

www.darFe.es

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 videos sobre:

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

Por lo que este video te va a encajar perfectamente.

1. ¿Qué es MITRE D3FEND?

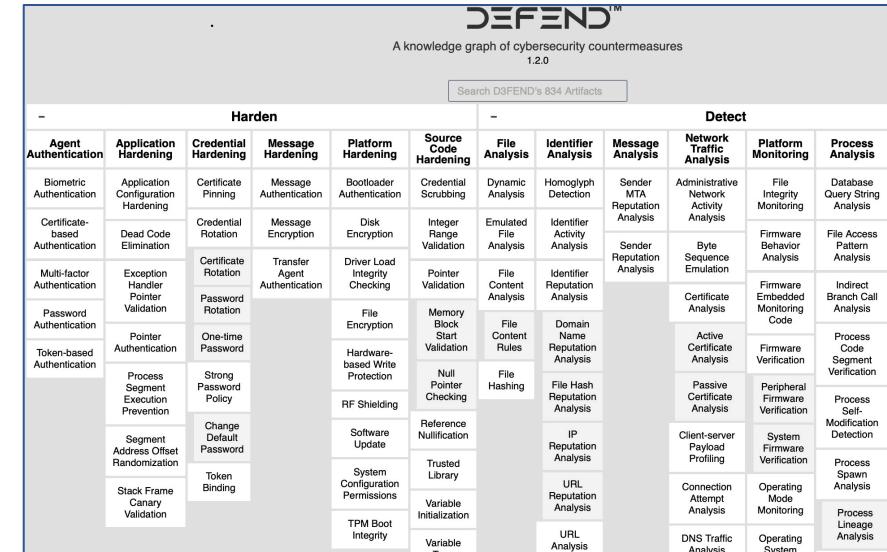
D3FEND es una base de conocimiento organizada que describe:

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 ✓ Configuración segura de RDP	✓ Desactivar macros por defecto ✓ 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*.

Detect							
File Analysis	Identifier Analysis	Message Analysis	Network Traffic Analysis	Platform Monitoring	Process Analysis	User Behavior Analysis	-
Dynamic Analysis	Homograph Detection	Sender MTA Reputation Analysis	Administrative Network Activity Analysis	File Integrity Monitoring	Database Query String Analysis	Authentication Event Thresholding	
Emulated File Analysis	Identifier Activity Analysis	Sender Reputation Analysis	Byte Sequence Emulation	Firmware Behavior Analysis	File Access Pattern Analysis	Authorization Event Thresholding	
File Content Analysis	Identifier Reputation Analysis		Certificate Analysis	Firmware Embedded Monitoring Code	Indirect Branch Call Analysis	Credential Compromise Scope Analysis	
File Content Rules	Domain Name Reputation Analysis		Active Certificate Analysis	Firmware Verification	Process Code Segment Verification	Domain Account Monitoring	
File Hashing	File Hash Reputation Analysis		Passive Certificate Analysis	Peripheral Firmware Verification	Process Self-Modification Detection	Job Function Access Pattern Analysis	
IP Reputation Analysis		Client-server Payload Profiling	System Firmware Verification	Process Spawn Analysis	Local Account Monitoring		
URL Reputation Analysis		Connection Attempt Analysis	Operating Mode Monitoring	Process Lineage Analysis	Resource Access Pattern Analysis		
URL Analysis		DNS Traffic Analysis	Operating System Monitoring	Script Execution Analysis	Session Duration Analysis		
		File Carving	Endpoint Health Beacon	Shadow Stack Comparisons	User Data Transfer Analysis		
		Inbound Session Volume Analysis	Input Device Analysis	System Call Analysis	User Geolocation Pattern Analysis		
		IPC Traffic Analysis	Memory Boundary Tracking	File Creation Analysis	Scheduled Job	Web Session Activity	



