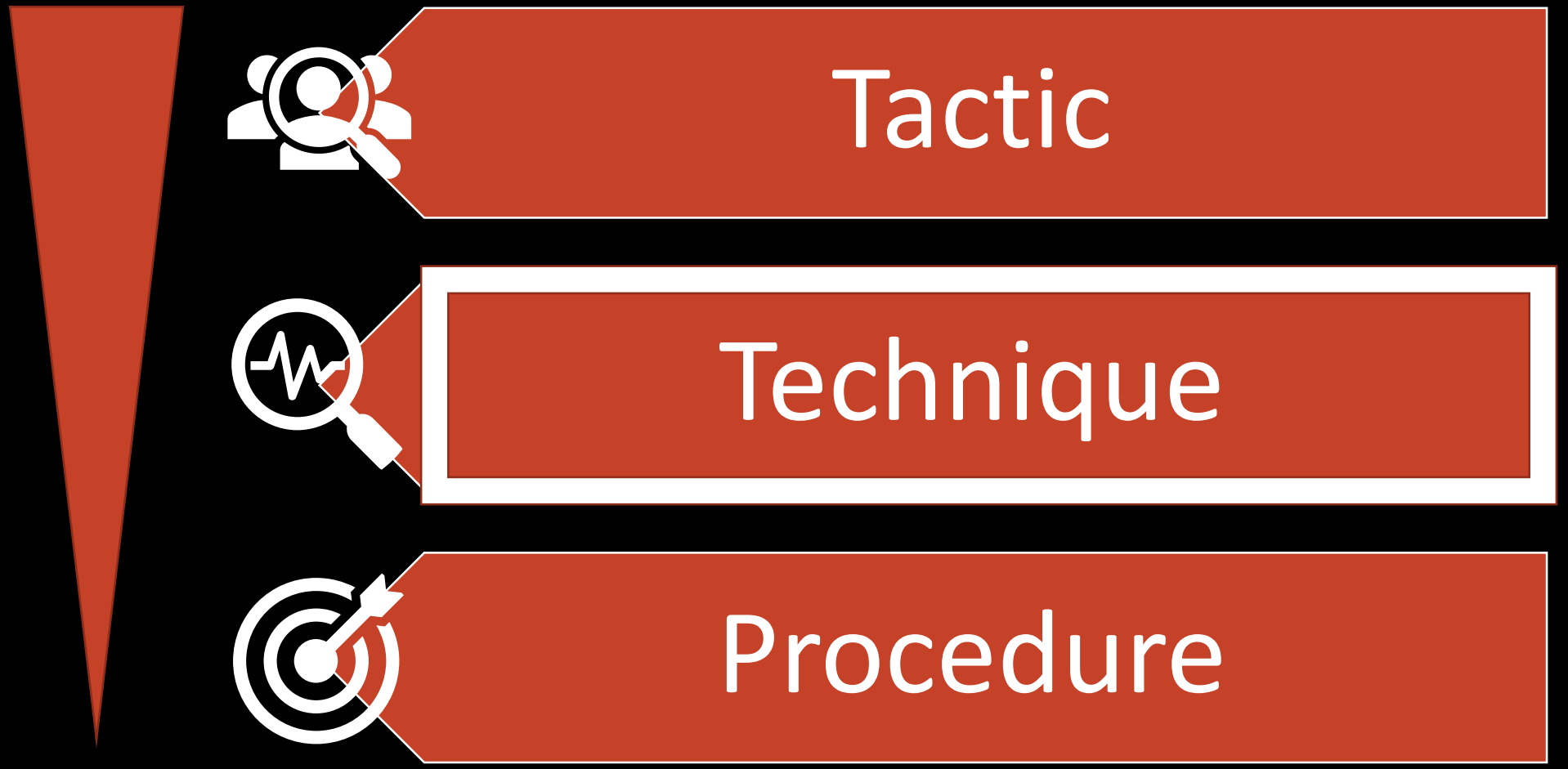


ATT&CK

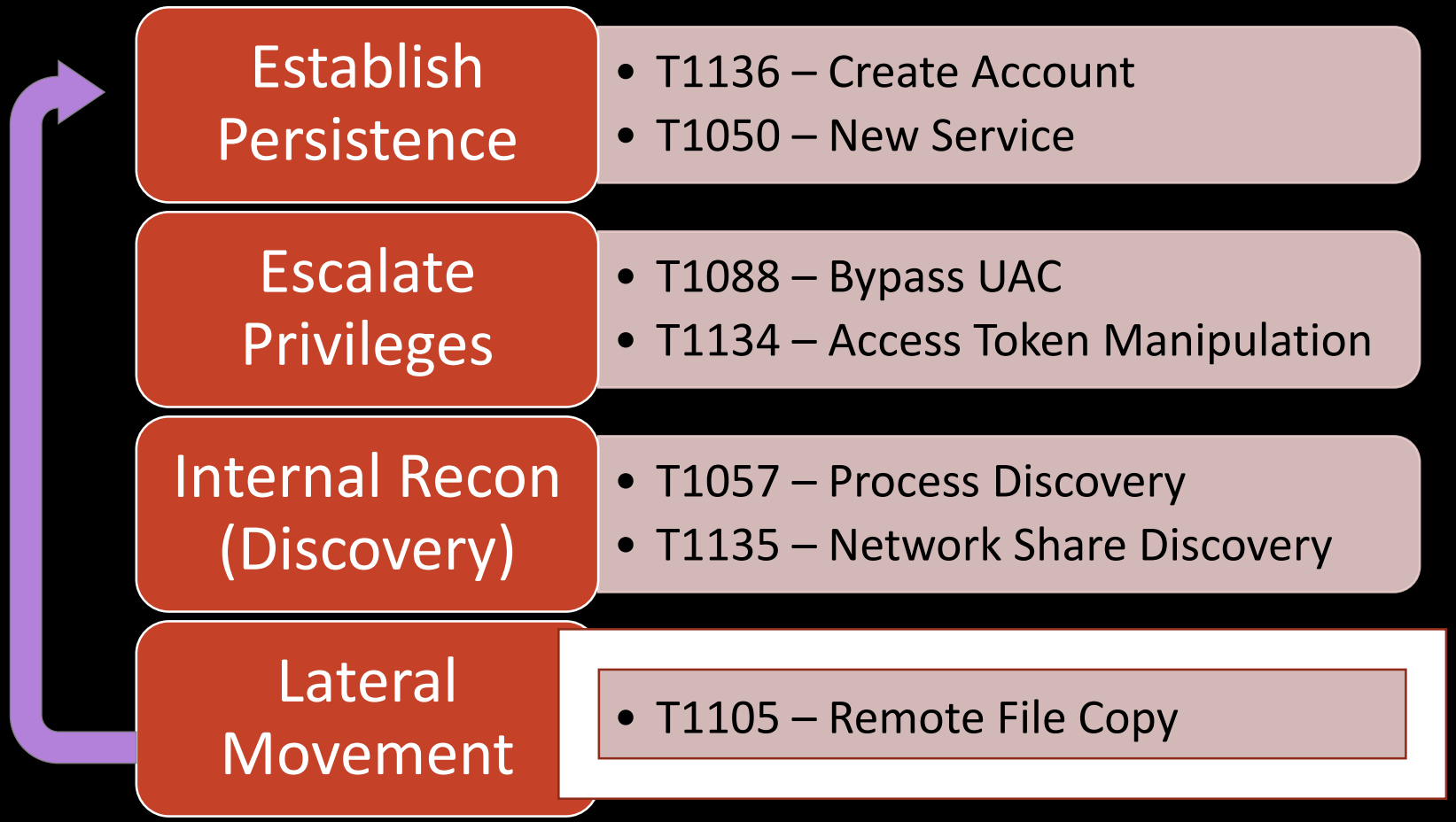
MITRE

Solution: Variance in TTP

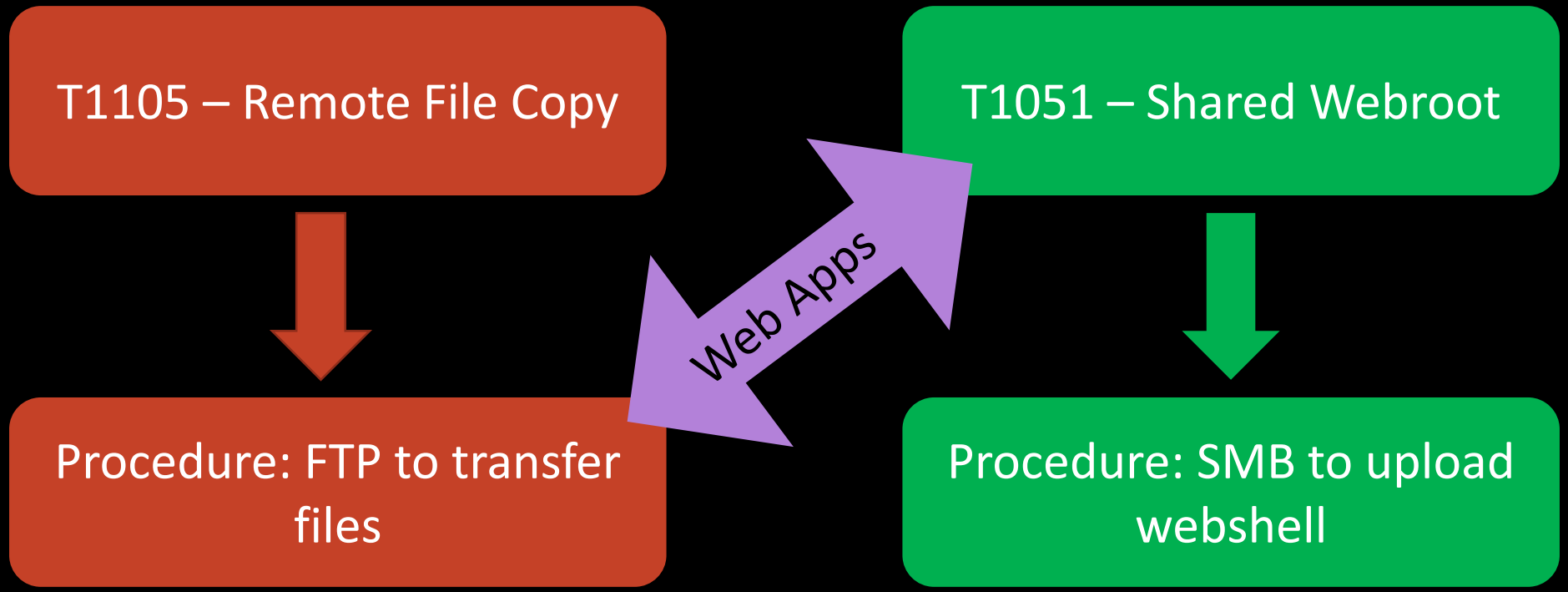
Deliberate ATT&CK



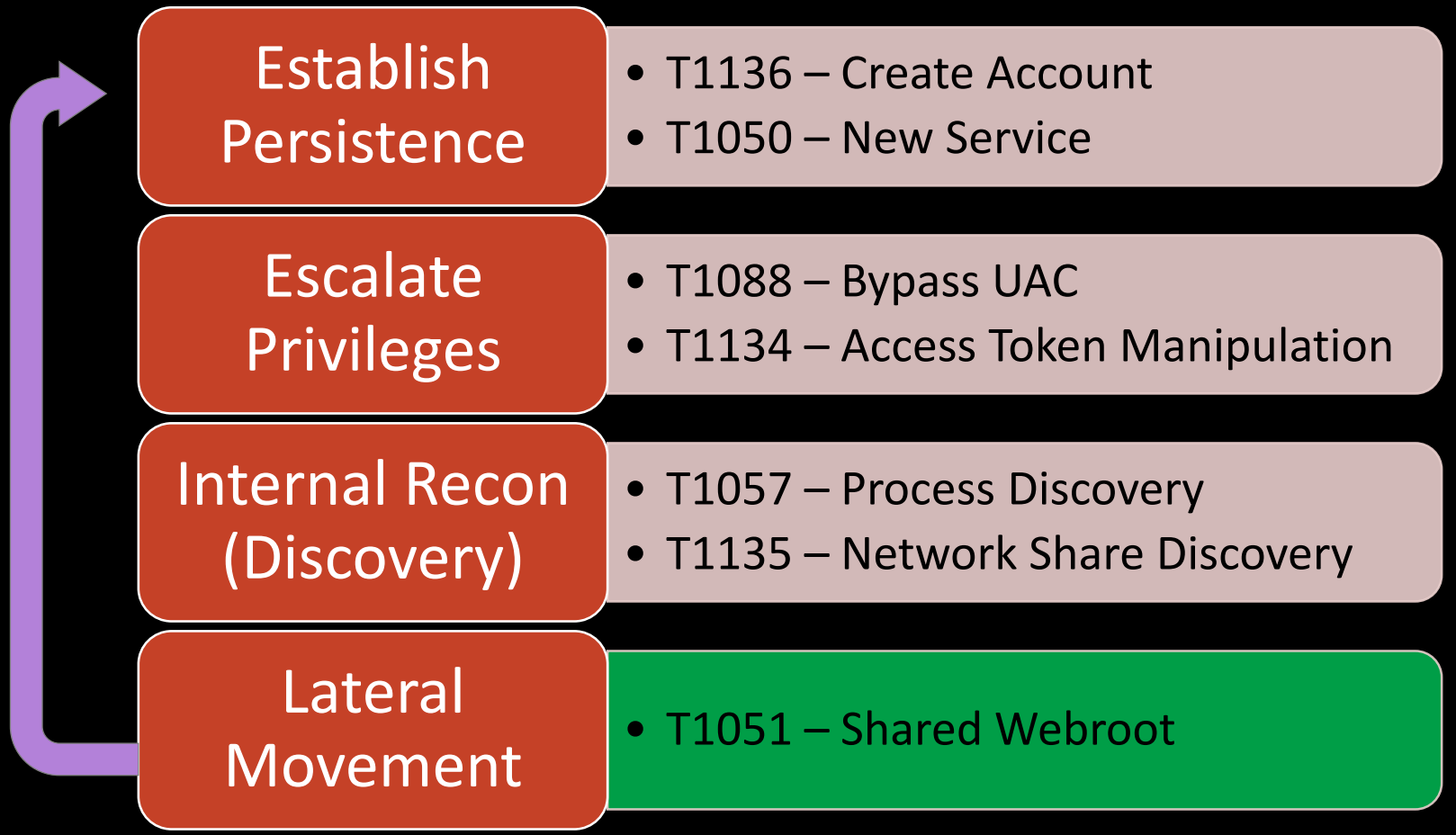
Adapt: Example Emulation Plan



Adapt: Lateral Movement



Adapt: New Emulation Plan

