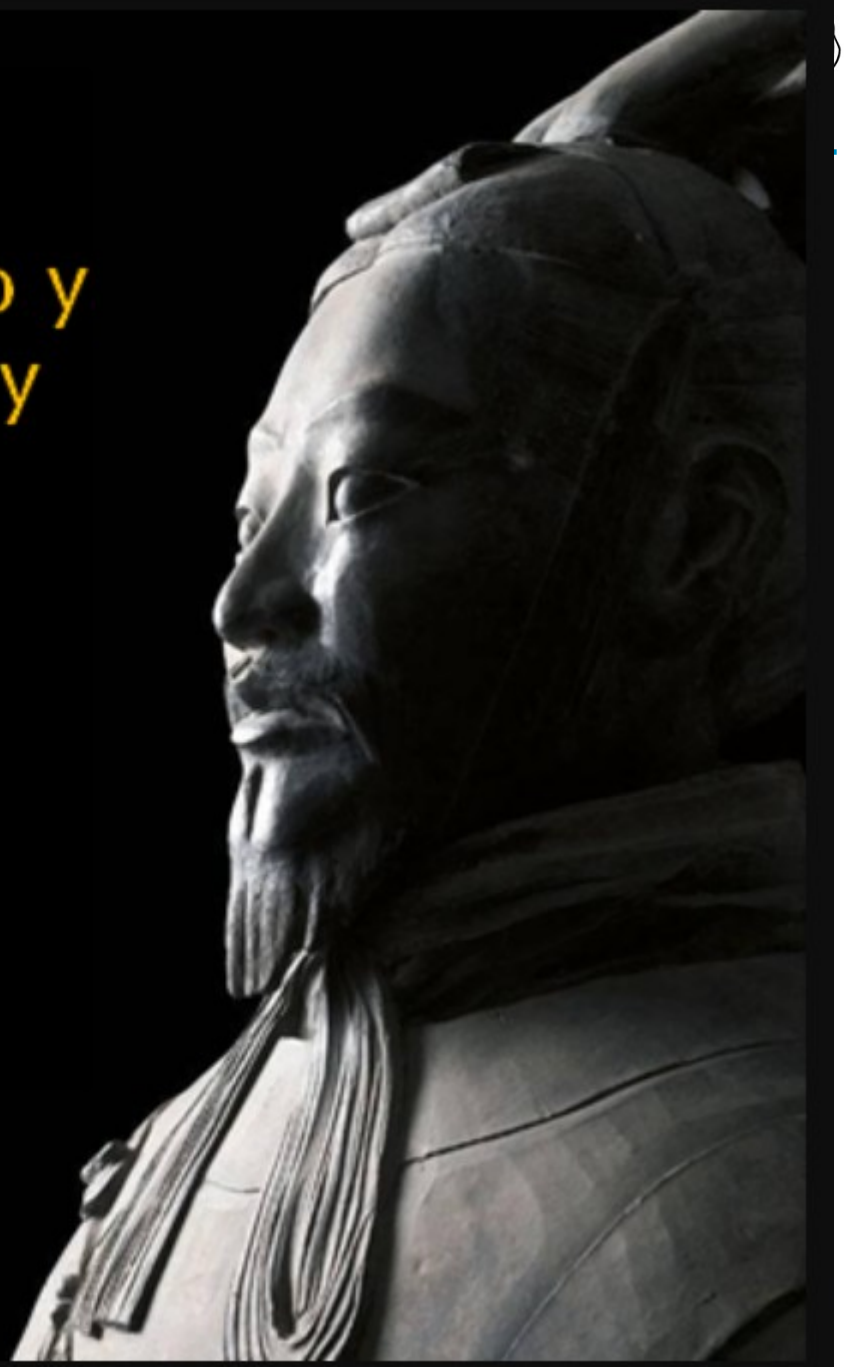
8636 Criptografía y Seguridad Informática

Modelado de Amenazas

“Conoce a tu enemigo y conócete a ti mismo, y saldrás triunfador en mil batallas”

— *Sun Tzu, "El Arte de la Guerra"*



Tactica y estrategia

La estrategia sin táctica es el camino más lento hacia la victoria. Las tácticas sin estrategia son el ruido antes de la derrota.

Sun Tzu

La estrategia es un patrón en una corriente de decisiones.

Henry Mintzberg

En la preparación para la batalla he encontrado que los planes son inútiles, pero la planificación es indispensable.

Dwight D. Eisenhower

Aunque los planes detallados pueden desmoronarse debido a la incertidumbre, la actitud de preparación y la comprensión cuidadosa de los objetivos y estrategias son fundamentales.

Proporcionan una base sólida y una estructura para la toma de decisiones en situaciones cambiantes y caóticas

El hombre de pensamiento que no va a actuar es ineficaz; el hombre de acción que no piensa es peligroso.

Richard M. Nixon

Es necesaria la seguridad????

HAY VULNERABILIDADES

NUESTRO SISTEMA VA A SER ATACADO

ALGÚN ATAQUE FUNCIONARÁ.

CADA DECISIÓN CAMBIA

EL NIVEL DE SEGURIDAD

DE NUESTRA APLICACIÓN

AUN SI NO TENEMOS EN CUENTA

SU SEGURIDAD EN LA DECISIÓN

https://www.argentina.gob.ar/sites/default/files/cbpdsp/consideraciones_importantes_para_la_seguridad_de_aplicaciones_guia_rapida__onti_v03_feb_2019.pdf

Agenda

- NIST.IR.8397 Directrices de Verificación de SW
- PASTA Metodologia iterativa
  - DFD diagrama de flujo de datos
  - CIA
  - STRIDE para la identificación de amenazas
  - DREAD para calcular el riesgo de una amenaza
  - Cyber Kill chain
  - CVE CWE Mitre ATT&CK
- Herramienta OWASP Threat Dragon
- Trabajo Practico de Modelado de Amenazas

Modelado de Amenazas de NIST

El NIST define al modelado de amenazas como

- Método que capta el funcionamiento del sistema para identificar y entender las amenazas potenciales, los objetivos y tácticas de los agentes de amenazas
- Para establecer controles de seguridad que permitan mitigarlos.

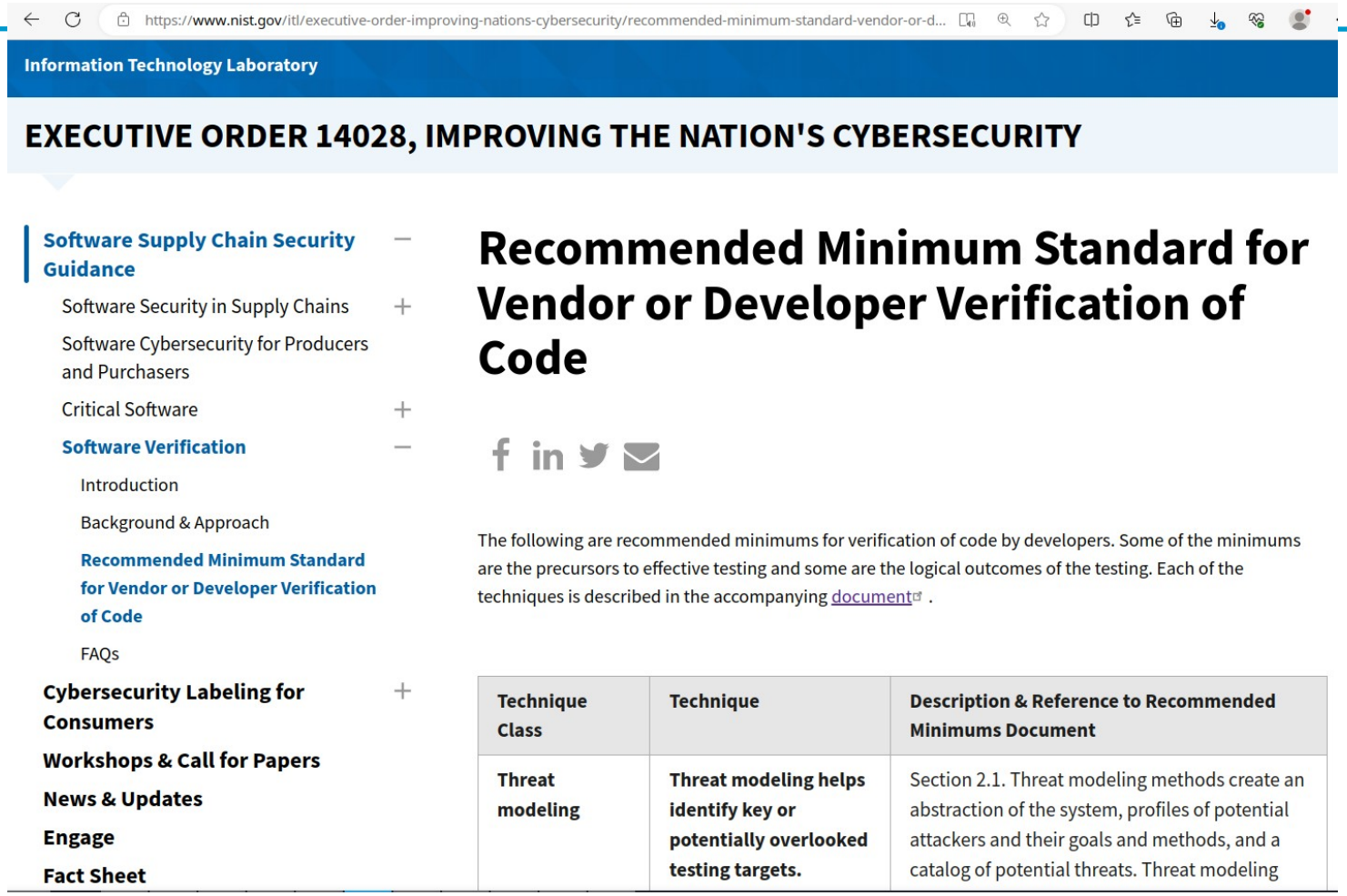
Con el propósito de captar la esencia del funcionamiento de un sistema

