UNIFIED KILL CHAIN

Un approccio integrato alla modellazione delle minacce

Genesi della modellazione

Dalla dottrina militare alla Cyber Kill Chain

~2000s

Dottrina Militare: F2T2EA

Find, Fix, Track, Target, Engage, Assess

2011

Lockheed Martin CKC

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

2017

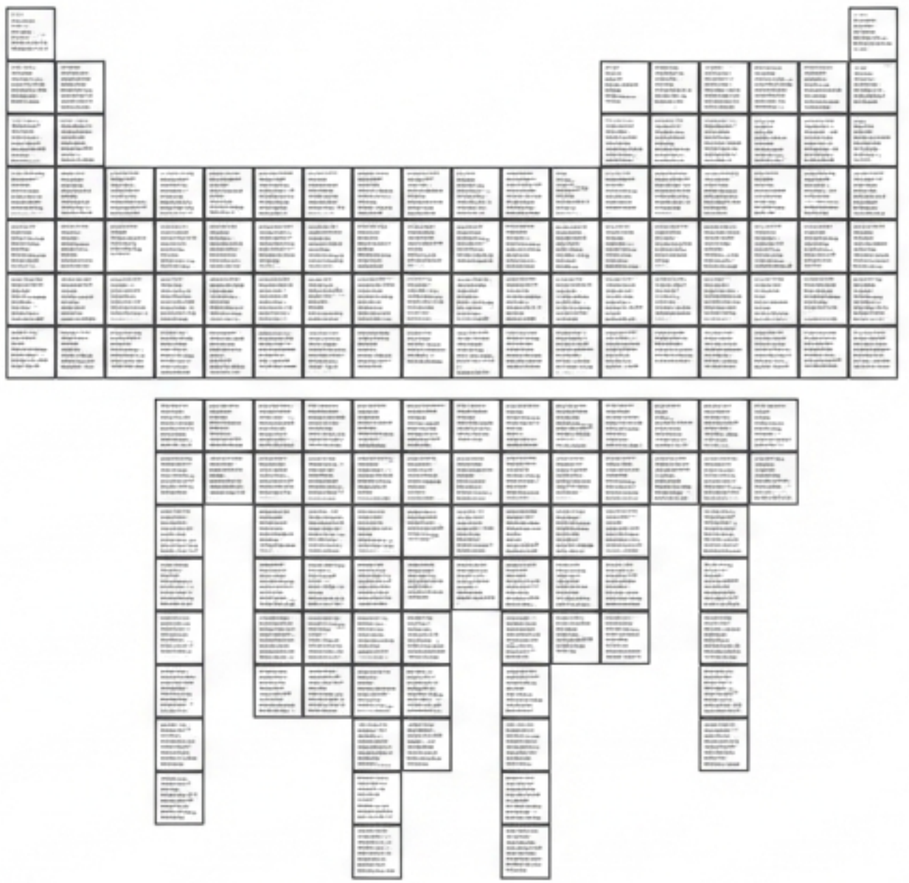
Unified Kill Chain

I limiti del modello tradizionale (CKC)

- **Focus Perimetrale:** Inefficace contro minacce interne.
- **Linearità Rigida:** Presuppone una sequenza deterministica.

- **Malware-Centrico:** Ignora attacchi fileless o basati su credenziali.

L’Antitesi: Il framework MITRE ATT&CK



Profondità Tattica (Time-Agnostic)

- **Approccio Comportamentale:** Inventario esaustivo di Tattiche e Tecniche (TTPs).
- **Granularità:** Dettaglio tecnico estremo.
- **Limite Strutturale:** Manca di un flusso strategico ordinato (Il ‘Quando’).

