
# MITRE D3FEND


Alejandro Corletti Estrada
*acorletti@darfe.es*

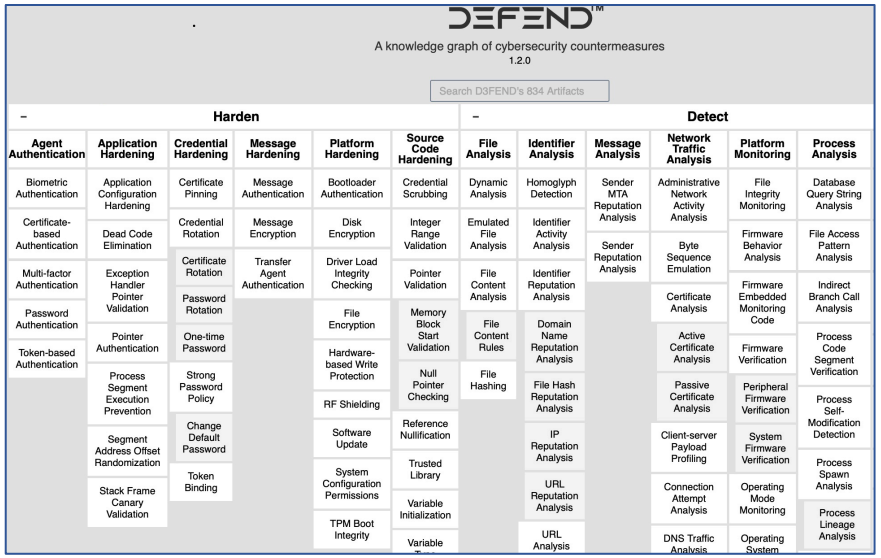
# MITRE D3FEND (https://d3fend.mitre.org)


Dentro de nuestro ciclo a "***Aprendiendo Ciberseguridad Paso a Paso***", Hoy vamos a ver **MITRE D3FEND**, la contraparte **defensiva** de MITRE ATT&CK, y una herramienta imprescindible para **Blue Teams**, **SOCs**, **analistas de amenazas** y **arquitectos de seguridad**.

En nuestro ciclo ya has visto nuestros vídeos sobre:

- MITRE ATT&CK (videos 150 a 160)
- Sysmon
- SIEM
- Análisis forense
- CVEs, CWEs y CAPEC
- Hardening

Por lo que este vídeo te va a encajar perfectamente.




# 1. ¿Qué es MITRE D3FEND?

**D3FEND** es una base de conocimiento organizada que describe:

1. **Técnicas defensivas**
2. **Mecanismos de defensa**
3. **Contramedidas específicas**
4. **Relaciones entre defensas y técnicas ATT&CK**

Dicho de forma simple:

👉 ATT&CK te explica **cómo te atacan**,
👉 D3FEND te explica **cómo defenderte**.

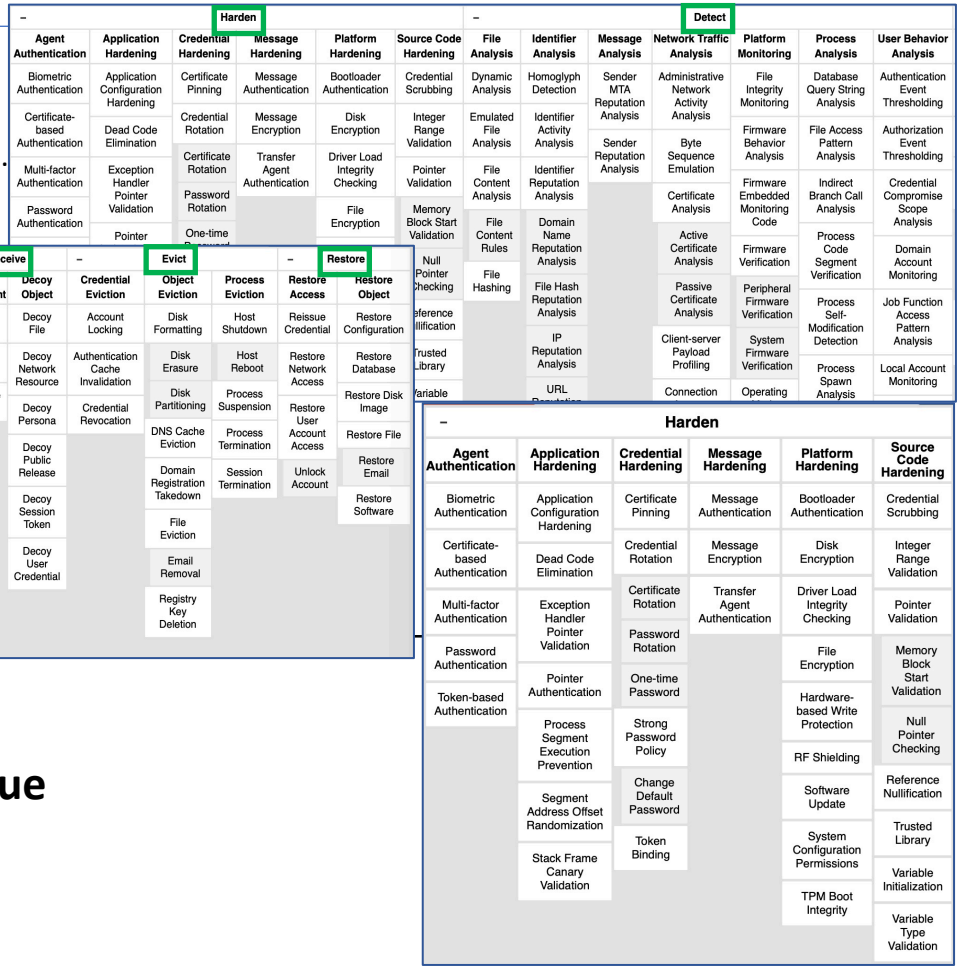
MITRE lo desarrolló financiado por la **NSA** (National Security Agency) con el objetivo de mejorar la defensa nacional y empresarial frente a APTs y ataques complejos.