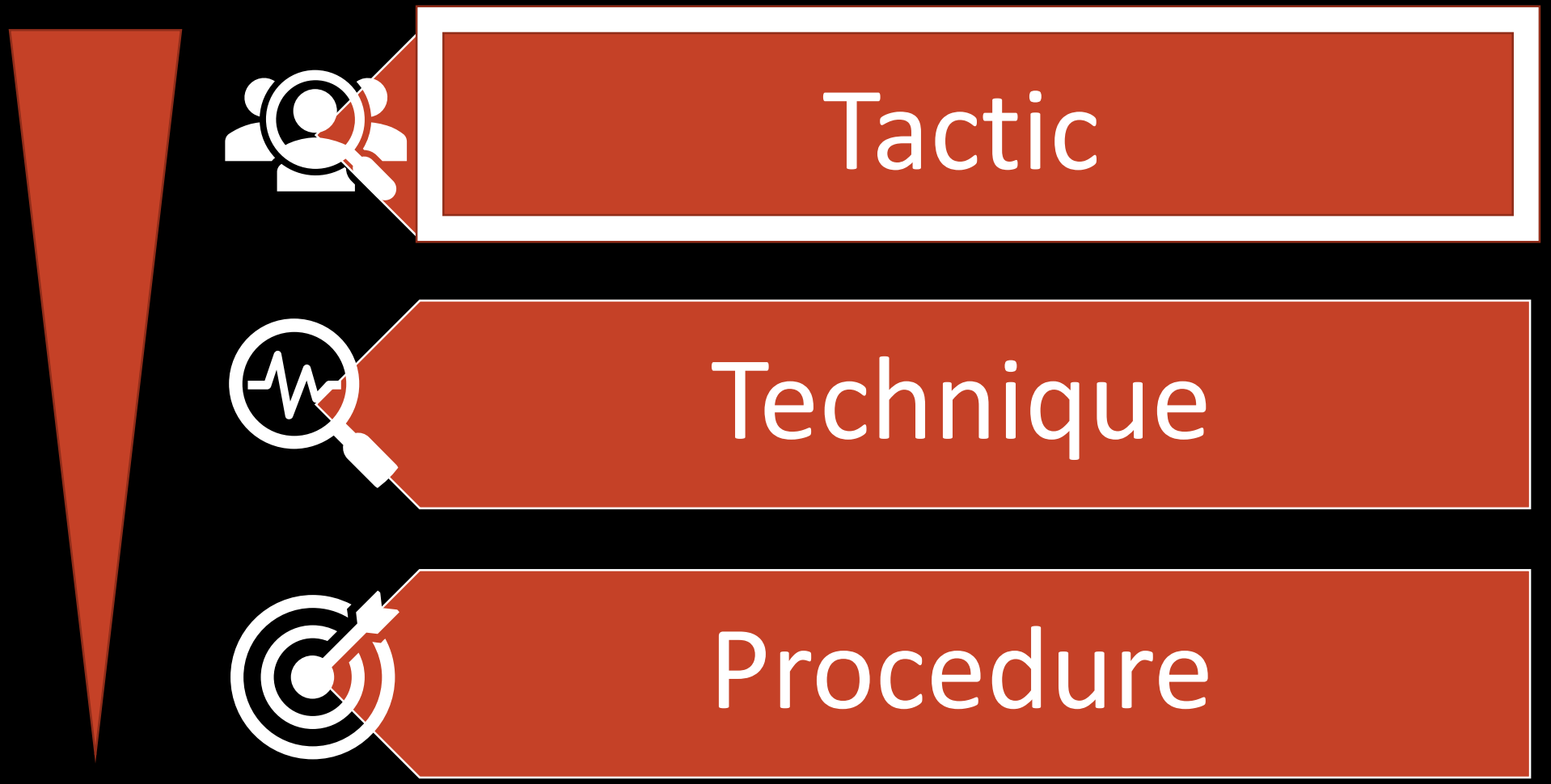


ATT&CK™

MITRE

Solution: Variance in TTP

Deliberate ATT&CK



Tactic Adaptation: Why & Challenges

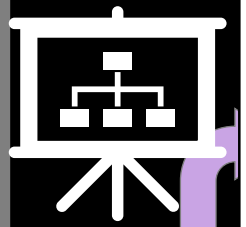
- New CTI
- Stories with holes
- Modernization requires extra tactics/techniques

- Lots of ambiguity
- Being deliberate
- Staying threat driven

ATT&CK™

MITRE

Adapt: Example Emulation Plan



Establish Persistence	T1136 – Create Account T1050 – New Service
Escalate Privileges	T1088 – Bypass UAC T1134 – Access Token Manipulation
Internal Recon (Discovery)	T1057 – Process Discovery T1135 – Network Share Discovery
Lateral Movement	T1105 – Remote File Copy

