Unified Kill Chain

Originating from the **military**, a **“Kill Chain”** is a term used to explain the various **stages of an attack**

Threat modelling, in a cybersecurity context, is a series of steps to **ultimately improv**e the security of a system
Threat modelling **= thinking like an attacker** so you can **secure your systems before they get hacked.**

It has **4 basic** steps:
Identify **what you need to protect** (assets)
Identify what **can go wrong** (threats & weaknesses)
Decide which **risks matter mos**t
Fix the risks (mitigations)

Kill Chain **= early-stage attack steps.**
Unified Kill Chain **= full end-to-end attack model** (much more detailed).

Unified Kill Chain, published in **2017,** aims to **complement (not compete with) other cybersecurity kill chain frameworks**, such as Lockheed Martin’s and MITRE’s ATT&CK.

The UKC states that there are **18 phases to an attack**: Everything from reconnaissance to data exfiltration and understanding an attacker's motive

---

Phase: In (Initial Foothold)

Reconnaissance

An attacker will employ numerous **tactics to investigate the system** for potential vulnerabilities that can be exploited to gain a foothold in the system

Reconnaissance:
techniques that an adversary employs to gather information relating to their **target.The** information gathered during this phase is used all **throughout the later stages** of the UKC **(such as the initial foothold)**.

systems and services are running on the target**, contact lists or lists of employees potential credentials** that may be of use in later stages, **network topology and other networked systems** can be used to pivot too.

Weaponization

setting up the **necessary infrastructure** to perform the attack. it could be **setting up a command and control server, or a system capable of catching reverse shells** and delivering payloads to the system.

Social Engineering

adversary can manipulate employees to perform actions that will **aid in the adversaries attack.**

Exploitation

This phase of the UKC describes **how an attacker takes advantage of weaknesses or vulnerabilities present in a system**. The UKC defines "Exploitation" as abuse of vulnerabilities to perform code execution

Persistence

It is rather short and simple. Specifically, this phase of the UKC describes the techniques an adversary **uses to maintain access to a system they have gained an initial foothold on .** Creating a service on the target system that will allow the attacker to **regain access.**
 Adding the target system to a Command & Control server where commands can be executed remotely at any time.

Defence Evasion

techniques an adversary uses to evade defensive measures put in place in the system or network. more valuable phases of the UKC.

adversary made during the "Weaponization" stage of the UKC to establish communications between the adversary and target system.

An adversary can establish command and control of a target system to achieve its action on objectives.

Pivoting

To reach other **systems** within a network **that are not otherwise accessible** (for example, they are **not exposed to the internet**)there are often many systems in a network that are **not directly reachable and often contain valuable data or have weaker security.**

Persistence = how attackers **stay inside the system** after they get in.
Command & Control (C2) = how **attackers communicate with the system and control it remotely.**

Pivoting = using the **first compromised machine as a "bridge" into deeper parts of the network.**

Phase: Through (Network Propagation)

This phase follows a successful foothold being established on the target net**work.seek to gain additional access and privileges** to systems and data to fulfil thei
Pivoting

Discovery

Discovery = when an **attacker explores the hacked system to learn what is** inside the computer and the network.What users exist

What software is installed

What files and folders are there

What other computers are connected

What permissions the current user has

What services or ports are open

Privilege Escalation

try to gain more **prominent permissions within the pivot system access** to one of the following superior levels:

SYSTEM/ ROOT.
Local Administrator.
A user account with Admin-like access.
A user account with specific access or functions.

Execution

deploy their **malicious code using the pivot system as their host**. Remote trojans, C2 scripts, malicious links and scheduled tasks are deployed

---

Credential Access

would attempt to **steal account names and passwords** through various methods, including keylogging and credential dumping

Pivoting = using the **first hacked machin**e as **a bridge** or **portal to reach other machines.**
(You use it because you cannot access the internal network directly.)

Lateral Movement = actually **moving from one machine to another inside the network** using credentials or exploits.
(You log into or hack more systems.)

