PRE-ATT&CK Integration

Adam Pennington
@_whatshisface

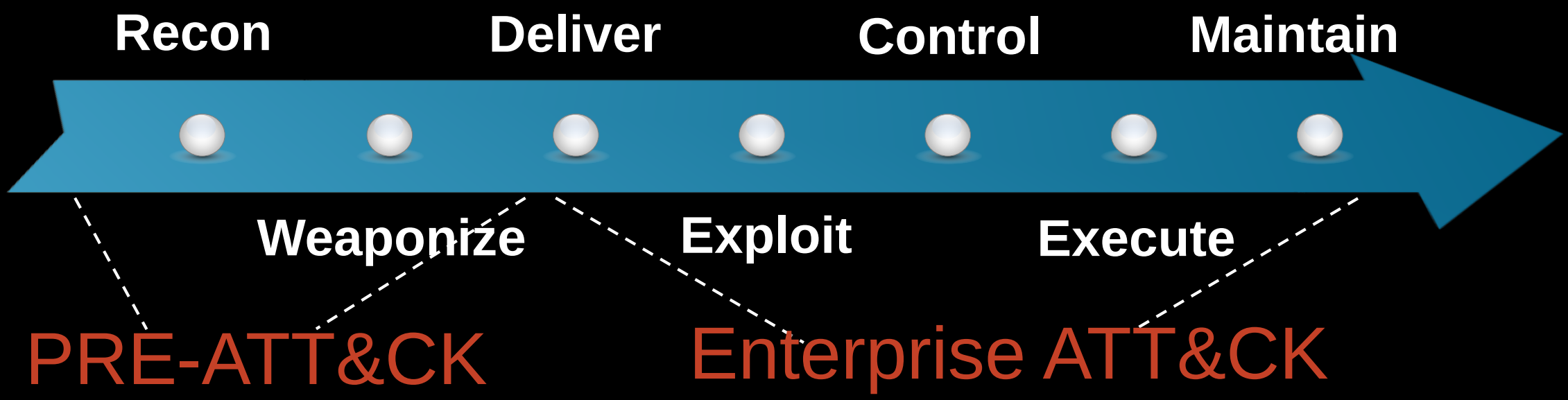
@MITREattack

#ATTACKcon

MITRE

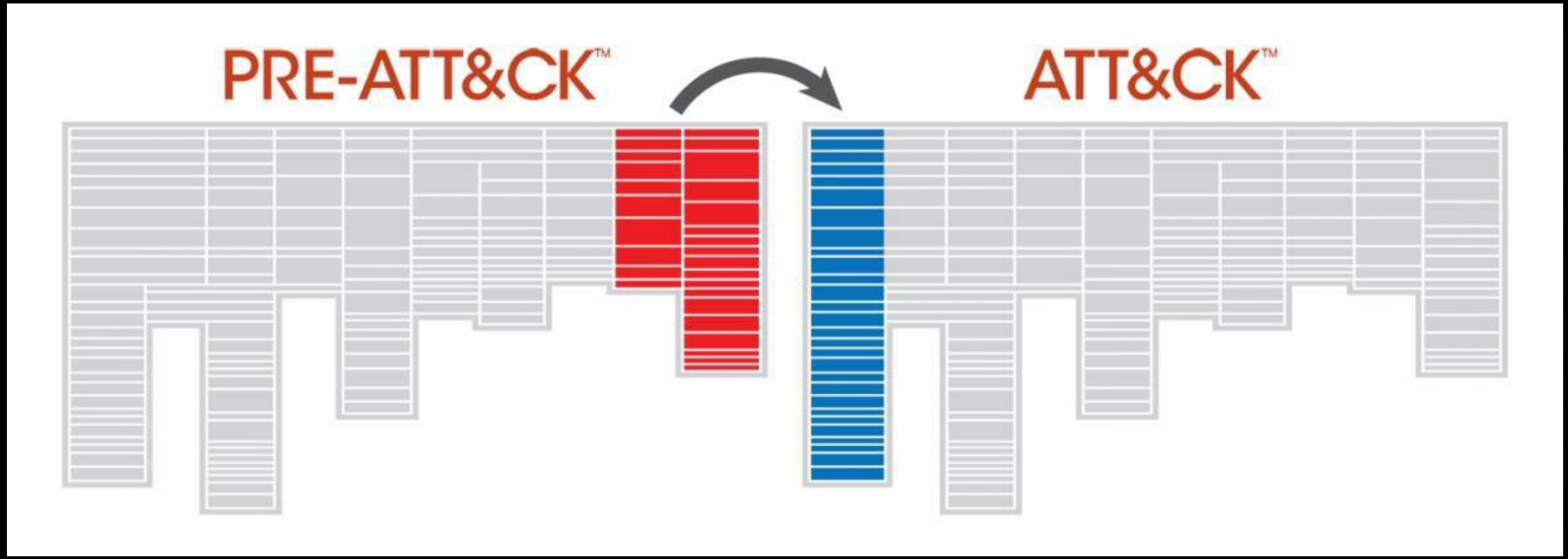
©2019 The MITRE Corporation. ALL RIGHTS RESERVED. Approved for public release. Distribution unlimited 19-01075-13.