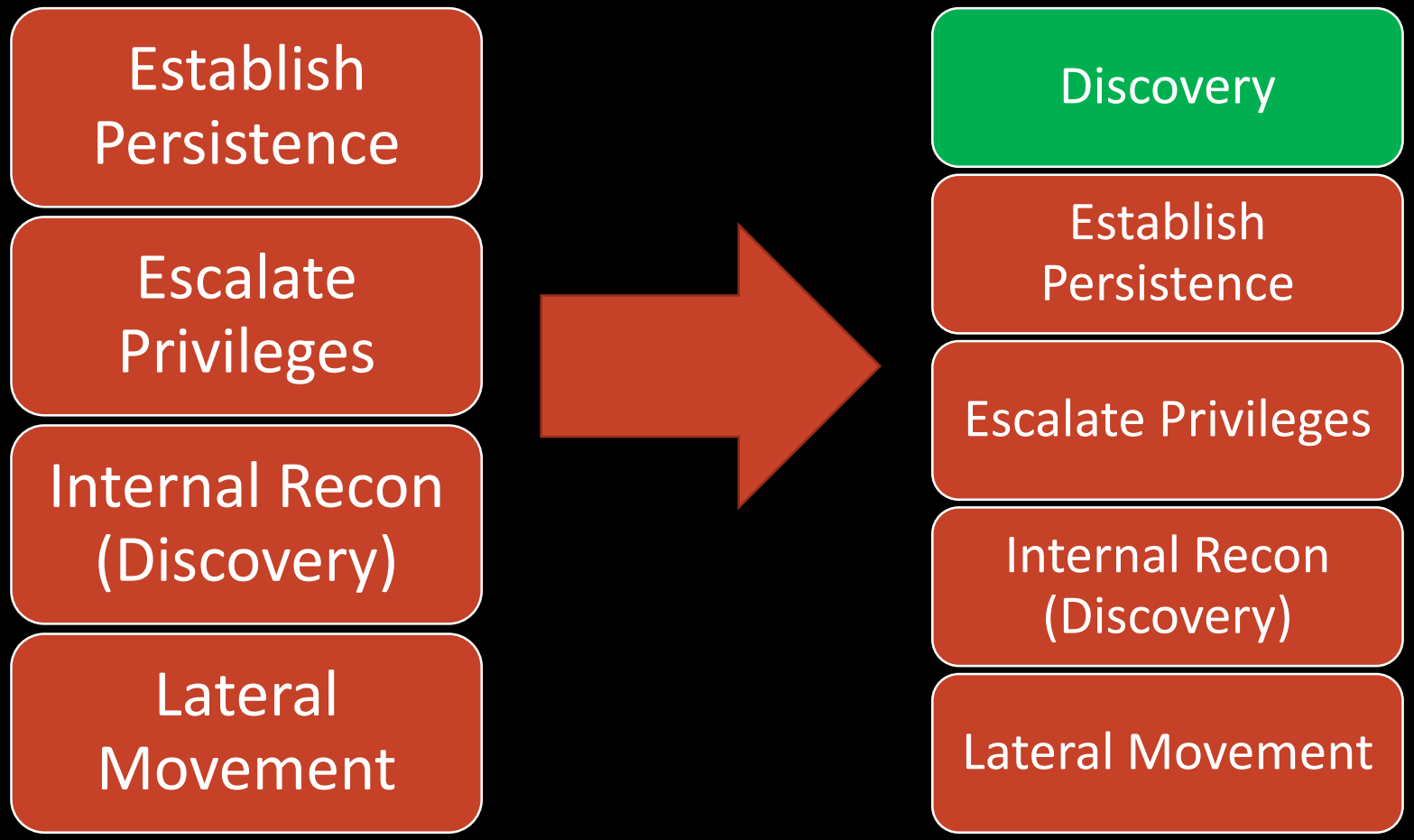
ATT&CK™

MITRE

Adapt: Example Emulation Plan

- Establish Persistence
- Escalate Privileges
- Internal Recon (Discovery)
- Lateral Movement

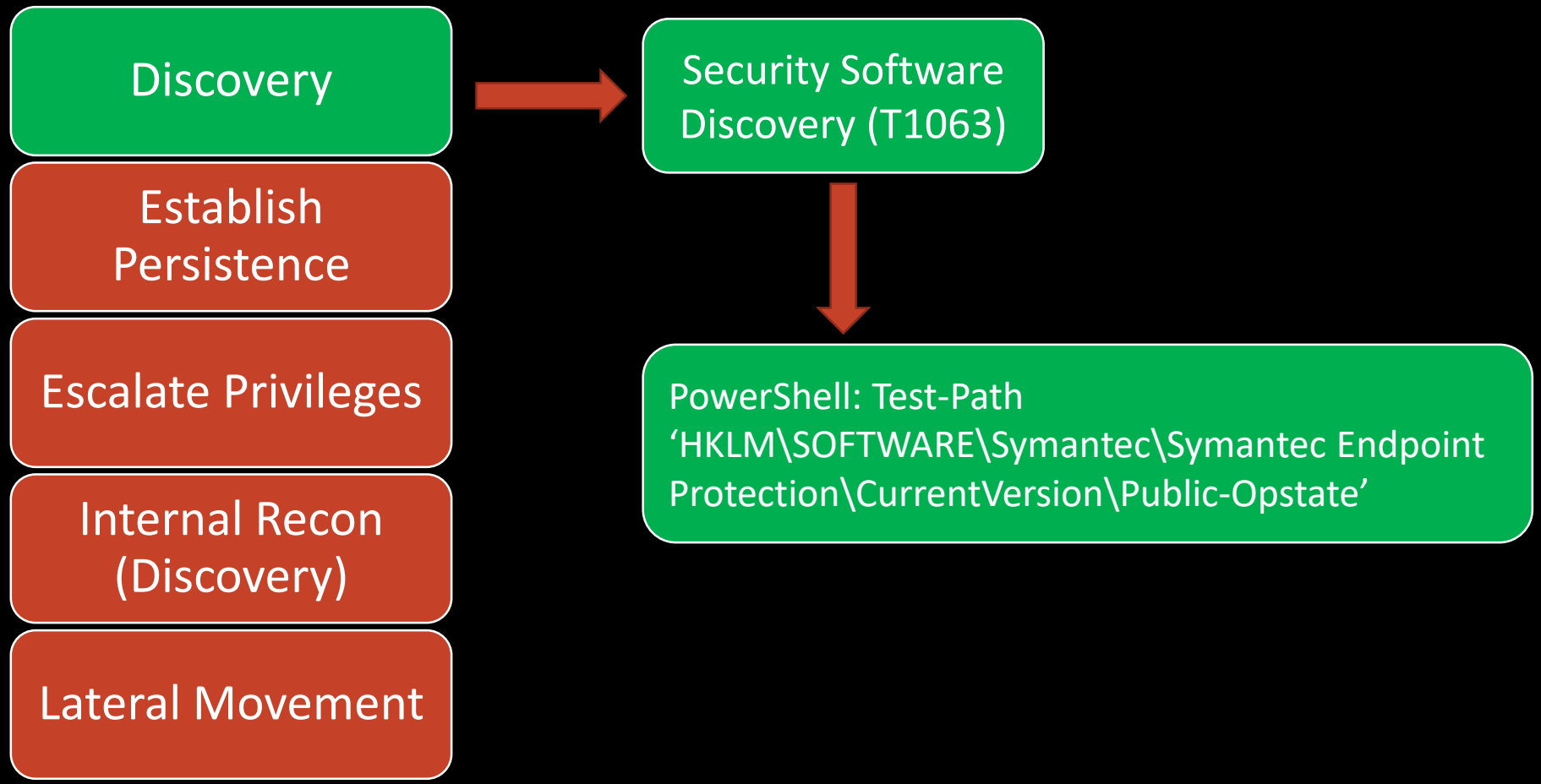
Adapt: Example Emulation Plan



ATT&CK™

MITRE

Adapt: Example Emulation Plan



Applying Adaptation: ATT&CK Evaluations

The Threat: APT 3

- “China-based threat group that researchers have attributed to China's Ministry of State Security.”

