



MITRE

ATT&CK

Background

Course

Ciberseguridad

Instructor

Acosta Bermejo Raúl

Lecture notes

2025-A

Febrero del 2025

Última actualización





Table of contents (outline)

Tabla de contenido

1. Introducción
2. MITRE ATT&CK
3. MITRE D3FEND





Conceptos Básicos

Definiciones

■





Introducción

Definiciones

- ❖ El MITRE es un centro de investigación y desarrollo con financiamiento federal de EU. Es el equivalente al CINVESTAV y los Centros CONACYT.
 - Fundado en 1958 (65 años) actualmente tiene 42 centros en diferentes estados.
- ❖ A lo largo de los años ha desarrollado varias propuestas que han sido mejoradas (versiones). Las más importantes son:



- ❖ URL
 - <https://mitre.org/>





MITRE ATT&CK

Framework

■





MITRE ATT&CK

Introducción

Ciclos de Vida del Adversario

1. Cyber Kill Chain
2. NIST CyberSecurity Framework (CSF)
3. MITRE ATT&CK

- ❖ ATT&CK.
 - **A**dversarial **T**actics **T**echniques & **C**ommon **K**nowledge
 - Es una base de conocimiento de tácticas de adversario y técnicas, todas obtenidas de observaciones del mundo real.
- ❖ Estructura de la base
 - Tres tipos de modelo (matrices):
Enterprise, Mobile, ICS (*Industrial Control Systems*, Ej. SCADA).
 - Tres elementos en cada matriz
TTP = **T**ácticas + **T**écnicas (sub-tec) + **P**rocedimientos
Objetivo Como
- ❖ URL
 - <https://attack.mitre.org/>





MITRE ATT&CK

Introducción

Las matrices están muy completas y se revisan y actualizan periódicamente.

Matriz	Tácticas	Técnicas	Otros elementos
Enterprise	14	235 435 Sub-técnicas	Software: 794 Data sources: 37 Mitigations: 43 Assets: 14 Grups: 152 Campaigns: 28
Mobile	12	86	
ICS	12	94	

Cada técnica incluye:

1. Una descripción de la técnica.
2. Una o varias sub-técnicas relacionadas.
3. Tácticas de mitigación.
4. Tácticas de detección.
5. Metadatos relacionados para propósitos de indexación.
6. Referencias a incidentes reales.





