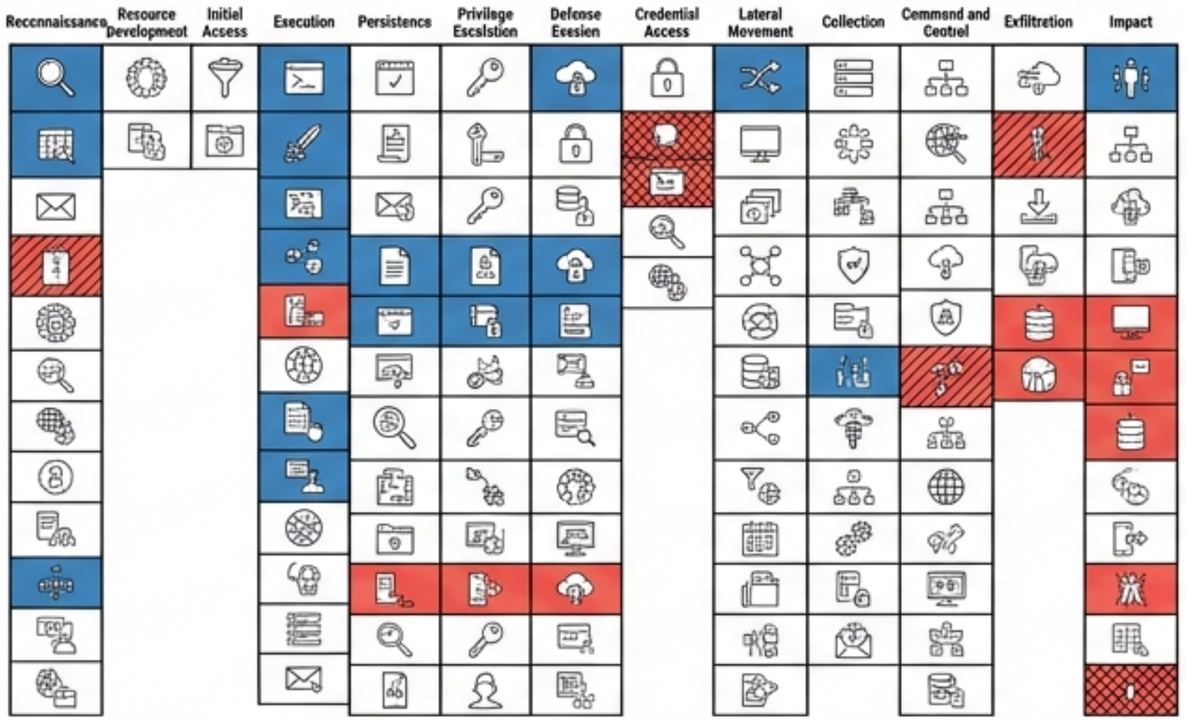
MITRE D3FEND™: Un’Ontologia per la Cyber Difesa

Dalla Teoria alla Pratica: Standardizzare il Linguaggio delle Contromisure

Il Divario Difensivo: Liste vs. Grafi

ATTACCANTI (Struttura)



DIFENSORI (Caos)

“I difensori pensano per liste. Gli attaccanti pensano per grafi.”

Mentre l’offensiva è standardizzata (TTPs), la difesa è spesso frammentata e dipendente dal linguaggio specifico dei vendor.

Serve una ‘Stele di Rosetta’ per unificare le contromisure tecniche.

Definizione e Struttura Epistemologica

Knowledge Graph: Una rete semantica di relazioni, non una semplice lista.

Detection, Denial, and Disruption Framework Empowering Network Defense

Finanziamento:
Supportato dalla NSA e gestito dal MITRE NSEC.

Ontologia OWL 2 DL:
Basata su logica descrittiva computabile (SROIQV).

Vendor-Neutral:
Indipendente da specifici prodotti commerciali.

