La Cyber Kill Chain

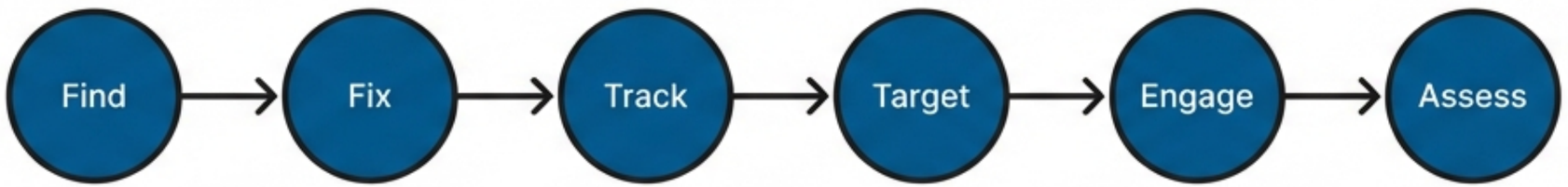
Analisi del Framework e Applicazioni Difensive

Vincenzo Calabrò

Genesi e Definizione

Dal Dominio Cinetico a Quello Digitale

DOTTRINA MILITARE (CINETICO)



Concetto Chiave:
Gli avversari devono completare tutti gli stadi per avere successo; ai difensori basta interromperne uno solo per spezzare la catena.

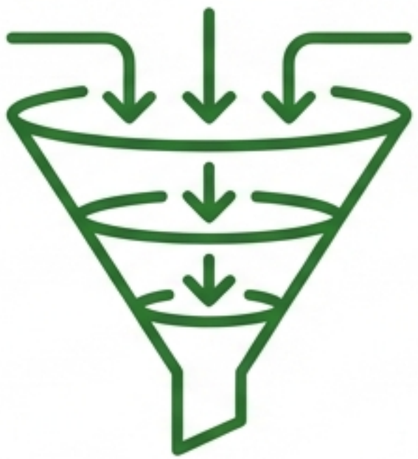
CYBER KILL CHAIN (DIGITALE)

Il Valore Strategico del Modello

Visibilità

Permette di mappare le TTPs (Tactics, Techniques, and Procedures) dell'avversario in modo strutturato.

Prioritizzazione



Alloca le risorse difensive dove hanno il massimo impatto. Bloccare la 'Delivery' è più efficace che mitigare l' 'Exploitation'.

Resilienza

Sposta il focus dalla prevenzione totale alla rilevazione precoce. Riduzione del Time-to-Detect vs. Time-to-Compromise.

Fasi Preliminari (Pre-Intrusion)

L'attacco avviene fuori dal perimetro difensivo

1. Ricognizione

Identificazione dei target, harvesting di email, analisi OSINT.

`Scanning porte, LinkedIn scraping.`

2. Armamento

Creazione del payload. Accoppiamento di un RAT con un exploit.

`PDF malevolo con script embedded.`

3. Consegna

Trasmissione dell'arma al target.

`Email di Phishing, Drive-by download.`

Intrusione e Persistenza

L'attacco entra nel perimetro

4. Sfruttamento

Esecuzione del codice malevolo sfruttando una vulnerabilità.

`Buffer overflow, Macro execution`

5. Installazione

L'avversario installa una backdoor per mantenere l'accesso.

`Registry key persistence, Webshell`

6. Comando e Controllo

Canale di comunicazione verso l'esterno per ricevere istruzioni.

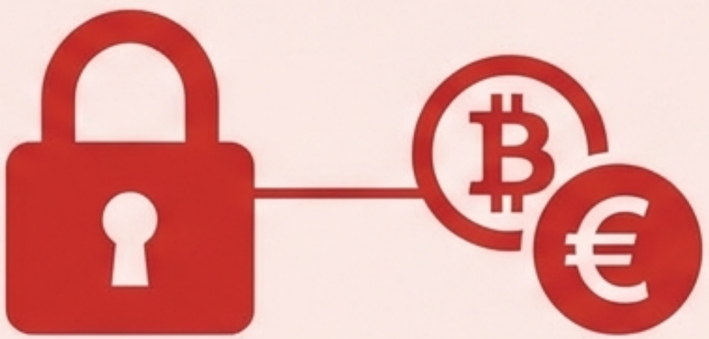
`DNS Tunneling, Traffico HTTPS cifrato`

Impatto e Obiettivi

7. Azioni sugli Obiettivi

Il compimento della missione: esfiltrazione, distruzione, manipolazione.

