MATURING

Threat Informed Adversary Emulation with ATT&CK

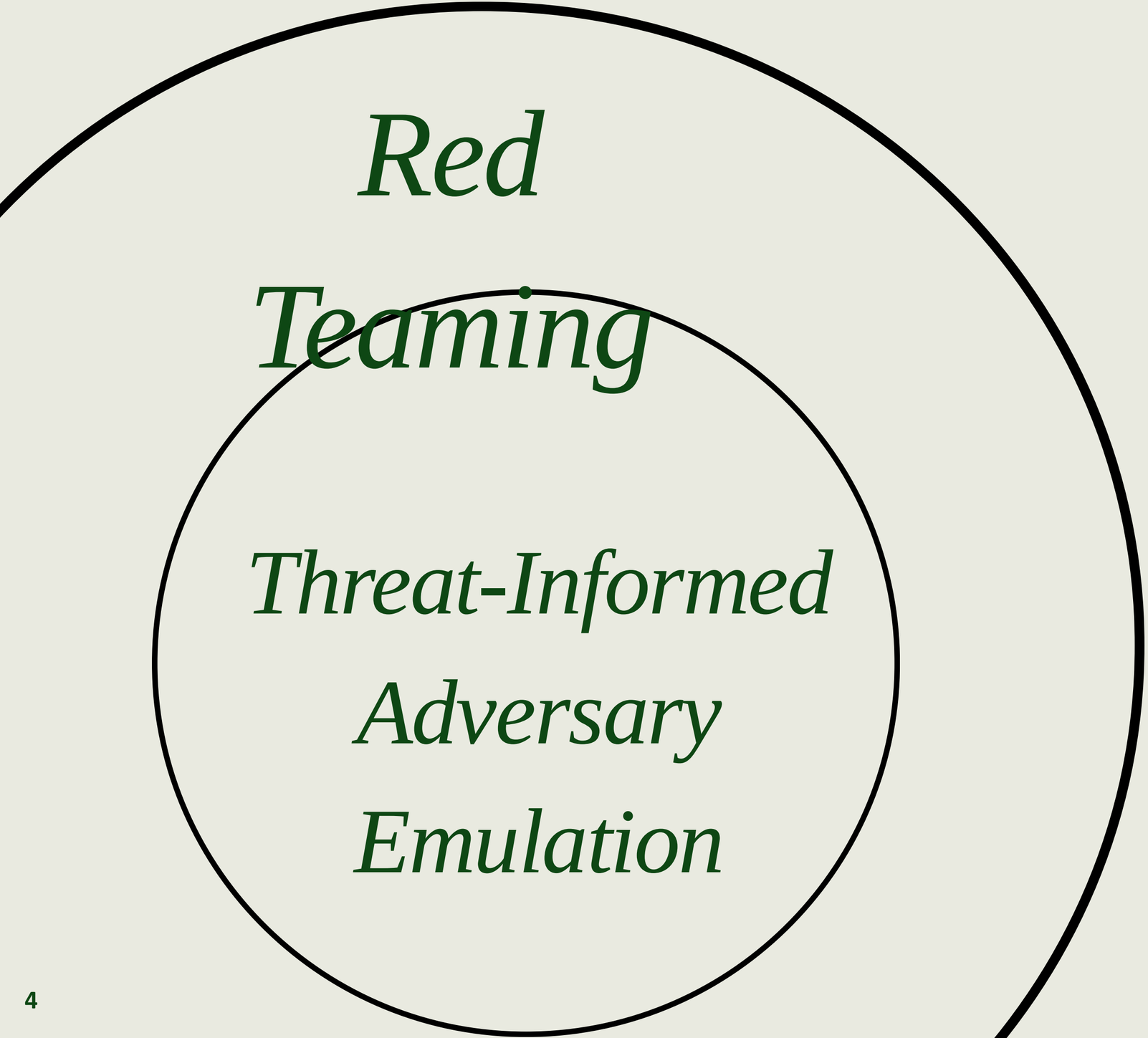
Crys Tan
Adversary Emulation Lead
7 March 2025

ADVERSARY EMULATION IS...

