Adapting Cyber Kill Chains for Insiders

Adversarial Behaviours

Cyber Kill Chains

Adversarial Behaviours

- Cyber kill chains supports organisations and individuals in formulating the **anatomy of an attack** as well as considering defences.
- Specifically the model considered is optimal for **intrusions**, arguably for other types of attacks the approach is not optimal.
- Not necessarily optimal for all types of intrusion attacks as the model is **fixated largely on external threats**.
- Consequently, may need to **adapt model** for some attacks as well as intrusion attacks, **such as insider threats**.

Phases

Hutchins *et al.* Cyber Kill Chain Model

Saxena Cyber Kill Chain Model

Phases

Saxena *et al.* Cyber Kill Chain Model

Tipping

Saxena *et al.* Cyber Kill Chain Model

- The insider resigns from the organisation or transfers from existing role to another role.
- The challenge is determining unusual behaviour on the part of the employee as this may inform the start of an insider threat.

Reconnaissance

Saxena *et al.* Cyber Kill Chain Model

- The insider will need to **identify valuable data or assets** to the enterprise. Initially this may start within authorised systems, before expanding their boundaries to other systems (possibly using privilege escalation techniques).
- Insiders may also reveal important roles, project names or sensitive relationships to external actors or may manipulate these using other means (e.g. dating applications).

Exploitation

Saxena *et al.* Cyber Kill Chain Model

- Tailoring malware or other weapons to the organisation, specifically targeting weaknesses within the organisation.
- External attackers may install remote access trojans (RATs), but insiders can utilise tools that they may have to perform their role.
- Insiders know the common documents within the organisation, defences and can typically know naming conventions, making documents useful to deliver payloads.

Acquisition

Saxena *et al.* Cyber Kill Chain Model

- Once assets have been determined and access can be exploited, the next step is for the insider to acquire the assets.
- Approach here could be to use back-up solutions, configured to ensure any changes to assets are properly captured.
- Assets such as data can then be captured and transferred to optimal locations for exfiltration.

Exfiltration

Saxena *et al.* Cyber Kill Chain Model

- Upon acquisition of assets the insider needs to exfiltrate them beyond the perimeter of the enterprise.
- Insider can exfiltrate data in number of ways, but common approach could be to exfiltrate data using USB thumb drives, hard disks or even smartphones.
- More sophisticated approaches can be used to exfiltrate data out of the organisation.

Phases

Saxena *et al.* Cyber Kill Chain Model

Discussion

Saxena *et al.* Cyber Kill Chain Model

- Adapting the cyber kill chain approach to focus on insiders can be valuable in focusing on the important aspects that are central to that attack.
- Saxena et al. approach is a strong starting point and be used alongside other cyber kill chain models to create a cyber kill approach for insiders.

