Understanding the Lockheed Martin and Unified Kill Chains in Cybersecurity

By Lucio Rodrigues

In the field of cybersecurity, understanding how attackers think and operate is critical not just for defense, but for effective offense - whether that's through red teaming, penetration testing, or threat hunting. Two frameworks stand out for mapping adversary behavior across the attack lifecycle: the **Lockheed Martin Cyber Kill Chain** and the **Unified Kill Chain**.

These models don't just enhance defensive posture, they elevate the situational awareness and threat modeling capabilities of any cybersecurity professional. This post outlines both frameworks, their stages, applications, and why every serious practitioner should master them.

🧾 Abbreviation Summary

CKC - **C**yber **K**ill **C**hain

ATT&CK - **A**dversarial **T**actics, **T**echniques & **C**ommon **K**nowledge

APT - **A**dvanced **P**ersistent **T**hreat

C2 - **C**ommand and **C**ontrol

RAT - **R**emote **A**ccess **T**rojan

IDS - **I**ntrusion **D**etection **S**ystem

EDR - **E**ndpoint **D**etection and **R**esponse

SIEM - **S**ecurity **I**nformation and **E**vent **M**anagement

TTPs - **T**actics, **T**echniques, and **P**rocedures

SMB - **S**erver **M**essage **B**lock

VLAN - **V**irtual **L**ocal **A**rea **N**etwork

DNS - **D**omain **N**ame **S**ystem

The Lockheed Martin Cyber Kill Chain

Developed by Lockheed Martin in 2011, the **CKC** offers a military-inspired, structured approach to understanding cyberattacks from a reconnaissance to data exfiltration phase. It is particularly effective for **APT** detection and mitigation.

📌 The 7 Phases

1. **Reconnaissance**
   The attacker gathers information about the target using OSINT, DNS harvesting, social engineering, and network scanning.

2. **Weaponisation**
   A tailored payload is created by coupling a **RAT** with an exploit, often using malware kits.

3. **Delivery**
   The payload is delivered via phishing emails, USB drops, drive-by downloads, or infected websites.

4. **Exploitation**
   A vulnerability is exploited in order to execute malicious code, often targeting unpatched software.

5. **Installation**
   Malware is installed, establishing persistence through techniques like registry changes, scheduled tasks, or service creation.

6. **Command and Control (C2)**
   The attacker opens a channel to remotely issue commands, usually via **HTTP/S, DNS** tunneling, or encrypted channels.

7. **Actions on Objectives**
   The adversary completes their goal → data exfiltration, data destruction, lateral movement, or system disruption.

🎯 Practical Application

As a penetration tester or red teamer, mapping your activities to the Cyber Kill Chain allows you to **emulate real-world APT behavior**. On the defensive side, each stage provides a specific opportunity for detection and response. For example:

- **IDS** alerts during Delivery.
- **EDR** logs catching privilege escalation during Exploitation.
- **C2** beaconing blocked by egress filtering in **C2** phase.

Mastering this model can guide both **attack simulation** and **defensive strategy** in SOC operations, threat hunting, and detection engineering.

The Unified Kill Chain

Introduced by Paul Pols in 2017, the **Unified Kill Chain** merges the Lockheed Martin CKC with MITRE ATT&CK tactics and other models. It addresses some of the CKC's limitations by extending the scope of detection and attribution across **three phases** and **18 attack nodes**.

🧠 Why It Was Needed

The Lockheed Martin model was limited primarily to perimeter-focused defense and lacked visibility into **post-compromise behavior**, such as internal recon or lateral movement. The Unified Kill Chain resolves this by offering a **comprehensive, end-to-end attack mapping**.

📚 The 3 Meta-Phases

1. Initial Foothold

- Reconnaissance
- Weaponisation
- Delivery
- Exploitation
- Installation
- Command & Control
- Internal Reconnaissance

2. Persistence and Lateral Movement

- Privilege Escalation
- Credential Access
- Lateral Movement
- Remote Access Enablement

3. Actions on Objectives

- Collection
- Exfiltration
- Impact (e.g., destruction, defacement)
- Defense Evasion
- Obfuscation
- Anti-Forensics

🛠️ Offensive Security Use Cases

In red team exercises, this model allows for **more realistic simulations** that align with adversary **TTPs** beyond just initial access. As a pentester, using this model supports:

- Identifying post-exploitation paths (like lateral movement to domain controllers).
- Prioritising privilege escalation opportunities.
- Planning persistence mechanisms and evasion strategies.

For threat hunters and blue teamers, it helps break down complex breaches into **actionable detection points**, aligning well with SIEM and EDR alert correlation.

Comparative Summary

Feature	**Lockheed Martin CKC**	**Unified Kill Chain**
Focus	Perimeter & Early Intrusion	Full Kill Chain Lifecycle
Structure	7 Linear Phases	3 Meta-Phases, 18 Nodes
Integration	Legacy SIEM, IDS	Compatible with MITRE ATT&CK
Use Cases	APT Detection, Defense Planning	Threat Hunting, Red/Blue Team Ops

---

🧠 Personal Reflections and Implementation

During red team labs and C2 tool development, I've often structured my operations around the **Unified Kill Chain**, especially when simulating **post-exploitation actions** like lateral movement or privilege escalation.

When automating scans or building internal recon scripts, it's critical to understand where in the chain your tool fits. Does it support the attacker in **gaining a foothold**, **maintaining access**, or **completing their mission**?

Understanding these frameworks not only improves my ability to simulate realistic attack paths, but also **enhances my defensive mindset**, allowing me to think one step ahead of attackers and design more intelligent detection logic.

Final Thoughts

Whether you're defending critical infrastructure or testing its resilience, the Cyber Kill Chain and Unified Kill Chain offer invaluable insights. They help **bridge the gap between offensive and defensive security**, enabling you to predict, detect, and prevent adversary activity with precision.

In my journey toward becoming a cybersecurity analyst and red teamer, these frameworks serve as **foundational blueprints** for mapping real-world attacks, creating smarter tools, and articulating technical findings to stakeholders and employers.