Images generated at deepai.org

WHY THREAT INFORMED?

Images generated at deepai.org


Red
Teaming
Threat-Informed
Adversary
Emulation

MATURITY MODEL

For mature red teams with sufficient resourcing and supporting CTI.

For teams with more resources.

For teams starting out on the adversary emulation journey.

THREAT INTELLIGENCE

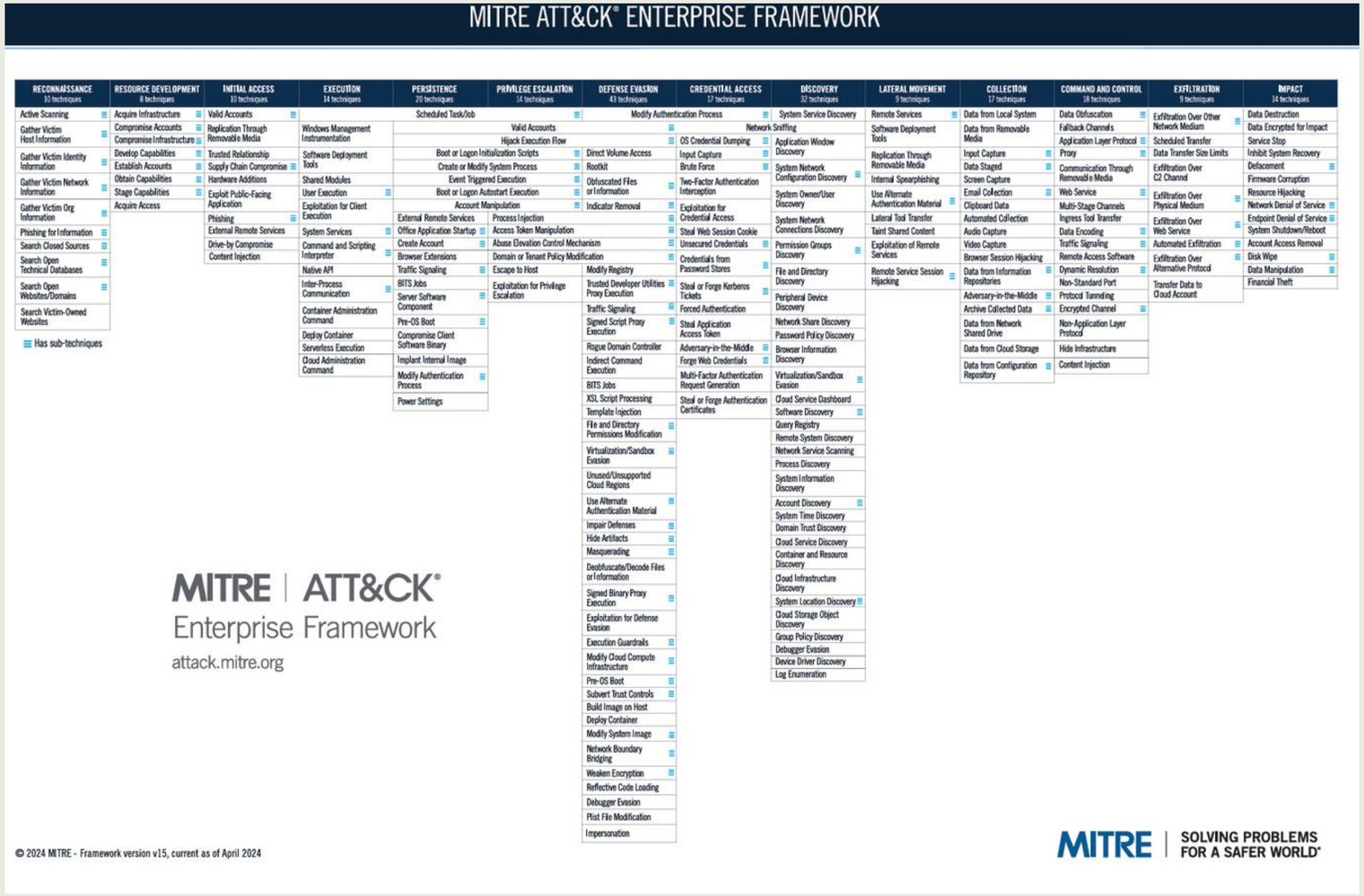
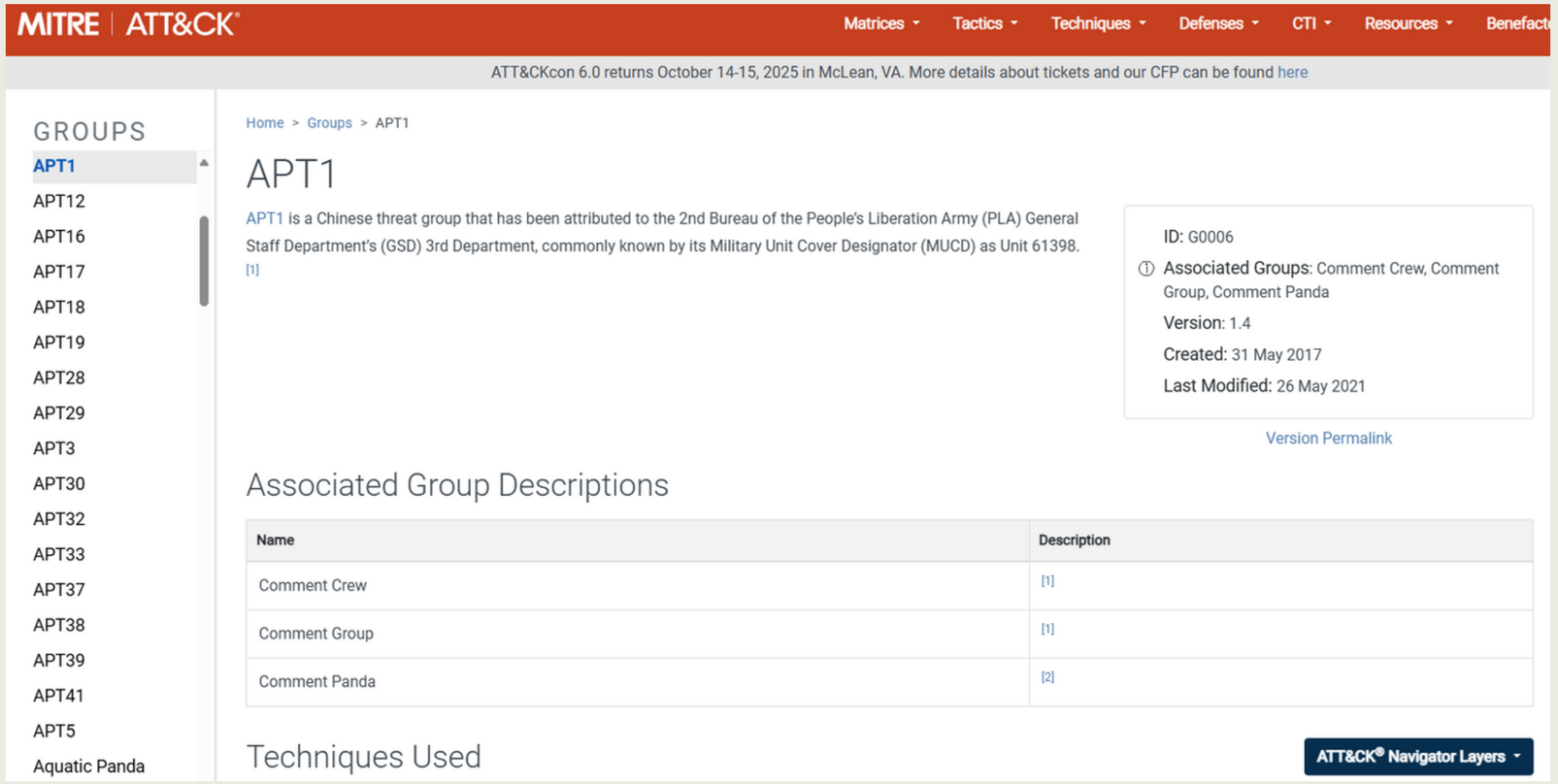


