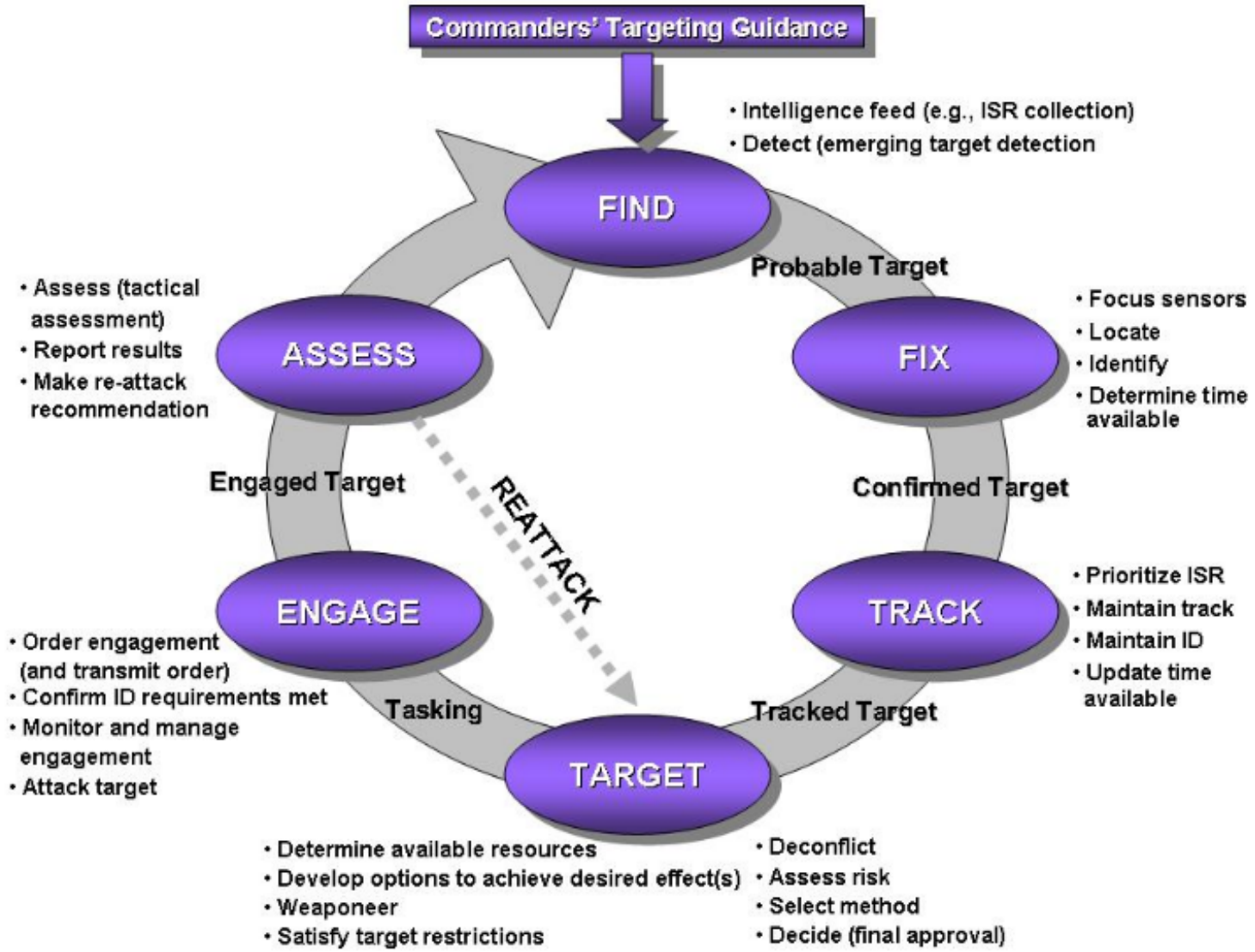
The Cyber-Killchain

Matthew Edwards

Focus: Threat Modelling

September 6, 2020

What are killchains?