PRE-ATT&CK



©2019 The MITRE Corporation. ALL RIGHTS RESERVED. Approved for public release. Distribution unlimited 19-01075-13.

Launch/Compromise -> Initial Access



2018

©2019 The MITRE Corporation. ALL RIGHTS RESERVED. Approved for public release. Distribution unlimited 19-01075-13.

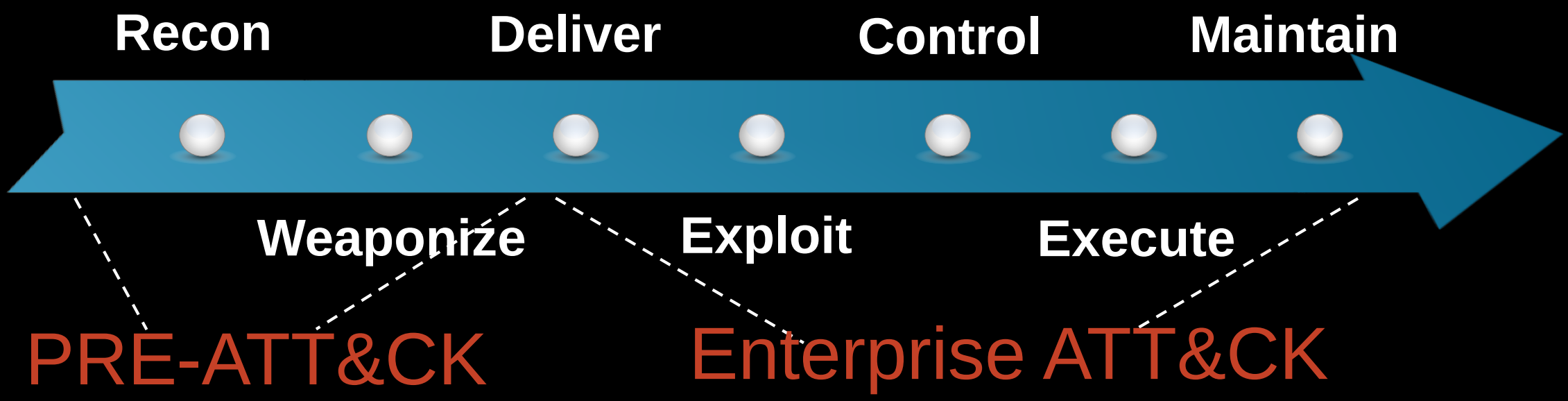
Enterprise ATT&CK

PRE-ATT&CK

} It's just ATT&CK™

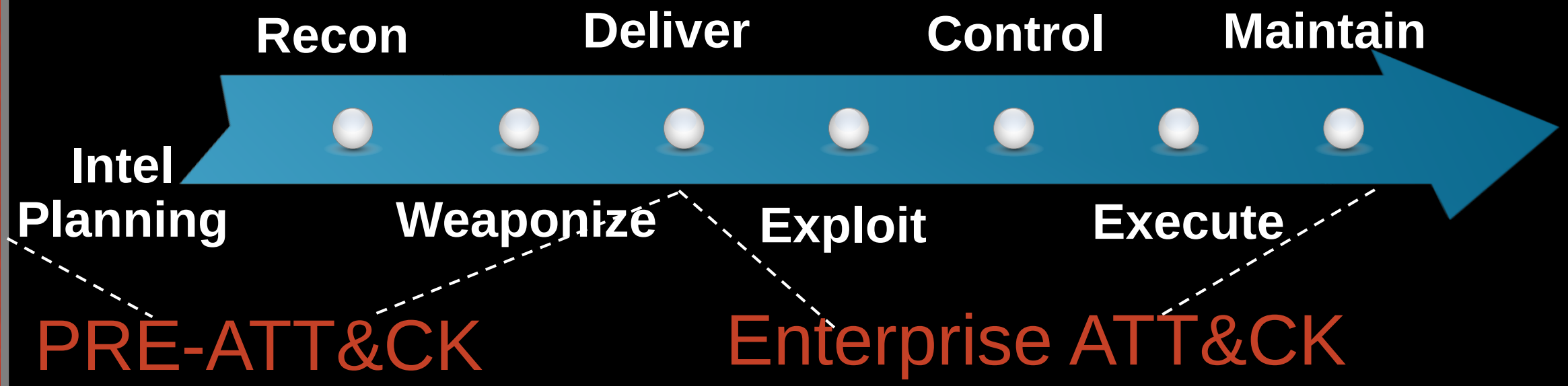
