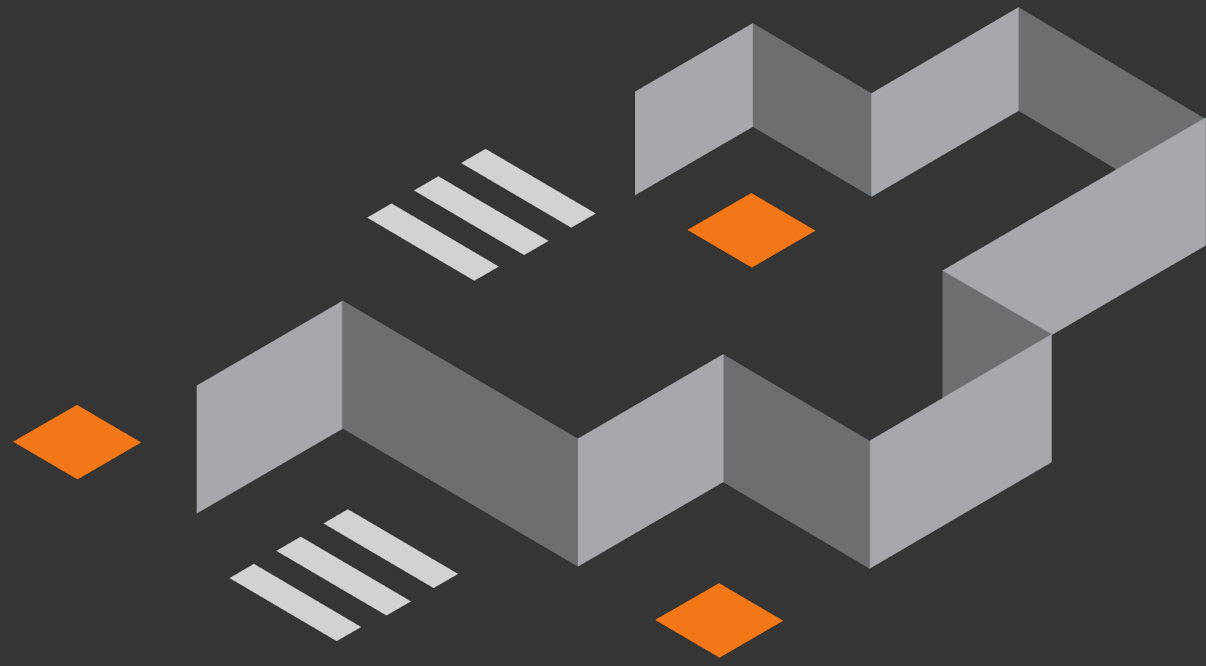
THERE IS NO TTP

PRESENTED BY MARTIN EIAN



mnemonic

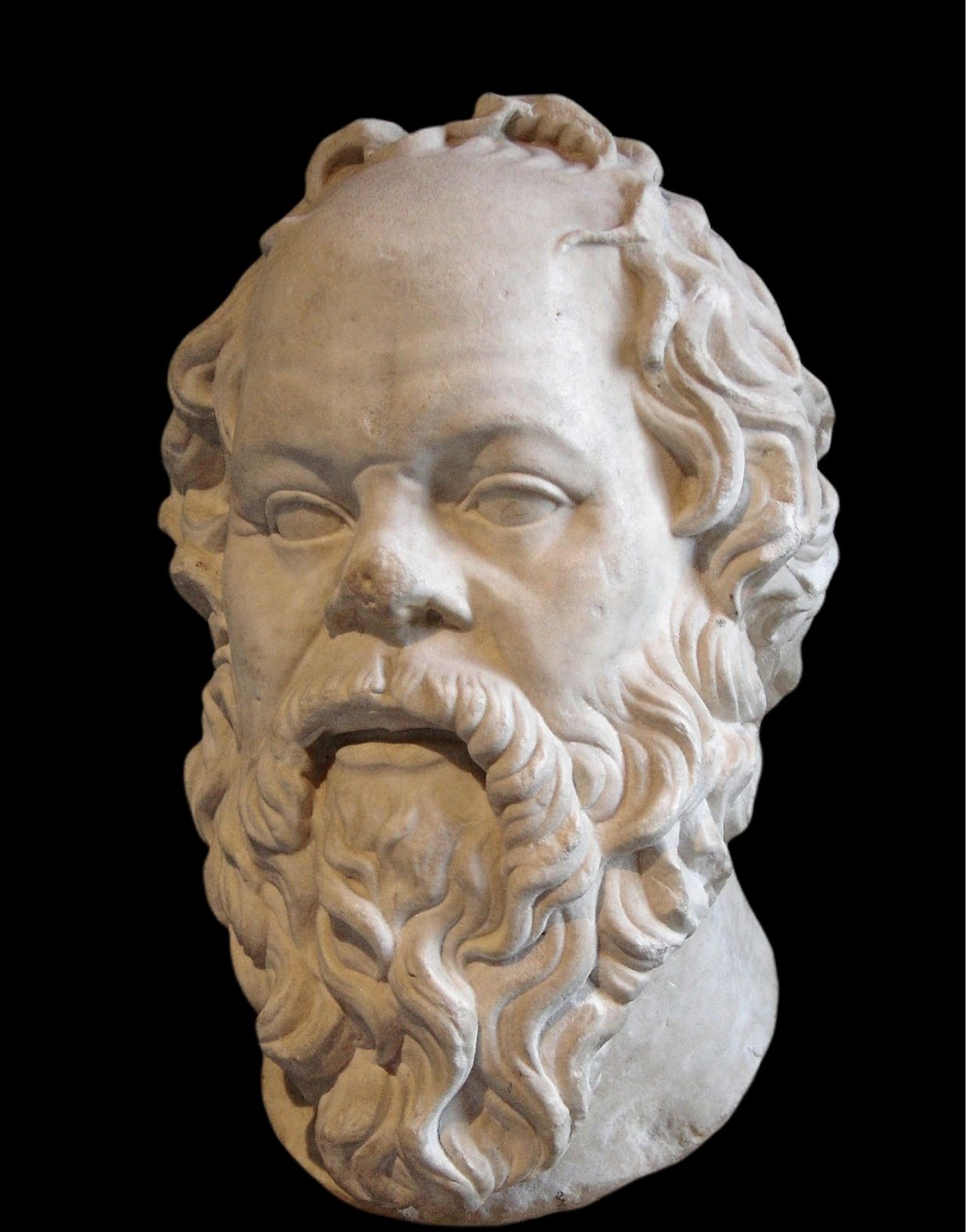
Tactic

Technique

