MITRE ATT&CK® Framework: Analisi Tattica e Comportamentale degli Avversari

Una disamina approfondita della tassonomia, delle matrici e dell'operatività per la difesa informatica moderna.

Definizione e Genesi del Framework

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) è una base di conoscenza globale delle tattiche e tecniche avversarie, basata su osservazioni del mondo reale.

Paradigm Shift:

Dagli Indicatori di Compromissione (Hash, IP) ai Comportamenti (TTPs).

2013 - Progetto FMX (Fort Meade Experiment). Ricerca interna per il rilevamento post-compromissione.

2015 - Rilascio Pubblico. Matrice Enterprise iniziale focalizzata su Windows.

2020+ - Espansione Globale. Aggiunta di Sotto-tecniche, Mobile, ICS e Cloud.

2025 - Versione 18. Introduzione di Detection Strategies e logica comportamentale.

I Domini Tecnologici e le Matrici Operative

ENTERPRISE

- Windows
- macOS
- Linux
- Cloud (AWS/Azure/GCP)
- Network Devices
- Containers

MOBILE

- iOS
- Android

Vettori specifici:
Smishing,
Accessibilità abusiva

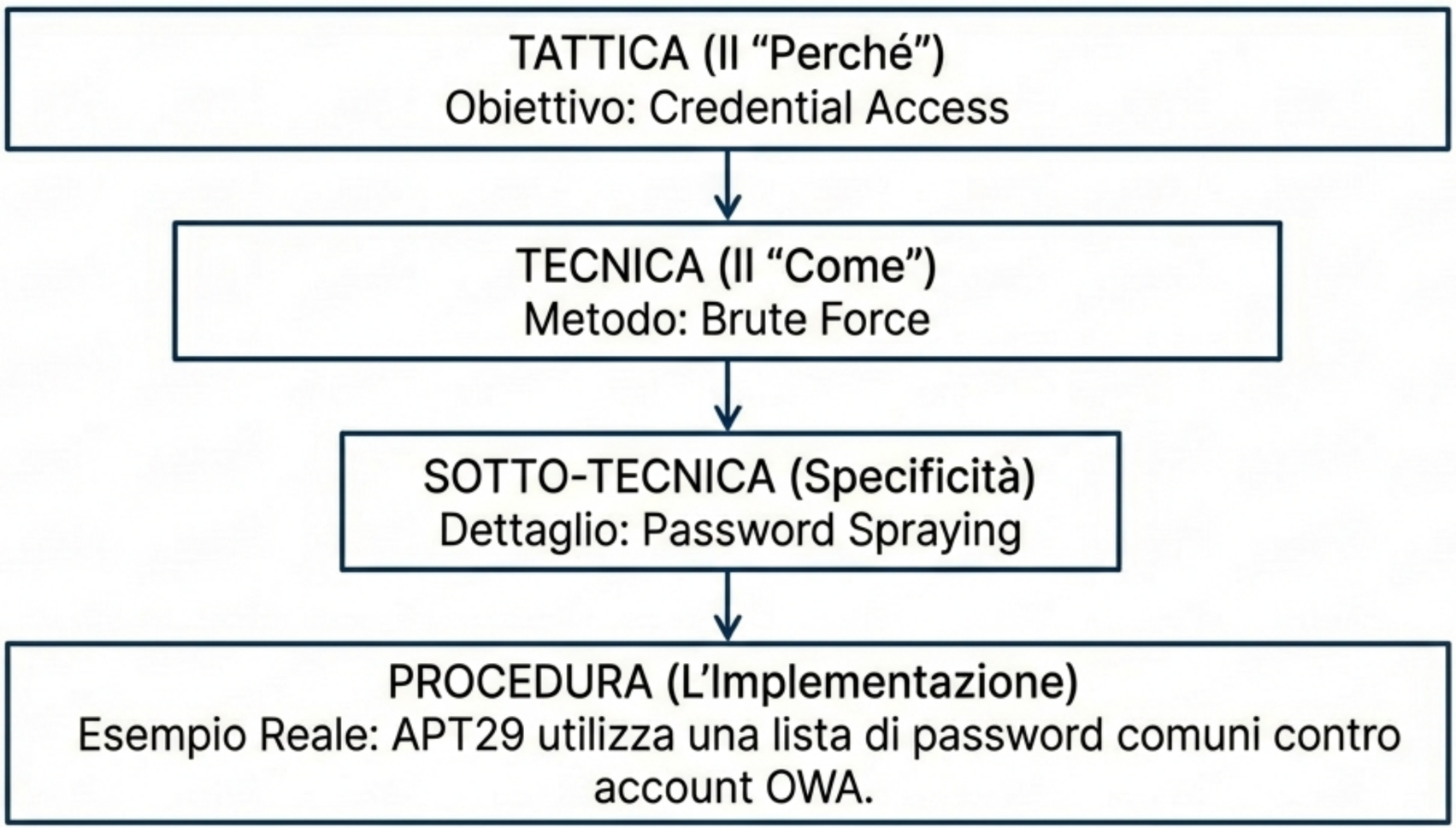
ICS

- Industrial Control Systems
- Operational Technology (OT)

Infrastrutture Critiche,
Manipolazione I/O

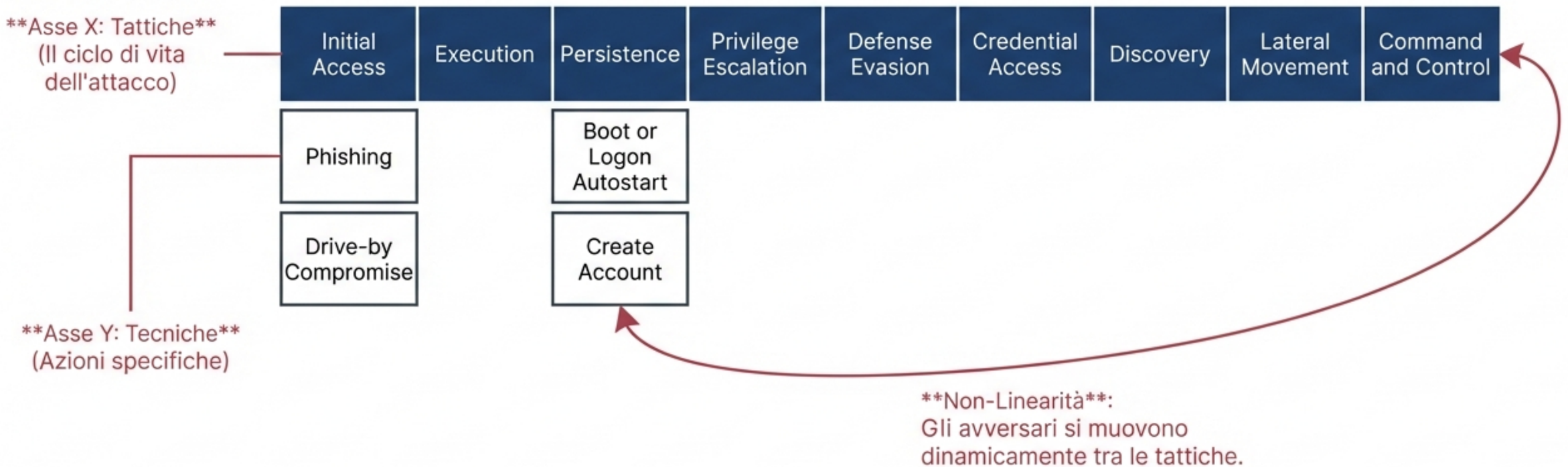
Il framework è strutturato per riflettere i diversi ecosistemi tecnologici in cui operano gli avversari.

La Gerarchia Ontologica: Tattiche, Tecniche e Procedure



Questa struttura tassonomica fornisce un linguaggio comune standardizzato per difensori e ricercatori.