Release **v1.3.0**: **267+** Tecniche Difensive

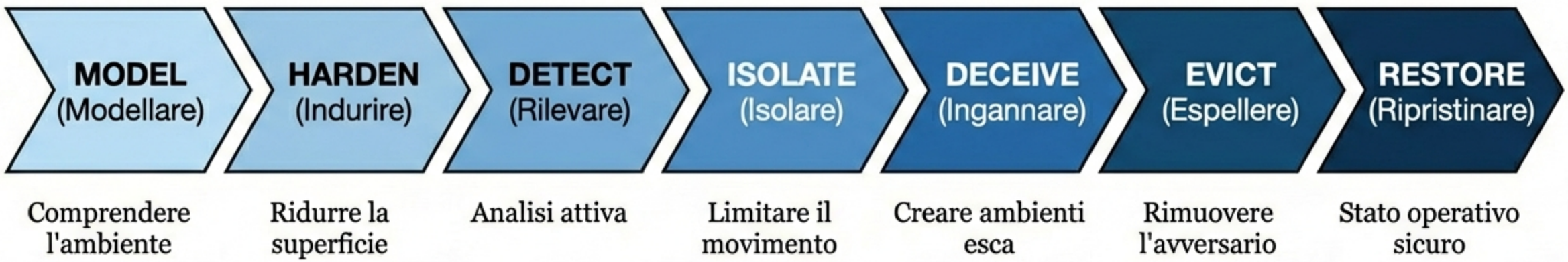
Simmetria Operativa: ATT&CK e D3FEND

1. **ATT&CK** cataloga l'offesa (Tattiche, Tecniche, Procedure).

2. **D3FEND** cataloga la difesa (Rilevamento, Negazione, Interruzione).

3. **Punto di Contatto:** Entrambi i framework interagiscono con gli stessi oggetti digitali.

La Matrice Tattica: Le 7 Colonne della Difesa

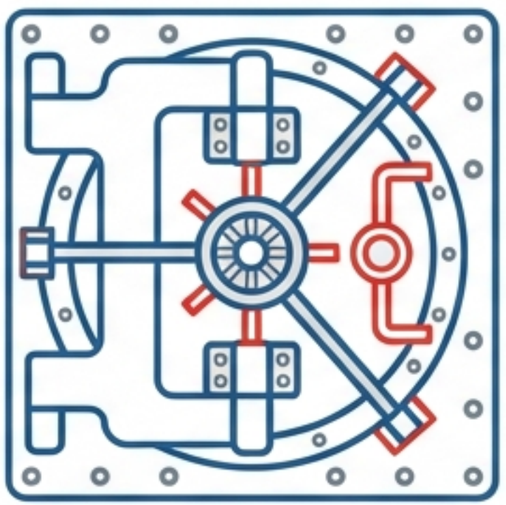


Fase Preparatoria: Modellare e Indurire

MODEL (Modellare)

- Focus: Mappatura delle risorse e delle relazioni operative.
- Esempi: Asset Inventory (Inventario Asset), Network Mapping (Mappatura di Rete).
- Principio: Non puoi difendere ciò che non conosci.

HARDEN (Indurire)



- Focus: Aumentare il costo dell'attacco per l'avversario prima che inizi.
- Esempi: Application Hardening, Credential Hardening (MFA).
- Principio: Allineato con Zero Trust ("Never trust, always verify").

Ingaggio Attivo: Rilevare e Isolare

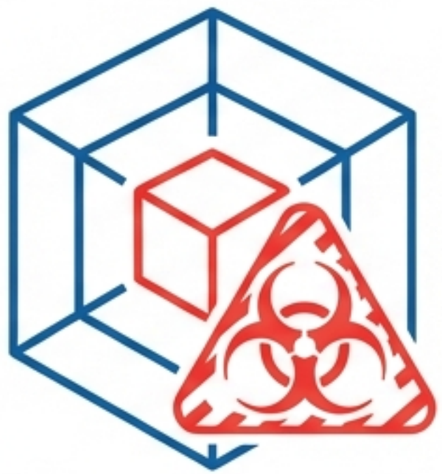
DETECT (Rilevare)

Focus: La categoria più ampia (90+ tecniche). Monitoraggio in tempo reale.