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

Isolate				
Access Mediation	Access Policy Administration	Content Filtering	Execution Isolation	Network Isolation
Credential Transmission Scoping	Domain Trust Policy	Content Modification	Application-based Process Isolation	Broadcast Domain Isolation
IO Port Restriction	Local File Permissions	Content Excision		DNS Allowlisting
Network Access Mediation	User Account Permissions	Content Format Conversion	Executable Allowlisting	DNS Denylisting
Routing Access Mediation		Content Redundancy	Executable Denylisting	Forward Resolution Domain Denylisting
Network Resource Access Mediation		Content Substitution	Hardware-based Process Isolation	Hierarchical Domain Denylisting
Remote File Access Mediation		Content Quarantine	Kernel-based Process Isolation	Homograph Denylisting
Web Session Access Mediation		Content Validation		Forward Resolution IP Denylisting
Endpoint-based Web Service Access Mediation		File Format Verification		Reverse Resolution IP Denylisting
Proxy-based Web Service Access Mediation		File Content Decompression Checking		Encrypted Tunnels
Operating Mode		File Internal Structure Verification		Network Traffic Filtering
		File Metadata Consistency Validation		Inbound Traffic Filtering
		File Metadata Value Verification		Email Filtering
		File Magic Byte Verification		

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.



- Deceive		- Evict		
Decoy Environment	Decoy Object	Credential Eviction	Object Eviction	Process Eviction
Connected Honeynet	Decoy File	Account Locking	Disk Formatting	Host Shutdown
Integrated Honeynet	Decoy Network Resource	Authentication Cache Invalidation	Disk Erasure	Host Reboot
Standalone Honeynet	Decoy Persona	Credential Revocation	Disk Partitioning	Process Suspension
	Decoy Public Release		DNS Cache Eviction	Process Termination
	Decoy Session Token		Domain Registration Takedown	Session Termination
	Decoy User Credential		File Eviction	
			Email Removal	
			Registry Key Deletion	

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.

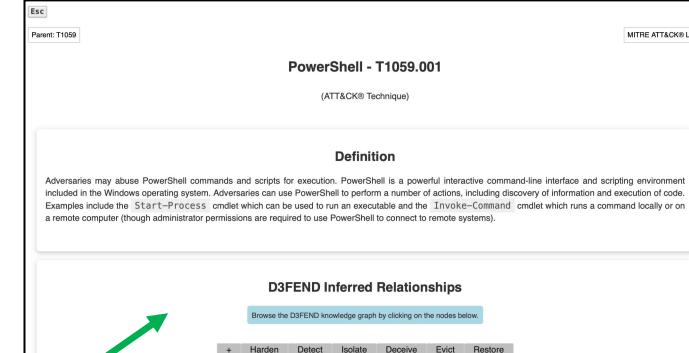
Ejemplos:

- **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

- Restore	
Restore Access	Restore Object
Reissue Credential	Restore Configuration
Restore Network Access	Restore Database
Restore User Account Access	Restore Disk Image
	Restore File
	Restore Email
Unlock Account	Restore Software



PowerShell - T1059.001
(ATT&CK® Technique)

Definition

Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system. Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the `Start-Process` cmdlet which can be used to run an executable and the `Invoke-Command` cmdlet which runs a command locally or on a remote computer (though administrator permissions are required to use PowerShell to connect to remote systems).

D3FEND Inferred Relationships

Browse the D3FEND knowledge graph by clicking on the nodes below.

+ Harden Detect Isolate Deceive Evict Restore

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:

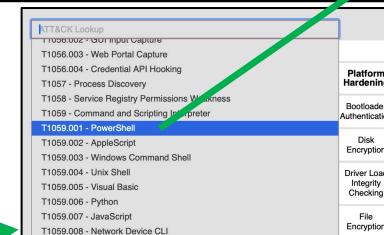
- **ATT&CK: T1059.001 – PowerShell** → **D3FEND: Execution Isolation, Script Blocking, Process Monitoring**

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: <ul style="list-style-type: none"> ✓ Crear reglas de detección alineadas a tácticas reales ✓ Mapear defensas existentes a amenazas relevantes ✓ Identificar huecos en la arquitectura defensiva 	Para arquitectos de seguridad: <ul style="list-style-type: none"> ✓ Diseñar defensas basadas en un estándar internacional ✓ Documentar controles de forma estructurada ✓ Justificar inversiones ante la dirección
Para Red Teams: <ul style="list-style-type: none"> ✓ Entender qué defensas van a activarse ✓ Planear ataques más realistas ✓ Simular APTs y validar eficacia defensiva 	Para formación: <ul style="list-style-type: none"> ✓ Explicar el “lado defensivo” de ATT&CK ✓ Construir laboratorios con roles Blue Team ✓ 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.