- Campaigns:
  - Operation Clandestine Fox
  - Operation Clandestine Wolf
  - Operation Double Tap

5

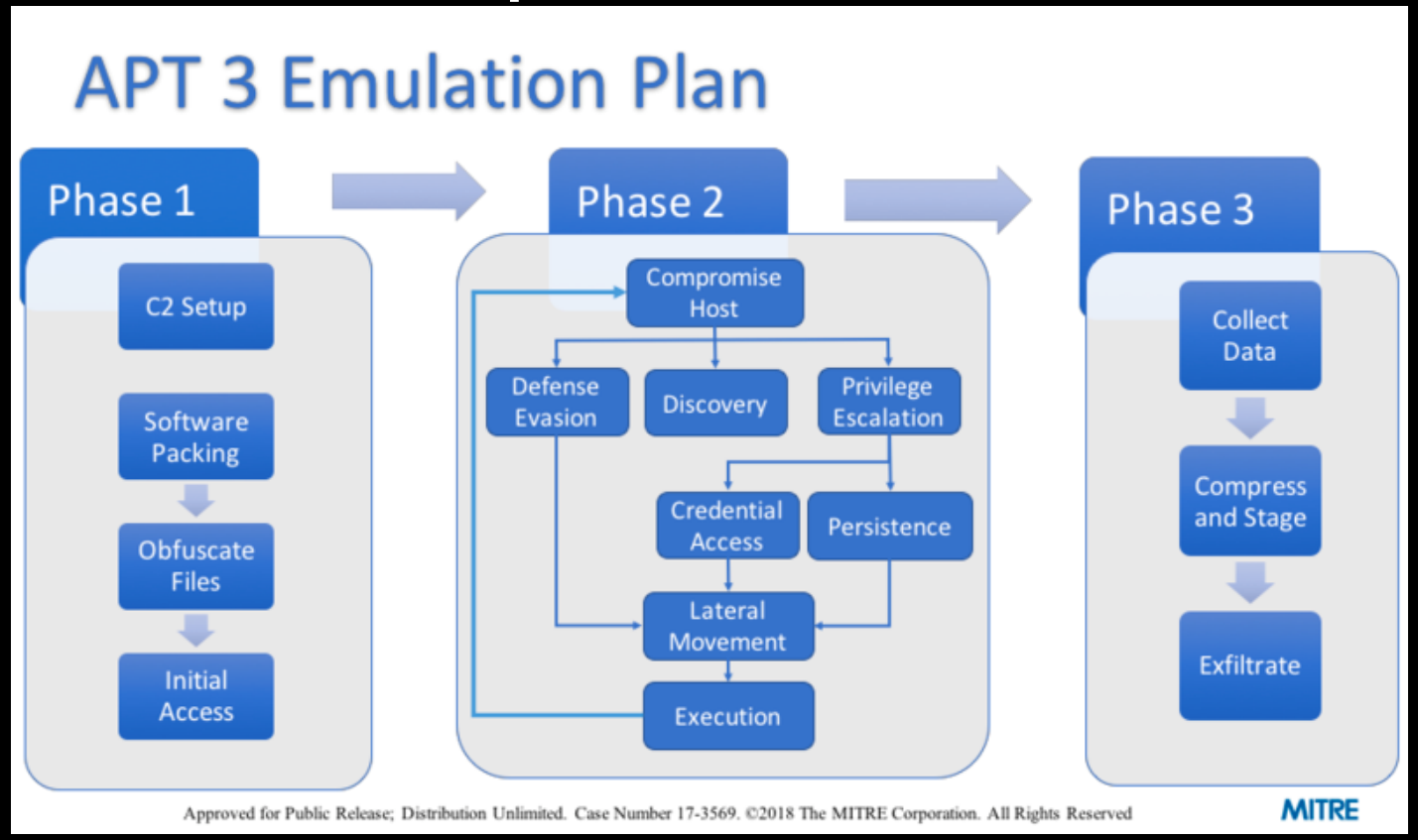
AKA:

- **Gothic Panda**
- **Pirpi**
- **UPS Team**
- **Buckeye**
- **TG-0110**

5. https://www.crowdstrike.com/blog/wp-content/uploads/2018/02/Gothic-panda.jpg
6. https://attack.mitre.org/groups/G0022/

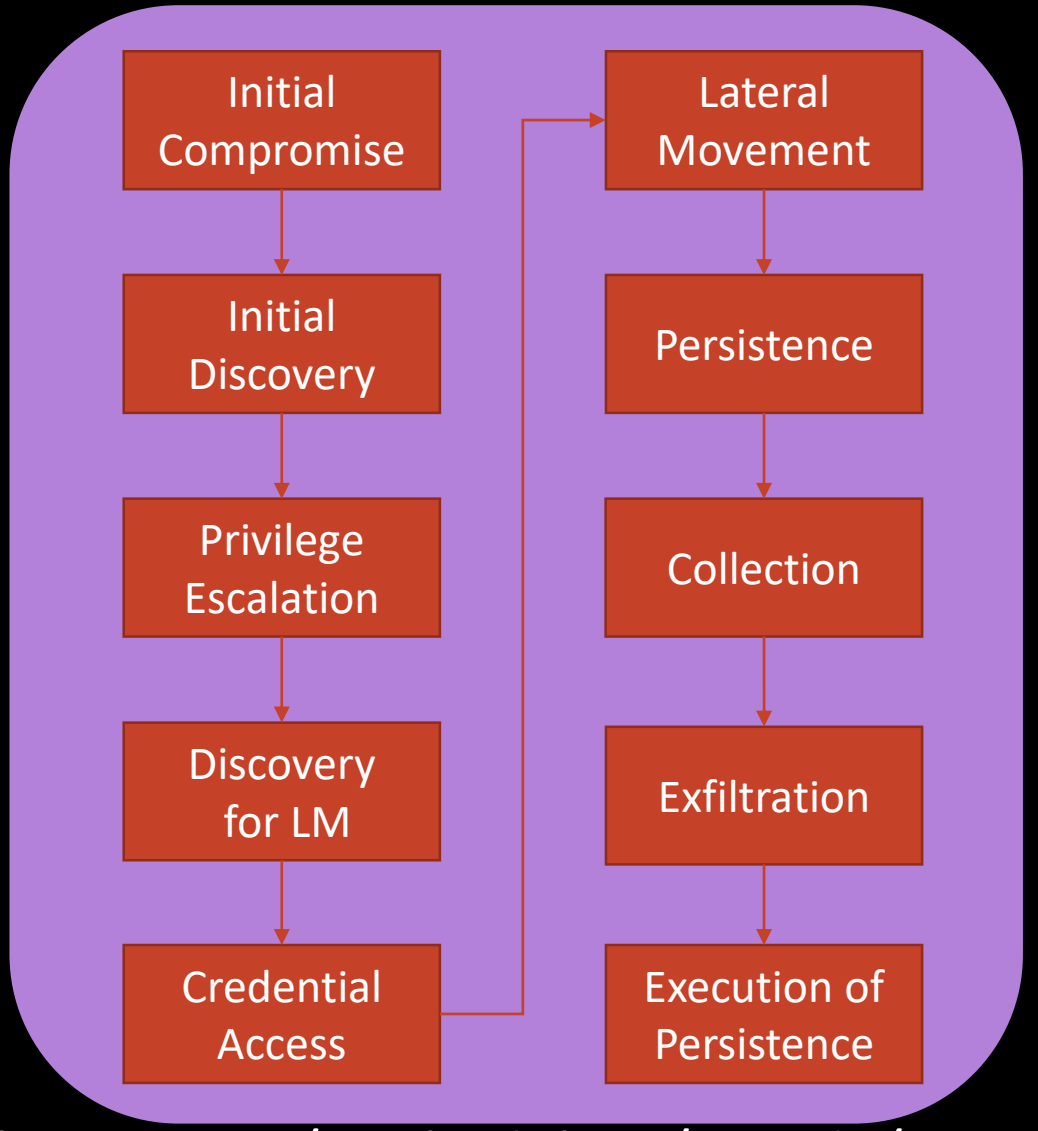
APT 3 Emulation: 2017

- MITRE released a white paper and adversary emulation plan and field manual back in September 2017