Esempi: `Process Analysis`, `User Behavior Analysis`.

Mapping: Punto di collegamento per strumenti SIEM ed EDR.

ISOLATE (Isolare)



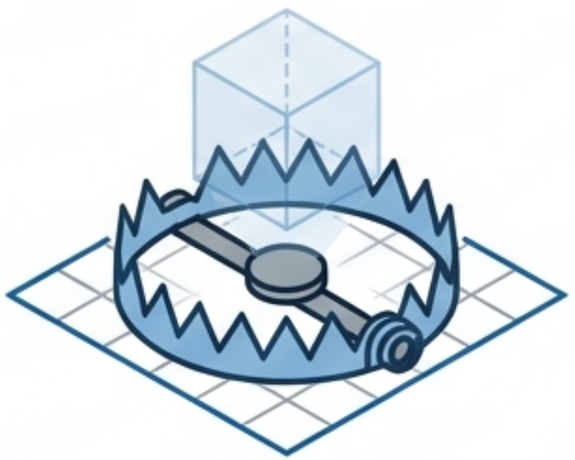
Focus: Contenimento del “blast radius” (raggio di esplosione).

Esempi: `Network Isolation` (Segmentazione), `Execution Isolation` (Sandboxing).

Scopo: Impedire il movimento laterale dell’attaccante.

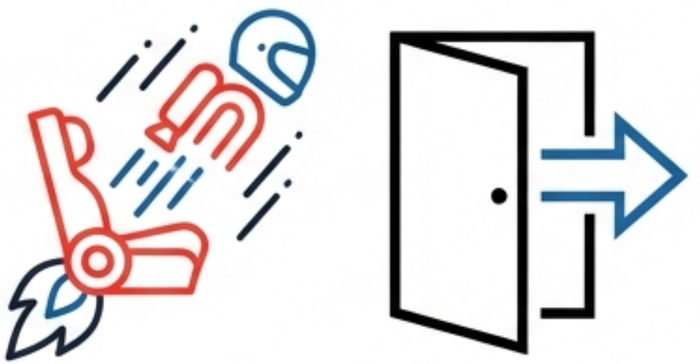
Risposta e Resilienza: Ingannare, Espellere, Ripristinare

DECEIVE



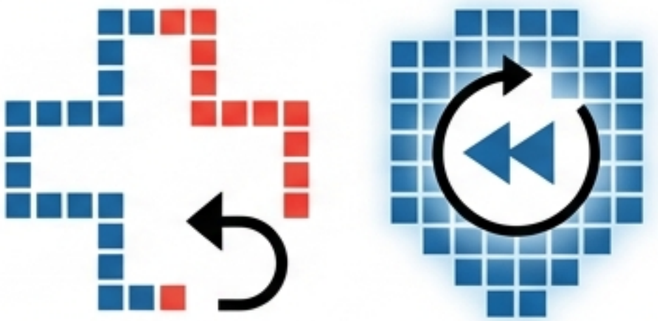
Uso di Honeypots e Decoy Objects. Genera allarmi ad alta fedeltà con bassi falsi positivi.