Image retrieved from attack.mitre.org

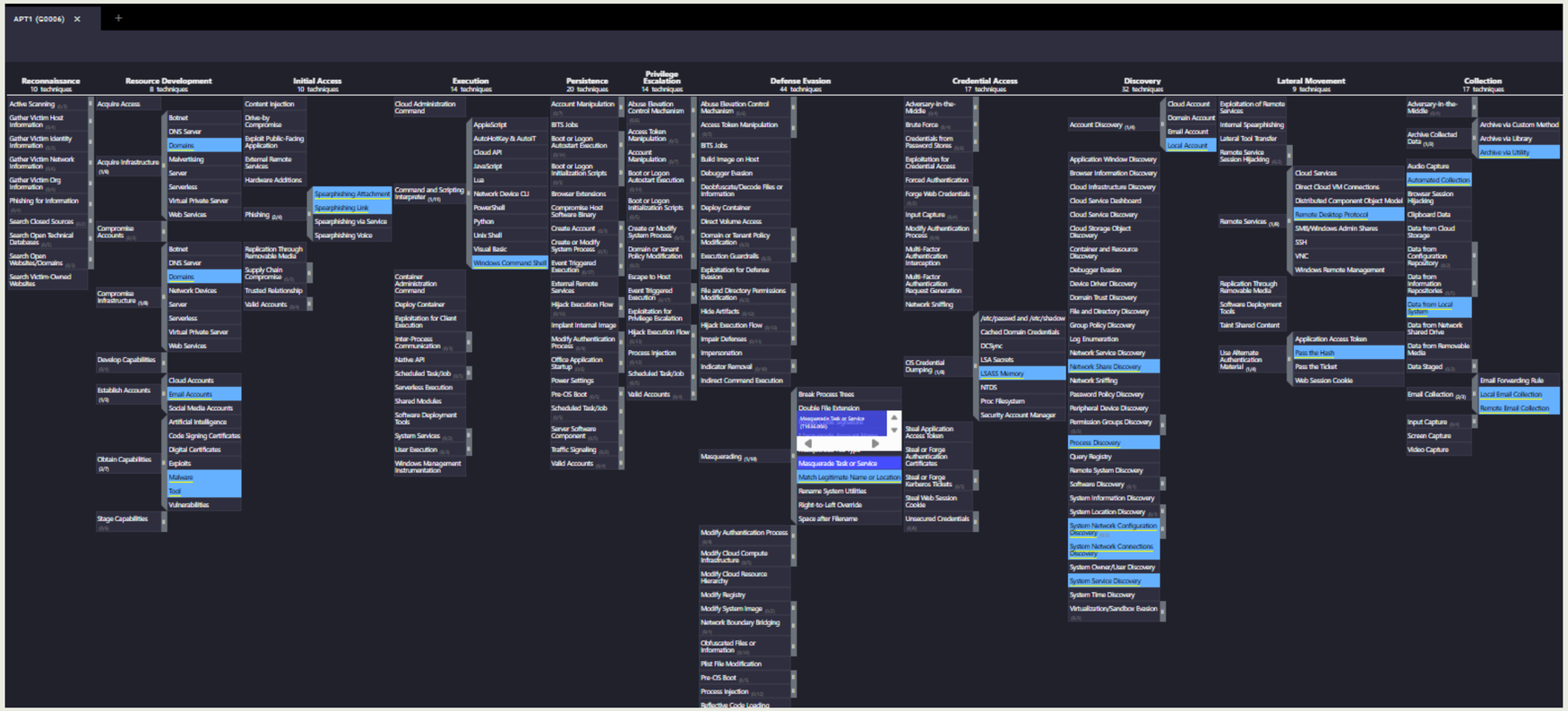
START WITH BABY STEPS

1. *(Optional)* Identify Threat Group(s) of Interest.
2. Identify TTPs of Interest.
3. Atomic testing of TTPs.
4. Work on Detection / Prevention as necessary.