Anatomia della Matrice Enterprise



Tattiche Chiave e il Ciclo di Vita dell'Avversario

Ingresso e Stabilità

- Initial Access
- Execution
- Persistence

Movimento e Controllo

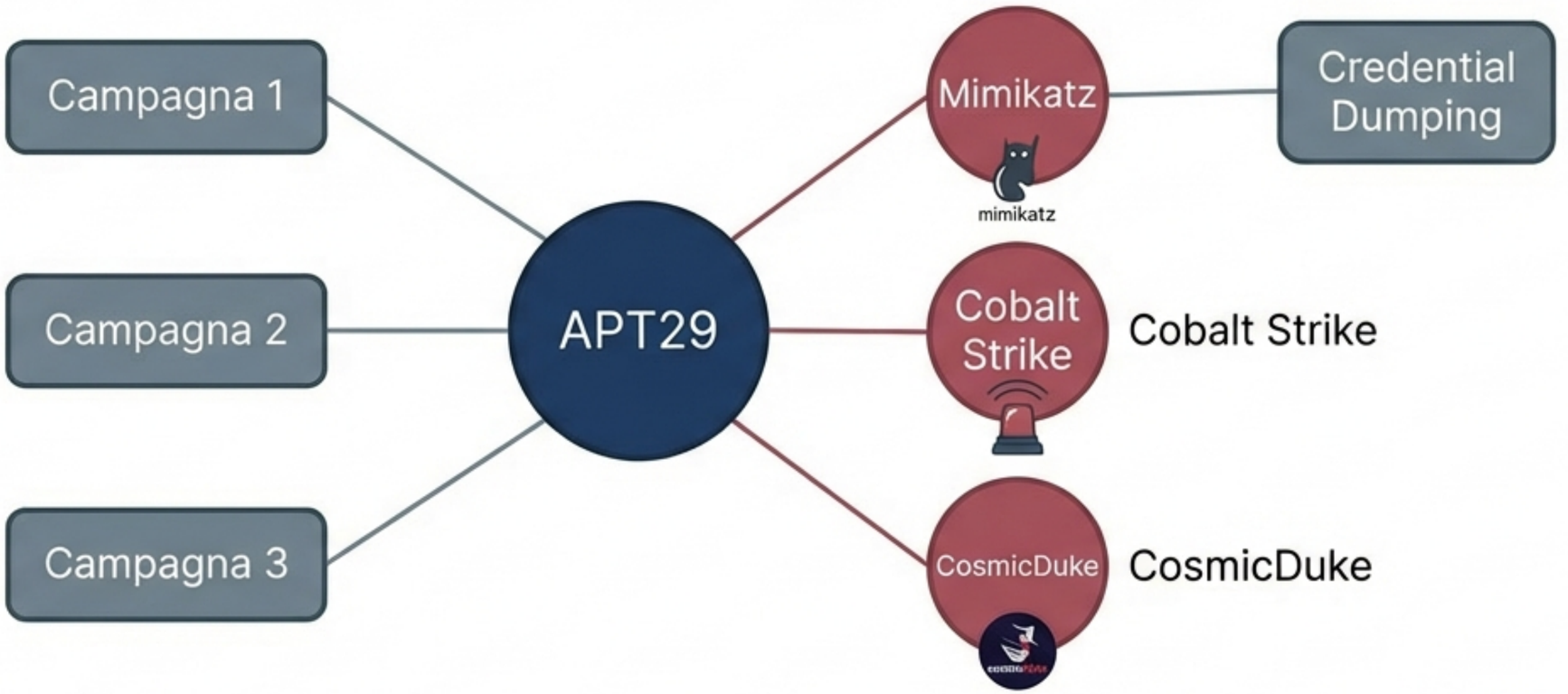
- Privilege Escalation
- Defense Evasion
- Lateral Movement
- Command and Control

Azione sugli Obiettivi

- Exfiltration
- Impact

Un raggruppamento logico per comprendere la progressione dell'intrusione, dal perimetro all'impatto finale.