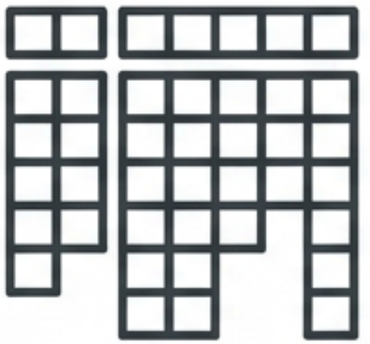
CKC (Strategia)

MITRE (Tattica)

La Sintesi: Unified Kill Chain (UKC)

Lockheed Martin CKC

+



MITRE ATT&CK

=

Unified Kill Chain

Unificazione

Unisce la visione strategica della CKC con la profondità tattica del MITRE.

Assume Breach

Sposta il focus dalla prevenzione perimetrale alla resilienza interna.

Copertura Totale

18 fasi, dalla ricognizione all’impatto finale.

Anatomia del Framework

Fase I: IN – Accesso Iniziale

Fase I: IN – Accesso Iniziale

- **Obiettivo:** Superare il perimetro.
- **Innovazione Chiave:** Inclusione esplicita di ‘Social Engineering’.
- **Nota:** Espansione del concetto di ‘Weaponization’ in ‘Resource Development’.

Fase II: THROUGH – Propagazione

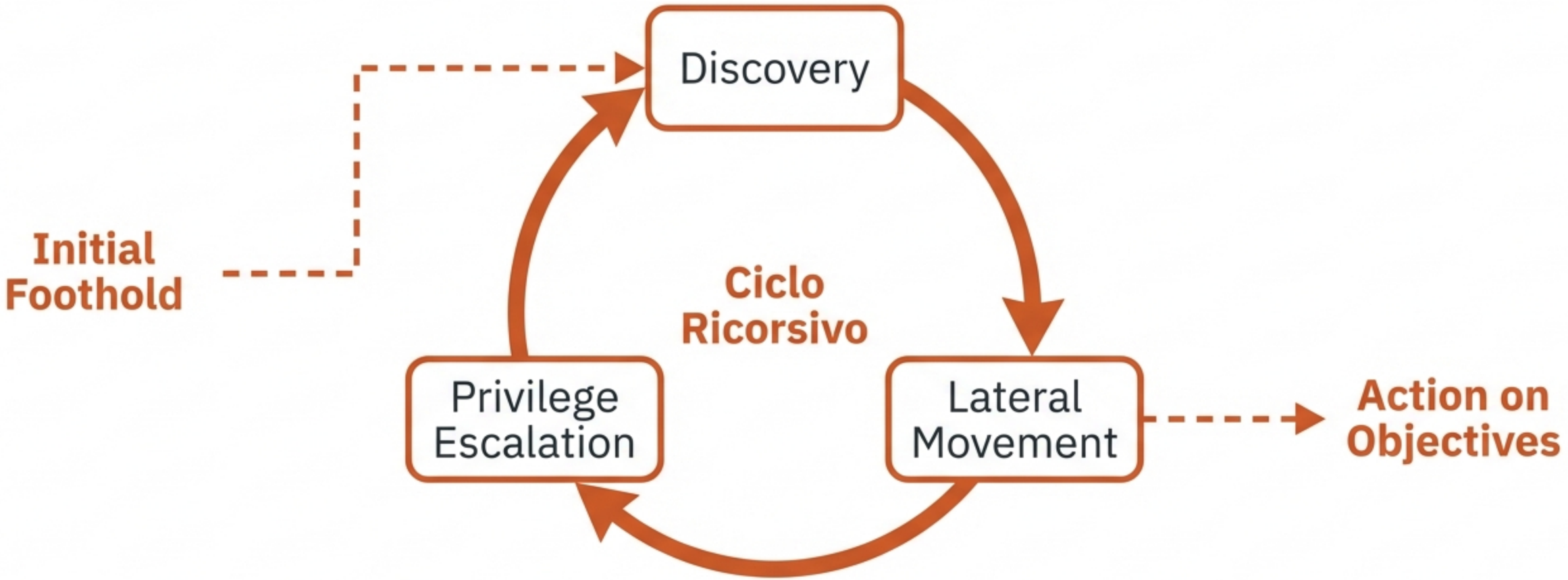
Obiettivo: Navigazione interna ed espansione del controllo.