- Se suele analizar la arquitectura de la aplicación
- Realizar diagramas de flujo de datos que destaquen de manera granular cómo cada componente o servicio interactúa entre sí
- Analizar cuáles vulnerabilidades podrían ser aprovechadas por las amenazas

https://csrc.nist.gov/pubs/sp/800/154/ipd

https://cualesmi-ip.com/blog/nist-trae-el-modelado-de-amenazas-al-centro-de-atencion/

NIST.IR.8397 Directrices de Verificación de SW



https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8397.pdf

https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/recommended-minimum-standard-vendor-or-developer

NIST.IR.8397 Directrices de Verificación de SW

Tipo	Técnica
Modelado de amenazas	Ayuda a identificar objetivos clave o potencialmente pasados por alto para las pruebas o el diseño.
Pruebas automatizadas	A medida que las pruebas se automatizan, se pueden repetir con frecuencia, por ejemplo, en cada confirmación o antes de que se cierre un problema.
Análisis basado en código (estático)	Utilice un escáner de código para buscar los principales errores.
	Buscar credenciales y claves en el codigo.
Análisis dinámico (es decir, ejecutar el programa en casos de prueba):	Ejecutar con controles y protecciones integrados.
	Crear casos de prueba de "caja negra".
	Crear casos de prueba estructurales (core) basados en el código.
	Utilizar casos de prueba creados para atrapar errores que se tuvieron antes.
	Ejecutar un "fuzzer" (Herramienta para probar la resistencia del software a entradas inesperadas).
	Si el software puede estar conectado a Internet, ejecutar un escáner de aplicaciones web.
Verificar bibliotecas	Utilizar técnicas similares para asegurarse de que las bibliotecas, paquetes, servicios, etc. incluidos no sean menos seguros que su propio código.
Corregir errores	Corregir los errores críticos que se descubran.

Queremos responder:

¿En que estamos trabajando?

¿que modulos o partes forman mi sistema?

¿Qué puede ir mal?

¿Qué vamos a hacer al respecto?

¿Hicimos un trabajo suficientemente bueno?

https://cualesmi-ip.com/blog/nist-trae-el-modelado-de-amenazas-al-centro-de-atencion/

Algunos porque?

Ahorrar tiempo y dinero al encontrar y abordar las amenazas potenciales lo antes posible en un proyecto.

No tener que volver atrás para rediseñar y corregir vulnerabilidades cuando el “producto” está cerca de su implementación.

Proporciona un lenguaje de seguridad para los ingenieros que desean crear sistemas seguros

https://cualesmi-ip.com/blog/nist-trae-el-modelado-de-amenazas-al-centro-de-atencion/

Gestion del Riesgo

Enfoque: La gestión del riesgo se centra en identificar, evaluar y mitigar los riesgos de seguridad de una organización.

→ activos. Amenazas, vulnerabilidades y controles de seguridad que se evaluan en funcion del riesgo (probabilidad e impacto)

- Se centran en requisitos de cumplimiento (normativas,lo que debe ser) mitigando los riesgos.
- Y en Vulnerabilidades conocidas

De alguna manera se corre el foco de lo mas critico de una aplicacion o sistema que son **las amenazas** al mismo. Por ejemplo las mismas vulnerabilidades y normativas en dos arquitecturas u organizaciones diferentes pueden tener distintas amenazas...

Modelado de amenazas

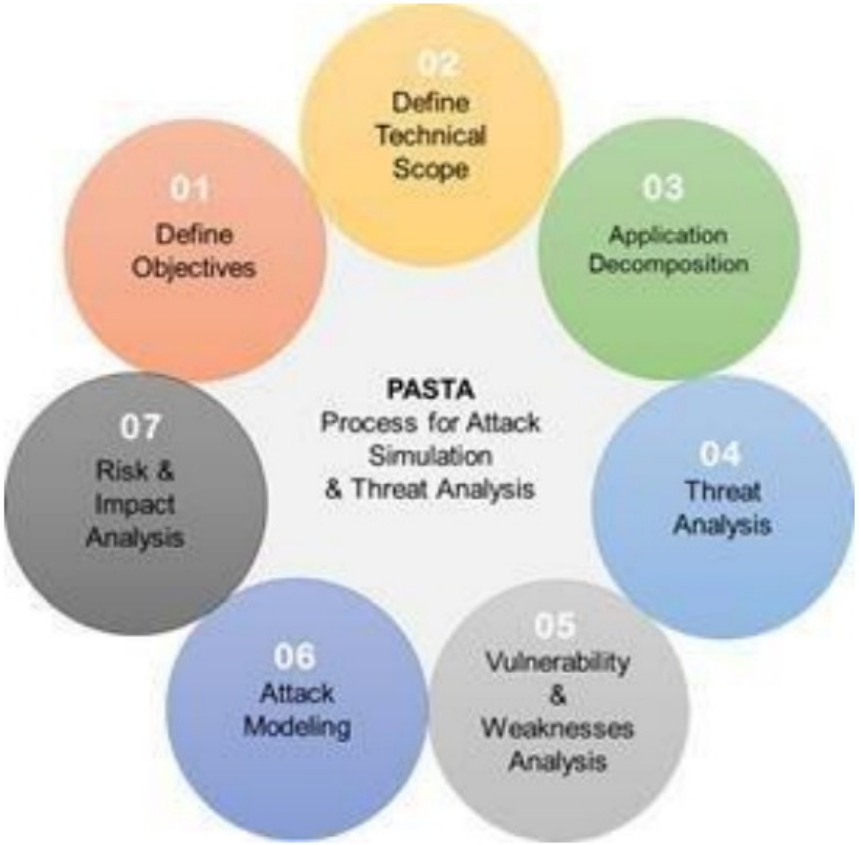
Enfoque: Se centra en comprender y modelar las amenazas específicas que pueden afectar a una aplicación, sistema o producto.

- **Identificación de amenazas**: Se identifican y documentan amenazas específicas que podrían explotar las vulnerabilidades en un sistema, generalmente a nivel de diseño y desarrollo.
- **Evaluación de amenazas**: Se evalúa cómo estas amenazas pueden explotar las vulnerabilidades y causar daño a un sistema o aplicación.
- **Diseño seguro**: A partir de la comprensión de las amenazas, se diseñan medidas de seguridad adecuadas para mitigar o prevenir las amenazas identificadas.

El profesional de seguridad aplicaran metodologias de gestion del riesgo.

Desarrolladores y Arquitectos de sistemas en general aplicaran metodologías de modelado de amenazas con el objetivo de crear sistemas mas seguros.

Fases del Modelo PASTA




1. Define Objectives
Identify Business Objectives
Identify Security and Compliance Requirements
Business Impact Analysis
2. Define Technical Scope
Capture the Boundaries of the Technical Environment
Capture Infrastructure | Application | Software Dependencies
3. Application Decomposition
Identify Use Cases | Define App. Entry Points & Trust Levels
Identify Actors | Assets | Services | Roles | Data Sources
Data Flow Diagramming (DFDs) | Trust Boundaries
4. Threat Analysis
Probabilistic Attack Scenarios Analysis
Regression Analysis on Security Events
Threat Intelligence Correlation and Analytics
5. Vulnerability & Weaknesses Analysis
Queries of Existing Vulnerability Reports & Issues Tracking
Threat to Existing Vulnerability Mapping Using Threat Trees
Design Flaw Analysis Using Use and Abuse Cases
Scorings (CVSS/CWSS) | Enumerations (CWE/CVE)
6. Attack Modeling
Attack Surface Analysis
Attack Tree Development | Attack Library Mgt.
Attack to Vulnerability & Exploit Analysis Using Attack Trees
7. Risk & Impact Analysis
Qualify & Quantify Business Impact
Countermeasure Identification and Residual Risk Analysis
ID Risk Mitigation Strategies