©2019 The MITRE Corporation. ALL RIGHTS RESERVED. Approved for public release. Distribution unlimited 19-01075-13.

PRE's Place in the Adversary Lifecycle



©2019 The MITRE Corporation. ALL RIGHTS RESERVED. Approved for public release. Distribution unlimited 19-01075-13.

PRE's Place in the Adversary Lifecycle



©2019 The MITRE Corporation. ALL RIGHTS RESERVED. Approved for public release. Distribution unlimited 19-01075-13.

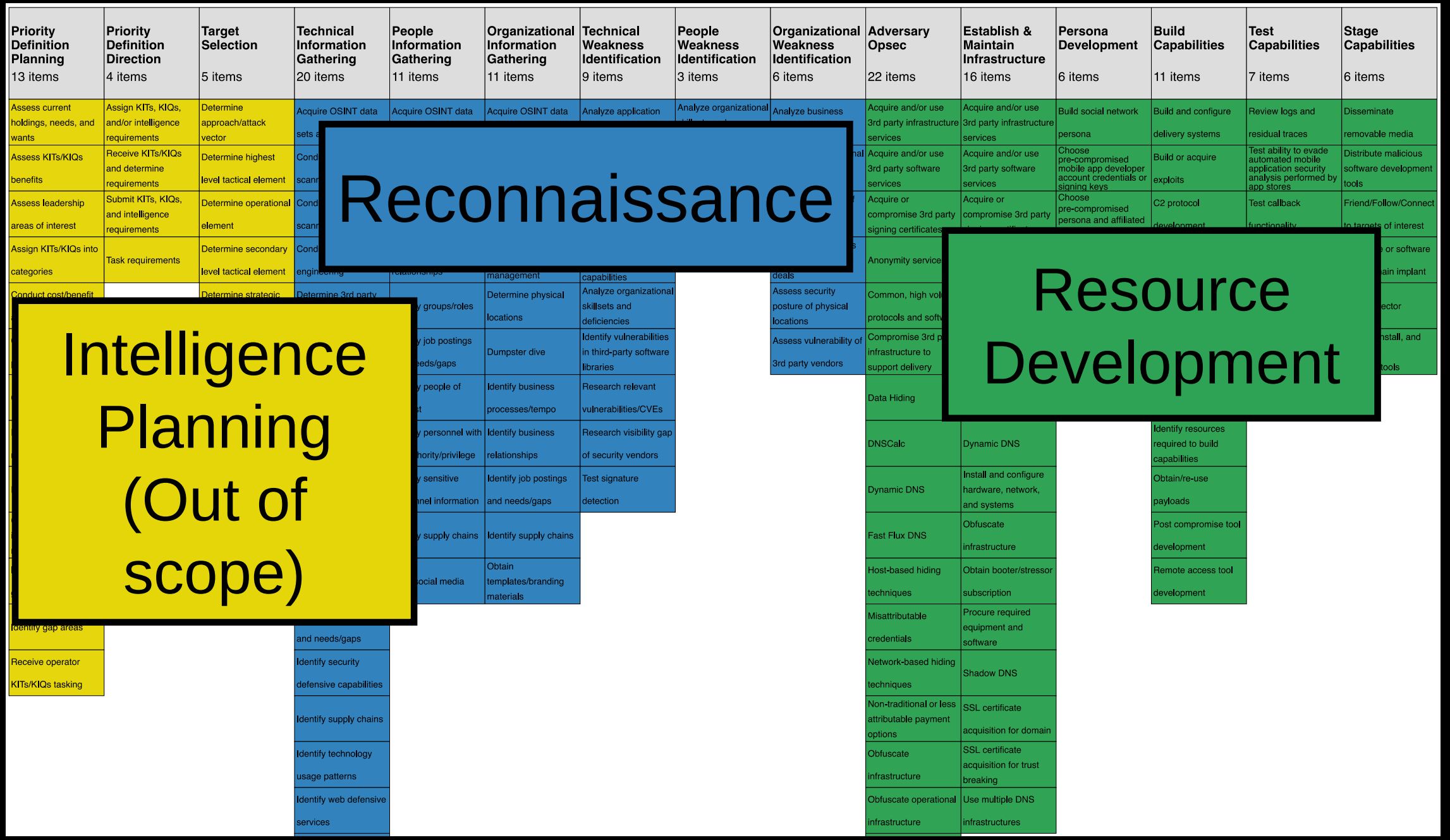
How do we scope techniques?