MITRE ATT&CK

Ejemplo de matriz

Tácticas

Técnicas

ATT&CK Matrix for Enterprise

layout: flat show sub-techniques hide sub-techniques

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	13 techniques	19 techniques	13 techniques	42 techniques	17 techniques	30 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (3) Gather Victim Host Information (4) Gather Victim Identity Information (3) Gather Victim Network Information (6) Gather Victim Org Information (4) Phishing for Information (3) Search Closed Sources (2) Search Open Technical Databases (3) Search Open Websites/Domains (3) Search Victim-Owned Websites	Acquire Infrastructure (7) Compromise Accounts (3) Compromise Infrastructure (7) Develop Capabilities (4) Establish Accounts (3) Obtain Capabilities (6) Stage Capabilities (6) Valid Accounts (4)	Drive-by Compromise Exploit Public-Facing Application External Remote Services Hardware Additions Phishing (3) Replication Through Removable Media Supply Chain Compromise (3) Trusted Relationship Valid Accounts (4)	Command and Scripting Interpreter (8) Container Administration Command Deploy Container Exploitation for Client Execution Inter-Process Communication (3) Native API Scheduled Task/Job (5) Serverless Execution Shared Modules Software Deployment Tools System Services (2) User Execution (3) Windows Management Instrumentation	Account Manipulation (3) BITS Jobs Boot or Logon Autostart Execution (14) Boot or Logon Initialization Scripts (5) Browser Extensions Compromise Client Software Binary Create Account (3) Create or Modify System Process (4) Event Triggered Execution (16) External Remote Services Hijack Execution Flow (12) Implant Internal Image Modify Authentication Process (7) Office Application Startup (6) Pre-OS Boot (5) Scheduled Task/Job (5) Server Software Component (5) Traffic Signaling (2) Valid Accounts (4)	Abuse Elevation Control Mechanism (4) Access Token Manipulation (5) Boot or Logon Autostart Execution (14) Boot or Logon Initialization Scripts (5) Create or Modify System Process (4) Domain Policy Modification (2) Escape to Host Event Triggered Execution (16) Exploitation for Privilege Escalation Hijack Execution Flow (12) Process Injection (12) Scheduled Task/Job (5) Valid Accounts (4)	Abuse Elevation Control Mechanism (4) Access Token Manipulation (5) BITS Jobs Build Image on Host Debugger Evasion Deobfuscate/Decode Files or Information Deploy Container Direct Volume Access Domain Policy Modification (2) Execution Guardrails (1) Exploitation for Defense Evasion File and Directory Permissions Modification (2) Hide Artifacts (10) Hijack Execution Flow (12) Impair Defenses (9) Indicator Removal (9) Indirect Command Execution Masquerading (7) Modify Authentication Process (7) Modify Cloud Compute Infrastructure (4) Modify Registry Modify System Image (2) Network Boundary Bridging (1) Obfuscated Files or Information (9)	Adversary-in-the-Middle (3) Brute Force (4) Credentials from Password Stores (3) Exploitation for Credential Access Forced Authentication Forge Web Credentials (2) Input Capture (4) Modify Authentication Process (7) Multi-Factor Authentication Interception Multi-Factor Authentication Request Generation Network Sniffing OS Credential Dumping (8) Steal Application Access Token Steal or Forge Authentication Certificates Steal or Forge Kerberos Tickets (4) Steal Web Session Cookie Unsecured Credentials (7)	Application Window Discovery Browser Bookmark Discovery Cloud Infrastructure Discovery Cloud Service Dashboard Cloud Service Discovery Cloud Storage Object Discovery Container and Resource Discovery Debugger Evasion Domain Trust Discovery File and Directory Discovery Group Policy Discovery Network Service Discovery Network Share Discovery Network Sniffing Password Policy Discovery Peripheral Device Discovery Permission Groups Discovery (3) Process Discovery Query Registry Remote System Discovery Software Discovery (1) System Information Discovery System Location Discovery (1) System Network Configuration Discovery (1)	Exploitation of Remote Services Internal Spearphishing Lateral Tool Transfer Remote Service Session Hijacking (2) Remote Services (6) Replication Through Removable Media Software Deployment Tools Taint Shared Content Use Alternate Authentication Material (4)	Adversary-in-the-Middle (3) Archive Collected Data (3) Audio Capture Automated Collection Browser Session Hijacking Clipboard Data Data from Cloud Storage Data from Configuration Repository (2) Data from Information Repositories (3) Data from Local System Data from Network Shared Drive Data from Removable Media Data Staged (2) Email Collection (3) Input Capture (4) Screen Capture Video Capture	Application Layer Protocol (4) Communication Through Removable Media Data Encoding (2) Data Obfuscation (3) Dynamic Resolution (3) Encrypted Channel (2) Fallback Channels Ingress Tool Transfer Multi-Stage Channels Non-Application Layer Protocol Non-Standard Port Protocol Tunneling Proxy (4) Remote Access Software Signal Signaling (2) Web Service (3)	Automated Exfiltration (1) Data Transfer Size Limits Exfiltration Over Alternative Protocol (3) Exfiltration Over C2 Channel Exfiltration Over Other Network Medium (1) Exfiltration Over Physical Medium (1) Exfiltration Over Web Service (2) Scheduled Transfer Transfer Data to Cloud Account	Account Access Removal Data Destruction Data Encrypted for Impact Data Manipulation (3) Defacement (2) Endpoint Denial of Service (4) Firmware Corruption Inhibit System Recovery Network Denial of Service (2) Resource Hijacking Service Stop System Shutdown/Reboot



MITRE ATT&CK

Introducción

Clasificación jerárquica

Deobfuscate/Decode Files or Inf

Adversaries may use [Obfuscated Files or Information](#) to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system.

One such example is use of [certutil](#) to decode a remote access tool portable executable file that has been hidden inside a certificate file. ^[1]

Another example is using the Windows `copy /b` command to reassemble binary fragments into a malicious payload. ^[2]

Defense Evasion

40 techniques

Abuse Elevation
Control Mechanism (4)

Setuid and Setgid

Bypass User Account Control

Sudo and Sudo Caching

Elevated Execution with Prompt

Access Token
Manipulation (5)

Token Impersonation/Theft

Create Process with Token

Make and Impersonate Token

Parent PID Spoofing

SID-History Injection

BITS Jobs

Build Image on Host

Deobfuscate/Decode
Files or Information

Deploy Container

Direct Volume Access

Domain Policy
Modification (2)

Group Policy Modification

Domain Trust Modification

Execution
Guardrails (1)

Environmental Keying



MITRE ATT&CK

Introducción

Ejemplo de Técnica

Procedimientos
Son descripciones
de incidentes reales

ATT&CK v12 is now live! [Check out the updates here](#)

Home > Techniques > Enterprise > Use Alternate Authentication Material

Use Alternate Authentication Material

Sub-techniques (4)

Adversaries may use alternate authentication material, such as password hashes, Kerberos tickets, and application access tokens, in order to move laterally within an environment and bypass normal system access controls.