EVICT



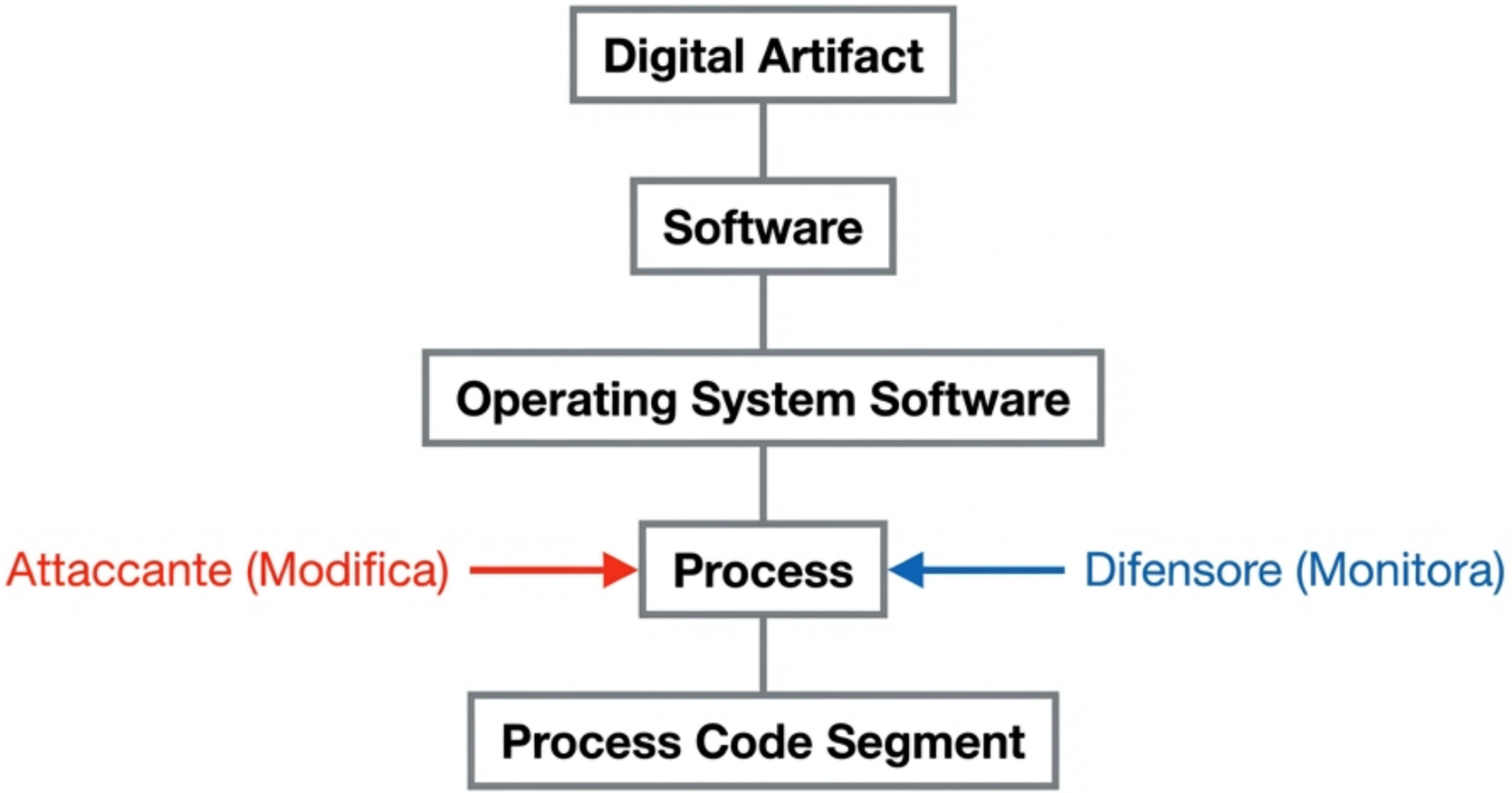
L’atto di rimuovere la minaccia. Esempi: Credential Eviction, Process Termination.