Insider Cyber Kill Chain Model

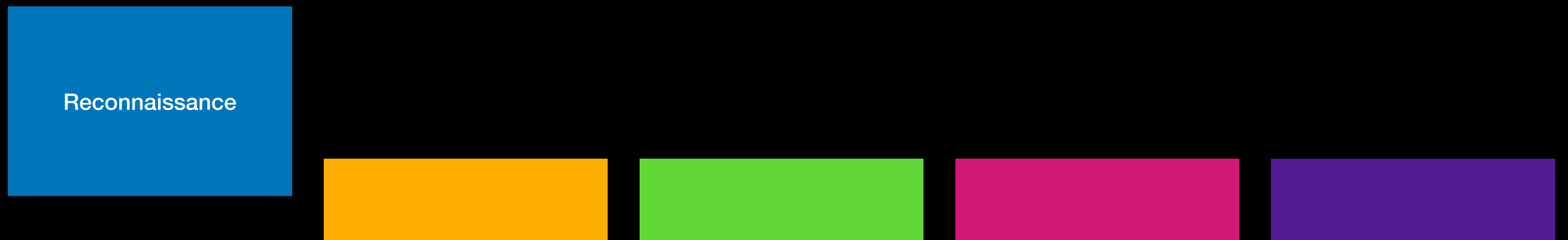
Phases

Insider Cyber Kill Chain Model

Reconnaissance

Insider Cyber Kill Chain Model Phases

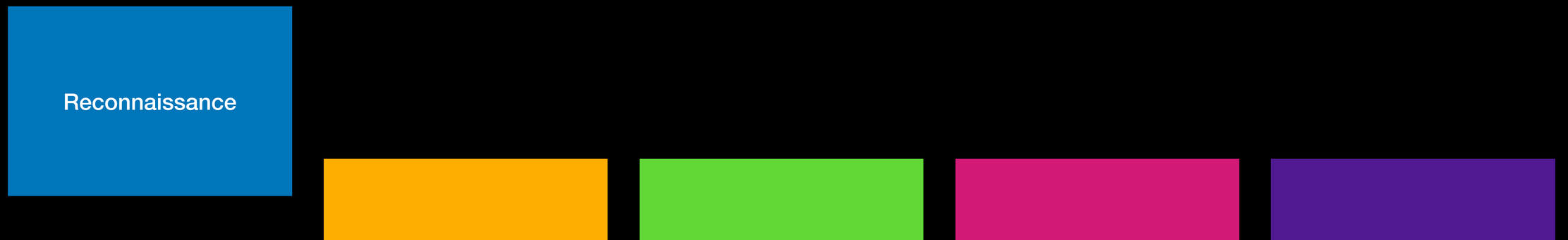
- The insider will need to **identify valuable data or assets** to the enterprise. Initially this may start within authorised systems, before expanding their boundaries to other systems (possibly using privilege escalation techniques).
- Insiders may also reveal important roles, project names or sensitive relationships to external actors or may manipulate these using other means (e.g. dating applications).



Reconnaissance

Insider Cyber Kill Chain Model Phases

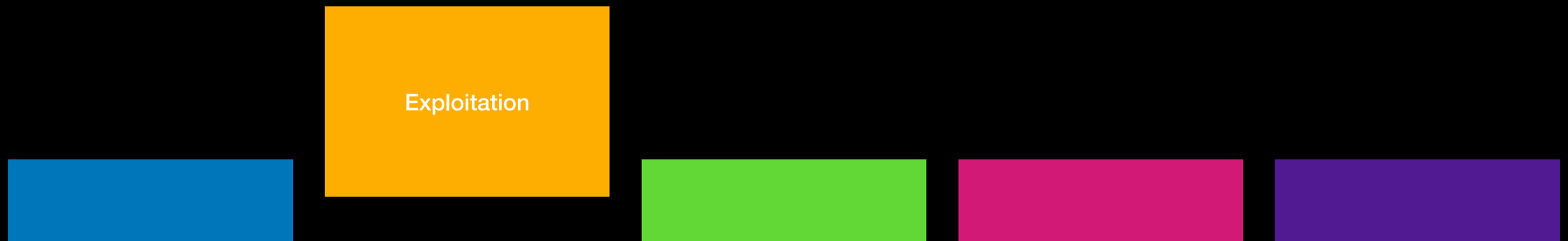
- Examples of reconnaissance techniques could be:
  - Specialised and unusal commands being executed on the system.
  - Access unauthorised locations or rarely accessed locations.
  - High access rates of specific files or folders.
  - Use of exploitation kits or other such malicious software.



Exploitation

Insider Cyber Kill Chain Model Phases

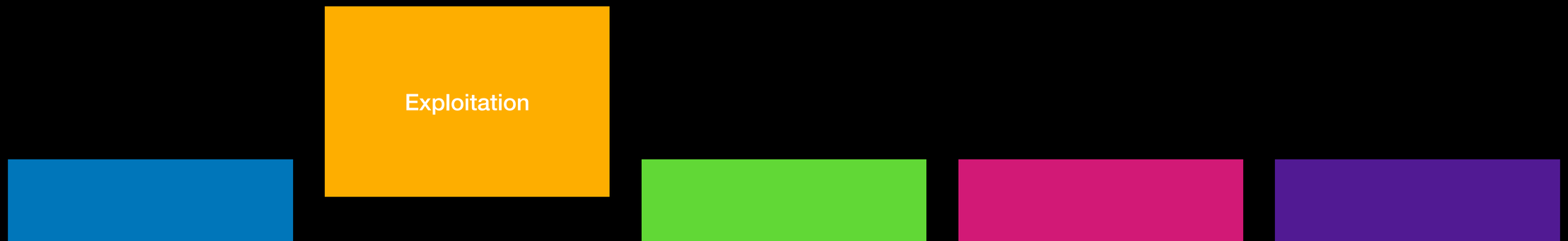
- The insider will exploit weakness in the security of systems or circumvent measures designed to protect security.
- Enterprises will want to ensure they routinely capture attempt to test security of systems or circumvent them.
  - Searches, uses of VPN tools, attempts to defeat security measures, use of alternative software solutions (e.g. alternative messaging solutions).
  - Potentially difficult to detect as may be part of role, potential to impact on business by interfering with autonomy - may even cause insiders!