Procedure

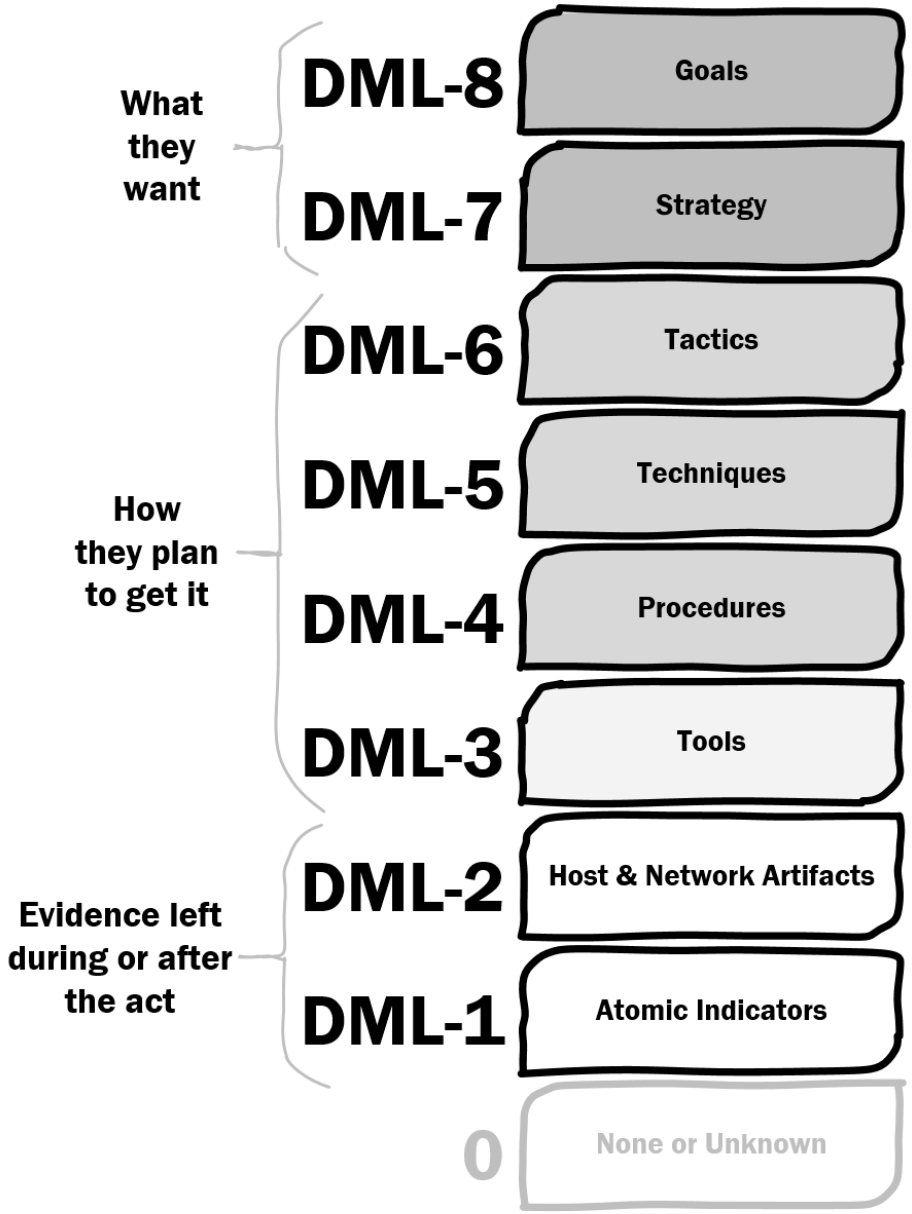
Tactic
Technique
Procedure


ΠΝΩΘΙ·CΑΥΤΟΝ



“The only true wisdom is in knowing you know nothing.”