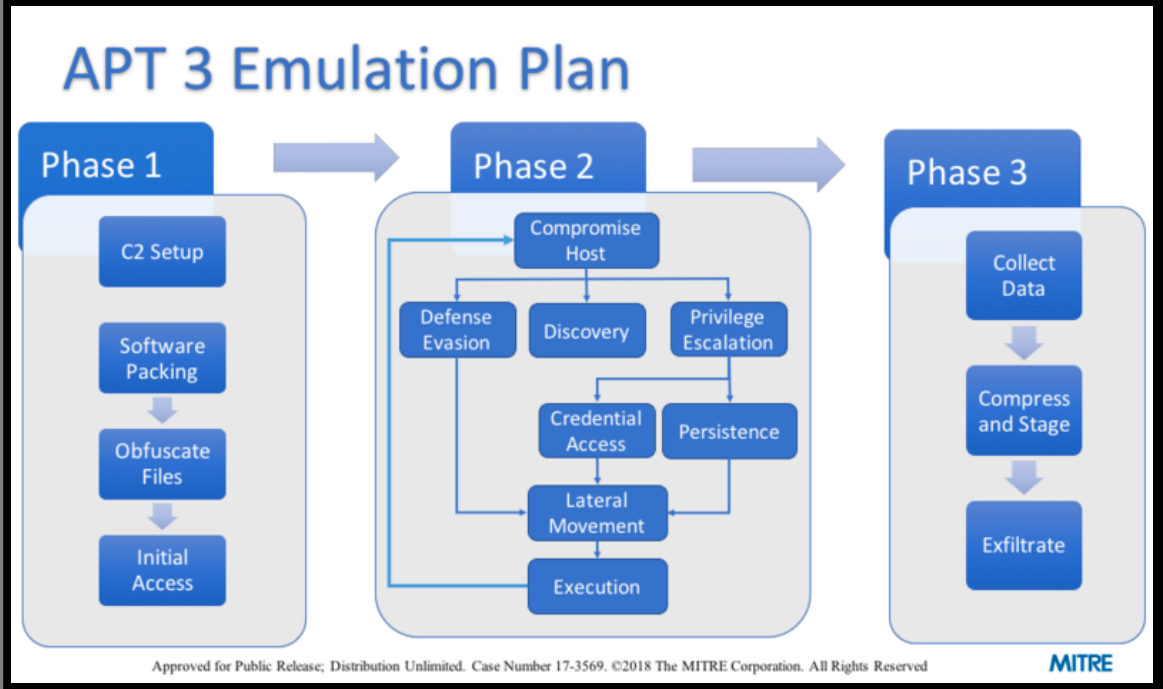
https://attack.mitre.org/resources/adversary-emulation-plans/