- Technical
- Visible to some defenders
- Evidence of adversary use

©2019 The MITRE Corporation. ALL RIGHTS RESERVED. Approved for public release. Distribution unlimited 19-01075-13.

Priority Definition Planning 13 items	Priority Definition Direction 4 items	Target Selection 5 items	Technical Information Gathering 20 items	People Information Gathering 11 items	Organizational Information Gathering 11 items	Technical Weakness Identification 9 items	People Weakness Identification 3 items	Organizational Weakness Identification 6 items	Adversary Opsec 22 items	Establish & Maintain Infrastructure 16 items	Persona Development 6 items	Build Capabilities 11 items	Test Capabilities 7 items	Stage Capabilities 6 items
Assess current holdings, needs, and wants	Assign KITs, KIQs, and/or intelligence requirements	Determine approach/attack vector	Acquire OSINT data sets and information	Acquire OSINT data sets and information	Acquire OSINT data sets and information	Analyze application security posture	Analyze organizational skillsets and deficiencies	Analyze business processes	Acquire and/or use 3rd party infrastructure services	Acquire and/or use 3rd party infrastructure services	Build social network persona	Build and configure delivery systems	Review logs and residual traces	Disseminate removable media
Assess KITs/KIQs benefits	Receive KITs/KIQs and determine requirements	Determine highest level tactical element	Conduct active scanning	Aggregate individual's digital footprint	Conduct social engineering	Analyze architecture and configuration posture	Analyze social and business relationships, interests, and affiliations	Analyze organizational skillsets and deficiencies	Acquire and/or use 3rd party software services	Acquire and/or use 3rd party software services	Choose pre-compromised mobile app developer account credentials or signing keys	Build or acquire exploits	Test ability to evade automated mobile application security analysis performed by app stores	Distribute malicious software development tools
Assess leadership areas of interest	Submit KITs, KIQs, and intelligence requirements	Determine operational element	Conduct passive scanning	Conduct social engineering	Determine 3rd party infrastructure services	Analyze data collected	Assess targeting options	Analyze presence of outsourced capabilities	Acquire or compromise 3rd party signing certificates	Acquire or compromise 3rd party signing certificates	Choose pre-compromised persona and affiliated accounts	C2 protocol development	Test callback functionality	Friend/Follow/Connect to targets of interest
Assign KITs/KIQs into categories	Task requirements	Determine secondary level tactical element	Conduct social engineering	Identify business relationships	Determine centralization of IT management	Analyze hardware/software security defensive capabilities		Assess opportunities created by business deals	Anonymity services	Buy domain name	Develop social network persona digital footprint	Compromise 3rd party or closed-source vulnerability/exploit information	Test malware in various execution environments	Hardware or software supply chain implant
Conduct cost/benefit analysis		Determine strategic target	Determine 3rd party infrastructure services	Identify groups/roles	Determine physical locations	Analyze organizational skillsets and deficiencies		Assess security posture of physical locations	Common, high volume protocols and software	Compromise 3rd party infrastructure to support delivery	Friend/Follow/Connect to targets of interest	Create custom payloads	Test malware to evade detection	Port redirector
Create implementation plan			Determine domain and IP address space	Identify job postings and needs/gaps	Dumpster dive	Identify vulnerabilities in third-party software libraries		Assess vulnerability of 3rd party vendors	Compromise 3rd party infrastructure to support delivery	Create backup infrastructure	Obtain Apple iOS enterprise distribution key pair and certificate	Create infected removable media	Test physical access	Upload, install, and configure software/tools
Create strategic plan			Determine external network trust dependencies	Identify people of interest	Identify business processes/tempo	Research relevant vulnerabilities/CVEs			Data Hiding	Domain registration hijacking		Discover new exploits and monitor exploit-provider forums	Test signature detection for file upload/email filters	
Derive intelligence requirements			Determine firmware version	Identify personnel with an authority/privilege	Identify business relationships	Research visibility gap of security vendors			DNSCalc	Dynamic DNS		Identify resources required to build capabilities		
Develop KITs/KIQs			Discover target logon/email address format	Identify sensitive personnel information	Identify job postings and needs/gaps	Test signature detection			Dynamic DNS	Install and configure hardware, network, and systems		Obtain/re-use payloads		
Generate analyst intelligence requirements			Enumerate client configurations	Identify supply chains	Identify supply chains				Fast Flux DNS	Obfuscate infrastructure		Post compromise tool development		
Identify analyst level gaps			Enumerate externally facing software applications technologies, languages, and dependencies	Mine social media	Obtain templates/branding materials				Host-based hiding techniques	Obtain booter/stressor subscription		Remote access tool development		
Identify gap areas			Identify job postings and needs/gaps						Misattributable credentials	Procure required equipment and software				
Receive operator KITs/KIQs tasking			Identify security defensive capabilities						Network-based hiding techniques	Shadow DNS				
			Identify supply chains						Non-traditional or less attributable payment options	SSL certificate acquisition for domain				
			Identify technology usage patterns						Obfuscate infrastructure	SSL certificate acquisition for trust breaking				
			Identify web defensive services						Obfuscate operational infrastructure	Use multiple DNS infrastructures				