389 Mbps
355 Mbps
51.0 Mbps
16.4 Bil

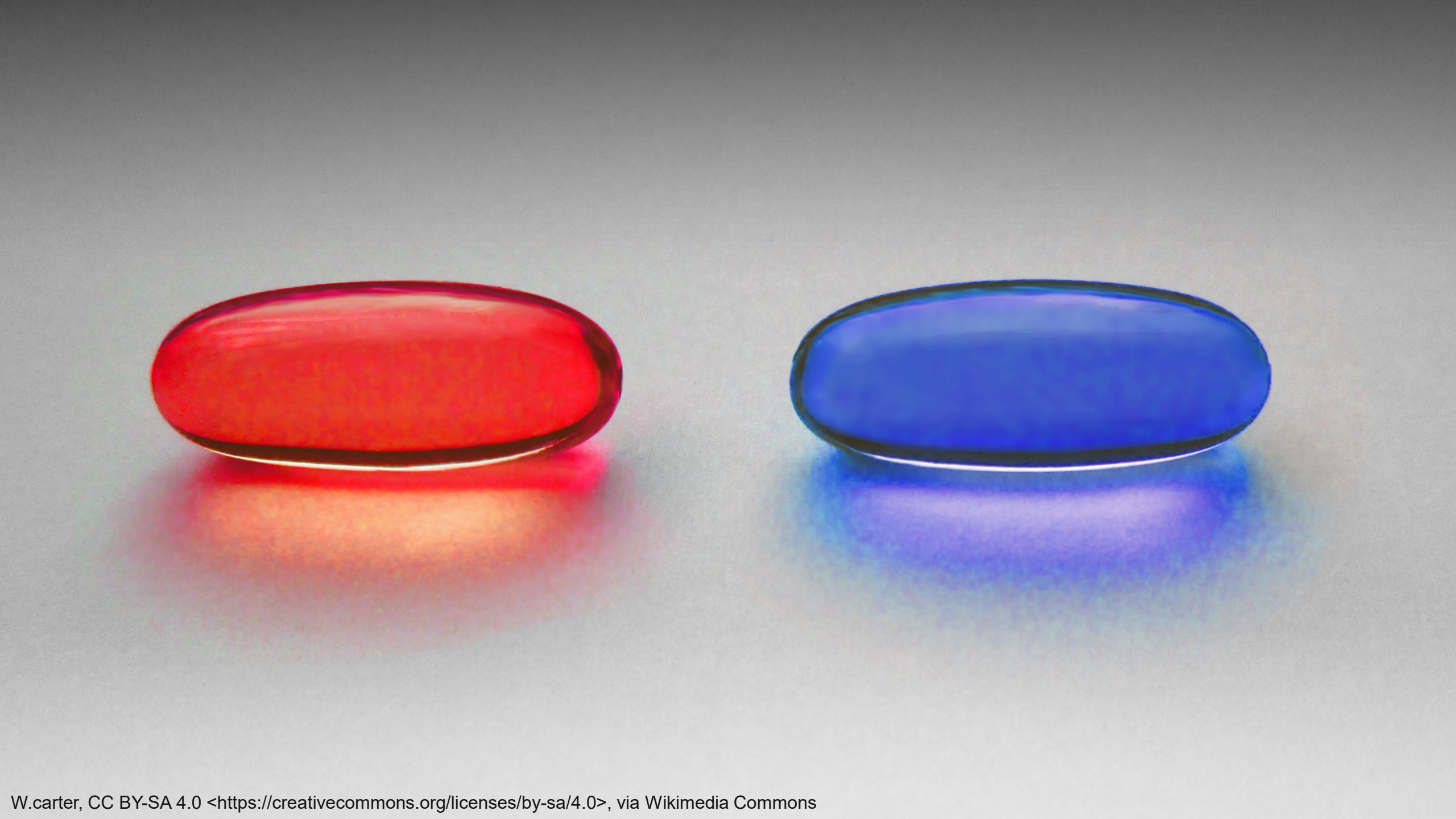


Detection Maturity Levels

http://ryanstillions.blogspot.com

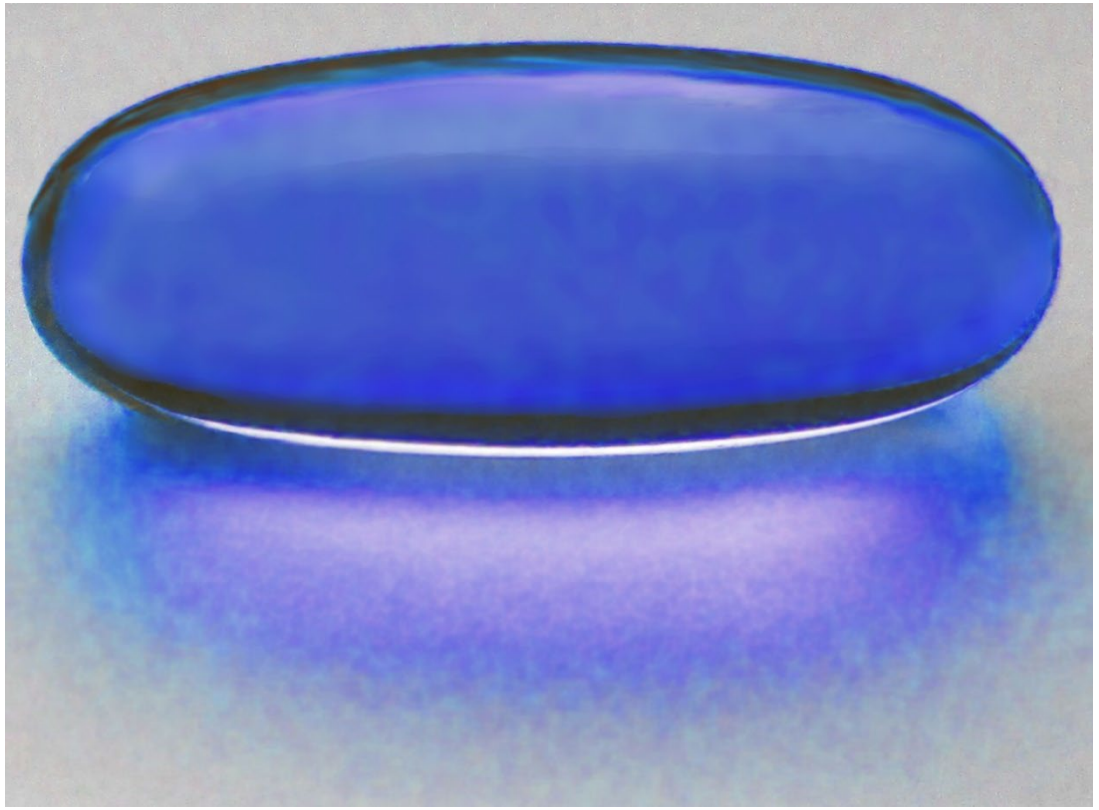
“MITRE ATT&CK is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary’s attack lifecycle and the platforms they are known to target.”