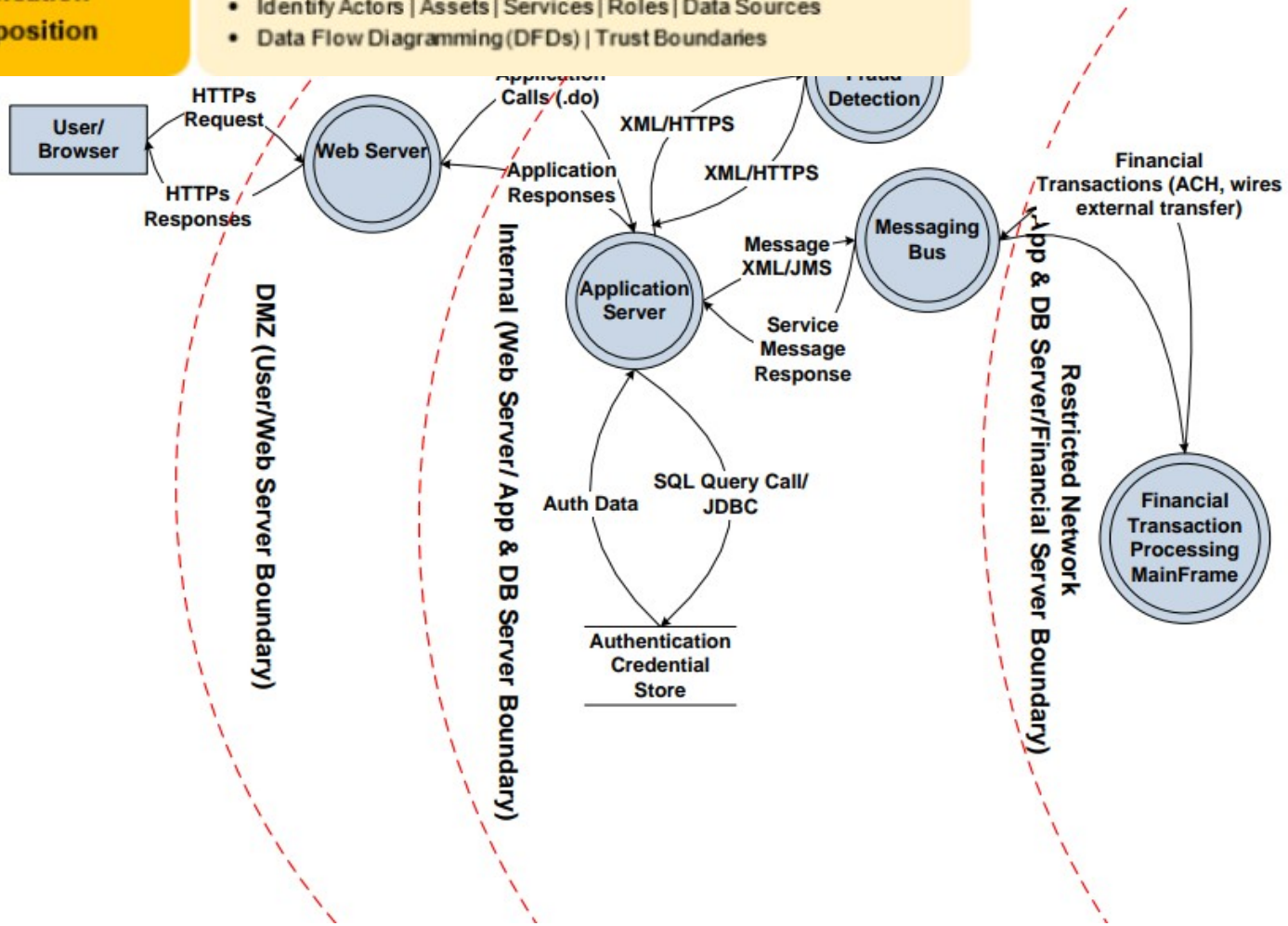
2. Define Technical Scope

- Capture the Boundaries of the Technical Environment
- Capture Infrastructure | Application | Software Dependencies

DFD

3. Application Decomposition

- Identify Use Cases | Define App. Entry Points & Trust Levels
- Identify Actors | Assets | Services | Roles | Data Sources
- Data Flow Diagramming (DFDs) | Trust Boundaries



4. Threat Analysis	• Probabilistic Attack Scenarios Analysis • Regression Analysis on Security Events • Threat Intelligence Correlation and Analytics
5. Vulnerability & Weaknesses Analysis	• Queries of Existing Vulnerability Reports & Issues Tracking • Threat to Existing Vulnerability Mapping Using Threat Trees • Design Flaw Analysis Using Use and Abuse Cases • Scorings (CVSS/CWSS) | Enumerations (CWE/CVE)
6. Attack Modeling	• Attack Surface Analysis • Attack Tree Development | Attack Library Mgt. • Attack to Vulnerability & Exploit Analysis Using Attack Trees
7. Risk & Impact Analysis	• Qualify & Quantify Business Impact • Countermeasure Identification and Residual Risk Analysis • ID Risk Mitigation Strategies

Pilares de la seguridad CIA

- Qué debe ser protegido?
- Por qué debe ser protegido?
- De qué debe ser protegido?
- Cómo protegerlo?

Categorizando una amenaza modelo STRIDE

Categoria	Dominio de Seguridad	Descripción
Spoofing	Autenticidad	Suplantar la identidad del usuario es decir intentar ser alguien que no es.
Tamperin g	Integridad	Intentar modificar los datos que se intercambian entre la aplicación y un usuario legítimo.
Repudiati on	No repudio	Denegación de acciones de un sistema de tal forma que no exista método de verificación alguno de que esto sucedió.
Informatio n Disclosure	Confidenciali dad	Exposición de información a personas que no deberían tener acceso.

https://learn.microsoft.com/en-us/archive/msdn-magazine/2006/november/uncover-security-design-flaws-using-the-stride-approach

Categorizando una amenaza modelo STRIDE

Categoria	Dominio de Seguridad	Descripción
Denial of service	Disponibilidad	Interrupción de un servicio a un usuario valido de la organización.
Elevation of Privileges	Autorización	Darle privilegios a un usuario que no debería tener ningún tipo de accesos, lo que en consecuencia provocaría que el sistema este en peligro a causa de las acciones que pudiera realizar este usuario

Evaluación del riesgo modelo DREAD

Herramienta cualitativa que depende de la interpretación del evaluador de seguridad

Tipo	Descripción
Damage	daño, impacto que tiene la explotación de la amenaza a causa de la vulnerabilidad
Reproducibility	Reproducción del incidente, probabilidad de repetirse el daño.
Exploitability	Explotación de la vulnerabilidad, que tan complejo es mitigarla y que costos están asociados a este proceso
Affected Users	Determinar el impacto de afectación del incidente, sobre qué cantidad de usuarios y recursos aplicados.
Discoverability	Grado de facilidad de exposición y descubrimiento de la vulnerabilidad

https://learn.microsoft.com/en-us/archive/blogs/david_leblanc/dreadful

Evaluación del riesgo modelo DREAD

Se evalua cada categoria con un valor de 0 a 10

El riesgo es la suma dividido 5

Tipo	Descripción
Damage	0 indica ningún daño y 10 representa una catastrofe
Reproducibility	0 indica que es muy difícil de explotar y 10 que es muy fácil
Exploitability	0 significa que es muy facil de mitigar, mientras que una puntuación alta (10) indica que es difícil de mitigar.
Affected Users	0 no afecta a ningún usuario, mientras que una puntuación alta (10) afecta a muchos usuarios o sistemas.
Discoverability	0 significa que es difícil de descubrir, mientras que una puntuación alta (10) indica que es muy fácil de detectar.

Mas preguntas a responder…

¿Cuales son los activos de valor a proteger?

- ¿En que estamos trabajando?

¿que modulos o partes forman mi sistema?

¿cuales son los apectos mas vulnerables?

¿Qué puede ir mal?

¿cuales son las principales amenazas que pueden afectarles?

- ¿Qué vamos a hacer al respecto?

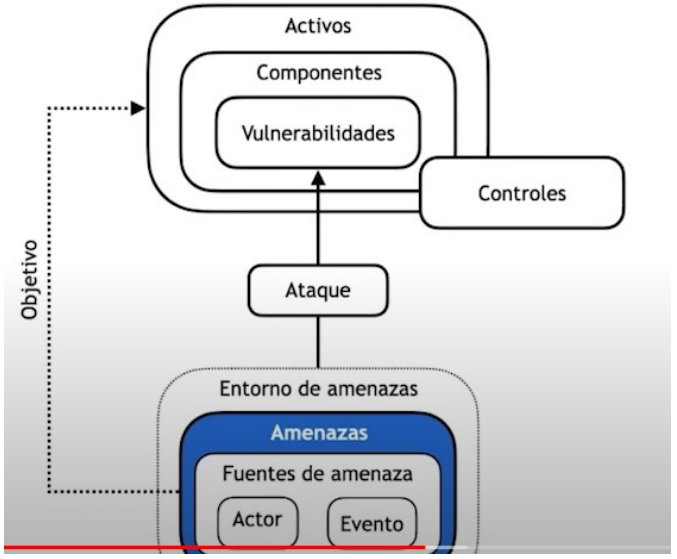
¿El analisis es completo, estamos pasando algo por alto?