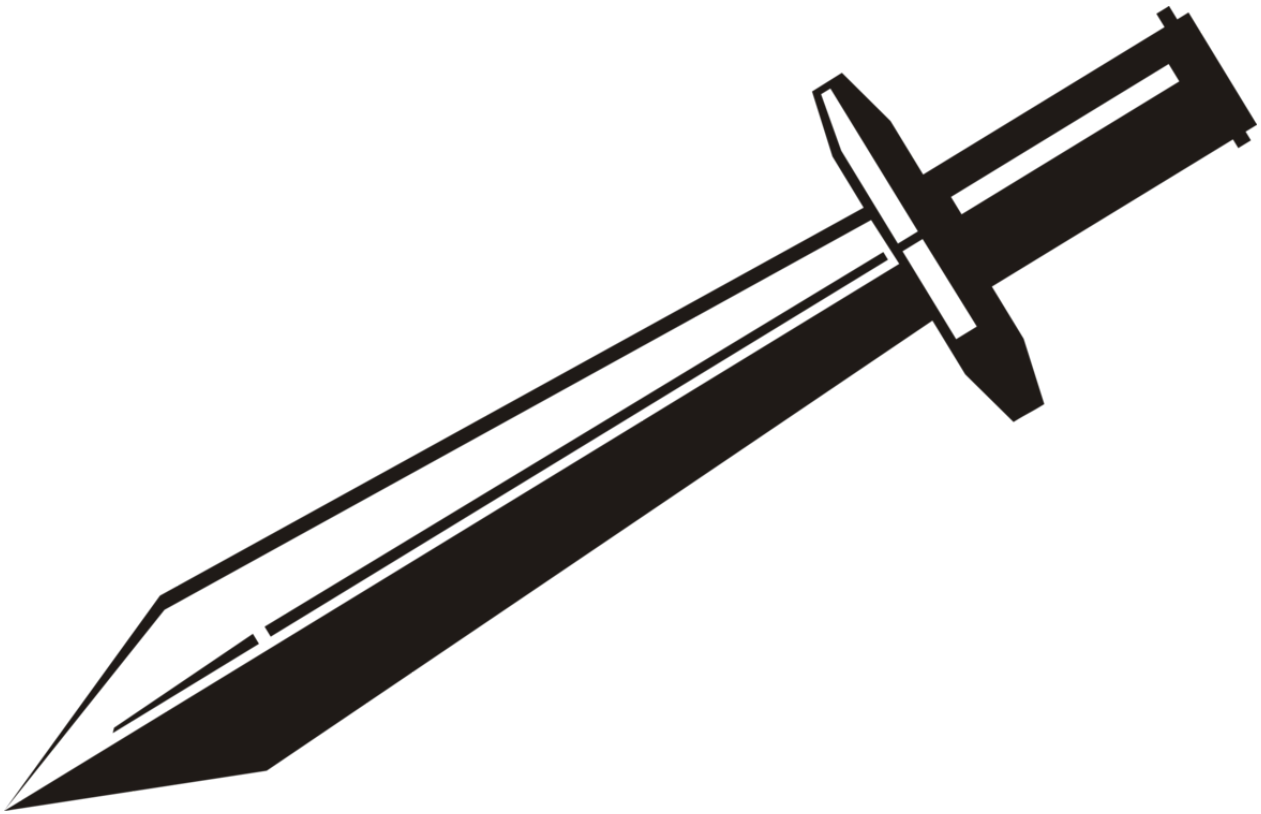
The cyber-killchain

Like F2T2EA, describes steps necessary to carrying out an attack. But unlike F2T2EA, the cyber-killchain is intended to be used by people who want to *interrupt* the chain.

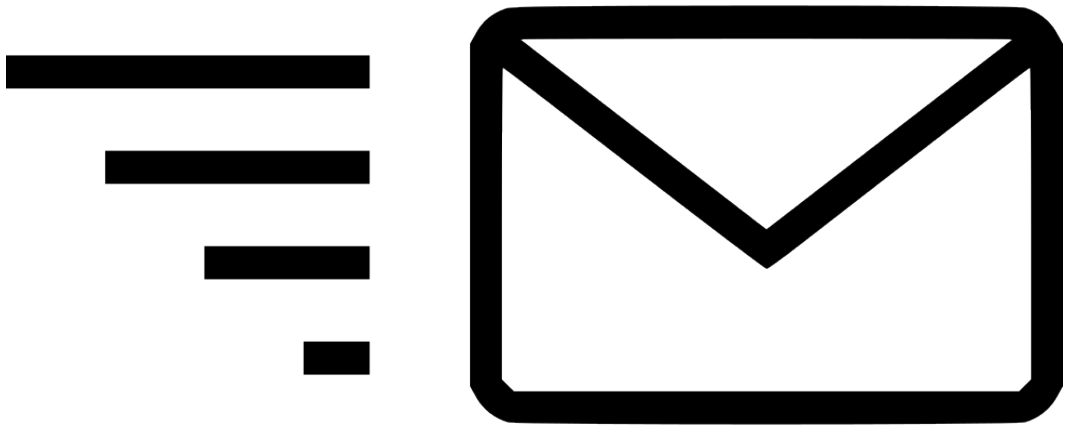
1. Reconnaissance
2. Weaponisation
3. Delivery
4. Exploitation
5. Installation
6. Command & Control
7. Actions on Objectives