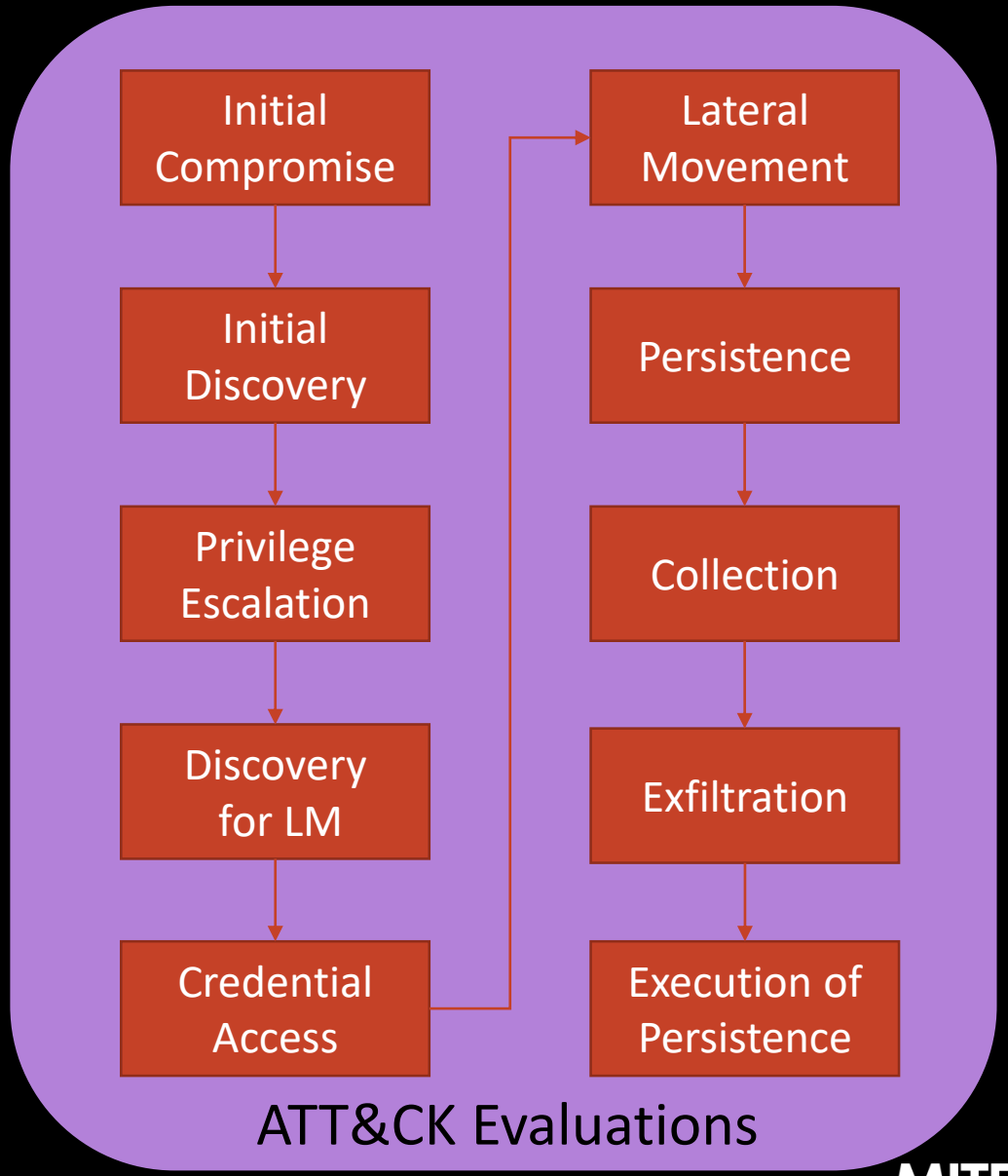
APT 3 Emulation: 2018



https://attackevals.mitre.org/methodology/round1/operational-flow.html

Adaptive APT 3: Operational Flow





Adaptive APT 3: Techniques

Execution of Persistence

T1060 – Registry Run Key

T1053 – Scheduled Task

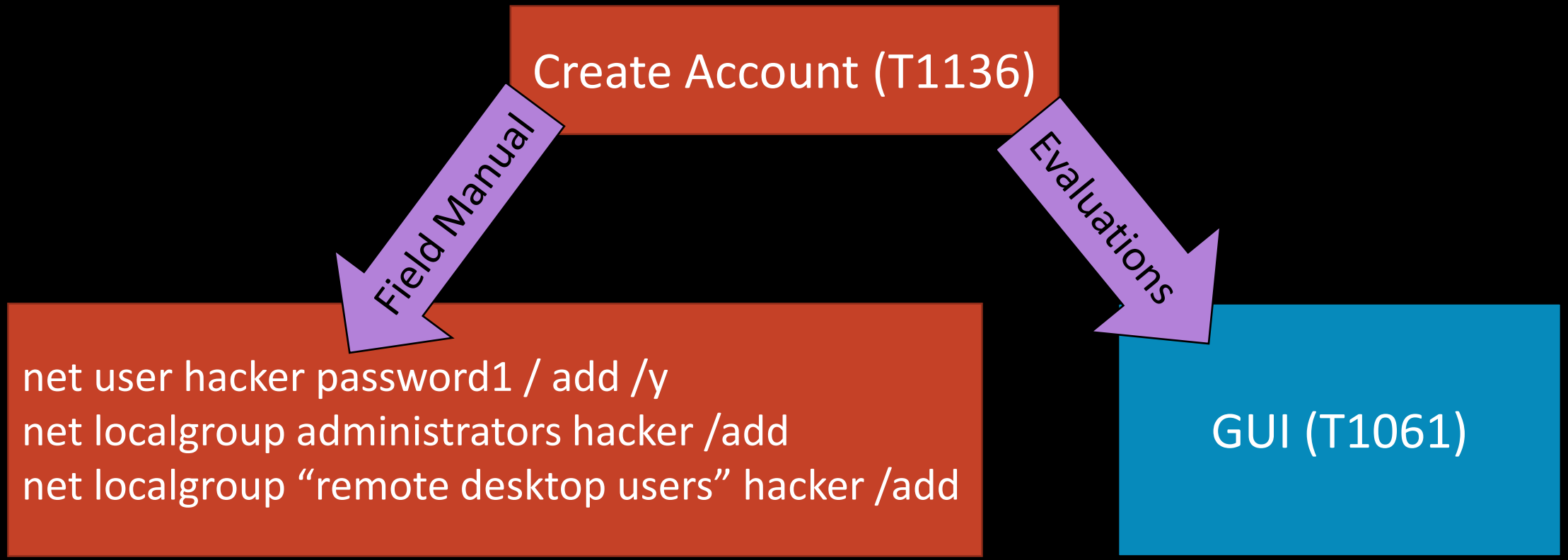
T1078 – Valid Accounts

Day 1

T1015 – Accessibility Features

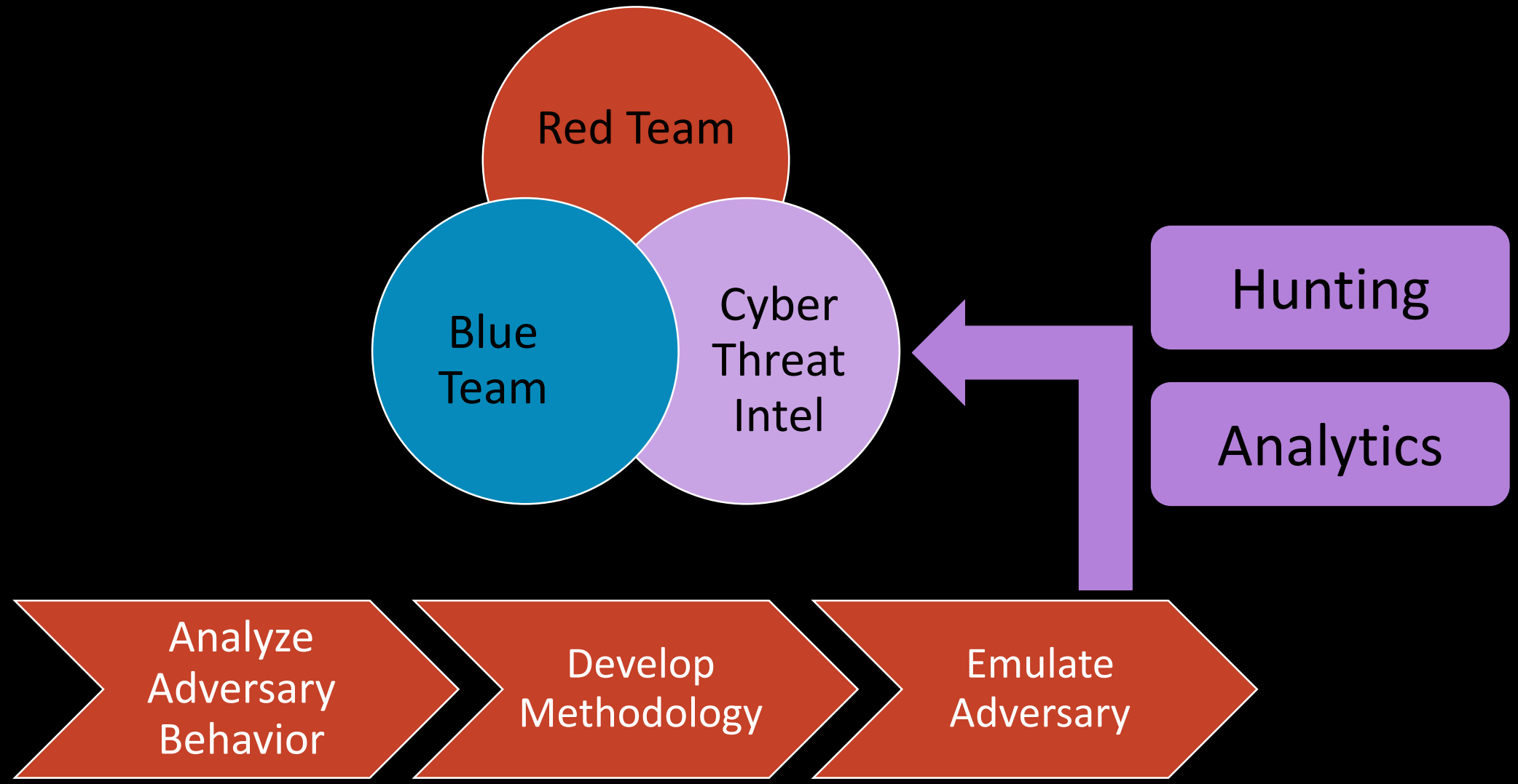
Day 2

Adaptive APT 3: Procedures



Bringing it all back

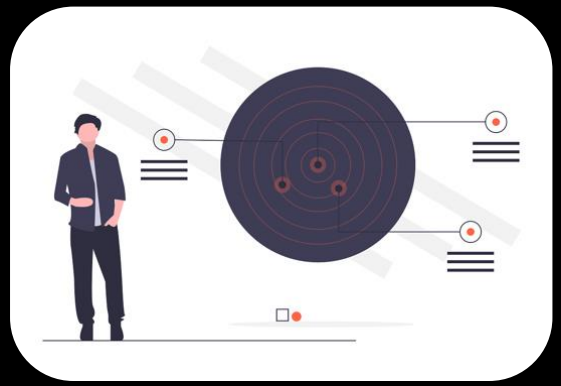
Results: Better tests!