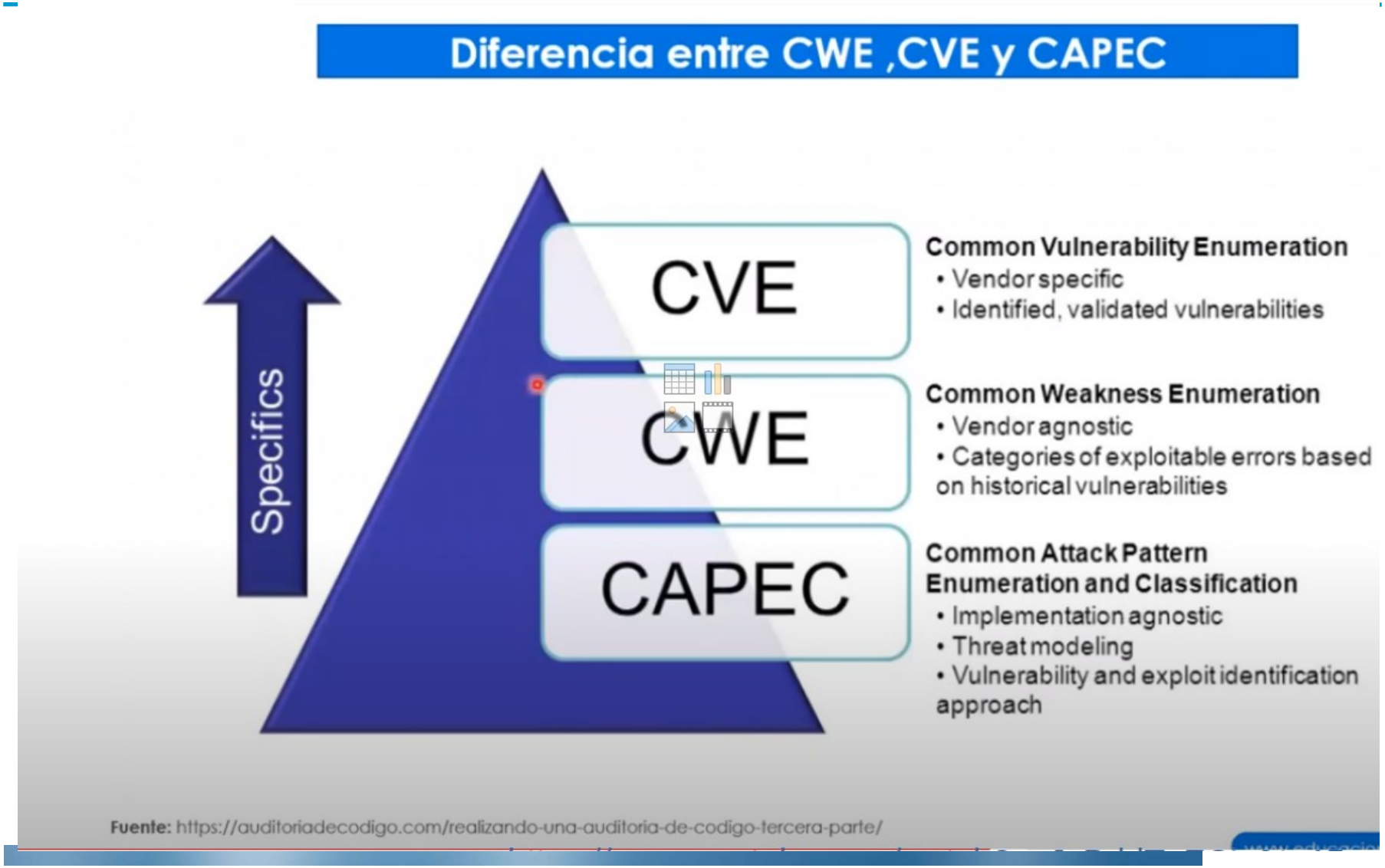
- ¿Hicimos un trabajo suficientemente bueno?

https://cualesmi-ip.com/blog/nist-trae-el-modelado-de-amenazas-al-centro-de-atencion/

Amenazas

Cualquier circunstancia o evento con el potencial de afectar negativamente las operaciones, activos de la organizacion o individuos por accesos no autorizados destruccion divulgación, alteración de la información y/o denegacion de servicio.





https://www.youtube.com/watch?v=JvBddTuFCic&t=15s

CVE => identificación de vulnerabilidades

CWE => la clasificación de debilidades

CAPEC => clasificación de patrones de ataque

CVSS => puntuación de la gravedad de las vulnerabilidades

MITRE CVE

Search Results

There are **1234** CVE Records that match your search.

Name	Description
CVE-2023-37973	Cross-Site Request Forgery (CSRF) vulnerability in David Pokorny Replace Word plugin <= 2.1 versions.
CVE-2023-31146	Vyper is a Pythonic smart contract language for the Ethereum virtual machine. Prior to version 0.3.8, during codegen, the length word of a dynarray is written before the data, which can result in out-of-bounds array acce in the case where the dynarray is on both the lhs and rhs of an assignment. The issue can cause data corrupti across call frames. The expected behavior is to revert due to out-of-bounds array access. Version 0.3.8 contai a patch for this issue.
CVE-2023-29335	Microsoft Word Security Feature Bypass Vulnerability

https://cve.mitre.org/cve/search_cve_list.html

Printer-Friendly Vi

CVE-ID	
CVE-2023-37973	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

Cross-Site Request Forgery (CSRF) vulnerability in David Pokorny Replace Word plugin <= 2.1 versions.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC:https://patchstack.com/database/vulnerability/replace-word/wordpress-replace-word-plugin-2-1-cross-site-request-forgery-csrf-vulnerability?_s_id=cve
- URL:https://patchstack.com/database/vulnerability/replace-word/wordpress-replace-word-plugin-2-1-cross-site-request-forgery-csrf-vulnerability?_s_id=cve

Assigning CNA

Patchstack OÜ

Date Record Created

20230711	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does n necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20230711)

CVE en la NVD

https://nvd.nist.gov/vuln/detail/CVE-2023-37973

An official website of the United States government Here's how you know

NIST

NVD MENU

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

NIST NATIONAL VULNERABILITY DATABASE NVD

VULNERABILITIES

CVE-2023-37973 Detail

Description

Cross-Site Request Forgery (CSRF) vulnerability in David Pokorny Replace Word plugin <= 2.1 versions.

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD	**Base Score:** 8.8 HIGH	**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
CNA: Patchstack	**Base Score:** 5.4 MEDIUM	**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: It is possible that the NVD CVSS may not match that of the CNA. The most common reason for this is that publicly available information does not provide sufficient detail or that information simply was not available at the time the CVSS vector string was assigned.

QUICK INFO

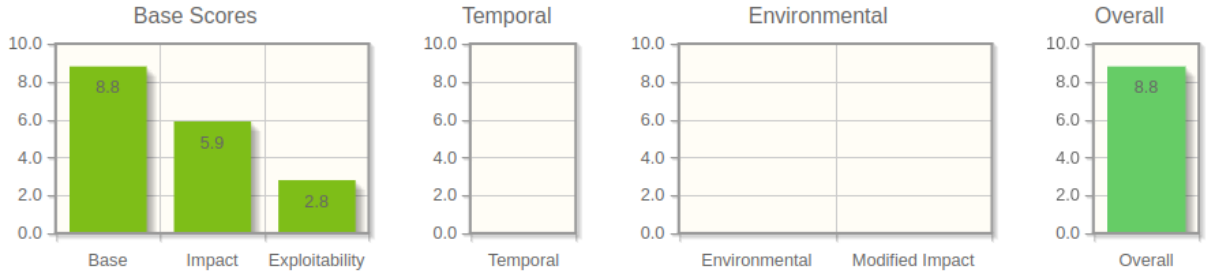
CVE Dictionary Entry:
CVE-2023-37973
NVD Published Date:
07/18/2023
NVD Last Modified:
07/25/2023
Source:
Patchstack

CVSS

https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?name=CVE-2023-37973&vector=AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H&version=3.1&source=NIST

Source: NIST

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.



CVSS Base Score: 8.8
Impact Subscore: 5.9
Exploitability Subscore: 2.8
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 8.8

Show Equations

CVSS v3.1 Vector
AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*
Network (AV:N) | Adjacent Network (AV:A) | Local (AV:L) | Physical (AV:P)

Attack Complexity (AC)*
Low (AC:L) | High (AC:H)

Privileges Required (PR)*
None (PR:N) | Low (PR:L) | High (PR:H)

User Interaction (UI)*
None (UI:N) | Required (UI:R)

Scope (S)*
Unchanged (S:U) | Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*
None (C:N) | Low (C:L) | High (C:H)

Integrity Impact (I)*
None (I:N) | Low (I:L) | High (I:H)

Availability Impact (A)*
None (A:N) | Low (A:L) | High (A:H)

https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

CWE - Common Weakness Enumeration

CWE-798: Use of Hard-coded Credentials

Weakness ID: 798
Abstraction: Base
Structure: Simple

View customized information: Conceptual | **Operational** | Mapping Friendly | Complete | Custom

For users who are interested in more notional aspects of a weakness. Example: educators, technical writers, and project/program managers.

Description

The product contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data.