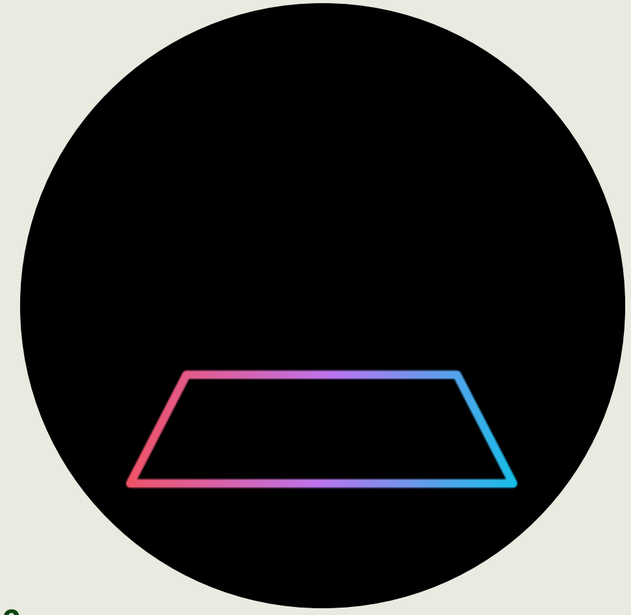
START WITH BABY STEPS



START WITH BABY STEPS



START WITH BABY STEPS



16 lsass

Tactic | Platforms | Executors | Elevation

ID	GUID	Name	Tactic	Platform(s)	Executor	Elevati...
T1003.001	0be2230c-9ab3-4ac2-8826-3199b9a0ebf8	Dump LSASS.exe Memory using ProcDump	credential-access			
T1003.001	2536dee2-12fb-459a-8c37-971844fa73be	Dump LSASS.exe Memory using comsvcs.dll	credential-access			
T1003.001	7ae7102c-a099-45c8-b985-4c7a2d05790d	Dump LSASS.exe Memory using direct system calls and API unhooking	credential-access			
T1003.001	dddd4aca-bbed-46f0-984d-e4c5971c51ea	Dump LSASS.exe Memory using NanoDump	credential-access			
T1003.001	dea6c349-f1c6-44f3-87a1-1ed33a59a607	Dump LSASS.exe Memory using Windows Task Manager	credential-access			
T1003.001	c37bc535-5c62-4195-9cc3-0517673171d8	LSASS read with pypykatz	credential-access			
T1003.001	6502c8f0-b775-4dbd-9193-1298f56b6781	Dump LSASS.exe Memory using Out-Minidump.ps1	credential-access			
T1003.001	7cede33f-0acd-44ef-9774-15511300b24b	Create Mini Dump of LSASS.exe using ProcDump	credential-access			
T1003.001	9d0072c8-7cca-45c4-bd14-f852cfa35cf0	Dump LSASS with createdump.exe from .Net v5	credential-access			
T1003.001	86fc3f40-237f-4701-b155-81c01c48d697	Dump LSASS.exe using imported Microsoft DLLs	credential-access			

Rows per page: 10

1 2

START WITH BABY STEPS

Useful Resources:

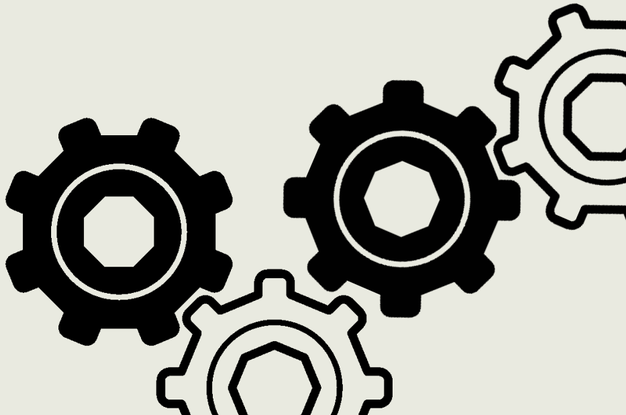
- MITRE CTID Adversary Emulation Library - Micro Emulation Plans
  - https://github.com/center-for-threat-informed-defense/adversary_emulation_library?#getting-started-with-micro-emulation-plans
- Atomic Red Team
  - https://github.com/redcanaryco/atomic-red-team

STEPPING UP

Automate testing and re-testing.