# 2. Estructura de MITRE D3FEND

**D3FEND** se organiza en varias categorías principales que representan **funciones defensivas**. Cada categoría contiene técnicas específicas, ejemplos prácticos y relaciones con ATT&CK.

## Las 6 categorías de D3FEND

A. **Harden (Endurecimiento)**
B. **Detect (Detección)**
C. **Isolate (Aislamiento)**
D. **Deceive (Engaño)**
E. **Evict (Expulsión/Erradicación)**
F. **Restore (Restauración)**




# 3. Categorías y Técnicas con Ejemplos Reales

## A. HARDEN — Fortificar y reducir superficie de ataque

Agrupa técnicas usadas para **evitar que un ataque tenga éxito**.

Ejemplos de técnicas:

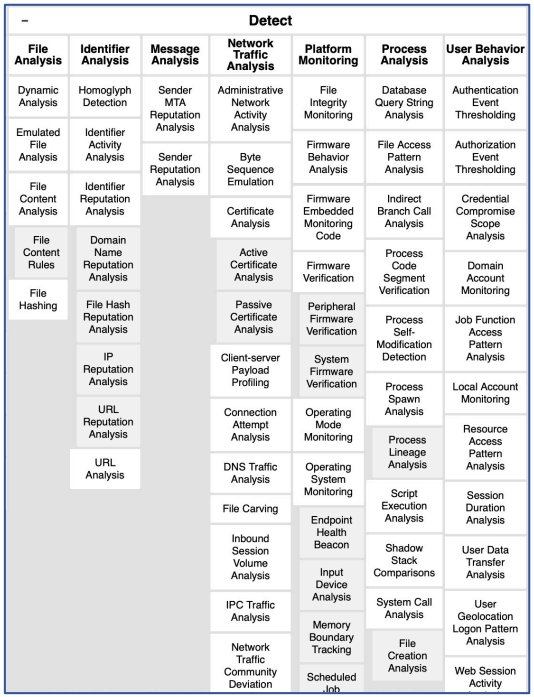
- **Credential Hardening**
- **Application Hardening**
- **Network Hardening**
- **File System Hardening**

Ejemplos aplicados:

| | |
|---|---|
| ✓ Deshabilitar PowerShell no firmado | ✓ Desactivar macros por defecto |
| ✓ Configuración segura de RDP | ✓ Modo |

**Relación con ATT&CK**: Mitiga técnicas como *Initial Access*, *Execution* o *Privilege Escalation*.

# B. DETECT — Identificar comportamientos sospechosos






Agrupa mecanismos que permiten **detectar un ataque en curso**.

Ejemplos de técnicas:

- **Process Monitoring**
- **Binary Analysis**
- **Network Traffic Analysis**
- **Memory Monitoring**

Casos reales:

✓ Sysmon

✓ Un IDS alertando del tráfico de C2

✓ Defender ATP detectando inyección de memoria

Relación con ATT&CK: Mapea a tácticas de *Command and Control* y *Execution*.