8. Monetizzazione (Modern Add-on)

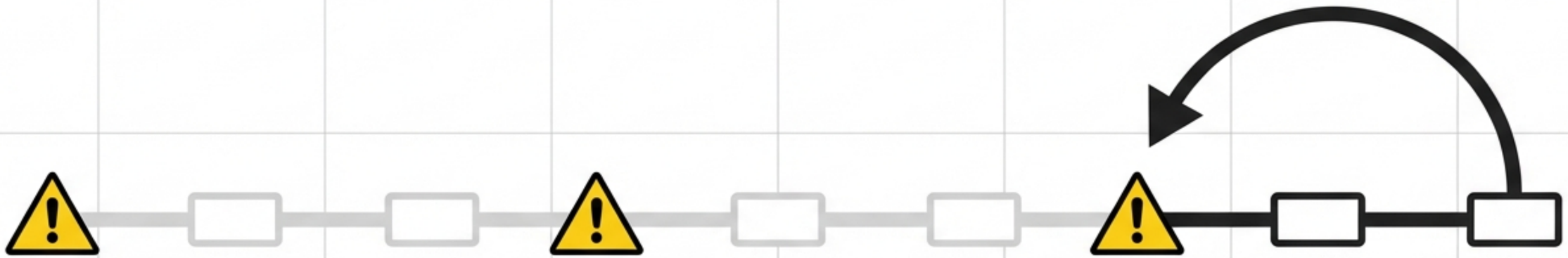


Conversione dell'accesso in profitto. Critico nel panorama Ransomware-as-a-Service (RaaS) del 2026.

La Matrice Difensiva: Mapping dei Controlli

	Rilevare	Negare	Interrompere	Degradare	Ingannare	Contenere
Ricognizione	--	--	--	--	--	--
Armamento	--	--	--	--	--	--
Consegna	--	Email Gateway / Antispam	--	--	--	--
Sfruttamento	--	--	Endpoint Protection / Patching	--	--	--
Installazione	--	--	--	--	--	--
C2	NIDS / DNS Analysis	--	--	--	--	--
Azioni	--	--	--	--	--	Network Segmentation / DLP

Analisi Critica: I Limiti del Modello Classico



Bias Perimetrale

Inter Regular
Assume distinzione “interno/esterno”. Obsoleto con Cloud e Zero Trust.

Minacce Interne

Inter Regular
L’insider o le credenziali compromesse saltano le fasi preliminari.