- **Il “Missing Link”:** Questa fase colma il vuoto tra l’ingresso e l’obiettivo finale.
- **Concetto Chiave:** Pivoting (Tunneling attraverso sistemi controllati).

Fase III: OUT – Azione sugli Obiettivi

- **Obiettivo:** Finalizzare l'attacco (CIA Triad).
- **Evoluzione:** Oltre il furto di dati (Exfiltration).
- **Impact**: Include sabotaggio, distruzione dati e Ransomware.

Dinamiche: Non-Linearità e Ciclicità

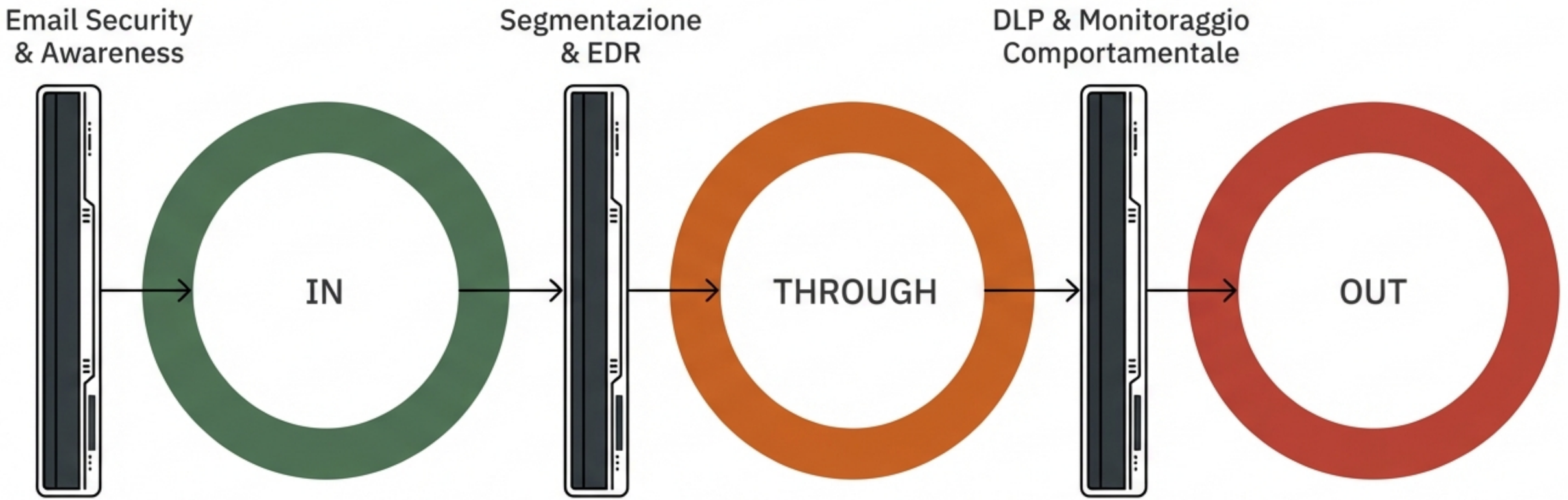


Le fasi non sono rigide. Gli attaccanti ciclano attraverso le fasi fasi “Through” finché non raggiungono l’asset target.