Authentication processes generally require a valid identity (e.g., username) along with one or more authentication factors (e.g., password, pin, physical smart card, token generator, etc.). Alternate authentication material is legitimately generated by systems after a user or application successfully authenticates by providing a valid identity and the required authentication factor(s). Alternate authentication material may also be generated during the identity creation process.^{[1][2]}

Caching alternate authentication material allows the system to verify an identity has successfully authenticated without asking the user to reenter authentication factor(s). Because the alternate authentication must be maintained by the system—either in memory or on disk—it may be at risk of being stolen through [Credential Access](#) techniques. By stealing alternate authentication material, adversaries are able to bypass system access controls and authenticate to systems without knowing the plaintext password or any additional authentication factors.

Procedure Examples

ID	Name	Description
G0016	APT29	APT29 used forged SAML tokens that allowed the actors to impersonate users and bypass MFA, enabling APT29 to access enterprise cloud applications and services. ^{[3][4]}
S0661	FoggyWeb	FoggyWeb can allow abuse of a compromised AD FS server's SAML token. ^[5]

Mitigations

Identificadores
Para técnicas y sub-técnicas

ID: T1550
Sub-techniques: [T1550.001](#), [T1550.002](#), [T1550.003](#), [T1550.004](#)
① Tactics: [Defense Evasion](#), [Lateral Movement](#)
① Platforms: [Containers](#), [Google Workspace](#), [IaaS](#), [Office 365](#), [SaaS](#), [Windows](#)
① Defense Bypassed: [System Access Controls](#)
Version: 1.2
Created: 30 January 2020
Last Modified: 01 April 2022
[Version](#) [Permalink](#)