Linearità

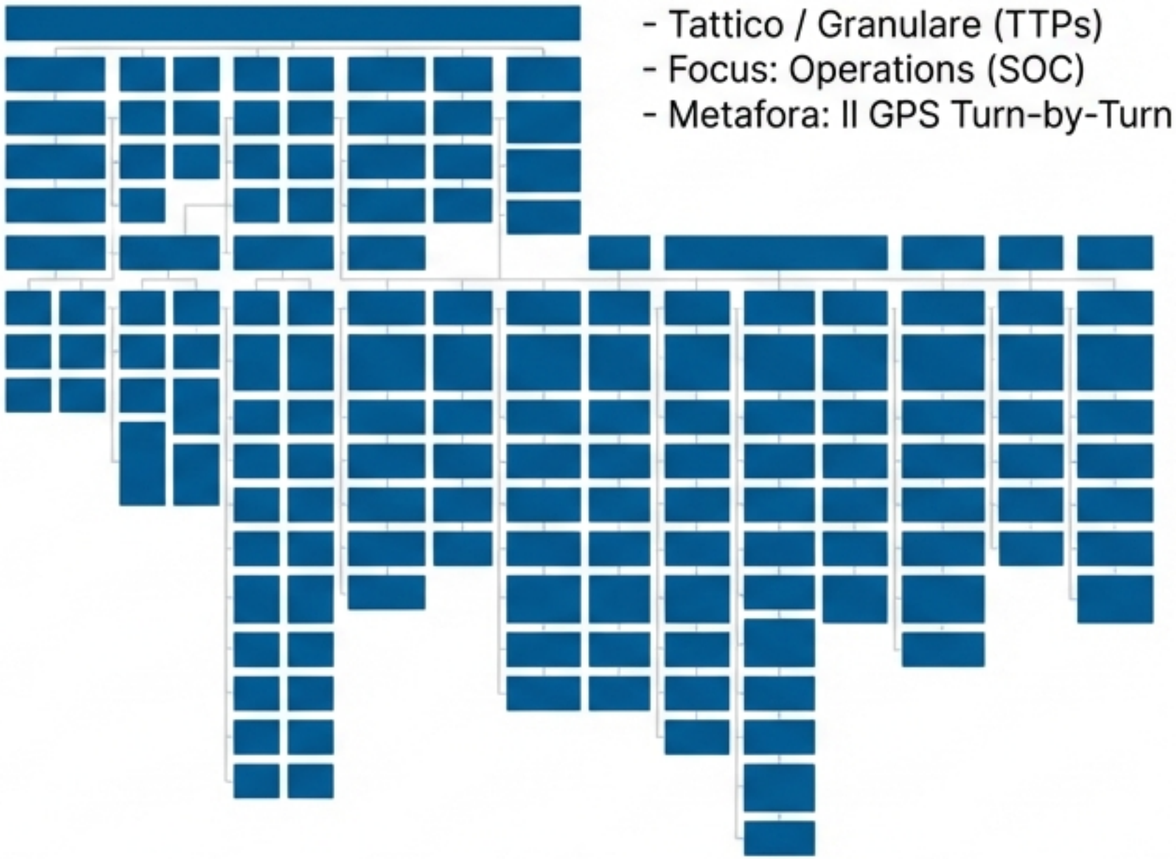
Inter Regular
Gli attacchi moderni sono ciclici, non lineari.