Value:

- Reduce manual efforts, sparing resources for more advanced work



STEPPING UP

Useful Resources:

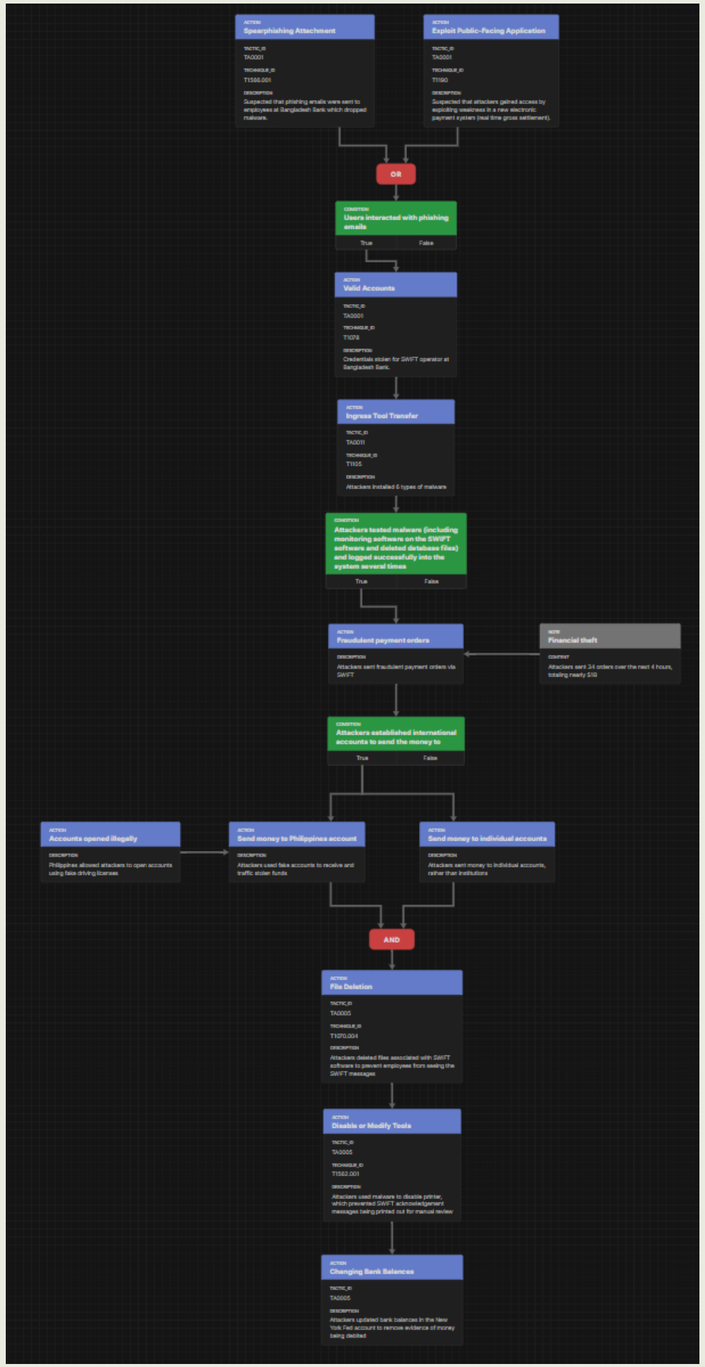
- MITRE’s Caldera
  - https://github.com/mitre/caldera
- Splunk’s Attack Range
  - https://github.com/splunk/attack_range
- Commercial BAS Tools

LET IT FLOW

Develop Attack Scenarios

- Build an attack flow of TTPs.
- Test in **purple team** engagements (with the Blue Team).

