breaking the cyber kill chain + mitre att&ck

Phases of a cyber attack

reconnaissance

01

Attackers gather information about their target

weaponisation

02

Now they create an attack that exploits vulnerabilities

delivery

03

They select their delivery method; phishing emails, infected USBs, etc.

exploitation

04

Now they execute the attack; SQL injection, buffer overflow, RCE, etc.

defence evasion: avoid detection

installation

05

The attacker gains better access; install malware, remote access, etc.

credential access: stealing usernames and passwords

discovery: gain knowledge about the system and network

lateral movement: pivot through machines to reach objective

privilege escalation: gain higher-level access

command + control

06

Attacker now sets up persistent access for remote manipulation

collection: gather information relevant to objective

persistence: maintain on-going access to systems

actions + objectives

07

With 'Hands on Keyboard' access, they achieve their goals - data exfiltration or destruction, denial of service, etc.

oryxalign