https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf



What if I told you... wait did you just take both pills

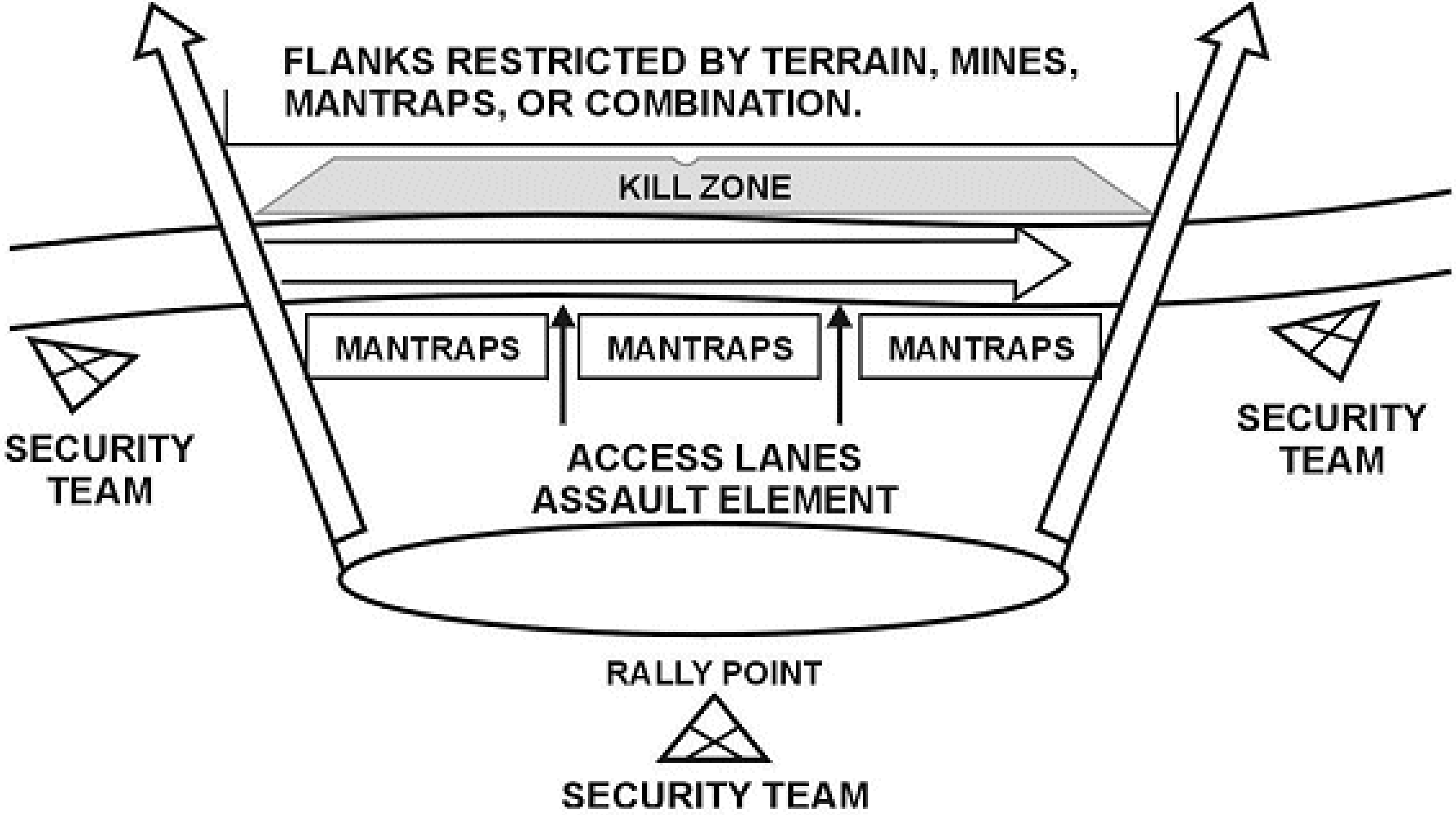