Tácticas asociadas
Note que pueden ser múltiples



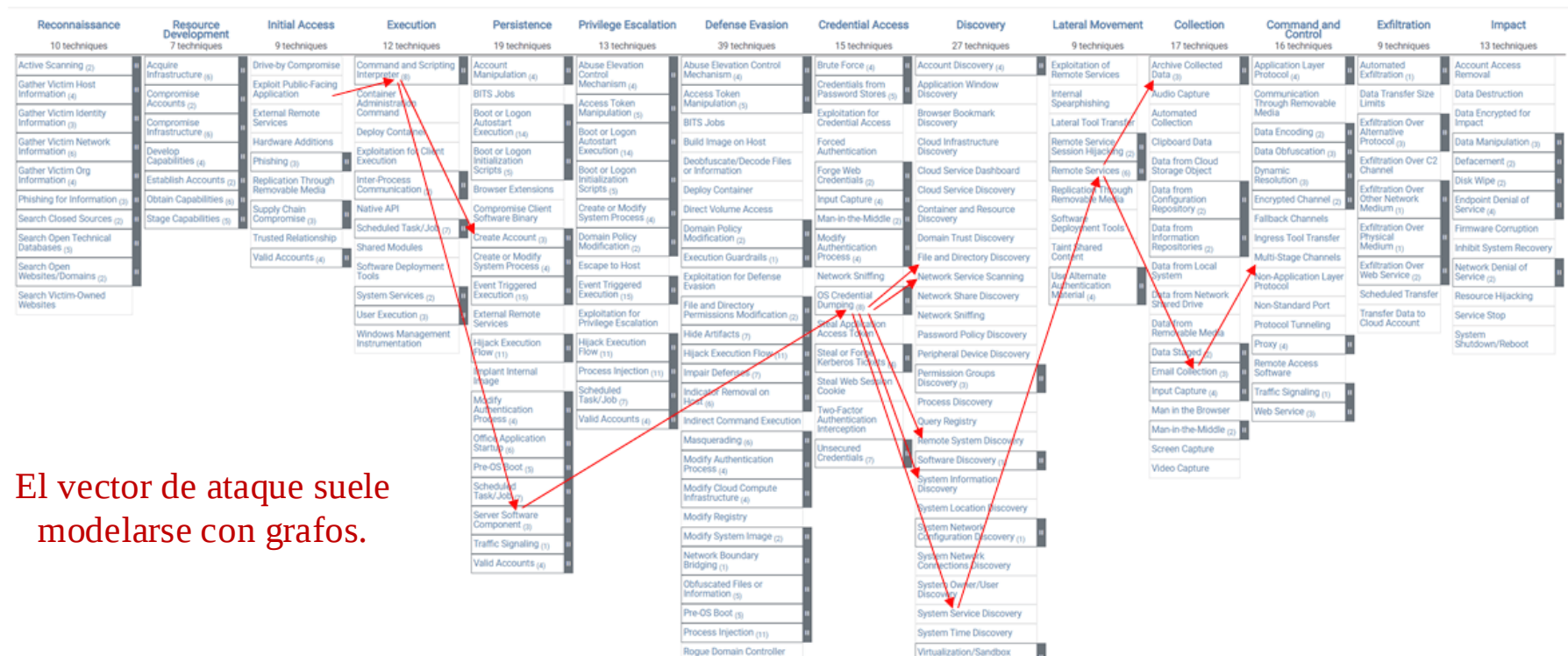
MITRE ATT&CK

Intro

Attack Vector

It is a method that a hacker uses to gain unauthorized access to a computer system, network, or application.

Un Vector de Ataque es la ejecución de múltiples TTPs realizados tanto en secuencia como en paralelo.



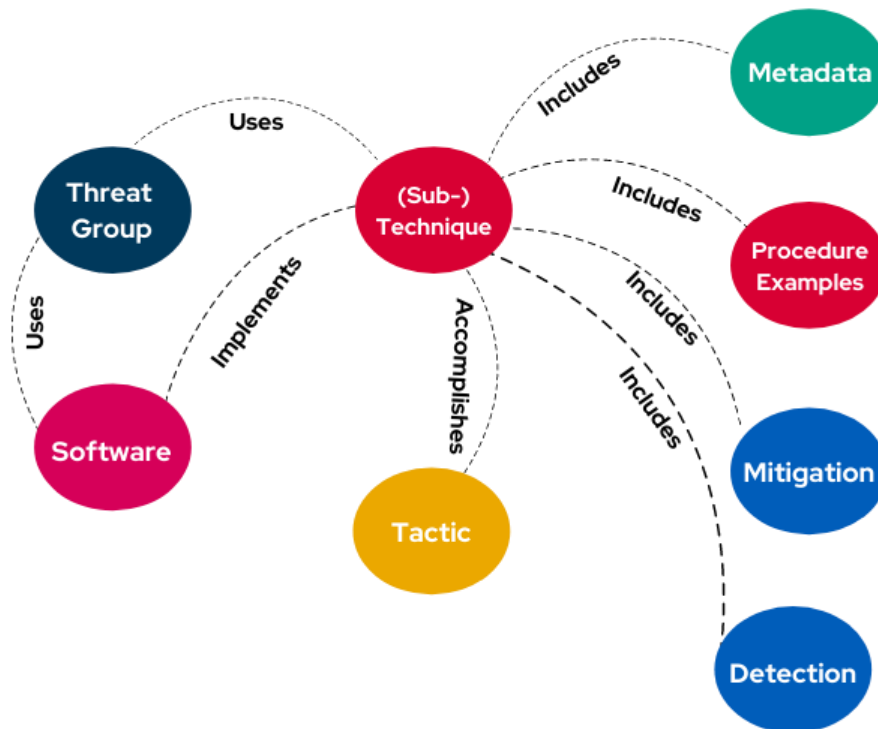
El vector de ataque suele modelarse con grafos.



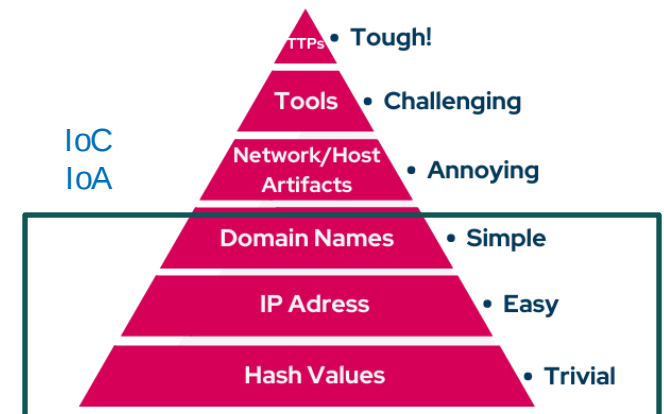
MITRE ATT&CK

Introducción

Fuente: <https://www.picussecurity.com/mitre-attack-framework-beginners-guide>



The Pyramid of Pain (David Bianco, 2013)



