CS-007 · Foundations

The Cyber Kill Chain

The stages of an intrusion, and how breaking any one stage can stop the whole attack.

Executive Summary

The cyber kill chain is a model that breaks a targeted intrusion into ordered stages, from early reconnaissance to the attacker's final objective. Its defensive value is that disrupting any single stage can stop the entire attack. It gives teams a structured way to think about detection and prevention across the whole intrusion, not just the moment of breach.

What It Is

The cyber kill chain, originally described by Lockheed Martin, models a targeted attack as a sequence of steps an adversary must complete to succeed. The commonly cited stages are reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives. The key insight is that an attacker has to move through these stages in order, so a defender who detects and disrupts the chain at any point can prevent the attacker from reaching the goal. It reframes defense from a single wall to a series of opportunities to intervene.

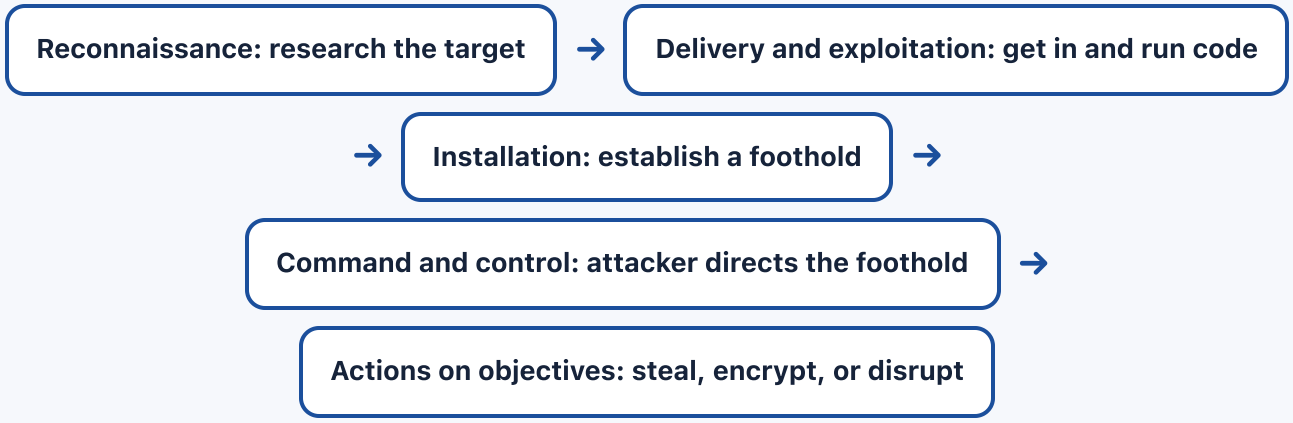
Why It Matters

Thinking in stages helps teams spread their defenses across the whole intrusion rather than concentrating only on prevention at the perimeter. It shows that even if early stages are missed, later stages such as command and control or data exfiltration offer more chances to detect and respond. It also helps analysts communicate where in an attack an incident was caught and what an attacker still needed to do. For professionals, the kill chain is a common interview topic and a mental model used constantly in security operations and incident response.

How It Works

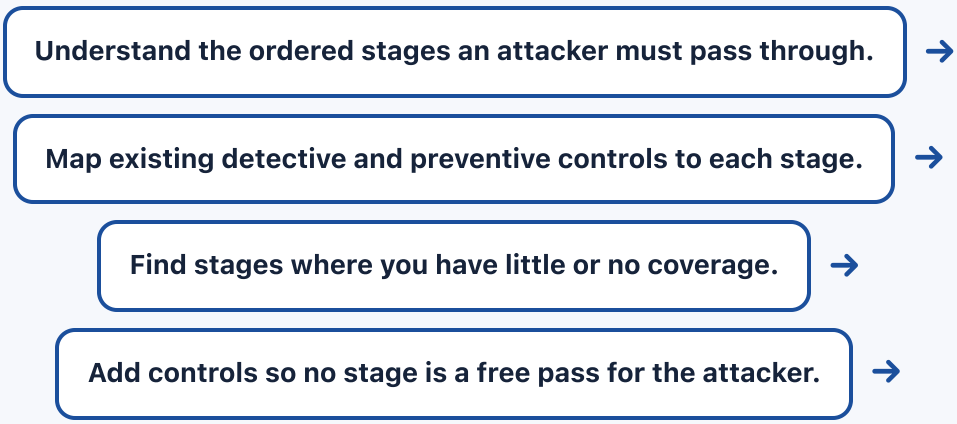
Defenders map their detective and preventive controls to each stage of the chain. Reconnaissance might be countered by reducing public exposure. Delivery is targeted by email filtering and web protection. Exploitation is reduced by patching and hardening. Installation and command and control are caught by endpoint detection and network monitoring. Actions on objectives, such as data theft, are limited by segmentation, access control, and egress monitoring. Analysts also use the chain in reverse during investigation, working backward from what they observed to understand how far the attacker progressed. The model pairs well with MITRE ATT&CK, which describes the specific techniques used within these stages.