Tactics

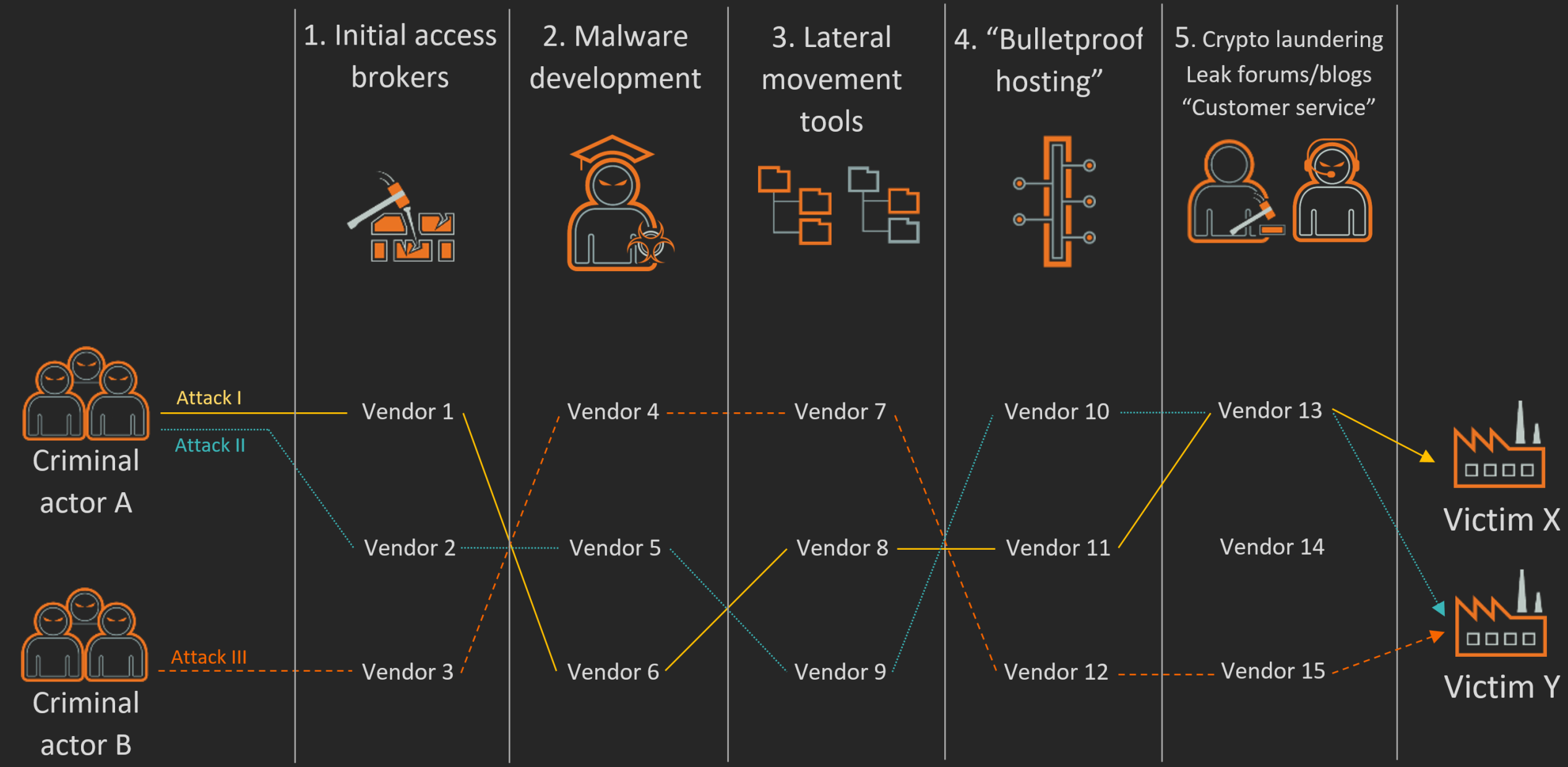


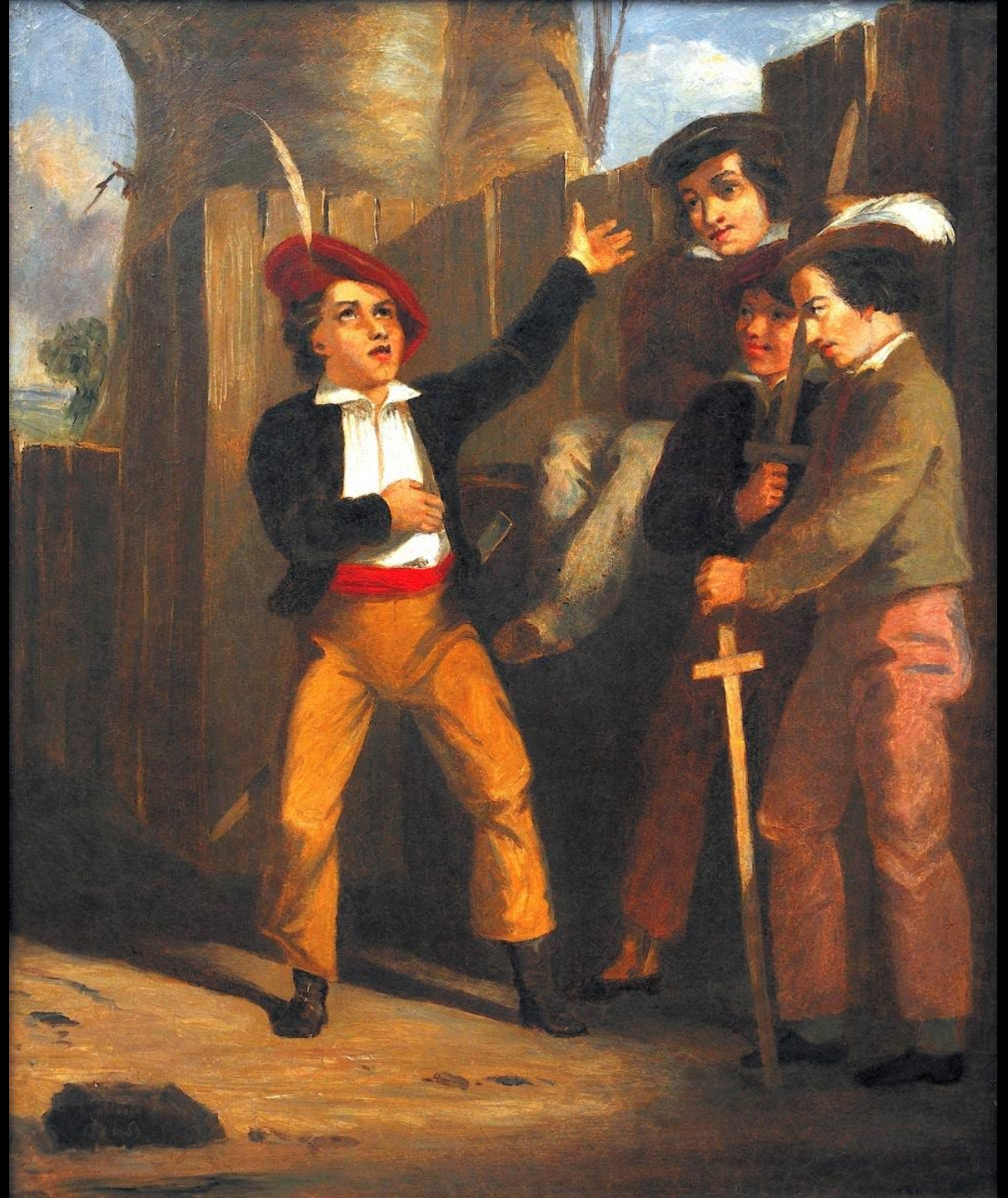
- Reconnaissance
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- …