Common Knowledge: Gruppi, Software e Campagne



Questa struttura relazionale permette l'attribuzione: collegare incidenti apparentemente isolati a specifici attori (Groups) attraverso l'uso di strumenti (Software) e procedure condivise.

Evoluzione Recente: MITRE ATT&CK v18 (Ottobre 2025)

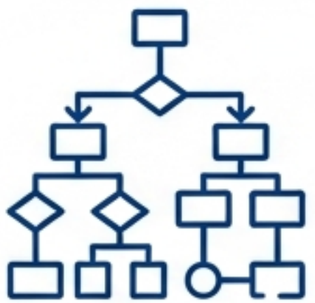
Il Cambio di Paradigma nel Rilevamento

PRIMA (v17)

- Note di rilevamento statiche e generiche.

Evoluzione

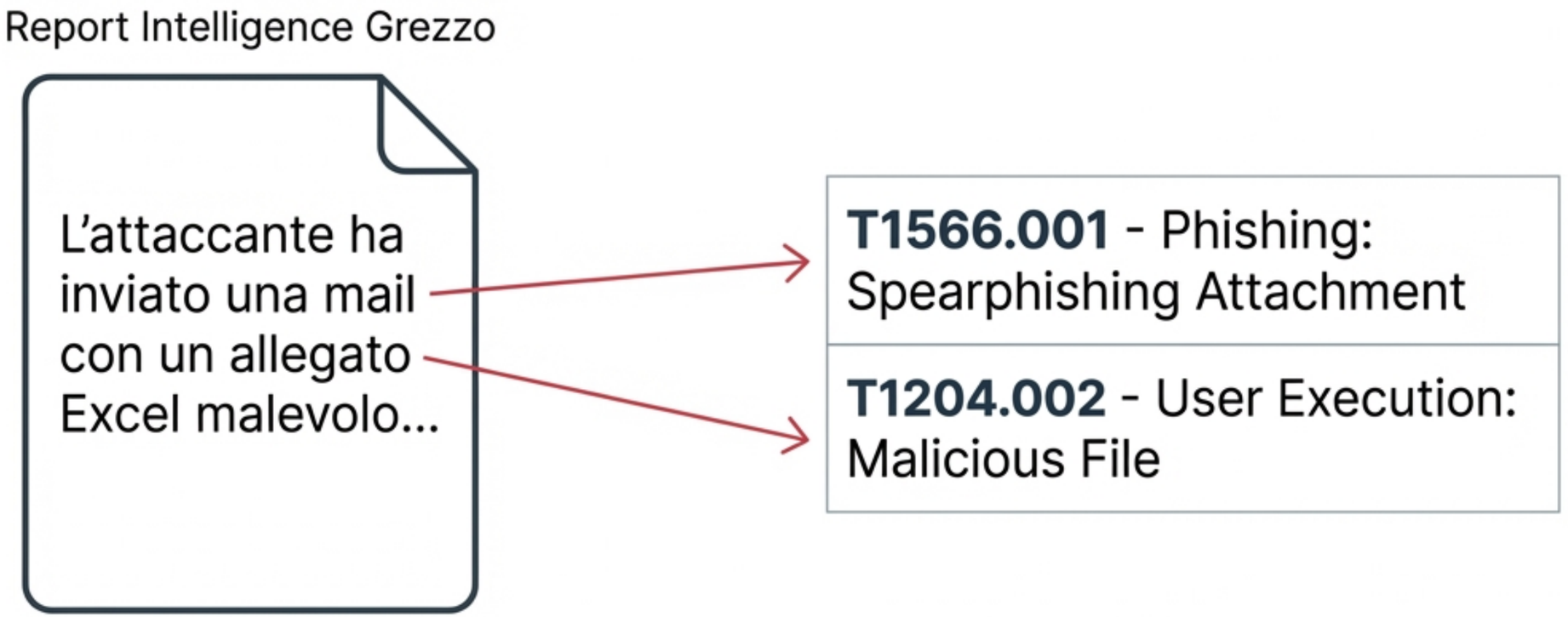
DOPO (v18)



- **Detection Strategies**: Logica strutturata focalizzata sul comportamento astratto.
- **Analytics**: Implementazioni tecniche specifiche (pseudo-codice, query).