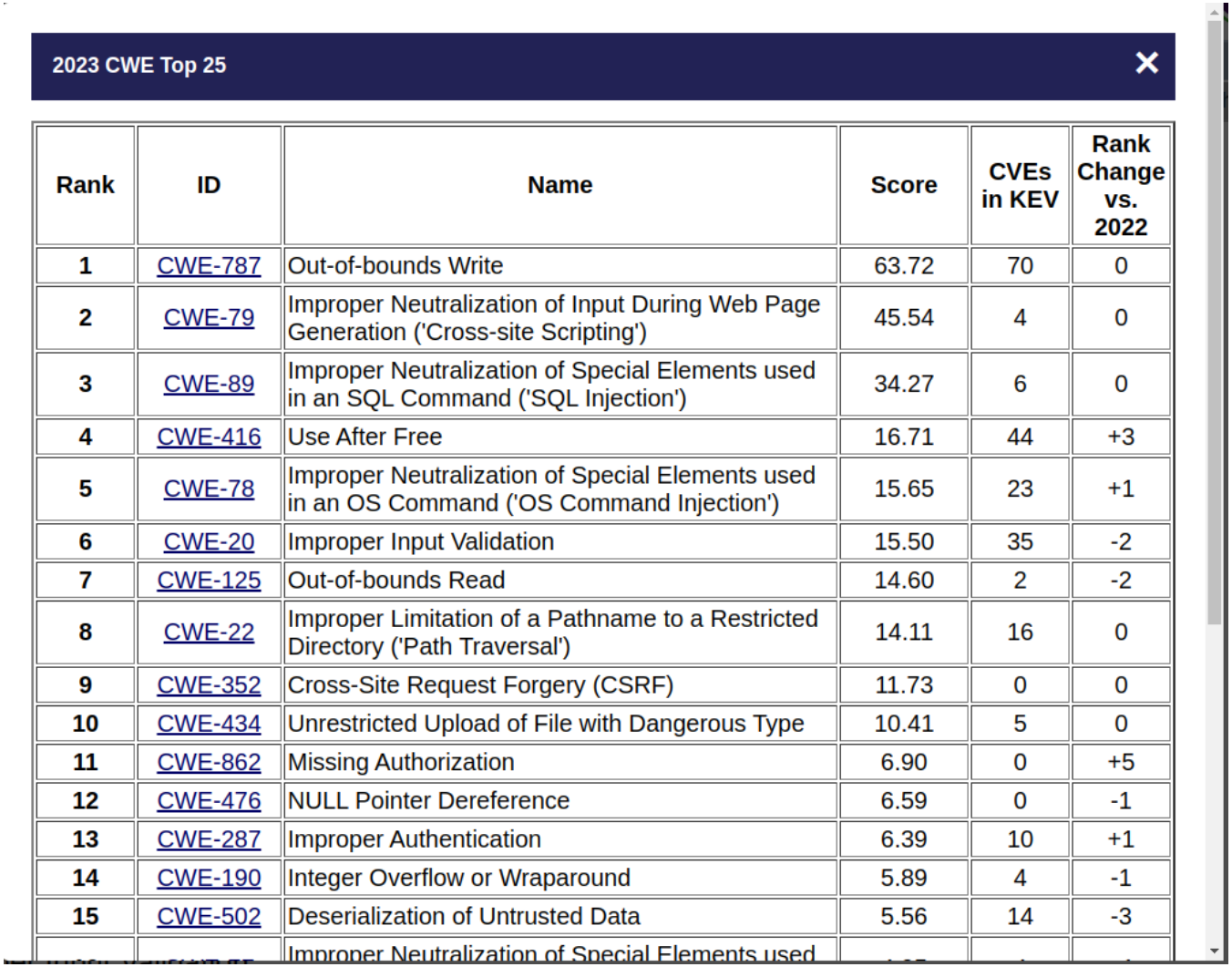
Example Language: **Java**

```
public boolean VerifyAdmin(String password) {
  if (password.equals("68af404b513073584c4b
    System.out.println("Entering Diagnostic Mod
    return true;
  }
  System.out.println("Incorrect Password!");
  return false;
```

Reference	Description
CVE-2022-29953	Condition Monitor firmware has a maintenance interface with hard-coded credential
CVE-2022-29960	Engineering Workstation uses hard-coded cryptographic keys that could allow for u
CVE-2022-29964	Distributed Control System (DCS) has hard-coded passwords for local shell access
CVE-2022-30997	Programmable Logic Controller (PLC) has a maintenance service that uses undocu
CVE-2022-30314	Firmware for a Safety Instrumented System (SIS) has hard-coded credentials for ac
CVE-2022-30271	Remote Terminal Unit (RTU) uses a hard-coded SSH private key that is likely to be
CVE-2021-37555	Telnet service for IoT feeder for dogs and cats has hard-coded password [REF-128
CVE-2012-3503	Installation script has a hard-coded secret token value, allowing attackers to bypass
CVE-2010-2772	SCADA system uses a hard-coded password to protect back-end database containi
CVE-2010-2073	FTP server library uses hard-coded usernames and passwords for three default acc
CVE-2010-1573	Chain: Router firmware uses hard-coded username and password for access to deb code
CVE-2008-2369	Server uses hard-coded authentication key
CVE-2008-0961	Backup product uses hard-coded username and password, allowing attackers to by
CVE-2008-1160	Security appliance uses hard-coded password allowing attackers to gain root acces
CVE-2006-7142	Drive encryption product stores hard-coded cryptographic keys for encrypted config
CVE-2005-3716	VoIP product uses hard-coded public credentials that cannot be changed, which allo
CVE-2005-3803	VoIP product uses hard coded public and private SNMP community strings that can sensitive information
CVE-2005-0496	Backup product contains hard-coded credentials that effectively serve as a back do system

https://cwe.mitre.org/data/definitions/798.html

CWE Top 25 Most Dangerous Software Weaknesses



2023 CWE Top 25

Rank	ID	Name	Score	CVEs in KEV	Rank Change vs. 2022
1	CWE-787	Out-of-bounds Write	63.72	70	0
2	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	45.54	4	0
3	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	34.27	6	0
4	CWE-416	Use After Free	16.71	44	+3
5	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	15.65	23	+1
6	CWE-20	Improper Input Validation	15.50	35	-2
7	CWE-125	Out-of-bounds Read	14.60	2	-2
8	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14.11	16	0
9	CWE-352	Cross-Site Request Forgery (CSRF)	11.73	0	0
10	CWE-434	Unrestricted Upload of File with Dangerous Type	10.41	5	0
11	CWE-862	Missing Authorization	6.90	0	+5
12	CWE-476	NULL Pointer Dereference	6.59	0	-1
13	CWE-287	Improper Authentication	6.39	10	+1
14	CWE-190	Integer Overflow or Wraparound	5.89	4	-1
15	CWE-502	Deserialization of Untrusted Data	5.56	14	-3
		Improper Neutralization of Special Elements used			

https://cwe.mitre.org/top25/archive/2023/2023_top25_list.html

CAPEC Patrones de Ataques comunes

1000 - Mechanisms of Attack

- Engage in Deceptive Interactions - *(156)*
- Abuse Existing Functionality - *(210)*
- Manipulate Data Structures - *(255)*
- Manipulate System Resources - *(262)*
- Inject Unexpected Items - *(152)*
- Employ Probabilistic Techniques - *(223)*
- Manipulate Timing and State - *(172)*
- Collect and Analyze Information - *(118)*
- Subvert Access Control - *(225)*

3000 - Domains of Attack

- Software - *(513)*
- Hardware - *(515)*
- Communications - *(512)*
- Supply Chain - *(437)*
- Social Engineering - *(403)*
- Physical Security - *(514)*

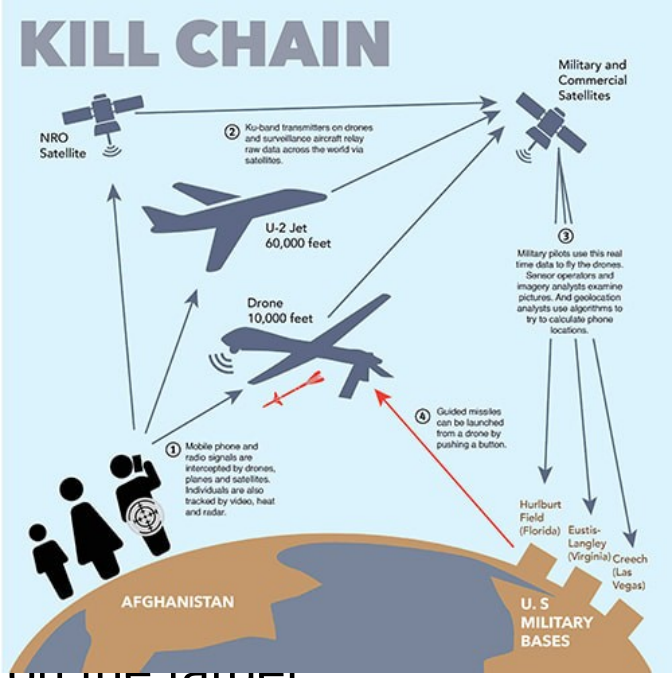
https://capec.mitre.org/data/definitions/3000.html

Kill chain

The term „kill chain” was originally used by the military, in the context of describing stages of attacks.

military kill chain framework, called “F2T2EA”,

consists of the following stages:



1. Find – identify the target,
2. Determine – determine the target’s location,
3. Route – monitor the target’s movement,
4. Target – choose an adequate measure to use on the target,
5. Implementation – use the chosen measure to conduct an attack,
6. Review – review the attack’s efficiency.