Exploitation

Insider Cyber Kill Chain Model Phases

- Examples of exploitation techniques could be:
  - Searches, uses of VPN tools, attempts to defeat security measures, use of alternative software solutions (e.g. alternative messaging solutions).
  - Potentially difficult to detect as may be part of role, potential to impact on business by interfering with autonomy - may even cause insiders!



Preparation

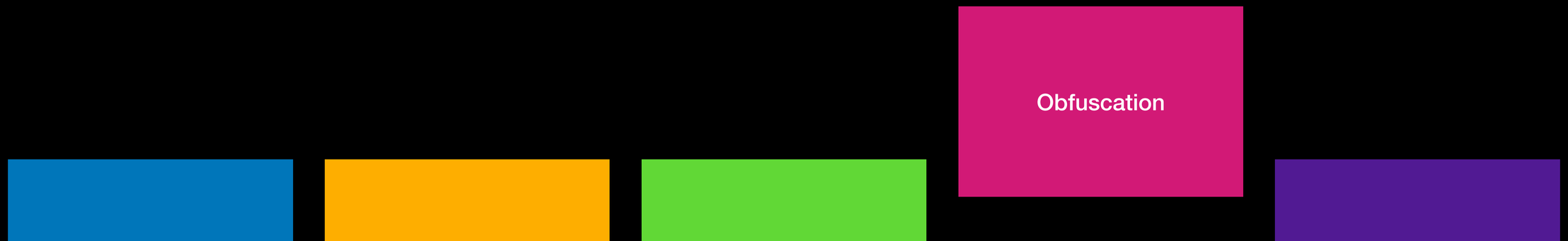
Insider Cyber Kill Chain Model Phases

- The insider needs to prepare the data or assets they are going to exfiltrate from the organisation.
- Examples of preparation techniques could be:
  - Generation and storage of unusual files, significant and/or unusual file activity.

Obfuscation

Insider Cyber Kill Chain Model Phases

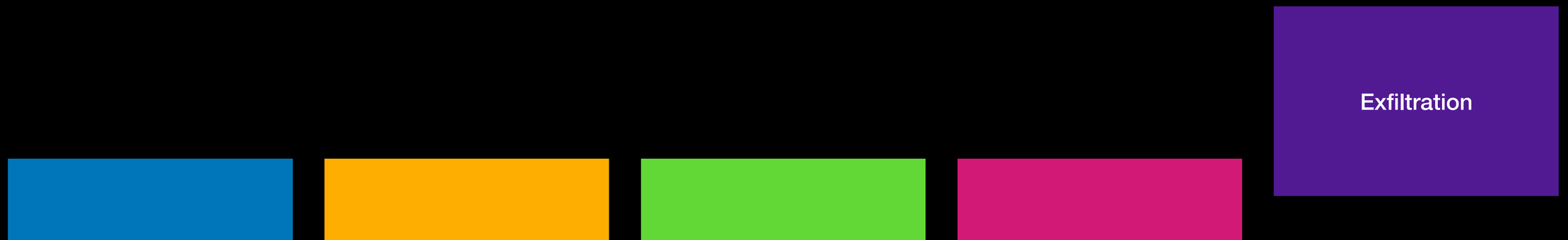
- The insider will attempt to essentially **cover their tracks** as to not be considered as the source of any attack.
- Examples of obstruction techniques could be:
  - Using techniques to smuggle the data out of the organisation using techniques such as steganography.
  - Attempting to turn-off security measures or cleanse logs or monitors.