LET IT FLOW


ACTION
Spearphishing Attachment
TACTIC_ID
TA0001
TECHNIQUE_ID
T1566.001
DESCRIPTION
Suspected that phishing emails were sent to employees at Bangladesh Bank which dropped malware.
ACTION
Exploit Public-Facing Application
TACTIC_ID
TA0001
TECHNIQUE_ID
T1190
DESCRIPTION
Suspected that attackers gained access by exploiting weakness in a new electronic payment system (real-time gross settlement).
OR
CONDITION
Users interacted with phishing emails
True
False
ACTION
Valid Accounts
TACTIC_ID
TA0001
TECHNIQUE_ID
T1078
DESCRIPTION
Credentials stolen for SWIFT operator at Bangladesh Bank.
ACTION
Ingress Tool Transfer
TACTIC_ID
TA0011
TECHNIQUE_ID
T1105
DESCRIPTION
Attackers installed 6 types of malware
CONDITION
Attackers tested malware (including monitoring software on the SWIFT software and deleted database files) and logged successfully into the system several times
True
False
ACTION
Fraudulent payment orders
DESCRIPTION
Attackers sent fraudulent payment orders via SWIFT
NOTE
Financial theft
CONTENT
Attackers sent 34 orders over the next 4 hours, totaling nearly $1B
CONDITION
Attackers established international accounts to send the money to
True
False
ACTION
Accounts opened illegally
DESCRIPTION
Philippines allowed attackers to open accounts using fake driving licenses
ACTION
Send money to Philippines account
DESCRIPTION
Attackers used fake accounts to receive and traffic stolen funds
ACTION
Send money to individual accounts
DESCRIPTION
Attackers sent money to individual accounts, rather than institutions
AND
ACTION
File Deletion
TACTIC_ID
TA0005
TECHNIQUE_ID
T1070.004
DESCRIPTION
Attackers deleted files associated with SWIFT software to prevent employees from seeing the SWIFT messages
ACTION
Disable or Modify Tools
TACTIC_ID
TA0005
TECHNIQUE_ID
T1562.001
DESCRIPTION
Attackers used malware to disable printer, which prevented SWIFT acknowledgement messages being printed out for manual review
ACTION
Changing Bank Balances
TACTIC_ID
TA0005
DESCRIPTION
Attackers updated bank balances in the New York Fed account to remove evidence of money being decited

LET IT FLOW

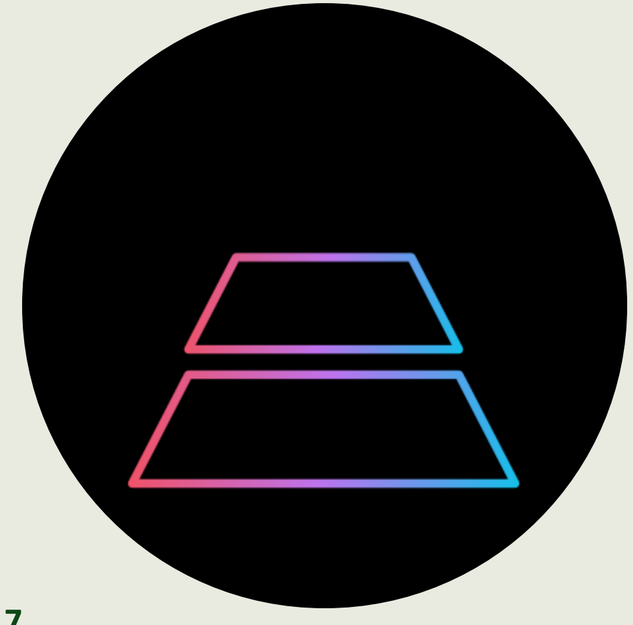
Develop Attack Scenarios

- Build an attack flow of TTPs.
- Test in **purple team** engagements (with the Blue Team).

Value:

- Identify opportunities for earlier detections.
- Over time, identify common chokepoints.