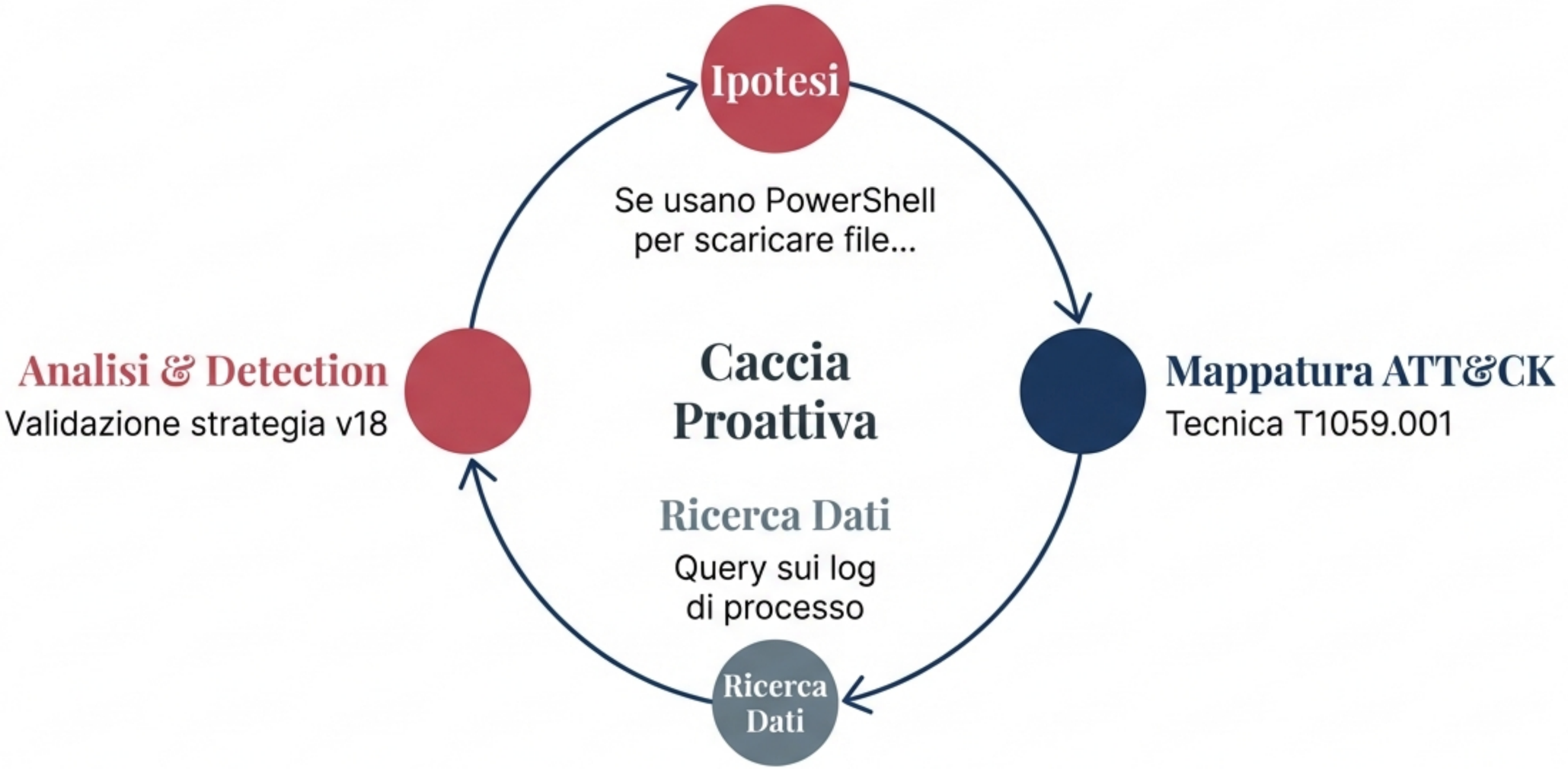
Obiettivo: Colmare il divario tra la teoria dell'intelligence e l'operatività pratica del SOC.