IoC (Indicators of Compromise) **Violación**
IoA (Indicators of Attack) **Sospecha**



MITRE ATT&CK

Introducción

Cada matriz tiene subdominios de especialización que la hacen de aplicación específica:

1. Enterprise
 - i. **PRE**
 - ii. Windows
 - iii. macOS
 - iv. Linux
 - v. Cloud
- i. Mobile
 - i. Android
 - ii. iOS
- ii. ICS
 - i. No tiene

Como PREpararse para un ataque

No es un estándar estático y
periódicamente saca nuevas
versiones que pueden agregar
nuevas técnicas

La versión actual es:

V15.1

23 de abril de 2024





MITRE ATT&CK

Introducción

Id.	G0018.
Name	admin@338
Desc.	It is a China-based cyber threat group

Otros elementos

Grupos

- Son grupos de actividades que son rastreadas con un nombre en común.
- Los analistas rastrean estos grupos utilizando diversas metodologías analíticas y términos como grupos de amenazas, grupos de actividades y actores de amenazas.
- Algunos grupos tienen varios nombres asociados con actividades similares debido a que varias organizaciones rastrean actividades similares con diferentes nombres.
- Las definiciones de grupos de las organizaciones pueden superponerse parcialmente con los grupos designados por otras organizaciones y pueden diferir en una actividad específica.





MITRE ATT&CK

Introducción

Otros elementos

Campañas

- La comunidad de seguridad rastrea actividades de intrusión usando varias metodologías analíticas y términos tales como operaciones, conjunto de intrusiones, y campañas.
- Para el equipo de MITRE ATT&CK utiliza el término Campaña para describir cualquier agrupación de actividades de intrusión realizadas durante un **período de tiempo específico con objetivos y metas comunes**.

Id. C0034

Grupos asociados: G0034

Desc. 2022 Ukraine Electric Power Attack

Documento (82 pag.)

<https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf>





MITRE ATT&CK

Cyber Kill Chain vs MITRE ATT&CK

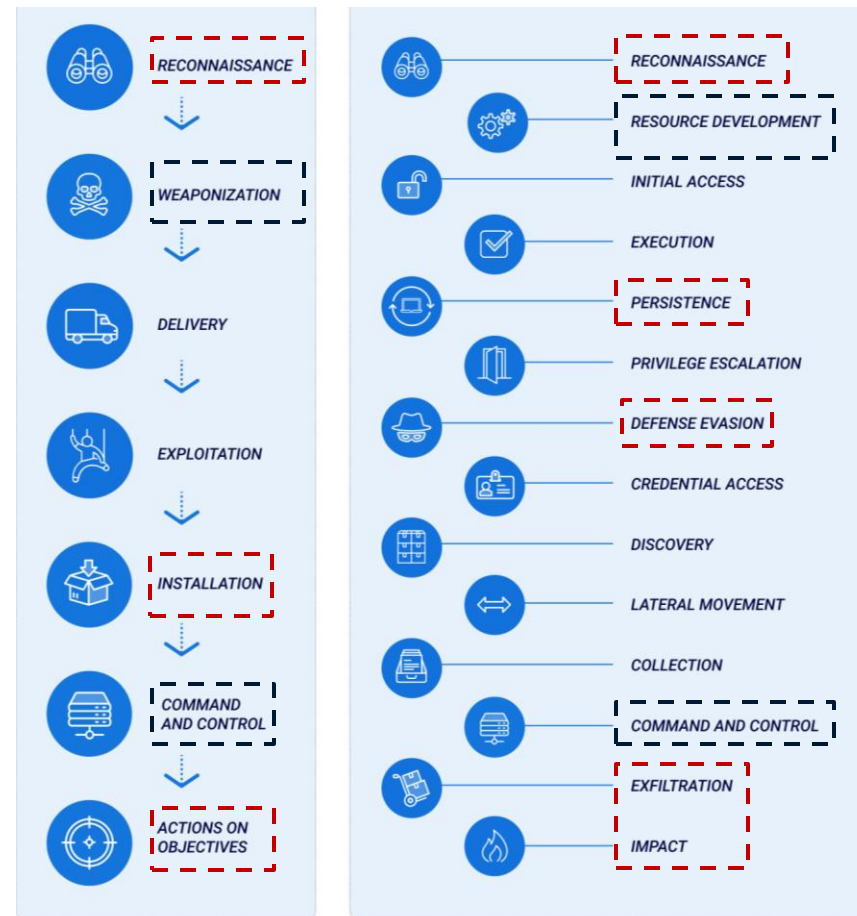
Cada framework tiene sus ventajas y desventajas.