LET IT FLOW



Useful Resources:

- MITRE CTID’s Attack Flow
  - https://github.com/center-for-threat-informed-defense/attack-flow
- MITRE CTID Adversary Emulation Library
  - https://github.com/center-for-threat-informed-defense/adversary_emulation_library
- MITRE Adversary Emulation Plan
  - https://attack.mitre.org/resources/adversary-emulation-plans/
- AttackGen
  - https://github.com/mrwadams/attackgen

TEST CONTROLS

Run Unannounced Attack Scenarios

- Test in **unannounced** engagements (against the Blue Team).

  - No start-overs! No save points!

Value:

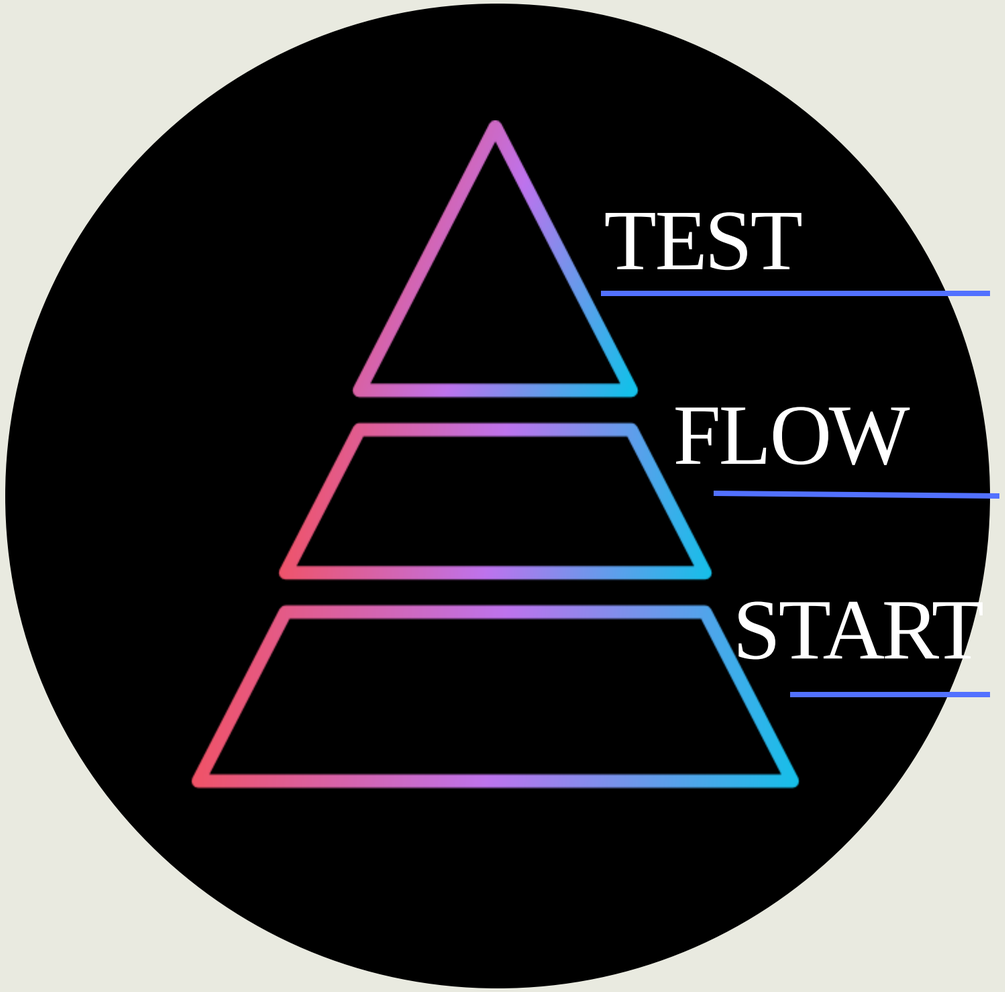
- More realistic view of controls and gaps.
- Evaluates MTTR and MTTD.

TEST CONTROLS

Useful Resources:

- MITRE Adversary Emulation & Red Teaming
  - https://attack.mitre.org/resources/get-started/adversary-emulation-and-red-teaming/

START - FLOW -TEST



Offense Informs Defense

- CIS Controls™

Thank you

Crys Tan
Adversary Emulation Lead
7 March 2025