Caso d’Uso 1: Threat Intelligence & Enrichment



Beneficio: Standardizzazione dei report e possibilità di confrontare matematicamente le attività di diversi Threat Actors.

Caso d’Uso 2: Threat Hunting e Detection Engineering



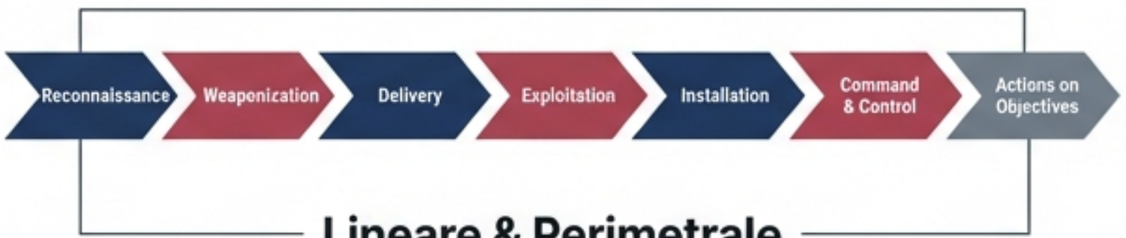
Non si cerca il malware specifico (Hash), ma il comportamento anomalo che ne rivela la presenza.

Caso d’Uso 3: Adversary Emulation (Red Teaming)

Piano di Emulazione APT29

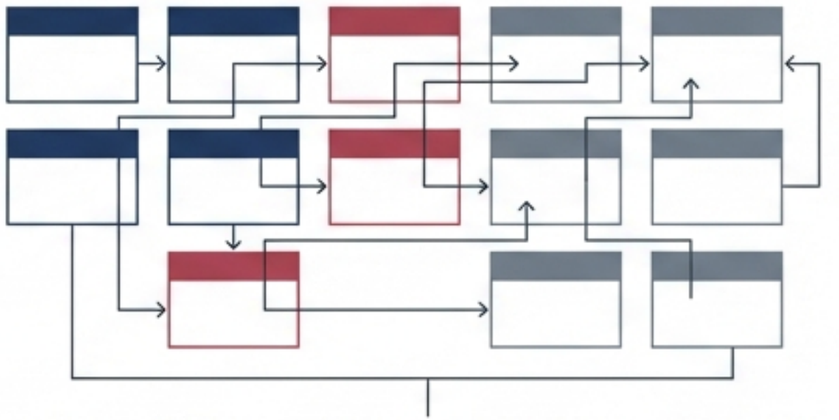
Analisi Comparativa: ATT&CK vs. Cyber Kill Chain