CKC

- Simple
- Centro en la seguridad perimetral
- Mejor para identificar riesgos.

ATT&CK

- Detallado
- Bueno para implementar Políticas y Controles.
- Lenguaje común entre especialistas.



Casos de Uso

Intro

El MITRE ATT&CK se puede usar de varias formas y la siguiente lista enuncia las más comunes:

❖ Defensa

1. Para realizar un Análisis de la Seguridad
 1. Gestión de riesgos, *Hunting Threats*, etc.
2. Para mejorar las defensas
 - Construir una plataforma defensiva.
3. Para entrenar a un equipo **Blue**
 - Respuesta a incidentes

❖ Ataque

1. Para emular a un adversario.
2. Para entrenar a un equipo **Rojo**
 - *Pentesting* / Hacking ético





Casos de Uso

Intro

El MITRE ATT&CK se puede usar de varias formas y la siguiente lista enuncia las más comunes:

1. En el análisis de incidentes
2. En trabajos de investigación
 - <https://www.sciencedirect.com/science/article/pii/S2405959523000620#b19>
3. Evaluaciones de seguridad
4. Análisis de riesgos y creación de controles
 - Ejemplo para Kubernetes
 - <https://expel.com/mitre-attack-in-kubernetes-toolkit/>

Varios ejemplos de uso:

- <https://www.picussecurity.com/mitre-attck>





Tools

Software

Las más conocidas

1. Navigator

- *It is a web-based tool for annotating and exploring ATT&CK matrices. It can be used to visualize defensive coverage, red/blue team planning, the frequency of detected techniques, and more.*
- URL: <https://mitre-attack.github.io/attack-navigator/>
<https://github.com/mitre-attack/attack-navigator>

2. Caldera

- *A Scalable, Automated Adversary Emulation Platform.*
- URL: <https://caldera.mitre.org/>
<https://caldera.readthedocs.io/en/latest/>

3. STIX

- Formato de intercambio de datos de ataque.





Tools

Software

Navigator

- Trabaja con capas (layers).
- Cada capa puede especificar un dominio tecnológico específico: matriz, sistema operativo, etc.

MITRE ATT&CK® Navigator

The ATT&CK Navigator is a web-based tool for annotating and exploring ATT&CK matrices. It can be used to visualize defensive coverage, red/blue team planning, the frequency of detected techniques, and more.