Tactics

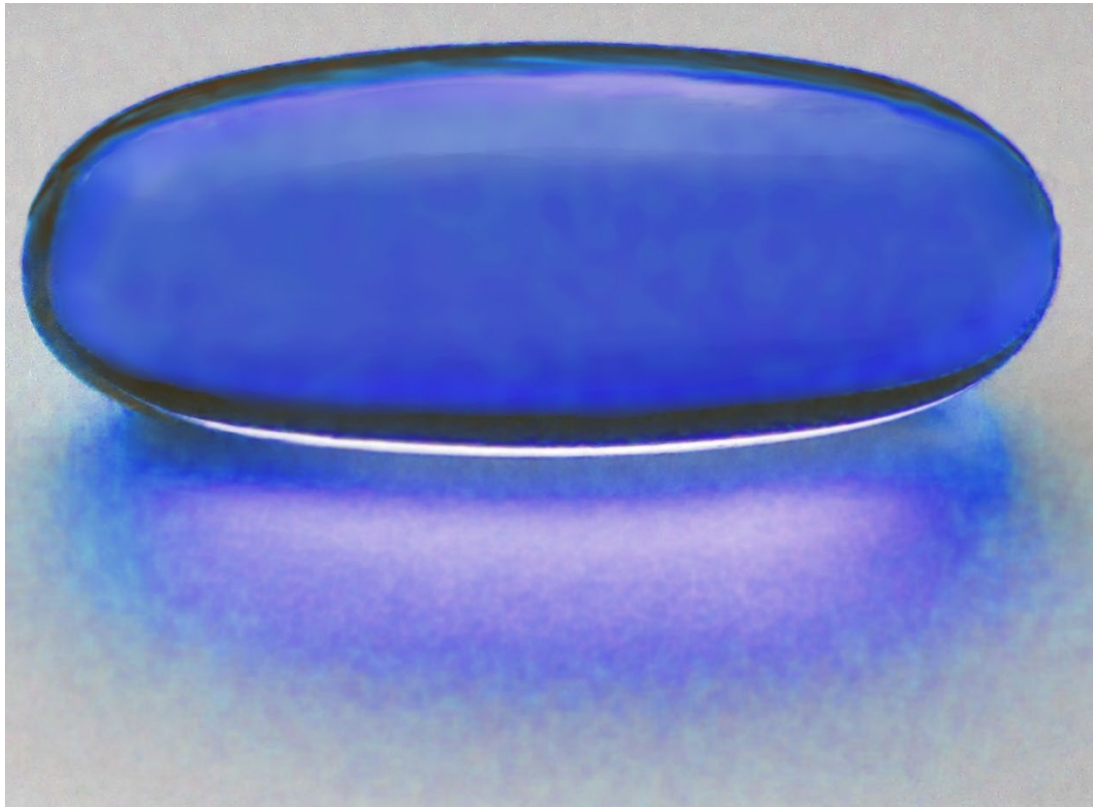
- Tactical Objectives
- Attack Phases


FLANKS RESTRICTED BY TERRAIN, MINES, MANTRAPS, OR COMBINATION.
KILL ZONE
MANTRAPS
MANTRAPS
MANTRAPS
SECURITY TEAM
ACCESS LANES ASSAULT ELEMENT
SECURITY TEAM
RALLY POINT
SECURITY TEAM


1. Initial access brokers
2. Malware development
3. Lateral movement tools
4. "Bulletproof hosting"
5. Crypto laundering
Leak forums/blogs
"Customer service"
Criminal actor A
Criminal actor B
Attack I
Attack II
Attack III
Vendor 1
Vendor 2
Vendor 3
Vendor 4
Vendor 5
Vendor 6
Vendor 7
Vendor 8
Vendor 9
Vendor 10
Vendor 11
Vendor 12
Vendor 13
Vendor 14
Vendor 15
Victim X
Victim Y



Techniques



- *How*
- Attribution
- Detection
- Heat Maps

Techniques

- *How and What*
  - Example: Valid Accounts
- Too General for Attribution
- Detection of Procedures

MITRE ATT&CK Coverage (1/2)

“The techniques within ATT&CK may have many procedures for how an adversary could implement them — and because adversaries are always changing, it is difficult to know what all those procedures are in advance.

That makes discussing coverage of a technique tough, especially when some ways of detecting behavior rely on individual procedures and some may span multiple procedures or even an entire technique.”

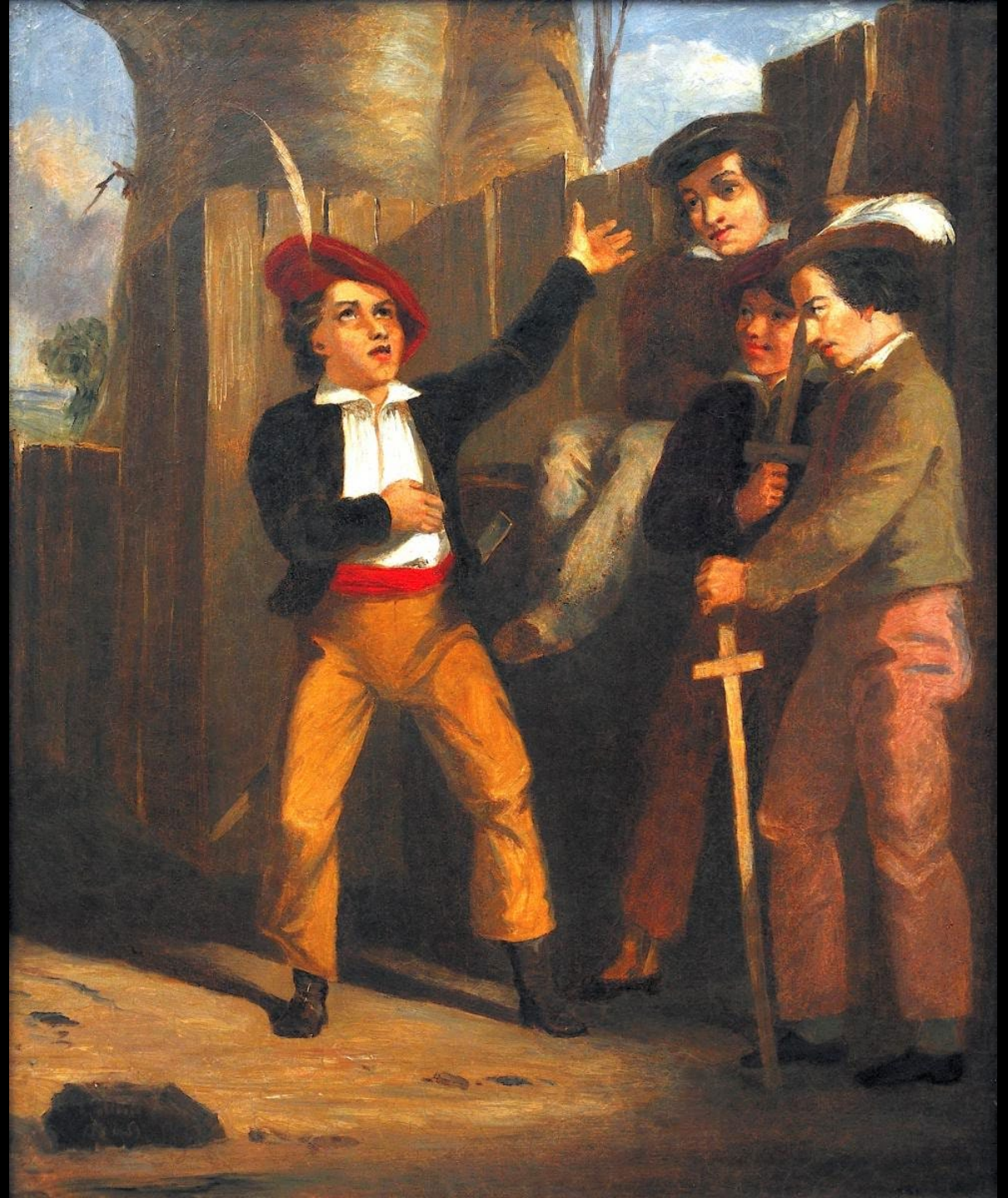
https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf

MITRE ATT&CK Coverage (2/2)