---

# C. ISOLATE — Limitar o contener el daño

Técnicas para evitar que un atacante se mueva lateralmente o comprometa más sistemas.

Ejemplos:

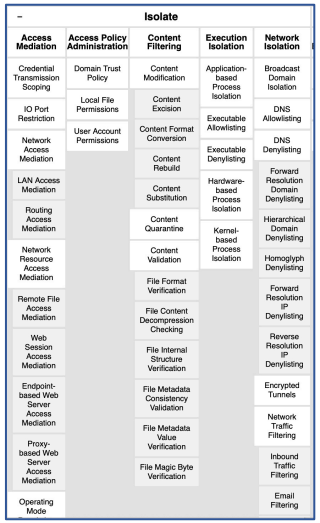
- **Network Isolation**
- **Sandboxing**
- **Application Isolation**

Aplicaciones reales:

✓ Poner un endpoint en modo “aislado” desde un EDR

✓ Navegadores con sandboxing (Chrome sandbox

✓ VLANs para impedir desplazamiento lateral



## D. DECEIVE — Engañar al atacante


Una de las categorías más potentes y menos utilizadas.

Técnicas:

- **Honeypots**
- **Honey Files / Honey Credentials**
- **Decoy Services**

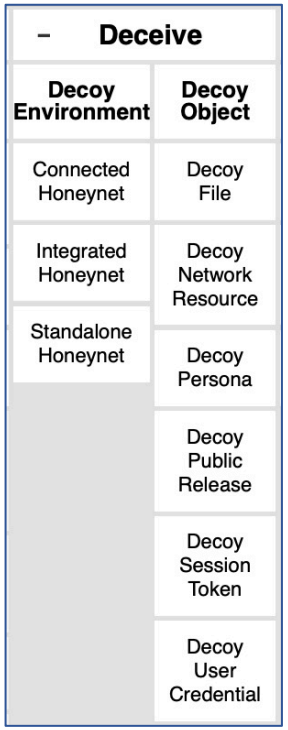
Casos reales:

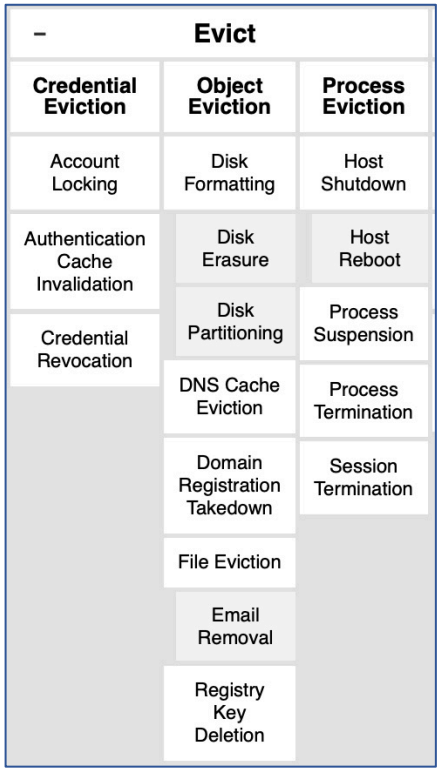
✔ Crear un archivo señuelo “Passwords.xlsx” con un canary token

✔ Honeypots detectando movimiento lateral

✔ Servicios falsos expuestos para estudiar escaneos

Esto permite **detectar actividad delictiva temprana** y recopilar inteligencia.




---

## E. EVICT — Cortar o eliminar actividad maliciosa

Conjunto de técnicas para **expulsar al atacante** y evitar persistencia.

Ejemplos:

- **Kill Process (terminar procesos maliciosos)**
- **Account Lockdown**
- **Quarantine File**
- **Network Block / Firewall Rules**

Aplicación real:

✔ Un EDR bloquea automáticamente mimikatz.exe o acciones similares

✔ Un SIEM activa respuesta automática para bloquear un hash en toda la red

## F. RESTORE — restaurar y analizar evidencias

Cubren técnicas de restauración e investigación y análisis profundo.