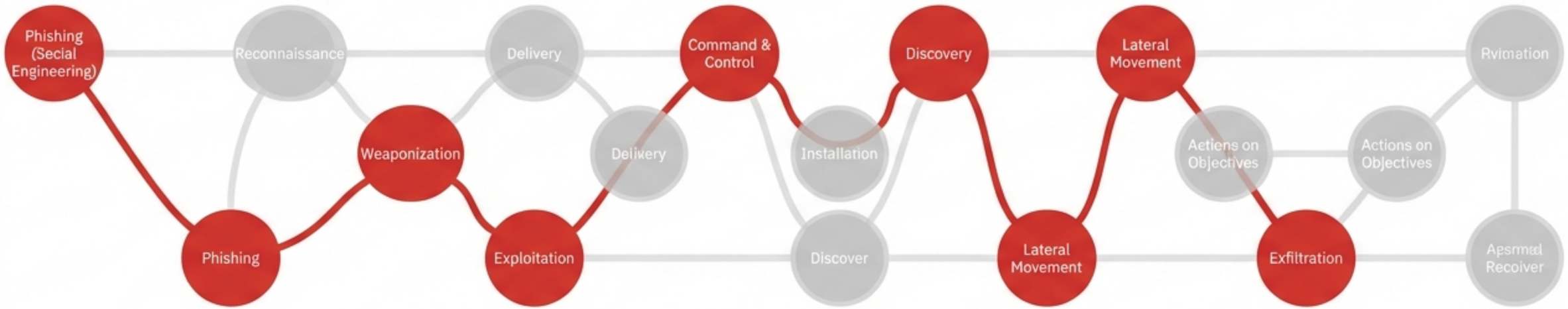
Analisi Comparativa dei Framework

	Cyber Kill Chain®	MITRE ATT&CK™	Unified Kill Chain
Social Engineering	✗	✗	✓
Exploitation	✓	✗	✓
Pivoting	✗	✗	✓
Lateral Movement	✗	✓	✓
Objectives	✓	✗	✓

Applicazione Difensiva: Gap Analysis

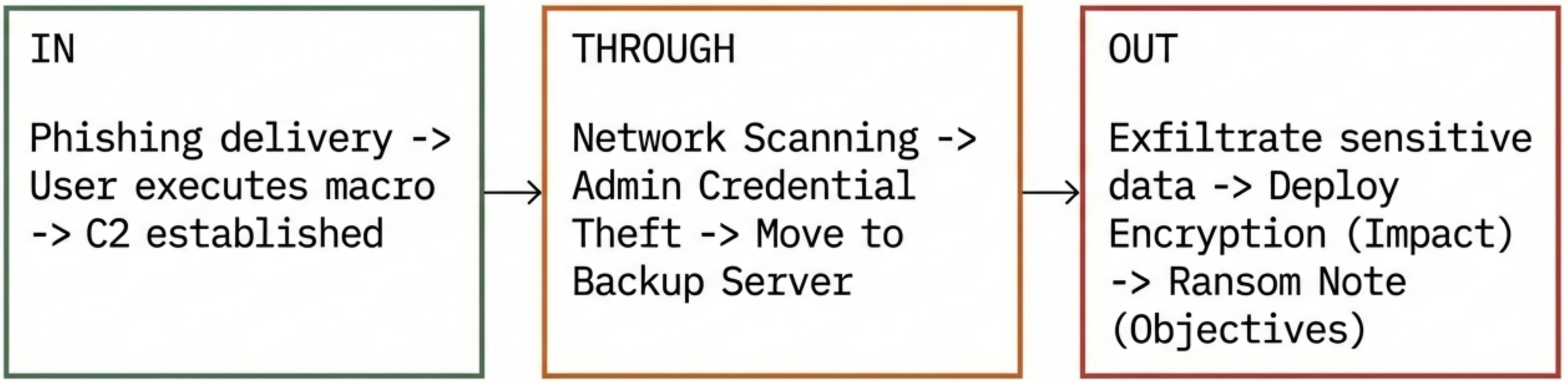


Applicazione Offensiva: Simulazione



Modellazione APT: Simulare percorsi reali, non solo vulnerabilità isolate

Case Study: Ransomware



Il percorso tipico di un attacco a doppia estorsione.

Conclusione: Verso la Resilienza

Dal Perimetro alla Profondità
Unificazione di Strategia e Tattica
Modellazione Olistica delle Minacce