©2019 The MITRE Corporation. ALL RIGHTS RESERVED. Approved for public release. Distribution unlimited 19-01075-13.



©2019 The MITRE Corporation. ALL RIGHTS RESERVED. Approved for public release. Distribution unlimited 19-01075-13.

<DRAFT>Reconnaissance</DRAFT>

- **Gather victim identity information**
  - Credentials
  - Email addresses
  - Employee names
- **Gather victim network information**
  - Domain properties
  - DNS
  - Network trust dependencies
  - Network topology
  - IP addresses
  - Firewall
  - NIDS
- **Gather victim host information**
  - Hardware
  - Software
  - Firmware
  - Client configurations
- **Search open websites/domains**
  - Social media
  - Search engines
- **Search victim-owned websites**
- **Active Scanning**
  - Scanning IP blocks
  - Vulnerability scanning
- **Search open technical databases**
  - Whois
  - DNS/passive DNS
  - TLS certs
  - CDNs
  - Scans databases
- **Search closed databases**
  - Threat intel vendors
  - Paid versions of open databases
- **Spearphishing for Information**
  - Service
  - Attachment
  - Link

DRAFT

Tactic and Technique names/list are draft and subject to change

ATT&CK™

MITRE

©2019 The MITRE Corporation. ALL RIGHTS RESERVED. Approved for public release. Distribution unlimited 19-01075-13.

<DRAFT>Resource Development</DRAFT>

- **Buy/Acquire Infrastructure**
  - Domains
  - DNS
  - VPS/Cloud VM
  - Server
  - Botnet
  - Web services
- **Compromise Infrastructure**
  - Domains
  - DNS
  - VPS/Cloud VMs
  - Server
  - Botnet
  - Web services
- **Create Accounts**
  - Social Media
  - Email accounts
- **Compromise Accounts**
  - Social Media
  - Email accounts
- **Develop Capabilities (Build)**
  - Malware
  - Software
  - SSL certs
  - Vulnerabilities
  - Exploits
- **Acquire Capabilities (Buy or steal)**
  - Malware
  - Software
  - SSL certs
  - Software certs
  - Vulnerabilities
  - Exploits

DRAFT

Tactic and Technique names/list are draft and subject to change

©2019 The MITRE Corporation. ALL RIGHTS RESERVED. Approved for public release. Distribution unlimited 19-01075-13.

Adam Pennington
@_whatshisface

ATT&CK™

attack@mitre.org
@MITREattack
#ATTACKcon

MITRE

©2019 The MITRE Corporation. ALL RIGHTS RESERVED. Approved for public release. Distribution unlimited 19-01075-13.