Exfiltration

Insider Cyber Kill Chain Model Phases

- The typical final step where the individual exfiltrates the data from the organisation.
- Examples of exfiltration techniques could be:
  - Large file transfers using personal email account, increased use of personal email account.
  - Increased use of remote working tools and use of removable media.



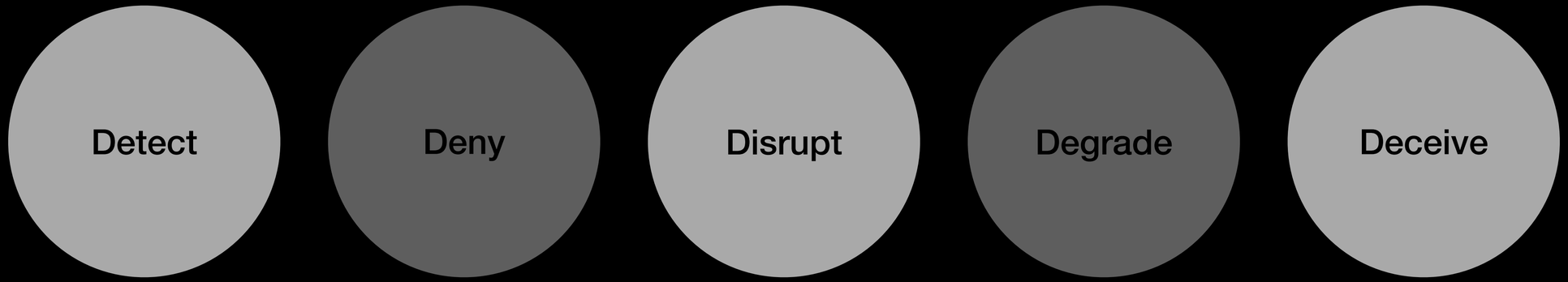
Phases

Insider Cyber Kill Chain Model Phases

Defensive steps

Defensive steps

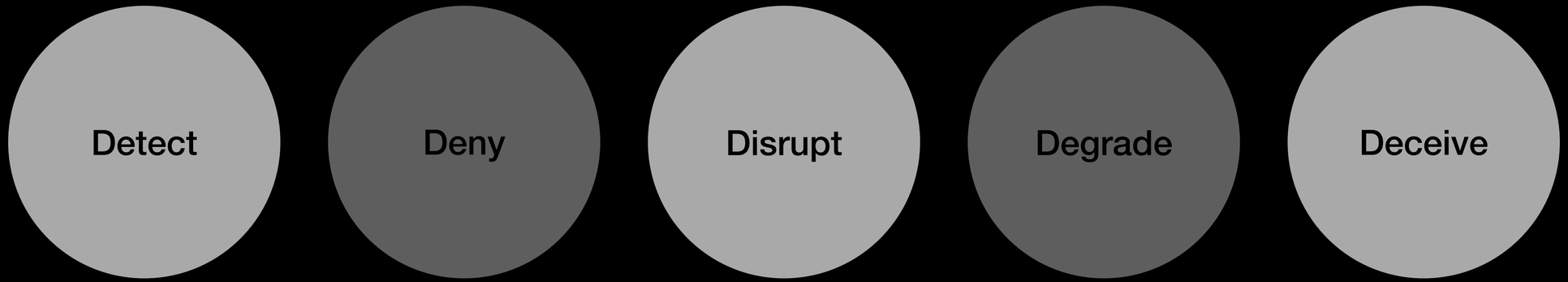
Insider Cyber Kill Chain Model Phases