Ejemplos:

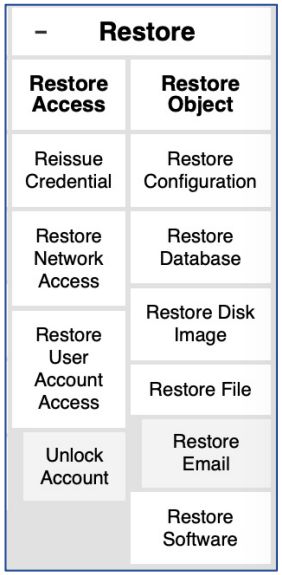
- **Disk Imaging**
- **Memory Forensics**
- **Log Analysis**
- **Packet Capture**

Usos reales:

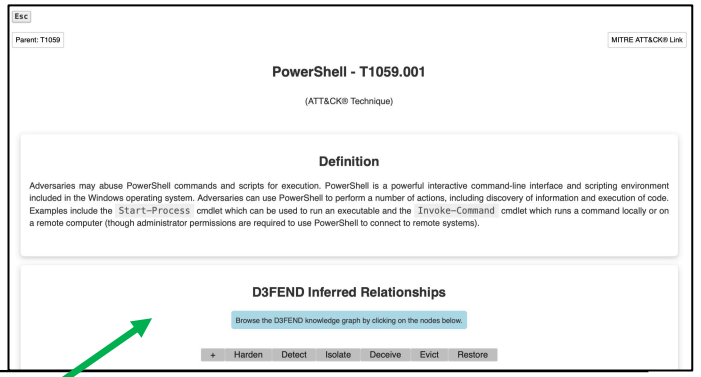
✓ Análisis de un volcado de memoria con Volatility

✓ Estudiar un binario malicioso

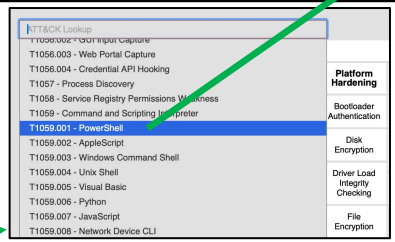
✓ Triage rápido de un endpoint comprometido






# 4. Cómo se relaciona D3FEND con ATT&CK




Este punto es clave para Blue Teams.

**D3FEND** "conecta" cada técnica defensiva con las técnicas ofensivas que pretende mitigar.

Ejemplo:

- **ATT&CK: T1059.001 – PowerShell**

  → **D3FEND: Execution Isolation, Script Blocking, Process Monitoring**

Otro ejemplo:

- **ATT&CK: Credential Dumping (T1003)**
  → **D3FEND: Credential Hardening, Memory Analysis, Behavior Monitoring**

Esto permite: ✓ Construir detecciones basadas en adversarios reales

✓ Justificar defensas ante auditorías

✓ Crear arquitecturas de seguridad alineadas al riesgo real

# 5. ¿Para qué sirve en la práctica?


**D3FEND** es útil para:

| | |
|---|---|
| **Para analistas SOC:**<br>✓ Crear reglas de detección alineadas a tácticas reales<br>✓ Mapear defensas existentes a amenazas relevantes<br>✓ Identificar huecos en la arquitectura defensiva | **Para arquitectos de seguridad:**<br>✓ Diseñar defensas basadas en un estándar internacional<br>✓ Documentar controles de forma estructurada<br>✓ Justificar inversiones ante la dirección |
| **Para Red Teams:**<br>✓ Entender qué defensas van a activarse<br>✓ Planear ataques más realistas<br>✓ Simular APTs y validar eficacia defensiva | **Para formación:**<br>✓ Explicar el "lado defensivo" de ATT&CK<br>✓ Construir laboratorios con roles Blue Team<br>✓ Enseñar detección, hardening y forense de forma ordenada |

# 6. Ejemplo práctico aplicado a nuestro ciclo

En tu serie de *Aprendiendo Ciberseguridad Paso a Paso*, **D3FEND** se relaciona con:

- **Videos de Sysmon** → "Process Monitoring"
- **Videos de SIEM** → "Log Analysis"
- **Videos de Firewalls** → "Network Isolation" / "Traffic Filtering"
- **Videos de Análisis Forense** → "Disk Imaging" / "Memory Forensics"
- **Videos de MITRE ATT&CK** → Defensa asociada a cada táctica
- **Videos de análisis de CVE/CWE** → Hardening + mitigación
- **Videos de GoPhish y phishing** → Engaño y detección

Es un framework (entorno) perfecto para consolidar el aprendizaje del ciclo.

# 7. Resumen corto para cierre de vídeo


**MITRE D3FEND** es:

- El catálogo de **técnicas defensivas** más completo.
- El complemento perfecto de MITRE ATT&CK.
- Una guía práctica para Blue Teams, SOCs y arquitectos de seguridad.
- Una herramienta esencial para entender cómo defenderse de actores reales.