Cyber Kill C

En 2011, Lockheed M
aplicó la estructura
a la seguridad
de la información,

como un método para
realizar un ataque a u
red de información.

https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

https://seqred.pl/en/cyber-kill-chain-what-is-it-and-how-to-use-it-to-stop-advanced-methods-of-attack/

MITRE ATT&CK

- Documentar y trazar las tecnicas que usa un atacante en las distintas fases de un ciberataque para entrar a la red y filtrar información

- Matriz con Tacticas, Tecnicas y Procedimientos utilizados por los atacantes.

https://www.youtube.com/watch?v=qLL3RG1QERM

Network Matrix

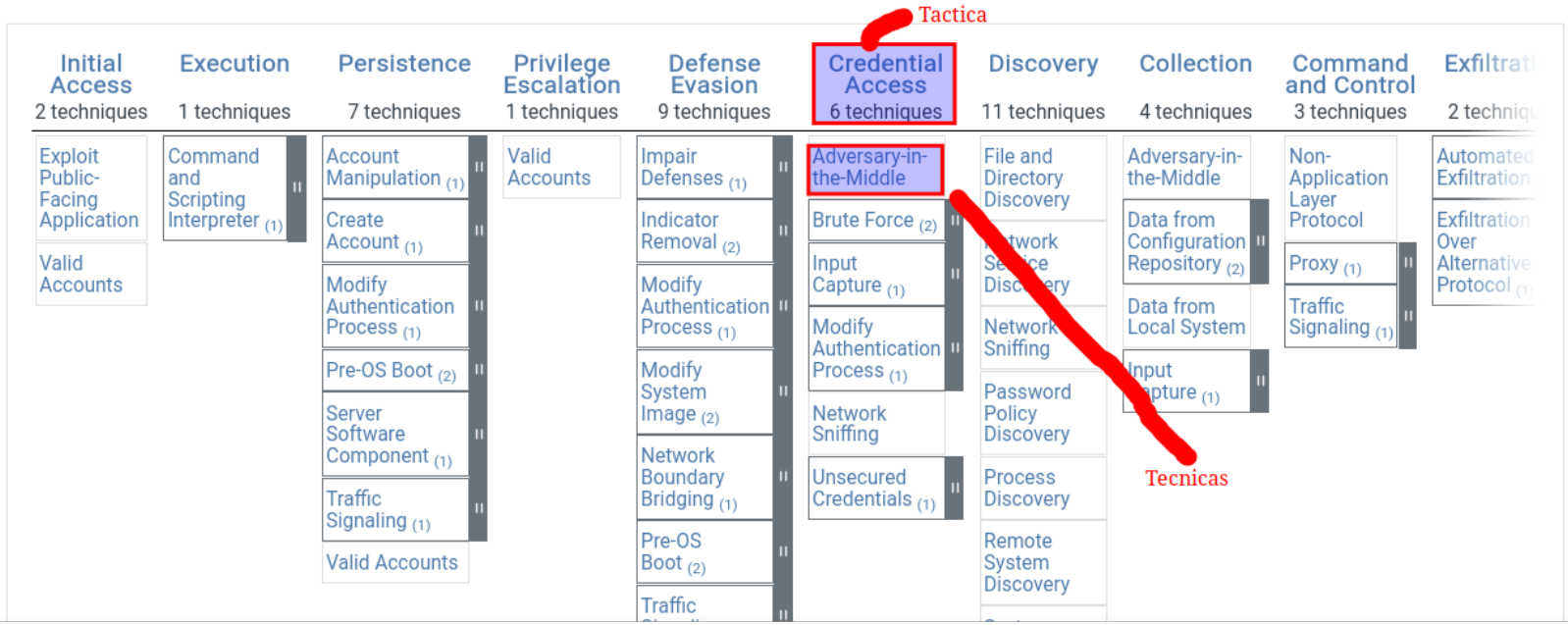
Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise covering techniques against network infrastructure devices. The Matrix contains information for the Network platform.

View on the ATT&CK® Navigator

Version Permalink

layout: side ▾

show sub-techniques | hide sub-techniques | help



https://attack.mitre.org/matrices/enterprise/network/

T1557 Adversary-in-the-Middle (1)

Adversary-in-the-Middle

Sub-techniques (3)

Adversaries may attempt to position themselves between two or more networked devices using an adversary-in-the-middle (AiTM) technique to support follow-on behaviors such as Network Sniffing or Transmitted Data Manipulation. By abusing features of common networking protocols that can determine the flow of network traffic (e.g. ARP, DNS, LLMNR, etc.), adversaries may force a device to communicate through an adversary controlled system so they can collect information or perform additional actions.[1]

Procedure Examples

ID	Name	Description
S0281	Dok	Dok proxies web traffic to potentially monitor and alter victim HTTP(S) traffic.[9][10]
G0094	Kimsuky	Kimsuky has used modified versions of PHProxy to examine web traffic between the website.[11]

https://attack.mitre.org/versions/v13/techniques/T1557/

T1557 Adversary-in-the-Middle (1)

Mitigations

ID	Mitigation	Description
M1042	Disable or Remove Feature or Program	Disable legacy network protocols that may be used to intercept network traffic if applicable, especially those that are not needed within an environment.
M1041	Encrypt Sensitive Information	Ensure that all wired and/or wireless traffic is encrypted appropriately. Use best practices for authentication protocols, such as Kerberos, and ensure web traffic that may contain credentials is protected by SSL/TLS.

at is not

Detection

ID	Data Source	Data Component	Detects
DS0015	Application Log	Application Log Content	Monitor application logs for changes to settings and other events associated with network protocols and other services commonly abused for AiTM.[12]
DS0029	Network Traffic	Network Traffic Content	Monitor network traffic for anomalies associated with known AiTM behavior.
		Network Traffic Flow	Monitor for network traffic originating from unknown/unexpected hardware devices. Local network traffic metadata (such as source MAC addressing) as well as usage of network management protocols such as DHCP may be helpful in identifying hardware.

https://attack.mitre.org/versions/v13/techniques/T1557/

Ejemplo de Procedimiento: “Dok”

Procedure Examples

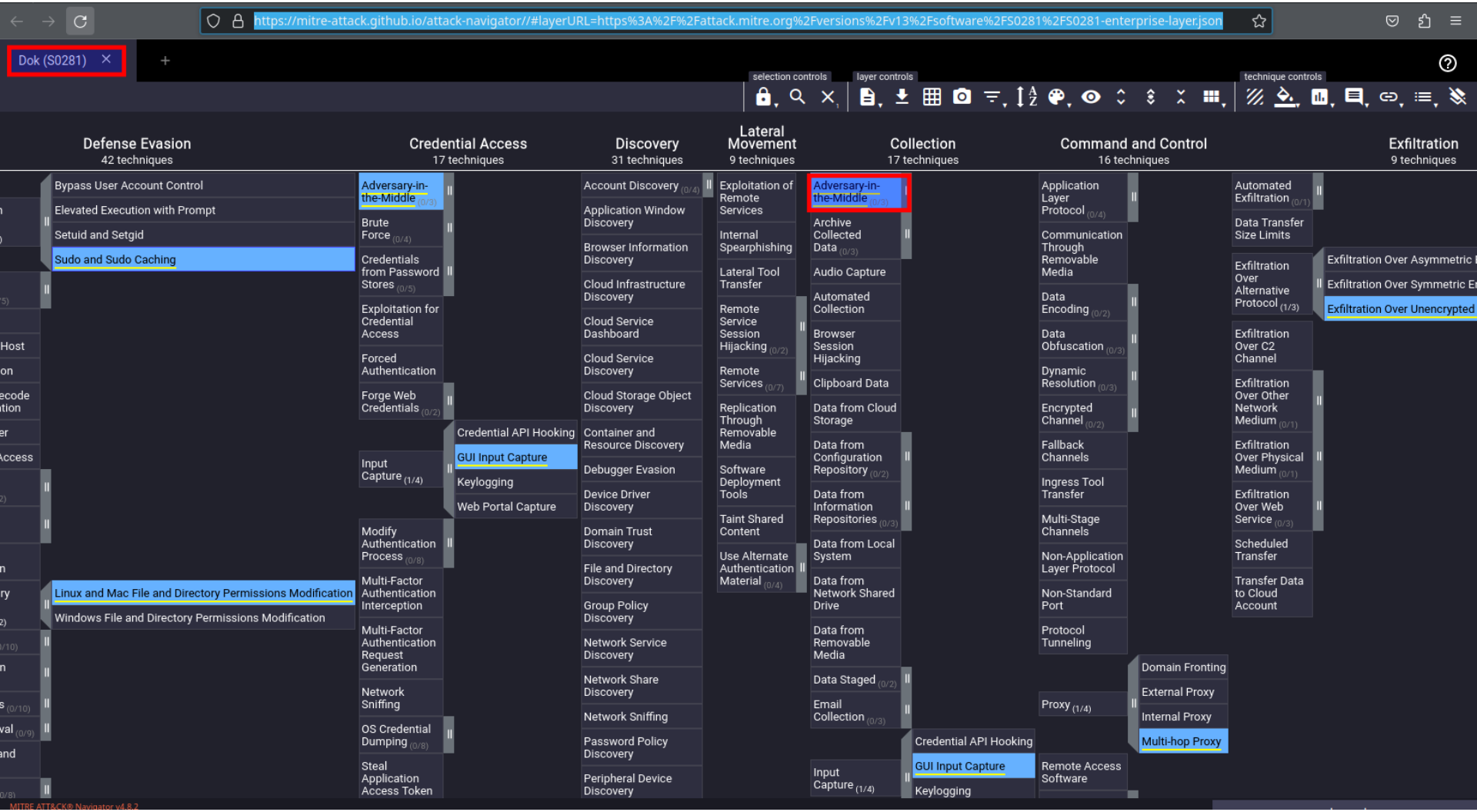
ID	Name	Description
S0281	Dok	Dok proxies web traffic to potentially monitor and alter victim HTTP(S) traffic.[9][10]
G0094	Kimsuky	Kimsuky has used modified versions of PHProxy to examine web traffic between the website.[11]

Dok

Dok is a Trojan application disguised as a .zip file that is able to collect user credentials and install a malicious proxy server to redirect a user's network traffic (i.e. Adversary-in-the-Middle).[1][2][3]