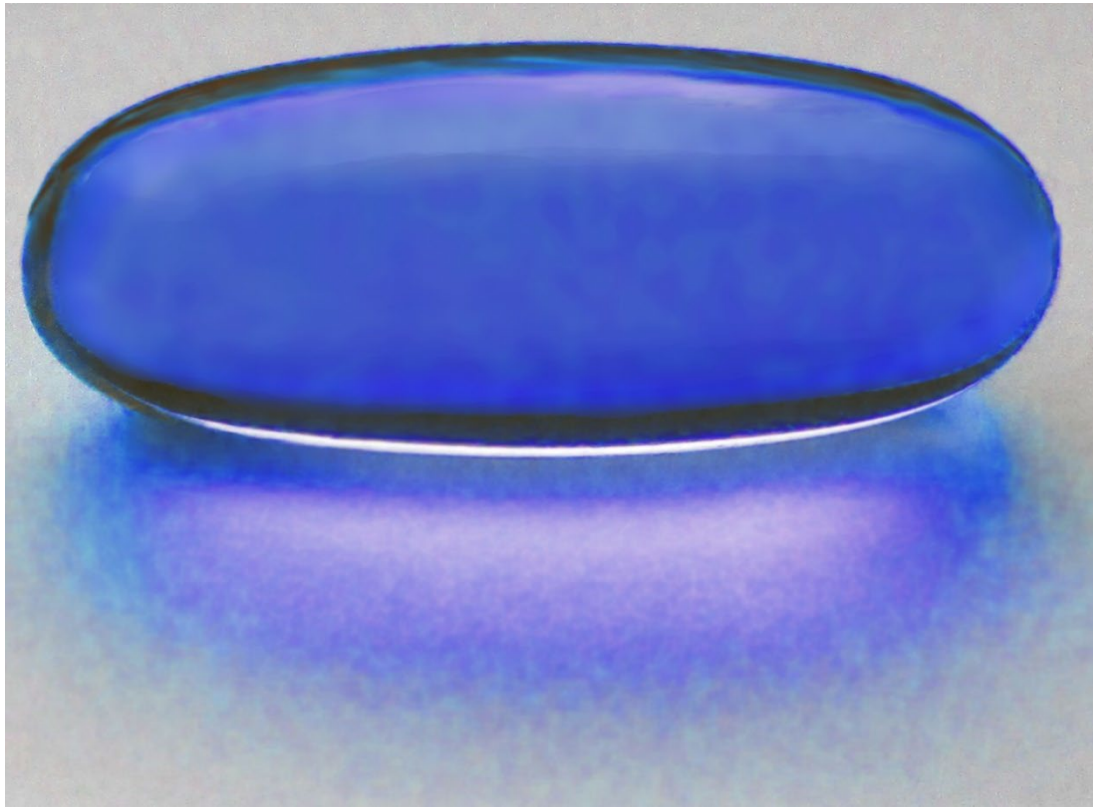
“Anyone mapping to ATT&CK should be able to explain the procedures they cover.

Similarly to how it’s unrealistic to expect coverage of 100% of ATT&CK techniques, it’s unrealistic to expect coverage of all procedures of a given technique, especially since we often cannot know all of them in advance.”