RESTORE



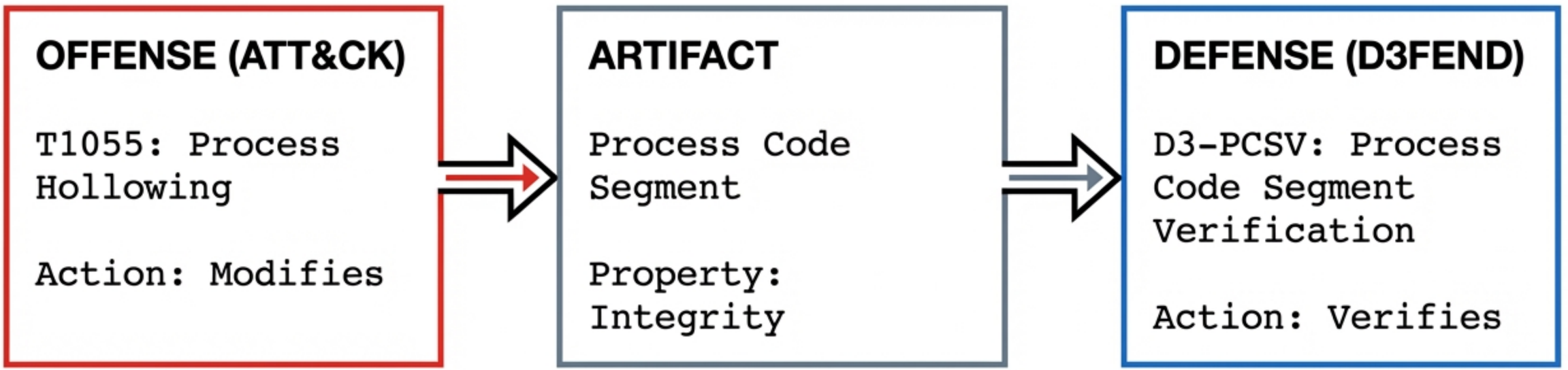
Oltre il backup. Ripristino a uno stato ‘known-good’ più resiliente di prima.

Il Motore Semantico: Digital Artifact Ontology (DAO)



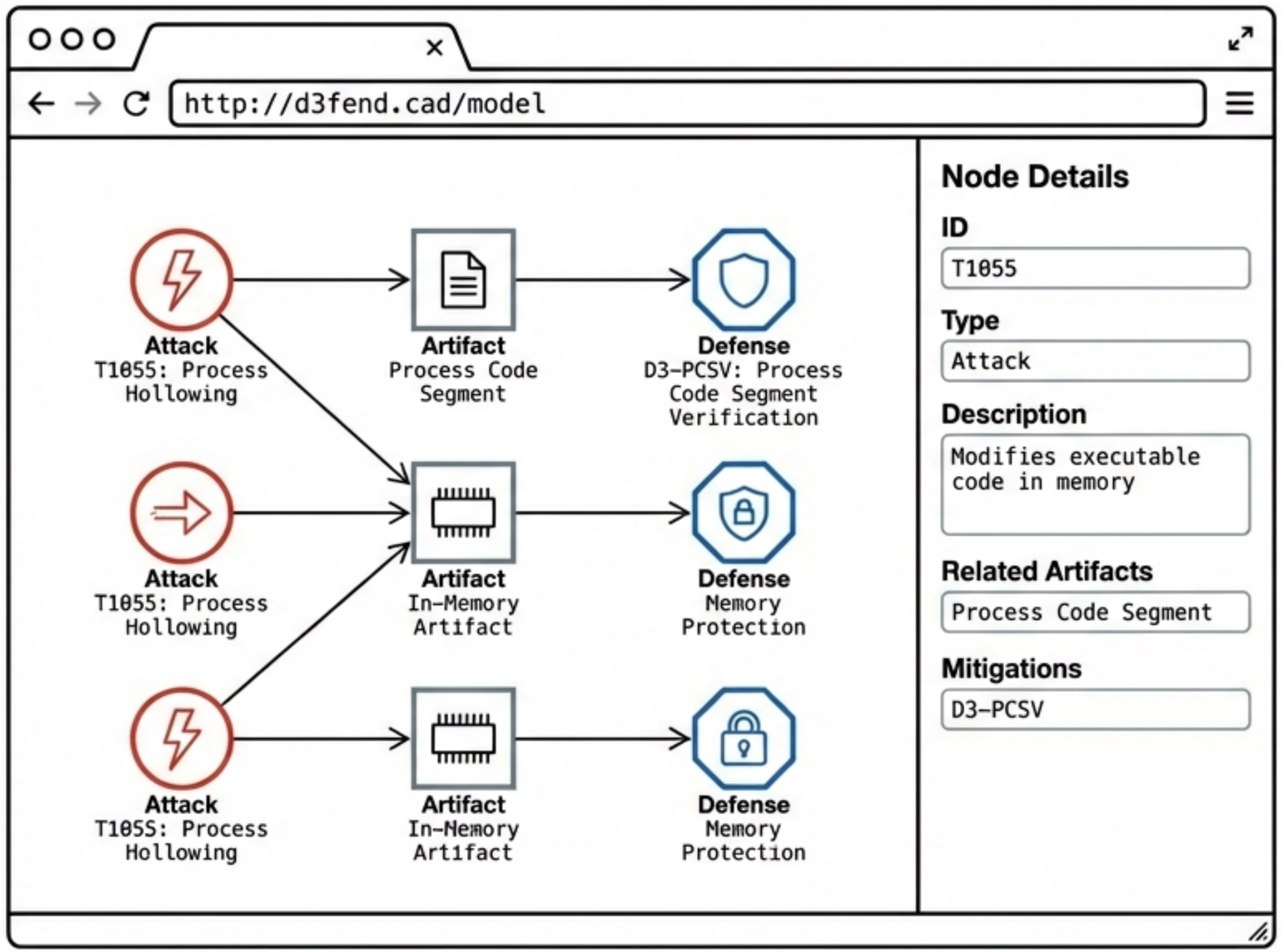
Il DAO contiene oltre 800 tipi di asset distinti. L'Artefatto è il ponte semantico che permette di mappare le relazioni in modo matematico, superando le semplici associazioni di parole chiave.