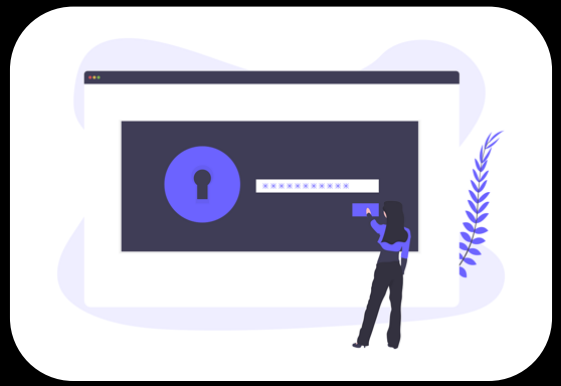
ATT&CK™

MITRE

Adaptive Emulation: Why?



Result Prioritization



Verify Defenses

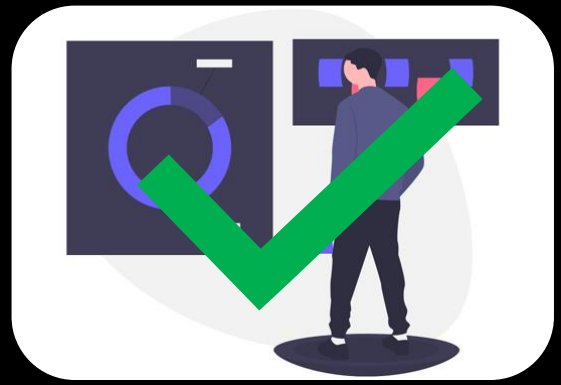
Identify Gaps

Adaptive Emulation: Why?

Adaptive testing presents new tests

Deliberate creativity

Modernization of old TTPs



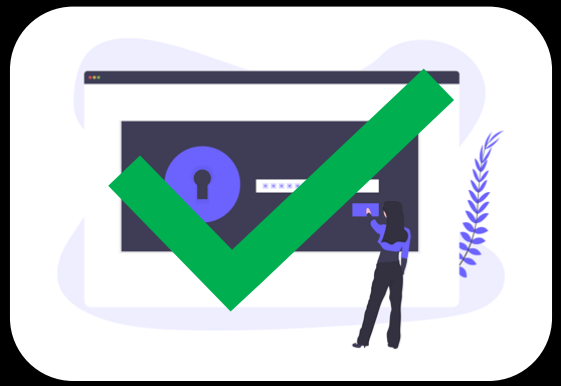
Identify Gaps

Adaptive Emulation: Why?

Modernization of old TTPs

Collaboration between red and blue

Testing against known organizational threats

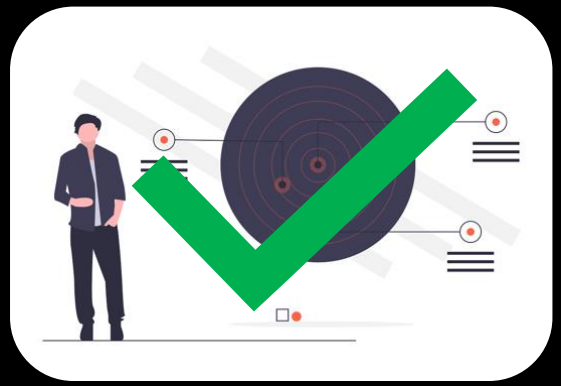


Verify Defenses

ATT&CK™

MITRE

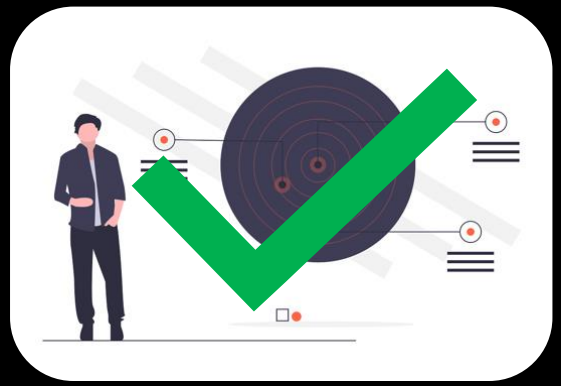
Adaptive Emulation: Why?



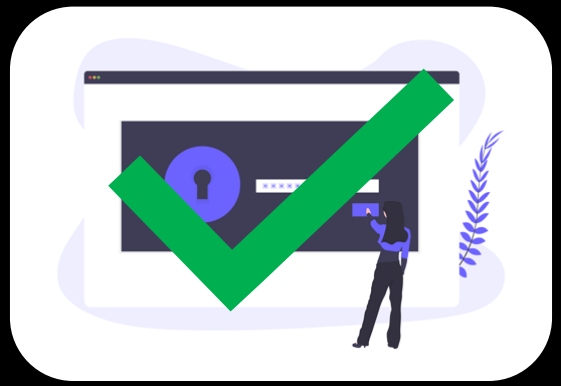
Result Prioritization

- Testing against known organizational threats
- Testing has additional significance
- Enables decision makers

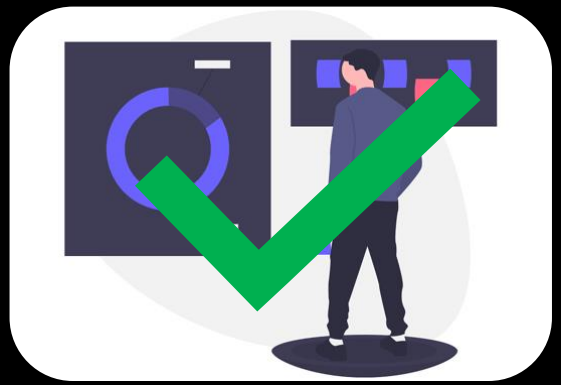
Adaptive Emulation: Why?



Result Prioritization



Verify Defenses



Identify Gaps

References

- https://attack.mitre.org
- https://attack.mitre.org/resources/adversary-emulation-plans/
- https://attack.mitre.org/groups/G0022/
- https://attackevals.mitre.org
- https://attackevals.mitre.org/methodology/round1/operational-flow.html

Images

- Katerina Limpitsouni, https://undraw.co/illustrations
- https://upload.wikimedia.org/wikipedia/commons/d/dc/Retrato_de_Julio_C%C3%A9sar_%2826724093101%29.jpg
- https://www.indiastrategic.in/wp-content/uploads/2019/04/Spyder-SR_1-1024x681.jpg
- https://images-na.ssl-images-amazon.com/images/I/61tcbl448lL._SY355_.jpg
- https://miro.medium.com/max/1200/1*XfjdqaabOCZj5CRb8QcmFg.jpeg
- https://www.crowdstrike.com/blog/wp-content/uploads/2018/02/Gothic-panda.jpg

Questions?

ATT&CK™

attack.mitre.org
medium.com/mitre-attack
attack@mitre.org
@MITREattack

@teschulz