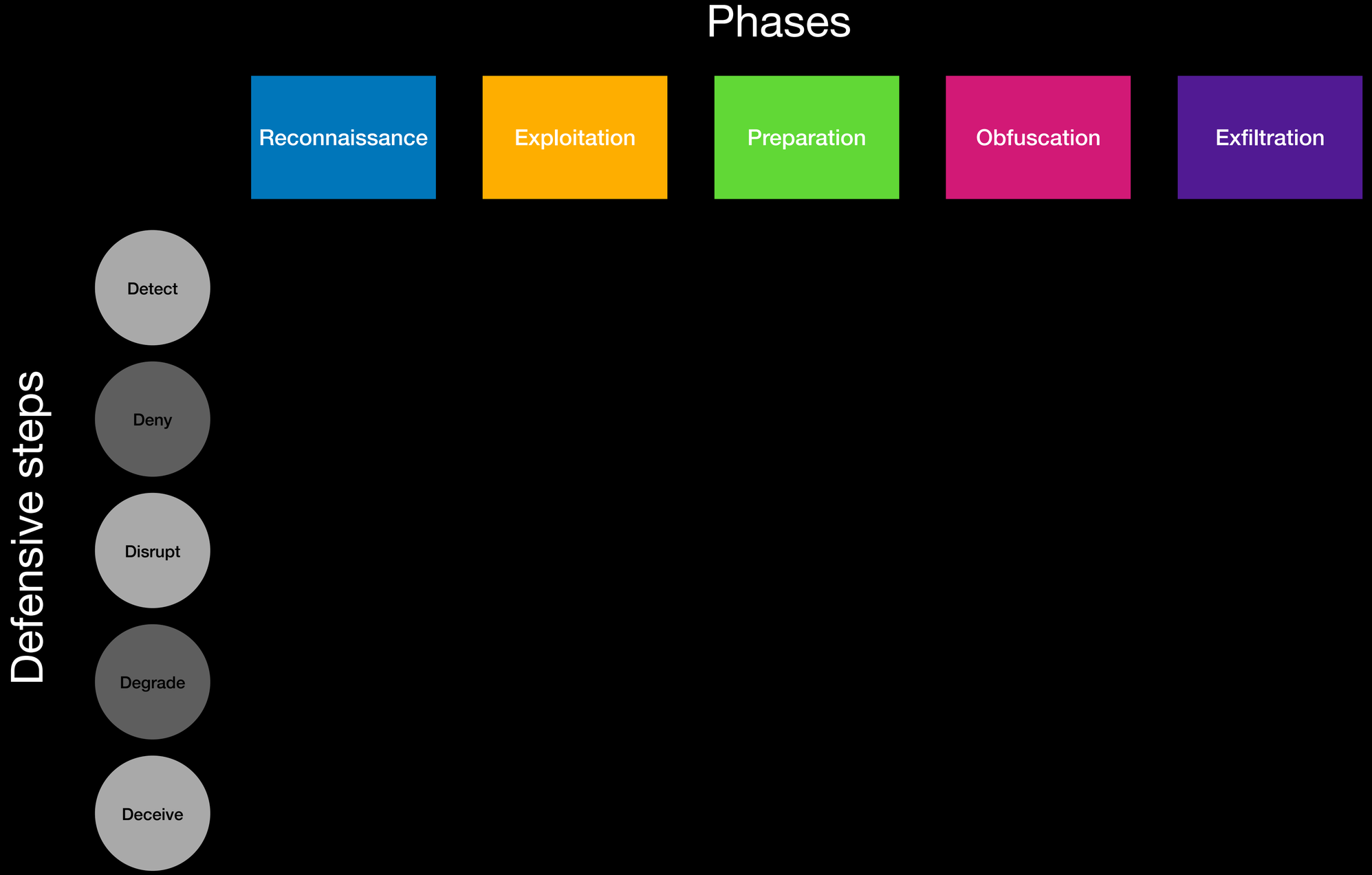


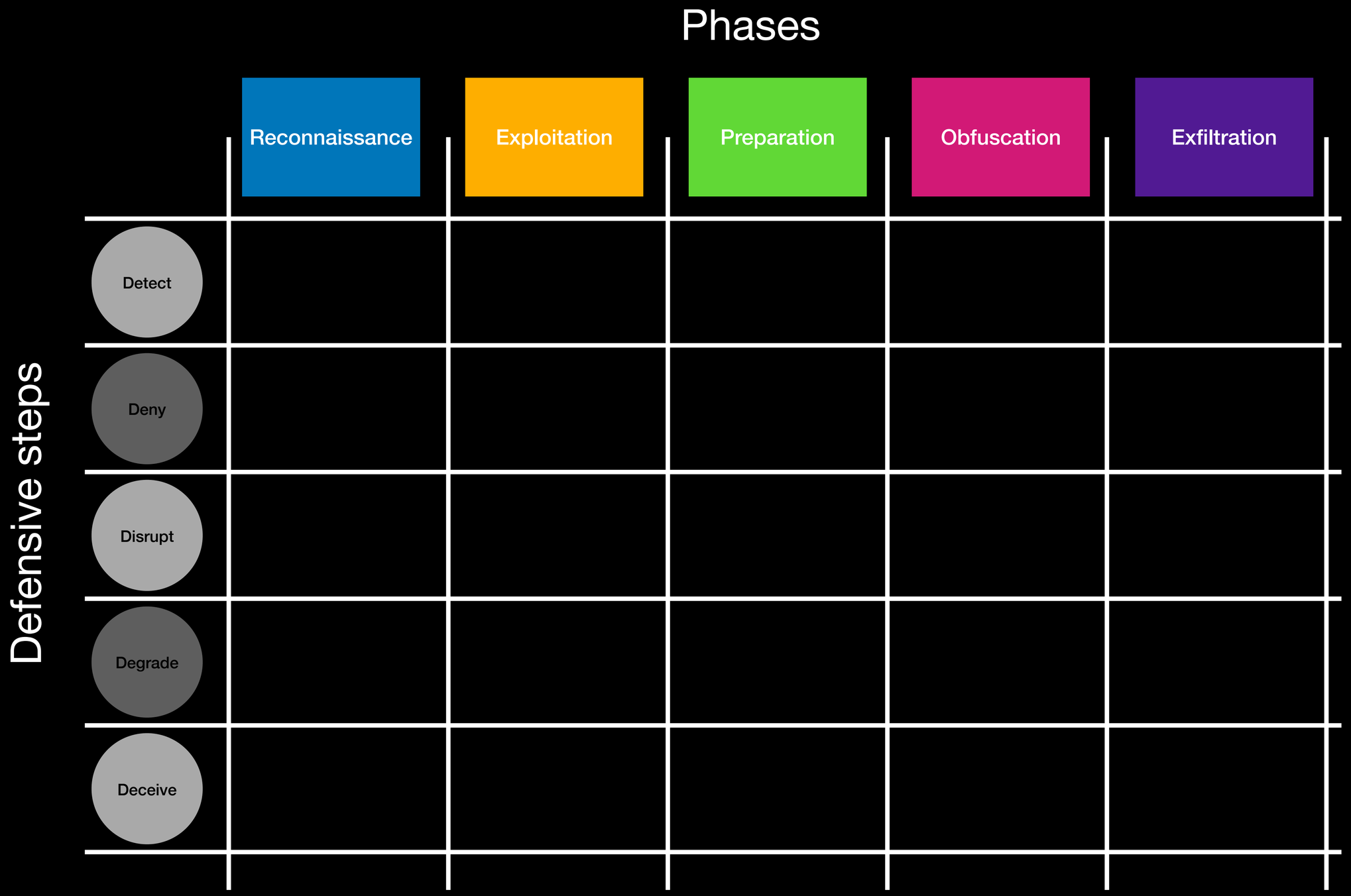
Course of Action (CoA) Matrix

Phases

Defensive steps




Phases
Reconnaissance
Exploitation
Preparation
Obfuscation
Exfiltration
Defensive steps
Detect
Deny
Disrupt
Degrade
Deceive


Phases
Reconnaissance
Exploitation
Preparation
Obfuscation
Exfiltration
Defensive steps
Detect
Deny
Disrupt
Degrade
Deceive

Cyber Kill Chains

Adversarial Behaviours

- Cyber kill chains supports organisations and individuals in formulating the **anatomy of an attack** as well as considering defences.
- Hutchins and Lockhead approach optimal at intrusion attacks and are mainly focused on external attacks. These Cyber Kill Chain models can still be used for insider attacks.
- Adapting the approach for the insider attack ensure focus is on that particularly insider attack, concern in using traditional approach is that certain aspects pertinent to insider threats are not fully appreciated.
- Focusing early on insider attacks could be wrong, if that is not the actual cause or inception of the attack.

Adapting Cyber Kill Chains for Insiders

Adversarial Behaviours