Architecture Diagram



An intrusion moves through ordered stages, and a defender can break the attack by disrupting any single stage.

Visual Workflow



During an incident, place observed activity on the chain to gauge progress. →

Use the position in the chain to guide containment and response priorities.

Common Attacks

- Phishing used for the delivery stage of an intrusion
- Exploitation of unpatched software to gain code execution
- Malware installation to establish a persistent foothold
- Command and control traffic used to direct compromised systems
- Data exfiltration or ransomware at the actions on objectives stage

Common Mistakes

- Focusing all defense on prevention at the earliest stages only
- Assuming a missed early stage means the attack cannot be stopped
- Having no detection for command and control or exfiltration
- Treating the model as rigid when real attacks can skip or reorder steps
- Using the chain to describe attacks but never mapping controls to it

Best Practices

- Distribute detection and prevention across every stage of the chain
- Invest in later-stage detection so early misses are not fatal
- Monitor for command and control and unusual outbound traffic
- Use segmentation and egress controls to limit actions on objectives
- Combine the kill chain with MITRE ATT&CK for technique-level detail
- Use the chain in investigations to measure how far an attacker got

Quick Checklist

- [ ] Controls mapped to each kill chain stage with gaps identified

- [x] Email and web defenses covering the delivery stage
- [x] Patching and hardening reducing exploitation
- [x] Endpoint detection covering installation and foothold
- [x] Network monitoring for command and control traffic
- [x] Egress and data controls limiting exfiltration

Recommended Tools

Email and web security gateways
Disrupt the delivery stage of intrusions

Endpoint Detection and Response (EDR)
Catches installation and post-exploitation activity

Network detection and monitoring
Surfaces command and control and exfiltration

SIEM
Correlates activity across stages into a coherent picture

Industry Standards

MITRE ATT&CK
Technique-level detail that complements the kill chain stages

NIST SP 800-61
Incident handling guidance that uses staged thinking

NIST Cybersecurity Framework (CSF) 2.0
Detect and Respond functions align with breaking the chain

Career Relevance

The cyber kill chain is core knowledge for SOC analysts, incident responders, threat hunters, and red teamers, who use it to structure detection and investigation. GRC analysts and risk

professionals use it to reason about where controls sit in an attack. It is a frequent interview question and a shared vocabulary across defensive and offensive roles.

Interview Questions

- What are the stages of the cyber kill chain?
- Why does breaking a single stage stop the whole attack?
- Which stages are often missed, and how would you add coverage?
- How do the kill chain and MITRE ATT&CK relate to each other?
- How would you use the kill chain during an active investigation?

Related Certifications

CompTIA Security+ | **GIAC Certified Incident Handler (GCIH)** | **CompTIA CySA+**

Further Reading

- MITRE ATT&CK
- NIST SP 800-61 Incident Handling
- CISA: Cybersecurity Best Practices

Key Takeaways

- The kill chain models an intrusion as ordered stages an attacker must complete.
- Disrupting any single stage can stop the entire attack.
- Later-stage detection matters because early stages are often missed.
- It reframes defense as many chances to intervene, not one wall.
- It pairs well with MITRE ATT&CK for technique-level detail.

FAQ

▶ **Is the kill chain the same as MITRE ATT&CK?**

▶ **Do real attacks always follow the kill chain in order?**

▶ **Why focus on later stages if I can stop attacks early?**

Related Careers

RELATED ROLES

Soc Analyst | Incident Responder | Penetration Tester

RELATED CERTIFICATIONS

CompTIA Security+ | GIAC Certified Incident Handler (GCIH) | CompTIA CySA+

CURRENT OPENINGS

Live roles are on the job board.

Browse all jobs

GUIDES & SALARY

Career guides | Role roadmaps | Salary data | Career tools

SUGGESTED LEARNING PATH

1. Ground the basics with CS-001 Cybersecurity
2. Study this sheet: **The Cyber Kill Chain**
3. Go deeper: Cybersecurity
4. Go deeper: Threat Actors
5. Validate it: work toward **CompTIA Security+**
6. Find the role: browse current openings

RELATED SHEETS

CS-001 Cybersecurity | CS-006 Threat Actors | CS-008 MITRE ATT&CK | CS-005 Attack Surface | CS-003 Defense in Depth