Lockheed Martin Cyber Kill Chain



Lineare & Perimetrale

MITRE ATT&CK

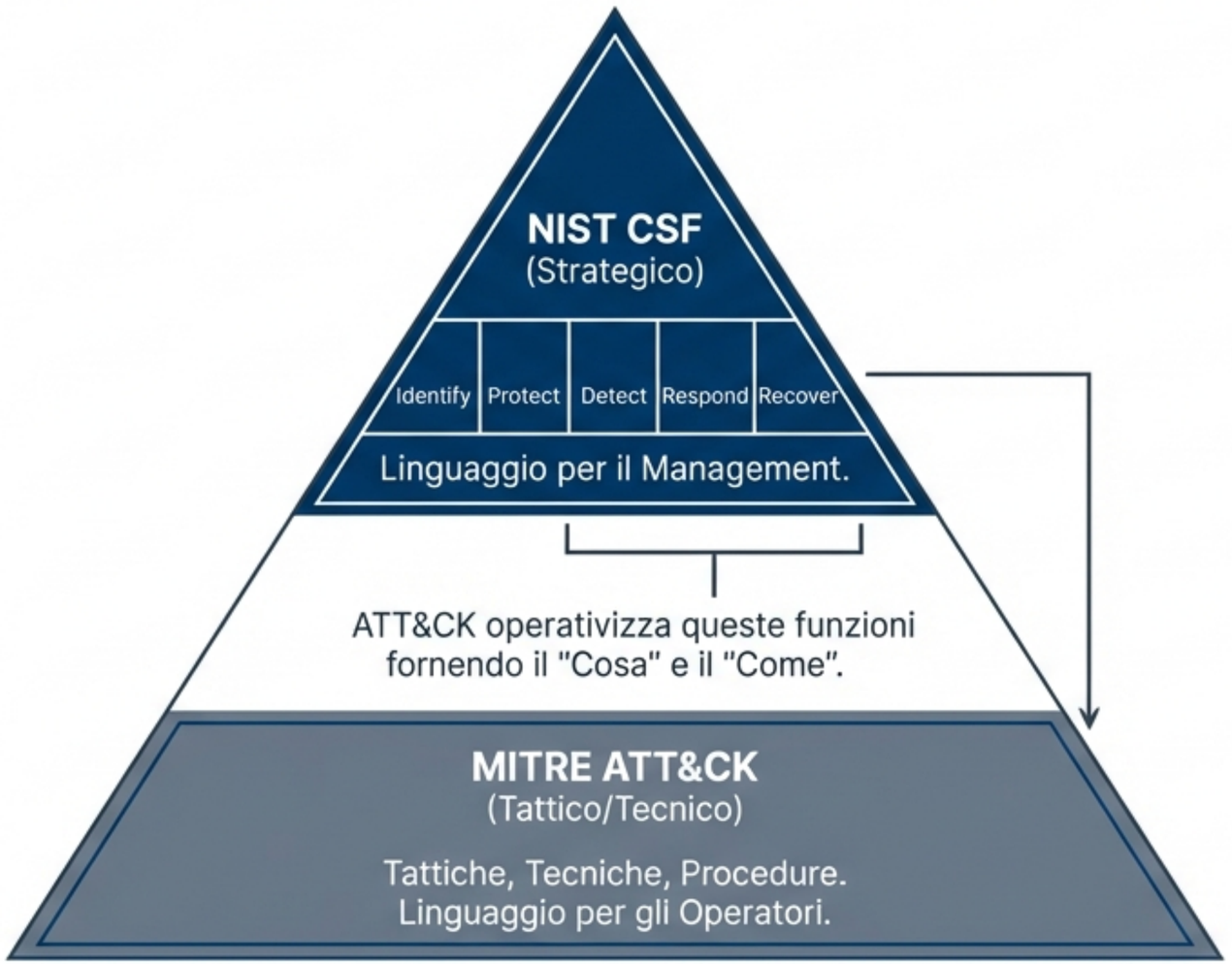


Non-lineare & Post-Compromissione

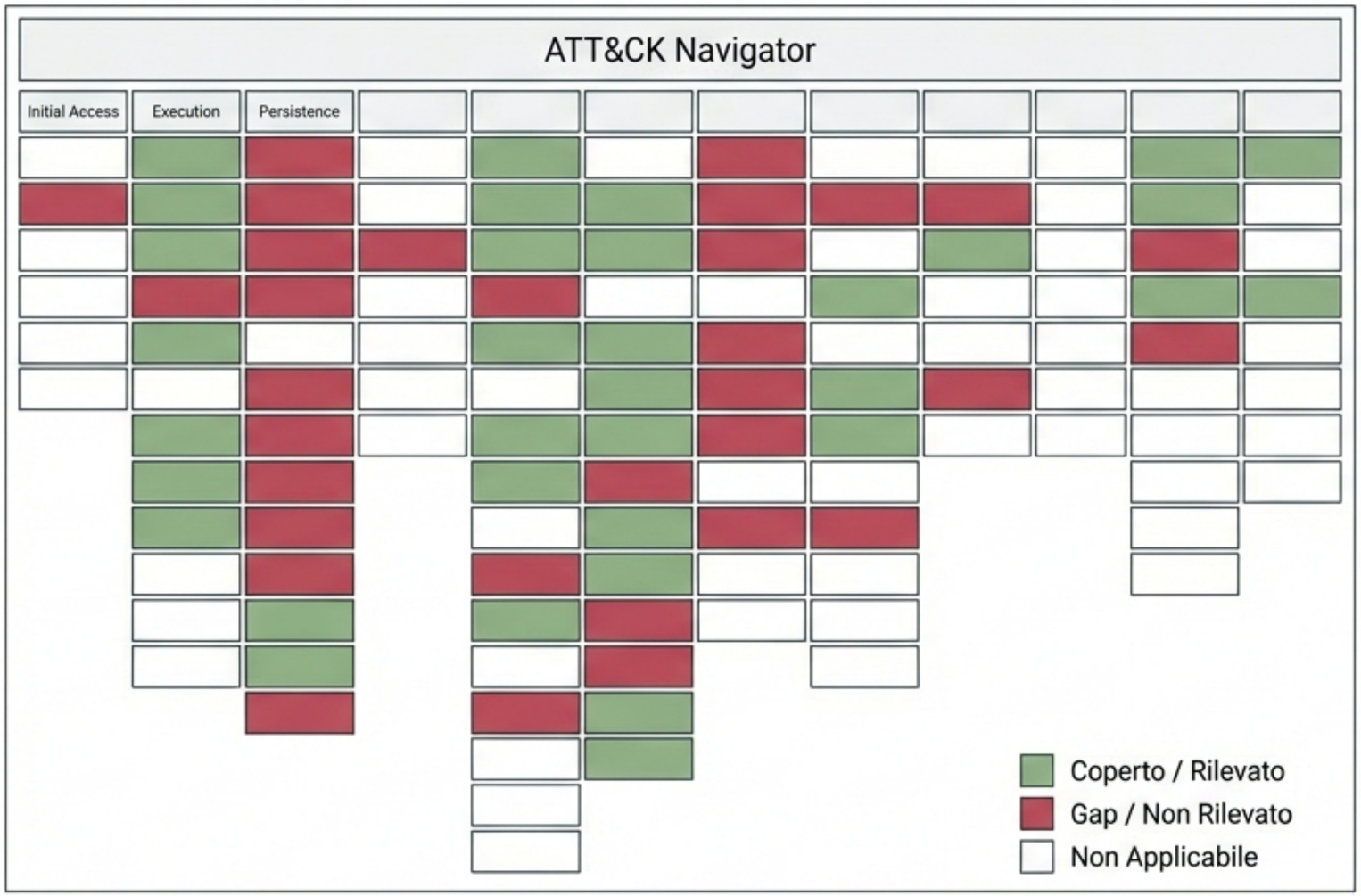
Kill Chain	ATT&CK
Livello Strategico	Livello Operativo
Focus sulla Prevenzione	Focus sul Rilevamento Interno
Sequenziale	Granulare (TTPs)

I modelli sono complementari: uno gestisce l'intrusione, l'altro il comportamento.

Analisi Comparativa: ATT&CK vs. NIST CSF



Implementazione: Gap Analysis e Roadmap



1. Mappare i controlli di sicurezza esistenti sulla matrice.
2. Identificare i “Blind Spots” (Tecniche non coperte).
3. Prioritizzare gli investimenti basandosi sulla Threat Intelligence.

Conclusioni: Verso una Difesa Informata sulle Minacce

- Transizione dalla difesa basata sulle firme alla difesa comportamentale.
- Adozione di un linguaggio globale comune.

"L'obiettivo non è bloccare ogni attacco, ma comprendere il comportamento dell'avversario per neutralizzarlo prima che raggiunga l'impatto."