L’Inferenza in Azione: Esempio Pratico



L'ontologia inferisce matematicamente che la contromisura corretta deve verificare l'integrità del segmento di codice, poiché l'attacco T1055 tenta di svuotare la memoria di un processo legittimo.

D3FEND CAD: Modellazione Visiva delle Minacce



- **Interfaccia Web:** Drag-and-drop per costruire scenari di attacco-difesa.
- **Inference Engine:** Funzione ‘Explode’ per suggerire automaticamente difese.
- **Interoperabilità:** Importazione STIX 2.1 e integrazione Threat Intel.
- **Export:** JSON e TTL per l’integrazione nei sistemi.

Applicazioni nell'Ingegneria della Sicurezza

GAP ANALYSIS

Sovrapporre le difese attuali alle tecniche ATT&CK per identificare i "buchi" nella copertura (specialmente in Detect e Isolate).

VALUTAZIONE VENDOR

Confrontare i prodotti commerciali basandosi sulle tecniche D3FEND specifiche, ignorando il marketing.

COMPLIANCE

Mappatura tecnica verso standard normativi:

- NIST 800-53 Rev. 5
- DISA CCI
- Integrazione CWE

Estensione OT: Proteggere i Sistemi Ciber-Fisici

- **Nuovi Artefatti**: Sensori, Attuatori, Controllori Programmabili (PLC).
- **Scopo**: Estende l'ontologia per coprire ambienti SCADA e ICS, dove la sicurezza fisica e la stabilità sono prioritarie.

Roadmap 2026: Il Futuro della Difesa

Summiting the Pyramid

Aumentare la robustezza del rilevamento per rendere l'evasione misurabilmente più difficile.

Fight Financial Fraud (F3)

Collegare gli eventi cyber alle frodi finanziarie materiali.

AI Security

Integrazione con MITRE ATLAS per difendere i sistemi basati su Intelligenza Artificiale (`Adversarial ML`).

Conclusioni: Verso una Scienza della Difesa

“MITRE D3FEND trasforma la sicurezza da una ‘lista di controllo’ statica in un’architettura semantica dinamica e computabile.”

d3fend.mitre.org
(Knowledge Graph)

d3fend.mitre.org/cad
(CAD Tool)

GitHub Repository
(Ontology & API)