help changelog theme

Create New Layer

Create a new empty layer

Enterprise

Mobile

ICS

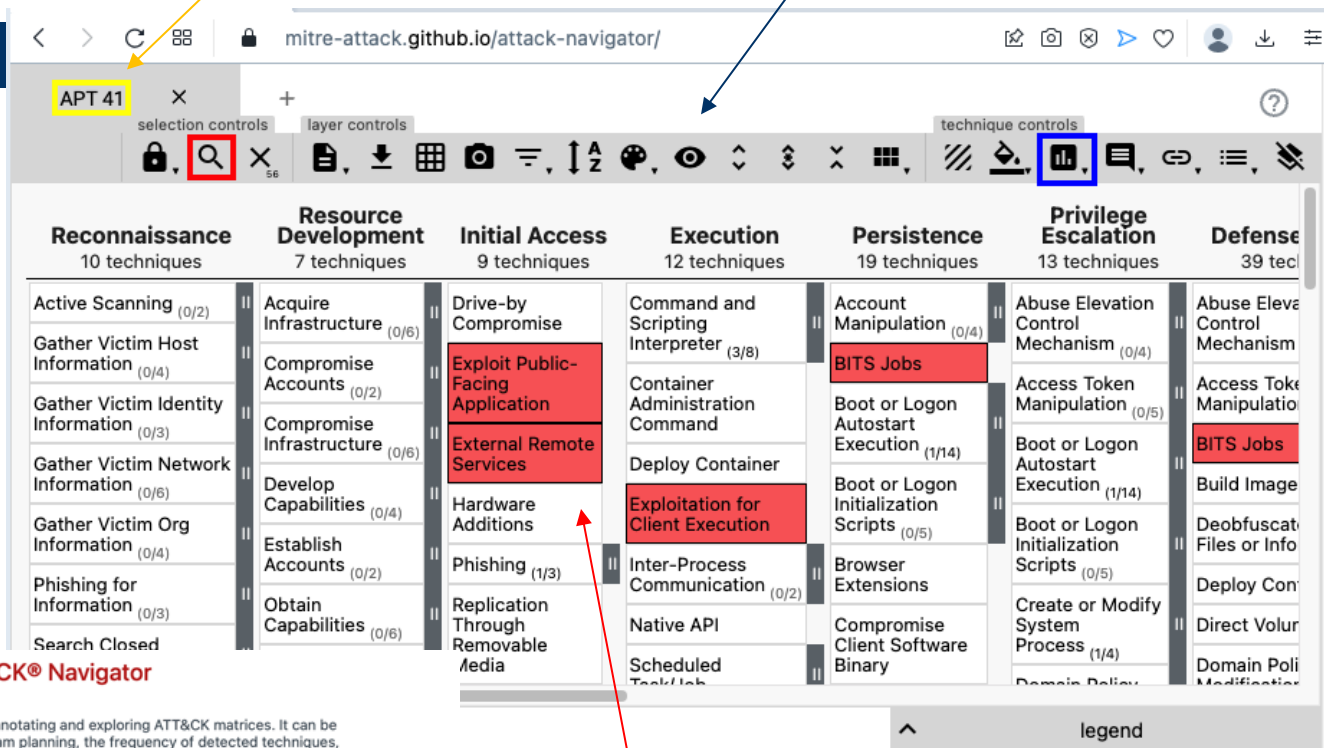
More Options

Layer

con nombre asignado

Controles

barra



Selección

Tácticas y Técnicas





Otras URLs

- <https://natasec.com/mitre-caldera-primeros-pasos/>
- <https://cyllab.be/blog/226/mitre-attck-in-practice-part-ii-caldera>

Tools

Software



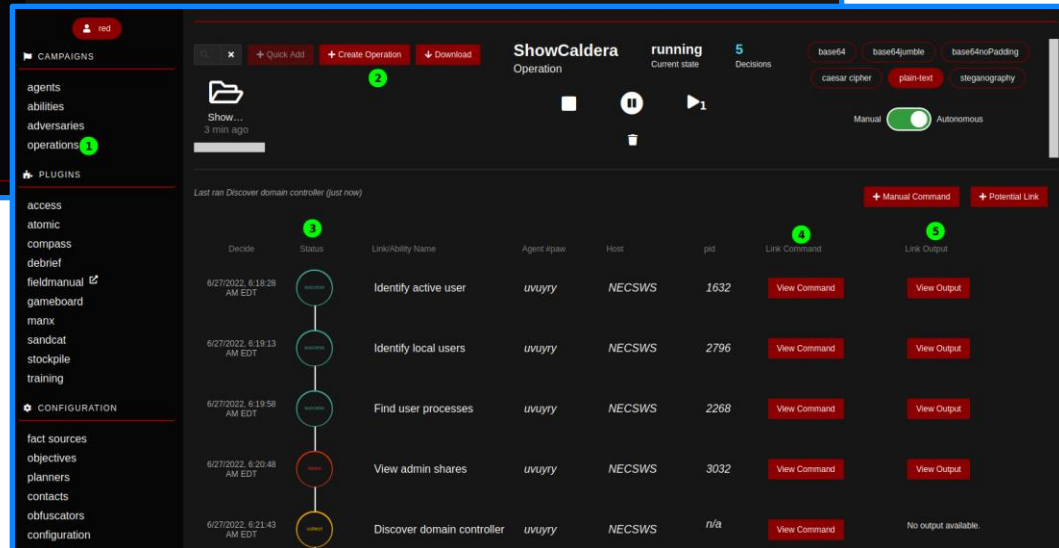
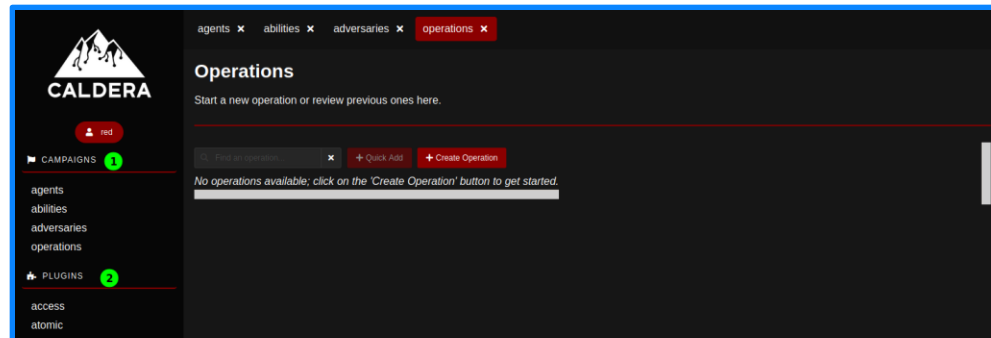
Caldera

Está formado por:

1. Servidor:
Web App + API rest.
2. Agentes.

Emula Ataques
Tutorial Español

<https://www.youtube.com/watch?v=QcjsMpgQOI&t>





Tools

Software

También se puede descargar la información en **Excel**.