https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf



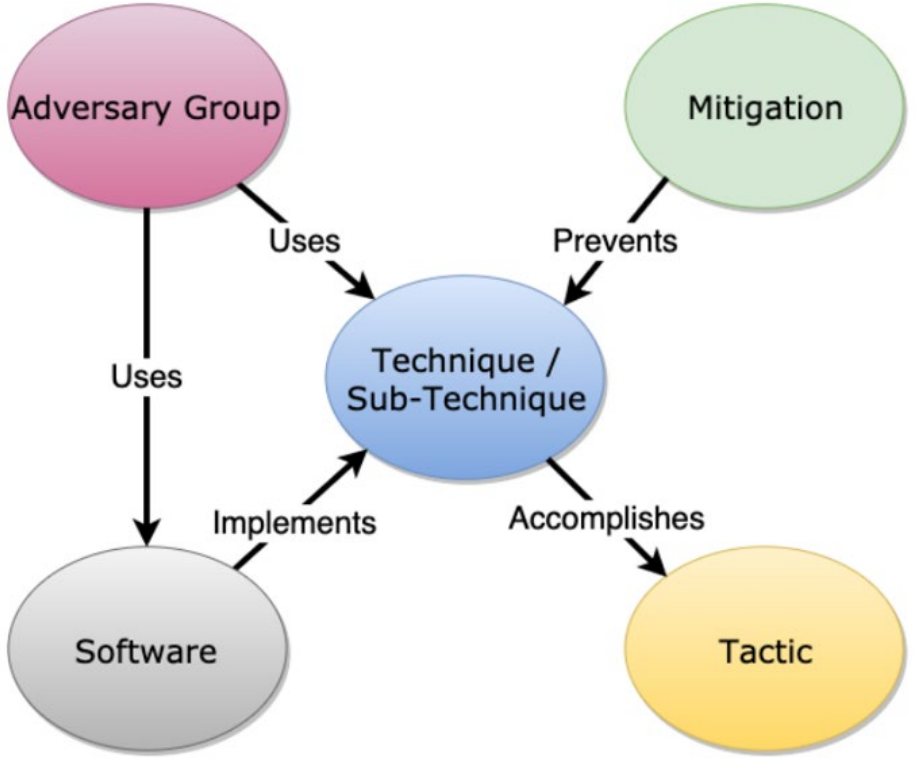
Procedures



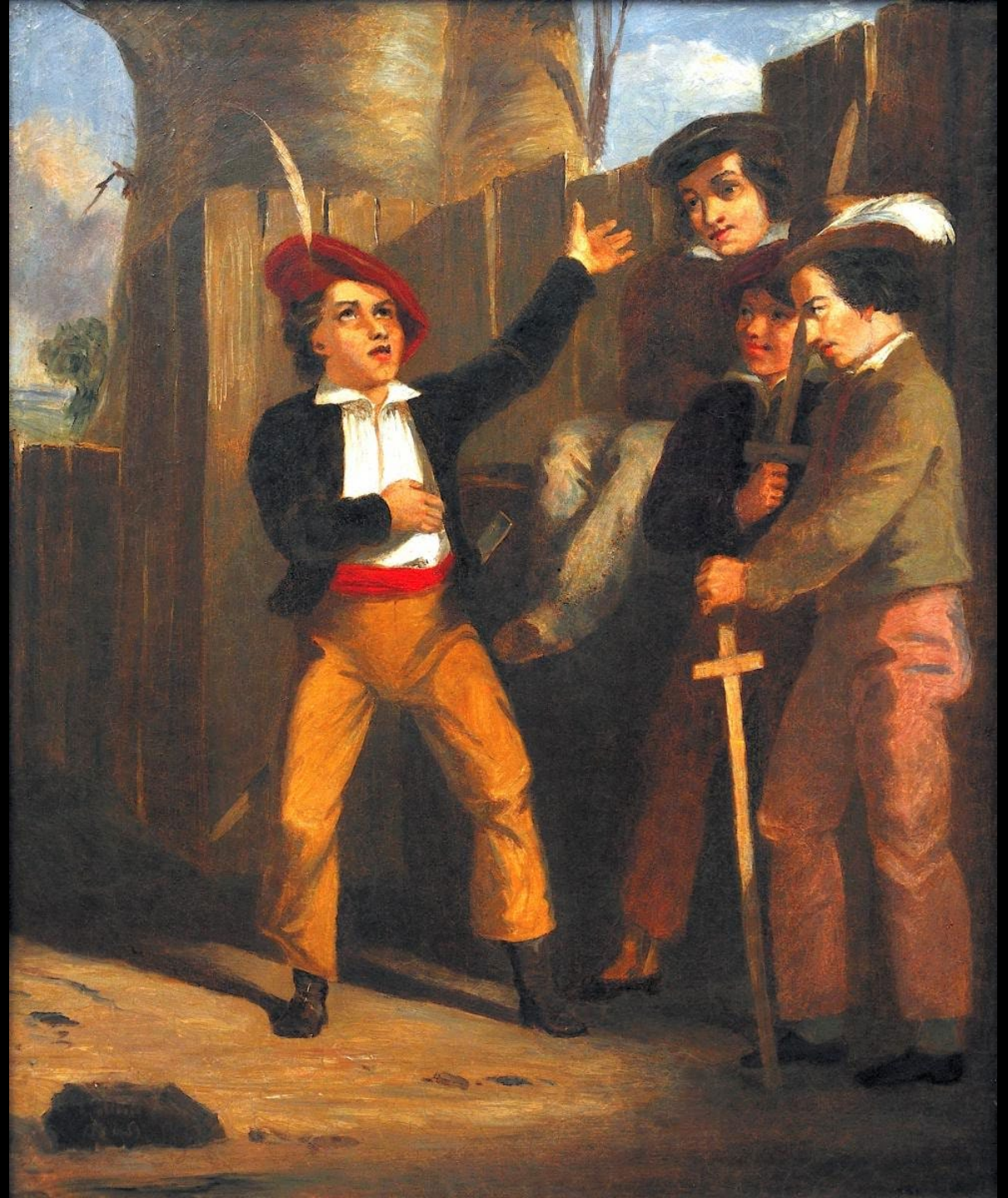
Procedure Examples

ID	Name	Description
G0007	APT28	APT28 exploited a Windows SMB Remote Code Execution Vulnerability to conduct lateral movement.[5][6][7]
S0606	Bad Rabbit	Bad Rabbit used the EternalRomance SMB exploit to spread through victim networks.[8]
S0608	Conficker	Conficker exploited the MS08-067 Windows vulnerability for remote code execution through a crafted RPC request.[9]
G0035	Dragonfly	Dragonfly has exploited a Windows Netlogon vulnerability (CVE-2020-1472) to obtain access to Windows Active Directory servers.[10]
S0367	Emotet	Emotet has been seen exploiting SMB via a vulnerability exploit like EternalBlue (MS17-010) to achieve lateral movement and propagation. [11][12][13][14]
S0363	Empire	Empire has a limited number of built-in modules for exploiting remote SMB, JBoss, and Jenkins servers.[15]
G0046	FIN7	FIN7 has exploited ZeroLogon (CVE-2020-1472) against vulnerable domain controllers.[16]
S0143	Flame	Flame can use MS10-061 to exploit a print spooler vulnerability in a remote system with a shared printer in order to move laterally.[17][18]
G0117	Fox Kitten	Fox Kitten has exploited known vulnerabilities in remote services including RDP.[19][20][21]
S0260	InvisiMole	InvisiMole can spread within a network via the BlueKeep (CVE-2019-0708) and EternalBlue (CVE-2017-0144) vulnerabilities in RDP and SMB respectively.[22]
S0532	Lucifer	Lucifer can exploit multiple vulnerabilities including EternalBlue (CVE-2017-0144) and EternalRomance (CVE-2017-0144).[23]
G0045	menuPass	menuPass has used tools to exploit the ZeroLogon vulnerability (CVE-2020-1472).[24]
S0368	NotPetya	NotPetya can use two exploits in SMBv1, EternalBlue and EternalRomance, to spread itself to other remote systems on the network.[25][26][27]
S0378	PoshC2	PoshC2 contains a module for exploiting SMB via EternalBlue.[28]
S0650	QakBot	QakBot can move laterally using worm-like functionality through exploitation of SMB.[29]
S0603	Stuxnet	Stuxnet propagates using the MS10-061 Print Spooler and MS08-067 Windows Server Service vulnerabilities.[30]
G0027	Threat Group-3390	Threat Group-3390 has exploited MS17-010 to move laterally to other systems on the network.[31]
G0131	Tonto Team	Tonto Team has used EternalBlue exploits for lateral movement.[32]
S0266	TrickBot	TrickBot utilizes EternalBlue and EternalRomance exploits for lateral movement in the modules wormwinDll, wormDll, mwormDll, nwormDll, tabDll.[33]
S0366	WannaCry	WannaCry uses an exploit in SMBv1 to spread itself to other remote systems on a network.[34][35][36]
G0102	Wizard Spider	Wizard Spider has exploited or attempted to exploit Zerologon (CVE-2020-1472) and EternalBlue (MS17-010) vulnerabilities.[37][38][39]

Procedures



https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf



The Road Ahead

- Remove «what» techniques
- Enumerate procedures
- Enumerate tactics
- Transform procedures to detection analytics
  - STIX Patterning

SOCCRATES and Contact Information

- Web Site
  - https://soccrates.eu
- E-Mail
  - meian@mnemonic.no
- LinkedIn
  - https://linkedin.com/in/martineian