Reconnaissance

Weaponisation

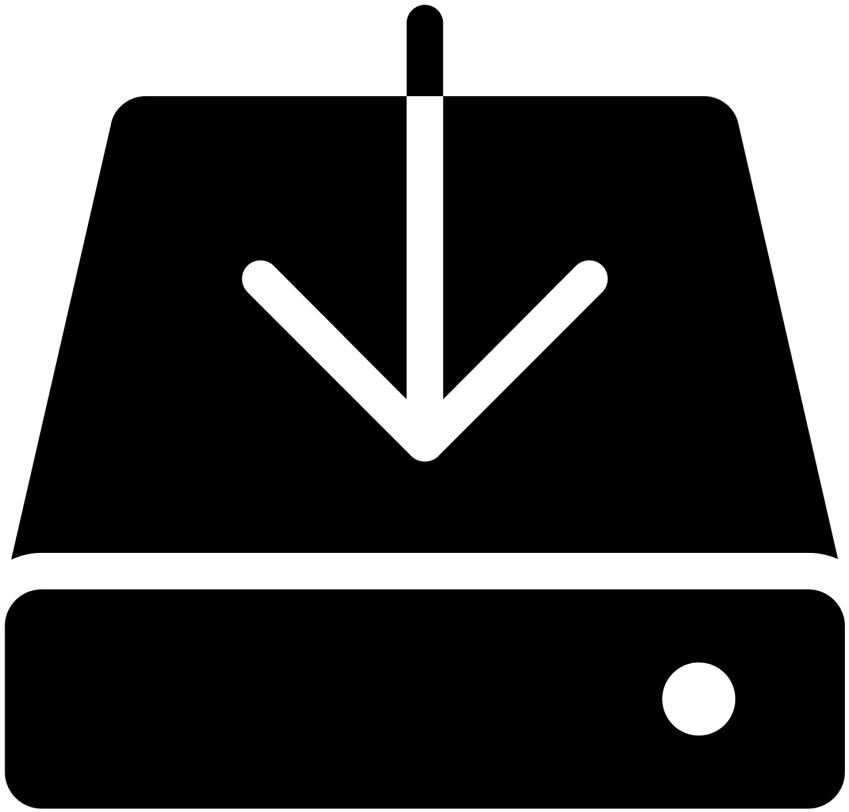


Delivery

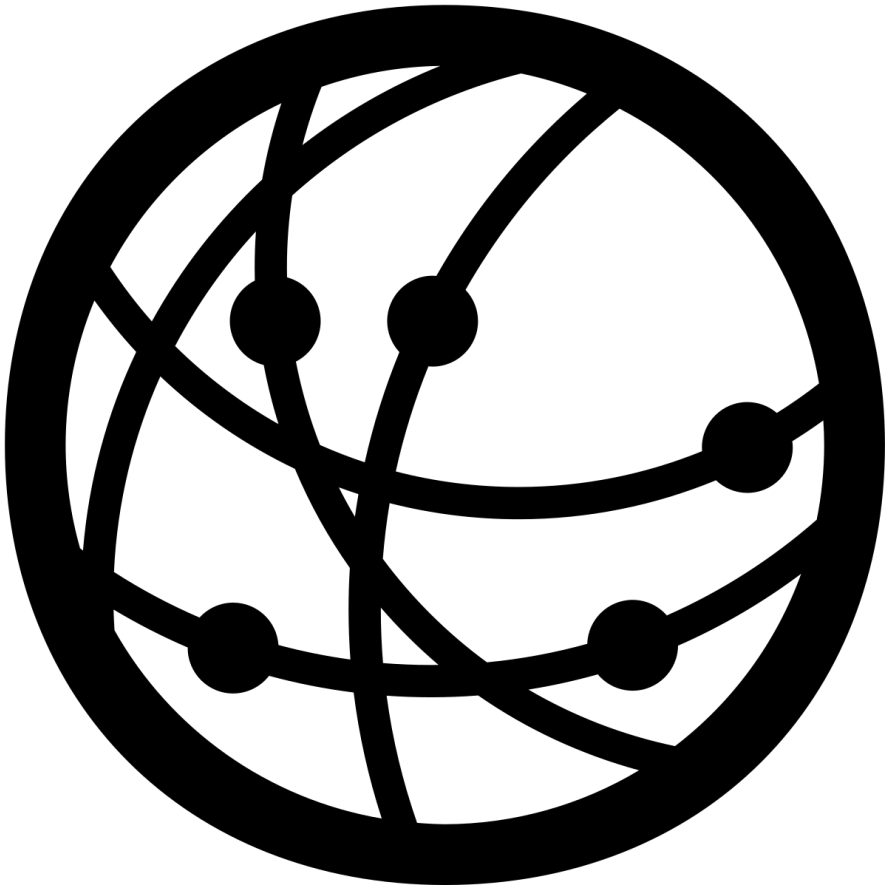


Exploitation

Installation



Command & Control



Actions on Objectives

Identifying countermeasures

For each stage of the killchain, the defender looks to create countermeasures that:

- **Detect** – identify that an attack is happening;
- **Deny** – make it impossible for the attack to proceed;
- **Disrupt** – make it more difficult for the attack to succeed;
- **Degrade** – slow down or hamper the attack;
- **Deceive** – mislead or misdirect the attacker.

Limitations of the killchain

The aim the cyber-killchain model is to help prevent an attack. It is very *situational*, but says little about:

- What came before the attack e.g., creating the attacker?
- What can we do after the attack e.g., recovery, prosecution?

The model also bakes-in some assumptions about the motives and methods of attackers.