Framework a Confronto: CKC vs. MITRE ATT&CK

Cyber Kill Chain

- Strategico / Alto Livello
- Focus: Management
- Metafora: La Mappa Stradale

MITRE ATT&CK

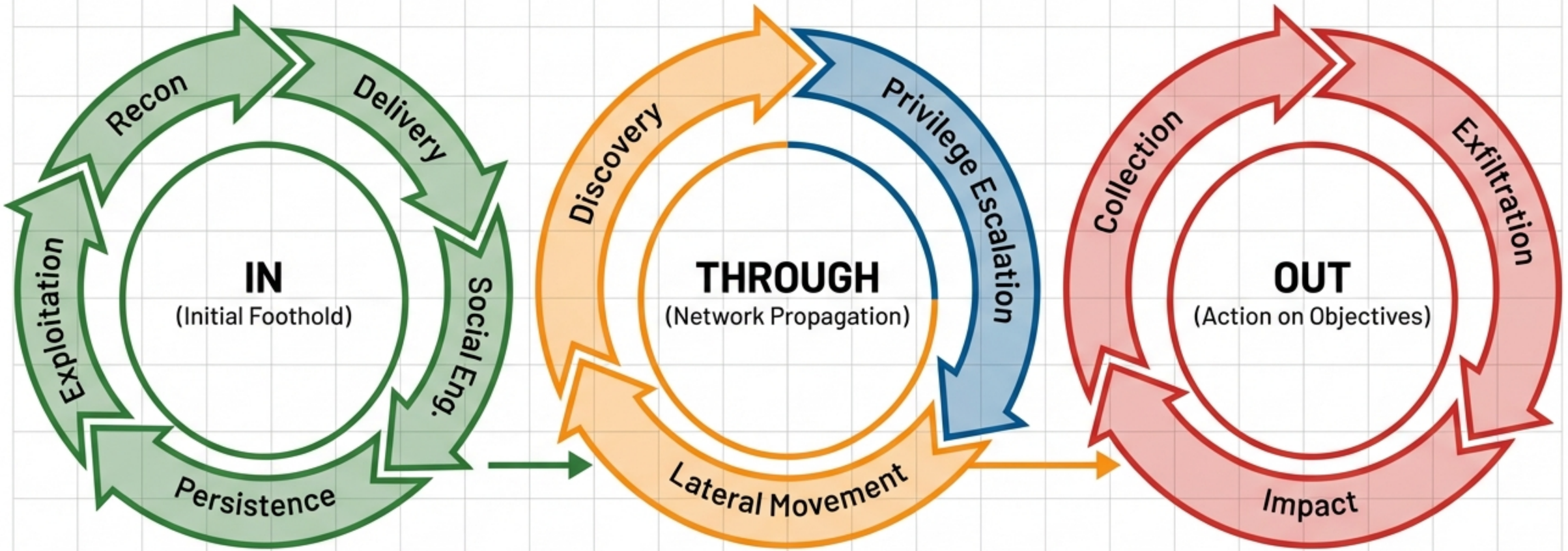


- Tattico / Granulare (TTPs)
- Focus: Operations (SOC)
- Metafora: Il GPS Turn-by-Turn

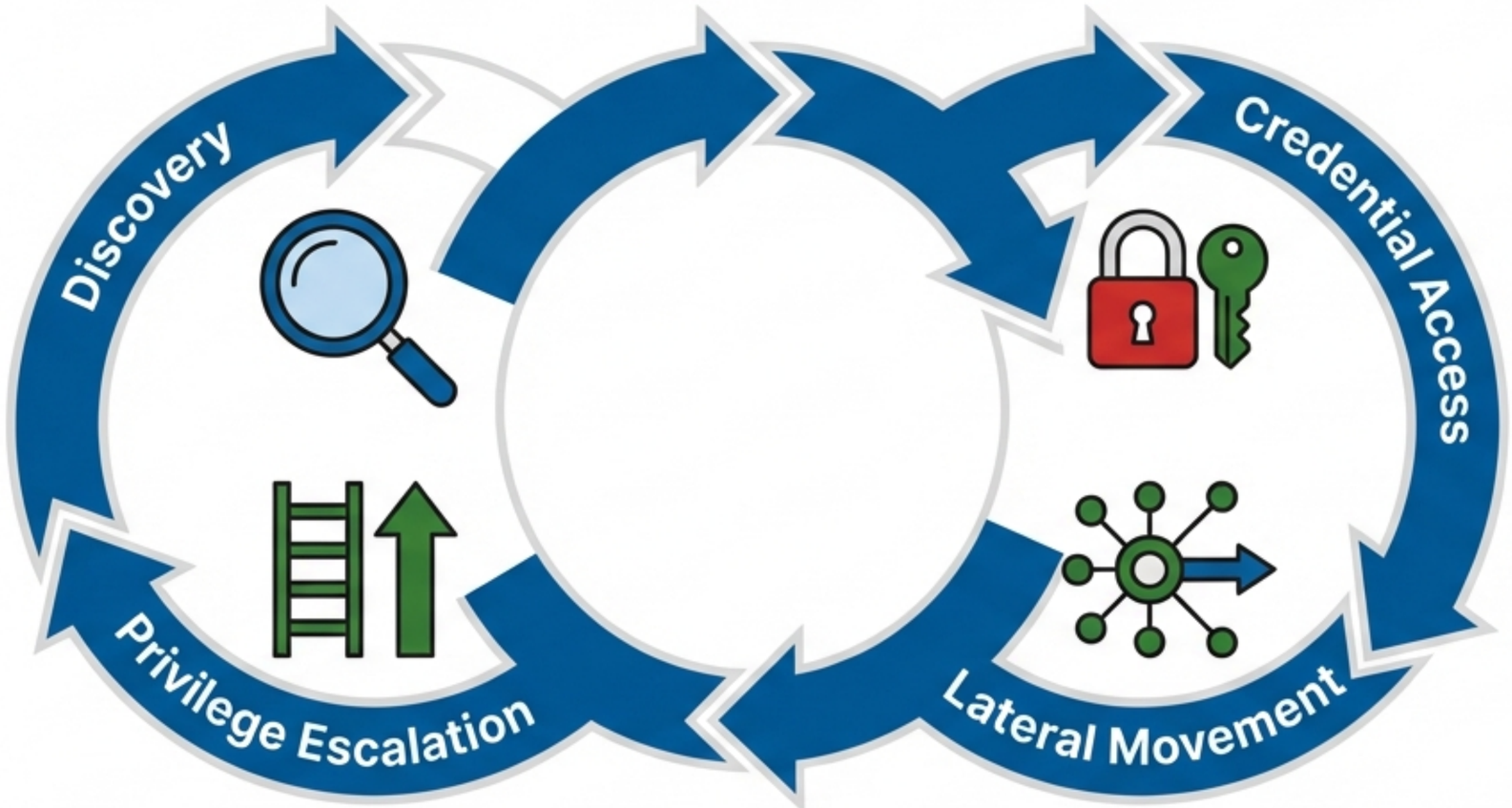
Non mutualmente esclusivi, ma complementari.