<https://attack.mitre.org/resources/attack-data-and-tools/>

STIX

Información oficial del sitio:

1. *Structured Threat Information Expression* (STIX™) is a language and serialization format used to exchange cyber threat intelligence (CTI). **JSON**
2. The ATT&CK dataset is available in STIX 2.0 and STIX 2.1.
3. Other presentations of this dataset, including the ATT&CK Navigator and this website, are built from the STIX data.
4. TAXII
 - i. The ATT&CK STIX data can also be accessed via the official ATT&CK TAXII™ server.
 - ii. *Trusted Automated Exchange of Intelligence Information* (TAXII) is an application protocol for exchanging CTI over HTTPS.
 - iii. The ATT&CK TAXII server provides API access to the ATT&CK STIX knowledge base.





Tools

Software

Otro tipo de herramientas

- ❖ Existen muchas herramientas comerciales y algunas gratuitas que basan su funcionamiento en el MITRE ATT&CK.
 - CrowdStrike: Falcon (EDR, *Endpoint Detection and Response*)
- ❖ Estas herramientas siempre inician con una idea/concepto clave que se prueba con un prototipo.
- ❖ Estas herramientas se pueden desarrollar a nivel Licenciatura o Posgrado.
 - *Automated generation of attack trees based on MITRE ATT&CK*
 - Trabajo Terminal de ESCOM, Andrés Nieves.
 - 24 de septiembre de 2024, <https://ccc.inaoep.mx/~cisma/>





Tools

Software

Ejemplos de uso del framework

- ❖ Atomic Red Team

- <https://atomicredteam.io/>

Muchos videos en internet

- <https://www.youtube.com/playlist?list=PL92eUXSF717XLqkiCitdSZSUijwdDsM20>





MITRE D3FEND

Framework

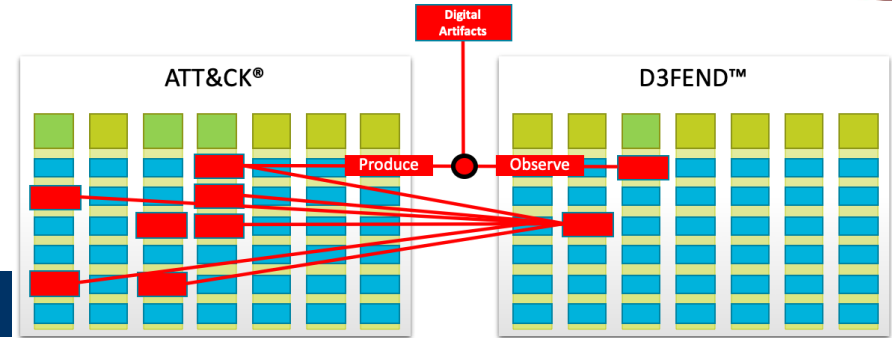
■





MITRE D3FEND

Introducción



- ❖ **In project work** for our sponsors, we have repeatedly encountered the need for a model that can precisely specify cybersecurity **countermeasure** components and capabilities. Furthermore, it is necessary that practitioners know not only what threats a capability claims to address, but specifically how those threats are addressed from an engineering perspective, and under what circumstances the solution would work. This knowledge is essential to estimate operational applicability, identify strengths and weaknesses, and develop enterprise solutions comprising multiple capabilities.
- ❖ To address this recurring need in the near-term, we created D3FEND, a **framework** in which we encode a **countermeasure** knowledge base, but more specifically, a **knowledge graph**. The graph contains semantically rigorous types and relations that define both the key concepts in the cybersecurity **countermeasure** domain and the relations necessary to link those concepts to each other. We ground each of the concepts and relations to particular references in the cybersecurity literature.
- ❖ URL
 - <https://d3fend.mitre.org/>





Introducción

27



The end

Contacto

Raúl Acosta Bermejo

<http://www.cic.ipn.mx>

<http://www.ciseg.cic.ipn.mx/>

racostab@ipn.mx

racosta@cic.ipn.mx

57-29-60-00

Ext. 56652