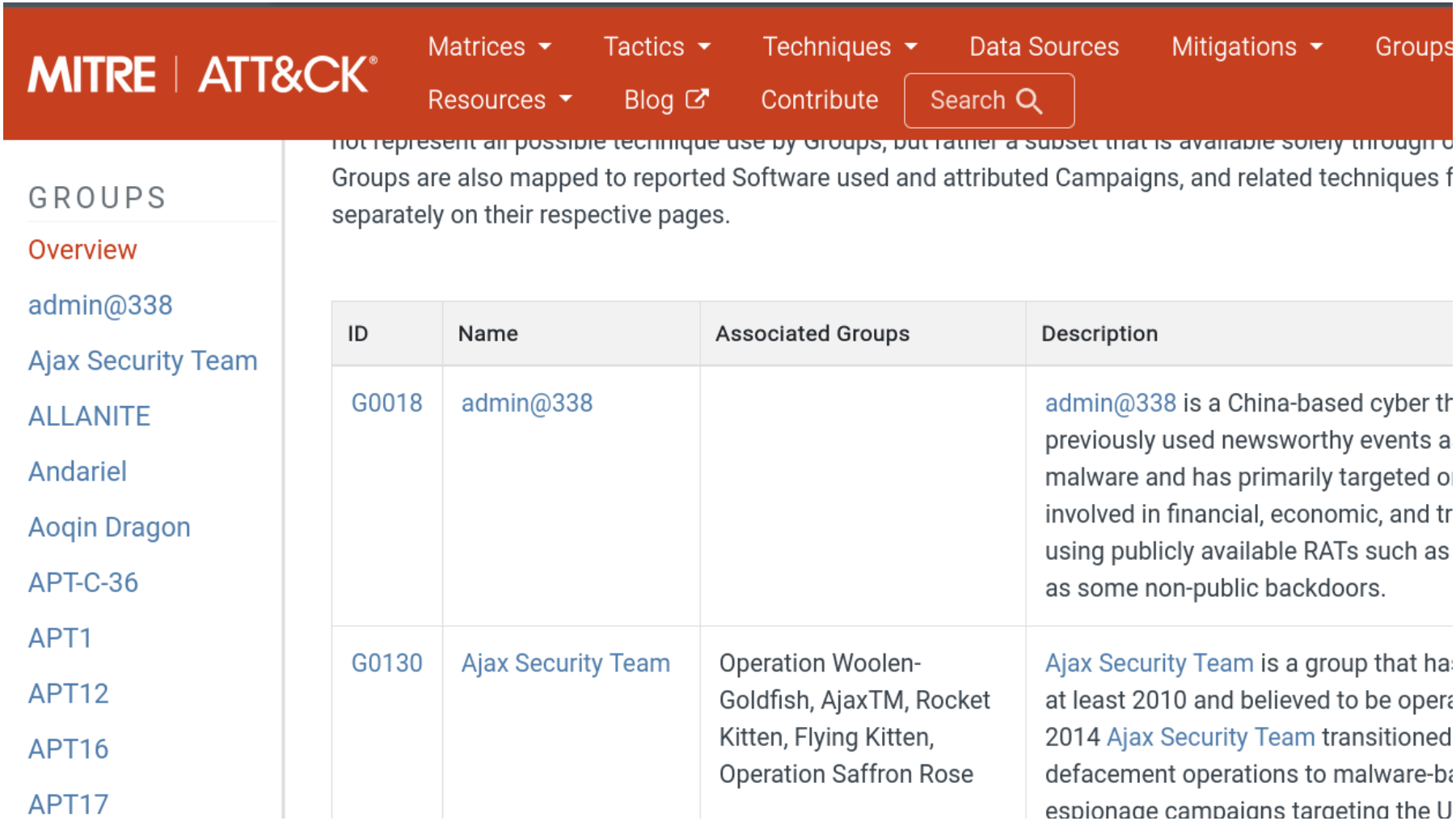
https://attack.mitre.org/versions/v13/software/S0281/

Attack-navigator: tacticas de “Dok”

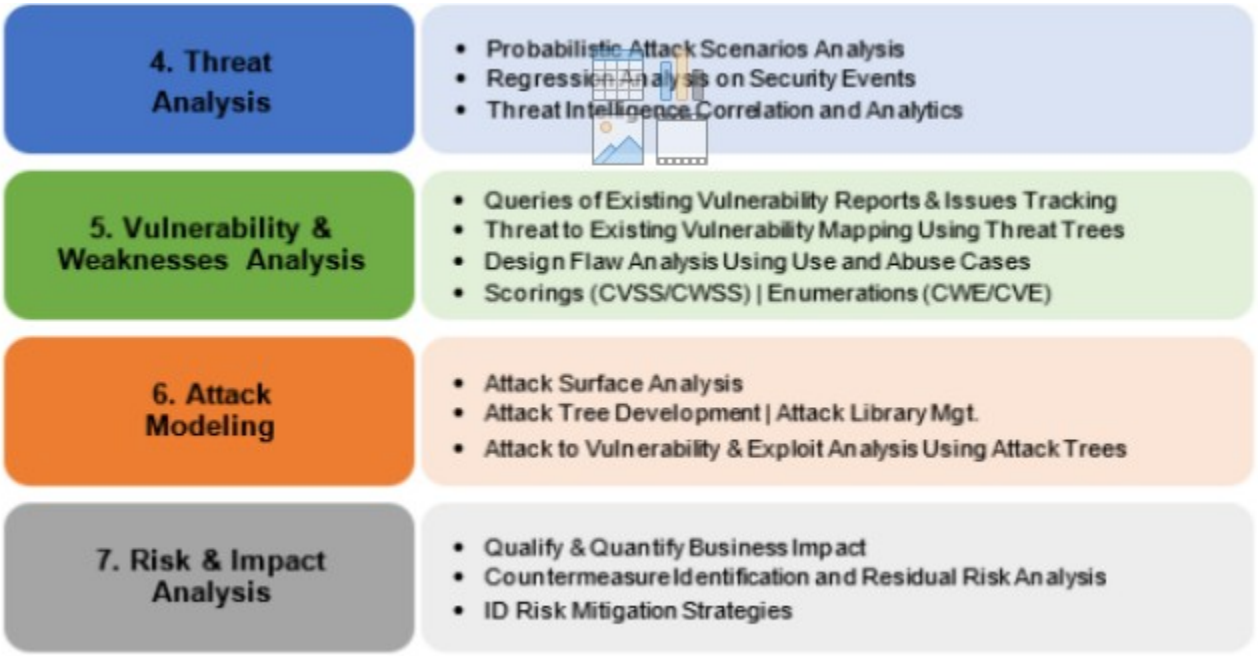


https://mitre-attack.github.io/attack-navigator/

Grupos de APT



https://attack.mitre.org/groups/


4. Threat Analysis
Probabilistic Attack Scenarios Analysis
Regression Analysis on Security Events
Threat Intelligence Correlation and Analytics
5. Vulnerability & Weaknesses Analysis
Queries of Existing Vulnerability Reports & Issues Tracking
Threat to Existing Vulnerability Mapping Using Threat Trees
Design Flaw Analysis Using Use and Abuse Cases
Scorings (CVSS/CWSS) | Enumerations (CWE/CVE)
6. Attack Modeling
Attack Surface Analysis
Attack Tree Development | Attack Library Mgt.
Attack to Vulnerability & Exploit Analysis Using Attack Trees
7. Risk & Impact Analysis
Qualify & Quantify Business Impact
Countermeasure Identification and Residual Risk Analysis
ID Risk Mitigation Strategies

Herramienta OWASP Threat Dragon

Descargas en

https://github.com/OWASP/threat-dragon/releases/tag/v2.0.4

Online en https://www.threatdragon.com

Trabajo Practico: Modelado de Amenazas

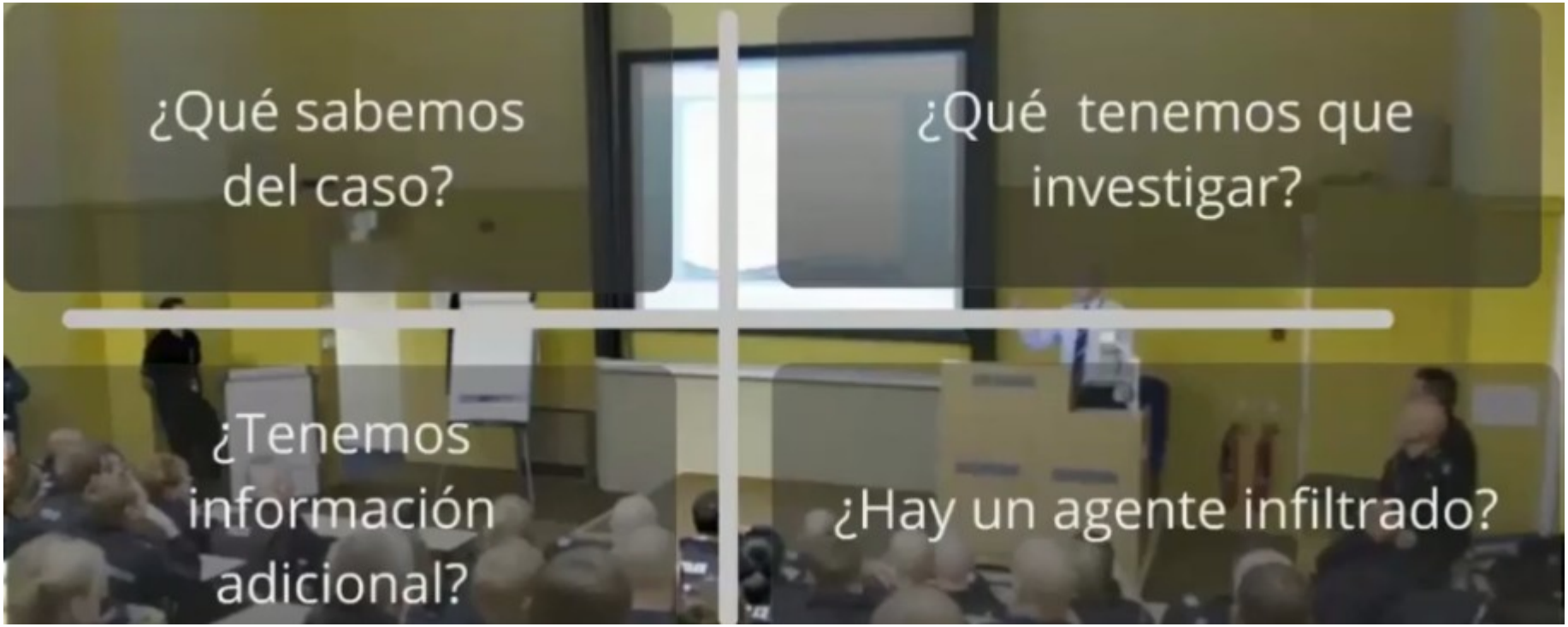
Utilizando el threat-dragon *Mitre ATT&CK deben implementar un modelo de amenazas de la arquitectura del trabajo final*.