L’Evoluzione: La Unified Kill Chain (UKC)

Fonte: Paul Pols (2017)



Il Movimento Laterale e la Propagazione

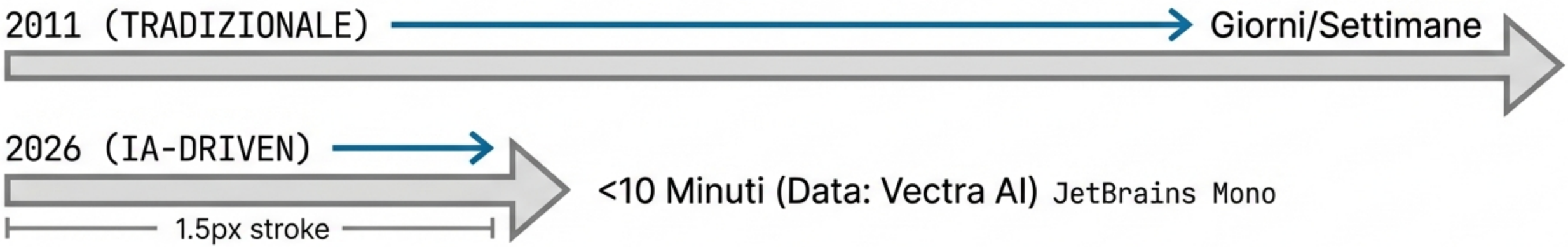


- **Credential Access**: Furto di password (es. Mimikatz).
- **Discovery**: Mappatura della rete interna.
- **Lateral Movement**: Spostamento verso asset critici (Crown Jewels).
- **Privilege Escalation**: Da User ad Admin.

Note: Opportunità chiave per rilevamento basato sul comportamento (UEBA).

Il Fattore Tempo: La Kill Chain nell'Era dell'IA (2026)

FAST FORWARD TIMELINE JetBrains Mono



PROMPTWARE KILL CHAIN JetBrains Mono

Velocità attacco > Reazione umana.
Necessità di difesa automatizzata (AI vs AI).

Caso Studio: Ransomware Moderno (RaaS)

Specializzazione: Un gruppo ottiene l’accesso, un altro monetizza.

Conclusioni: Verso la Resilienza Cybernetica

***Assume Breach:**
Operare assumendo che la violazione sia già avvenuta.

***Defense in Depth:**
Controlli ridondanti su ogni fase.

Intelligence Integrata:
CKC (Strategia) + MITRE (Tattica) + AI (Velocità).

La Cyber Kill Chain non è solo un modello di attacco, è una mappa per la sopravvivenza digitale.

Riferimenti Bibliografici

Hutchins, E., Cloppert, M., & Amin, R. (2011). Intelligence-Driven Computer Network Defense. Lockheed Martin Corporation.

Pols, P. (2017). The Unified Kill Chain. Cyber Security Academy / Fox-IT.

MITRE Corp. (2025). ATT&CK Framework Knowledge Base.

Vectra AI. (2026). Threat Landscape Report: The Acceleration of Cyber Attacks.

Schneier, B., et al. (2026). The Promptware Kill Chain. Lawfare.