Phase: Out (Action on Objectives)

Collection

will be seeking to **gather all the valuable data of interest.** This, in turn, compromises the confidentiality of the data and would lead to the next attack stage

Exfiltration

To elevate their compromise, **the adversary would seek to steal data, which would be packaged using encryption measures and compression to avoid any detection.**

Impact

they would manipulate, **interrupt or destroy these assets.** The goal would be to disrupt business and operational processes and may involve removing account access,

Objectives

With all the power and access to the systems and network, **the adversary would seek to achieve their strategic goal for the attack.**

MITRE:

ATT&CK gives cybersecurity teams a **standard language** for describing attacker behavior.
MITRE = a U.S. not-for-profit organization that conducts research and development across a range of domains, including cyber security, artificial intelligence, healthcare, and space systems, all to support its mission: "to solve problems for a safer world."

The MITRE ATT&CK® framework is “a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.

- Tactic: An adversary's goal or objective. The “why” of an attack.
- Technique: How an adversary achieves their goal or objective.
- Procedure: The implementation or how the technique is executed.

While incredibly valuable from a defensive perspective, red teams also rely on the framework to plan realistic attack simulations and test organizations' defenses.With so much data available, how do organizations actually make sense of it all?

Why ATT&CK Matters

ATT&CK provides cyber security professionals and organizations with a standard and consistent language for describing adversary behavior.

probably seen the same action or technique referred to by several different names. By providing standard terminology and unique IDs, the framework makes it easier to compare data and incidents, enabling effective communication across the security community.

Obfuscating files is like putting your important data into a secret code or disguise. For example:

- The file’s content might be **encrypted, renamed, or turned into unreadable code**.

- Security tools (like antivirus or EDR) **scan files for known patterns** to detect malware.
- If the file is obfuscated, those patterns are hidden, so the tool **cannot easily recognize it as malicious**.

Threat Intelligence and Defense

MITRE ATT&CK helps defenders turn threat intelligence into actionable defense by mapping **attacker behaviors (TTPs) to detection rules, queries, and response** playbooks, effectively bridging the gap between knowing about attacks and stopping them.Threat reports tell you **what attackers did**, but not **how to detect or stop them**.

ATT&CK organizes attacker behavior into **TTPs** (Tactics, Techniques, Procedures).

Cyber Analytics Repository (CAR):

MITRE's Cyber Analytics Repository (CAR) is a collection of ready-made detection analytics created by MITRE and built on the MITRE ATT&CK adversary model.

CAR is not a database of attacks — it is a repository of detection rules that show defenders how to identify attacker behavior.

CAR provides:

Detection analytics

Detection logic

Pseudocode

Real SIEM queries (Splunk, EQL, etc.)

Mapping to ATT&CK techniques

Required logs and data sources

CAR explains what attacker behavior looks like and how to detect it. It converts ATT&CK techniques into practical, usable detections that can run automatically in your SIEM.

Example:

ATT&CK Technique: T1059.001 – PowerShell

Used by a group such as APT29

CAR analytic: Detect suspicious PowerShell command execution

Includes Splunk and EQL queries

Mapped directly to T1059.001

CAR does not provide threat group profiles. Its purpose is to give defenders high-quality detection rules for real attacker behavior based on ATT&CK.

This links the detection rule directly to attacker behavior defined in MITRE ATT&CK.his section shows **how to detect the behavior** using different formats:

- **Pseudocode**
    - A human-readable description of the detection logic
    - Not tied to any specific SIEM
- **Splunk query**
    - A real query you can paste into Splunk
- **LogPoint search**
    - A similar query for LogPoint SIEM

Not all CAR analytics include every type of implementation, but some even have **Unit Tests** so analysts can verify the rules work correctly.

MITRE D3FEND,

you discover how to stop them.:
MITRE D3FEND shows you **how to defend** against those attacks—it maps defensive techniques to ATT&CK.
ATT&CK = "What attackers do"

D3FEND = "How defenders stop them"

ATT&CK: An attacker steals credentials.

D3FEND: Credential Rotation (D3-CRO) – you regularly change passwords so stolen credentials are useless

Other MITRE Projects

, MITRE offers several other projects designed to help cyber security professionals strengthen their skills, test their defenses, and outsmart attackers