Por supuesto asuman, si faltan datos asumanlos razonablemente. Ej, si no saben que base de datos usa, luego de hacer un poco de inteligencia, la inventan.

Trabajo Practico: Modelado de Amenazas

- Identificación de Actores y Datos Sensibles
- Análisis de Amenazas: Identificar posibles amenazas a la seguridad
- Modelado de Amenazas: Si es posible, incluir detalles como las vulnerabilidades, los activos comprometidos y los posibles impactos.
- Propuesta de Contramedidas: proponer contramedidas de seguridad adecuadas.
- Presentación y Documentación: informe que resuma su análisis de amenazas y las contramedidas propuestas (hasta 5 paginas) y el archivo del threat-dragon.


¿Qué sé?
¿Qué no sé?
¿Qué no sé que sé?
¿Qué no sé que no sé?


¿Qué sabemos del caso?
¿Qué tenemos que investigar?
¿Tenemos información adicional?
¿Hay un agente infiltrado?

Dimensiones del Conocimiento y Aprendizaje

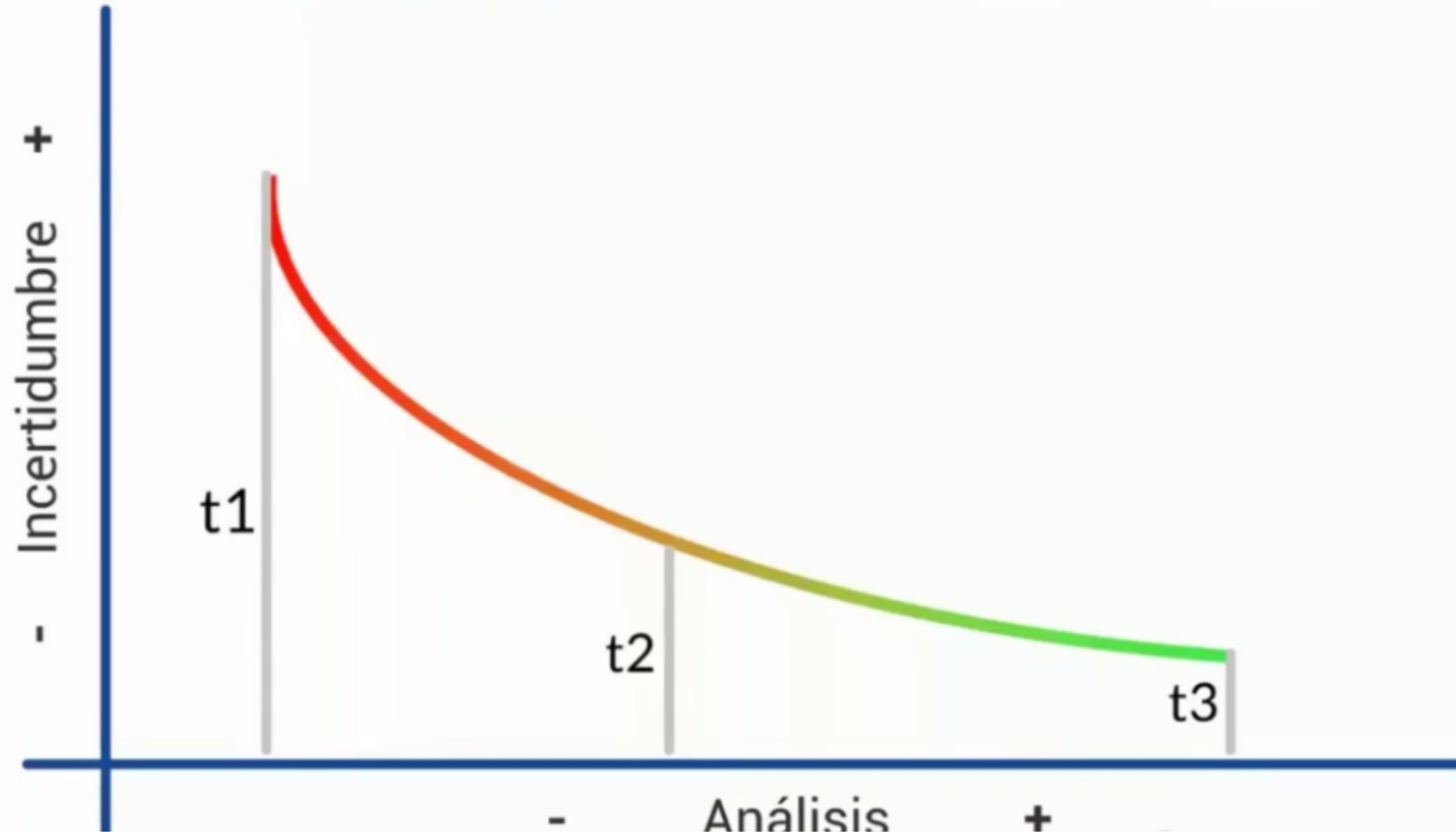
- **Conocimiento Explícito**: ¿que se?
  - Se refiere al entendimiento claro y consciente de información y hechos que ya poseemos.
  - No requiere esfuerzos adicionales de adquisición o análisis.

- **Conocimiento Ausente: ¿que no se?**
  - Identifica la información que conscientemente reconocemos como desconocida.
  - Requiere asignación de recursos para su adquisición y comprensión.

- **Conocimiento Tácito: ¿que no se que se? ¿perdido o escondido?**
  - Se trata de información o habilidades que poseemos sin ser plenamente conscientes de ello.
  - Descubrir este conocimiento implica reflexión y, a menudo, investigación, como explorar trabajos previos de colegas o antecesores en nuestra organización.

- **Área de Desconocimiento Total:**
  - Representa lo que desconocemos sin siquiera ser conscientes de esa carencia.
  - Este nivel de desconocimiento exige una profunda reflexión para ser identificado y minimizado, dado que impide el análisis integral y efectivo en diferentes áreas temáticas.

ANÁLISIS vs INCERTIDUMBRE



objetivo de la Ciberseguridad

dos conceptos claves

Robustez

capacidad de operar frente a un determinado nivel de perturbaciones producidas por ciberamenazas

Resiliencia

capacidad de restablecer o restaurar el sistema luego de producido un evento no deseado, con el mínimo impacto posible acorde a los riesgos tolerables definidos por la Organización.

El rango de lo que pensamos y hacemos

está limitado por aquello de lo que no nos damos cuenta.

Y es precisamente el hecho de no darnos cuenta

de que no nos damos cuenta

lo que impide

que podamos hacer algo

por cambiarlo.

Hasta que nos demos cuenta

de que no nos damos cuenta

seguirá moldeando nuestro pensamiento y nuestra acción.

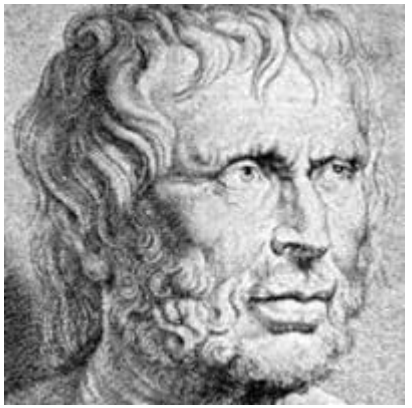
R. D. Laing

Qué es, pues, lo que puede hacerte escolta para protegerte en esta vida? Una sola y única cosa, la filosofía.

Marco Aurelio

No nos da miedo hacer las cosas porque sean difíciles, sino que las cosas son difíciles porque nos da miedo hacerlas.

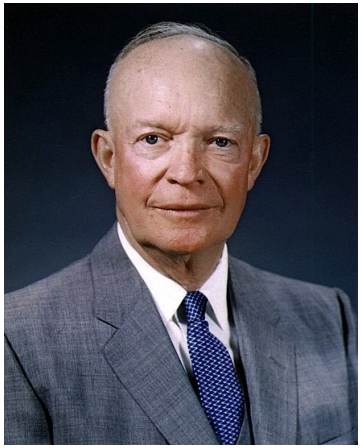
– Seneca



No es valiente quien no tiene miedo (temerario) sino quien es capaz de actuar a pesar del miedo.

Lo que es importante, rara vez es urgente. Y lo que es urgente rara vez es importante.

Dwight Eisenhower



Tareas Urgentes vs Importantes