Unidad 7: Procesos que alimentan el análisis del ciberriesgo

BLOQUE II – El análisis del ciberriesgo: enfoques cualitativos y cuantitativos

Grado en Ingeniería de la Ciberseguridad, curso 2022-2023

CONTENIDOS

1. Root Cause Analysis.
2. Modelado de amenazas.
3. Inteligencia de amenazas.

Nota

- Las técnicas y procesos que vamos a estudiar en esta unidad no se utilizan exclusivamente en el contexto del análisis y gestión del riesgo.
  - Ni siquiera se asocian en muchas ocasiones a esta disciplina.
- Pero pueden ser realmente útiles para enriquecer los procesos.
  - Y otros similares.

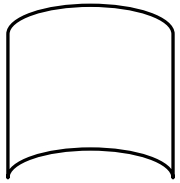
1. Root Cause Analysis

- También se denomina Fault Tree Analysis (FTS) y es una técnica probabilística, ya que más que identificar los riesgos, permite determinar cuantitativamente la probabilidad de que se produzcan.
- Se basa en escoger una situación no deseada para el sistema (fallo, anomalía, error), comprender el comportamiento del sistema y las posibles causas de esta situación no deseada, así como la probabilidad de que ocurran, y construir un árbol de probabilidad mediante lógica booleana (puertas AND y OR).
- Este árbol permite determinar la probabilidad de cada situación no deseada.
  - ¿Recordáis los diagramas de amenazas de CORAS? Esta técnica ayuda a razonar las probabilidades en diagramas de este tipo.

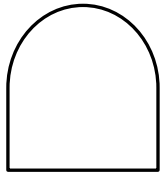
1. Root Cause Analysis

Fallo o situación no deseada para el sistema (top event)

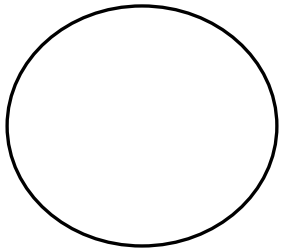
Eventos intermedios



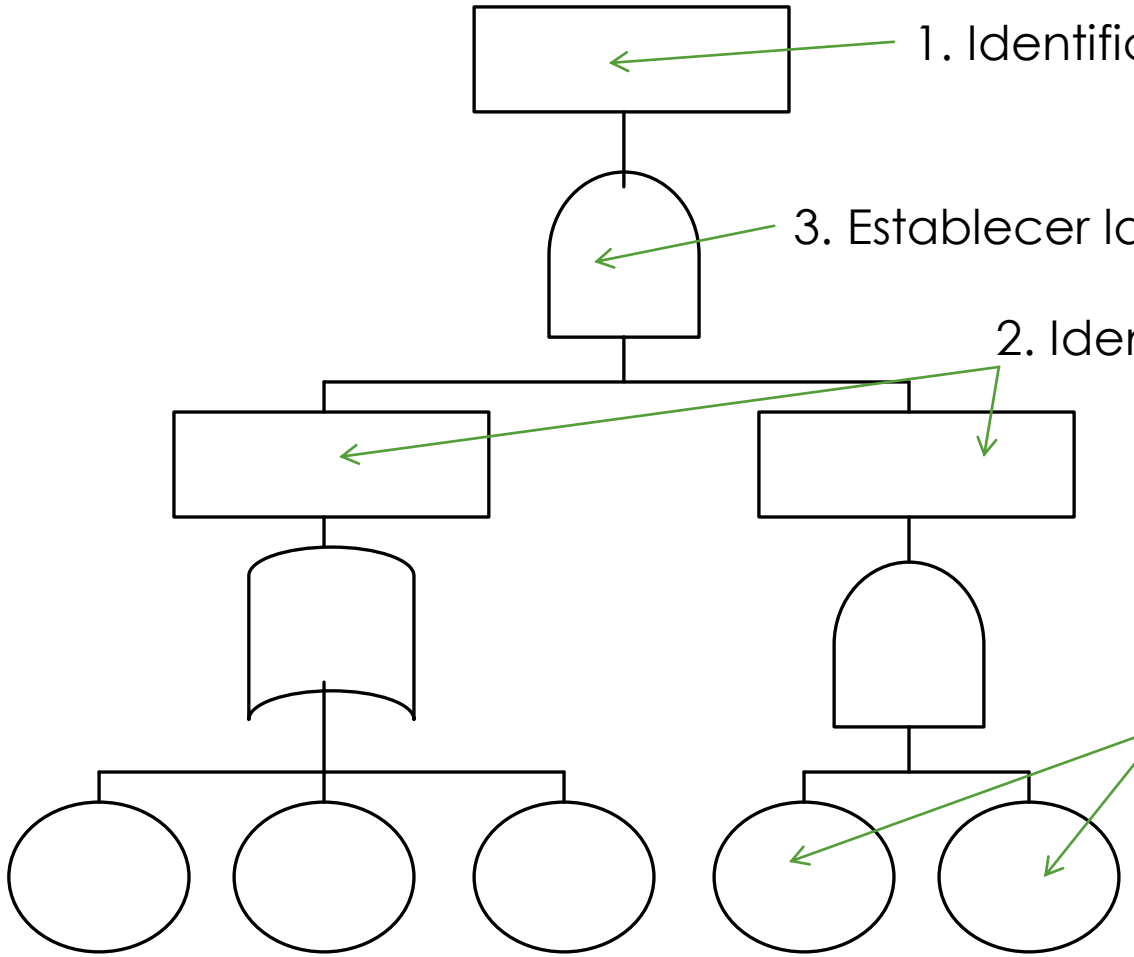
Puerta OR: Para que su salida se active, basta con se active alguna de sus entradas



Puerta AND: Para que su salida se active, se tienen que activar todas sus entradas



Causas básicas, ya no se descomponen más y limitan la resolución del análisis



1. Identificar el incidente o situación no deseada

3. Establecer las relaciones

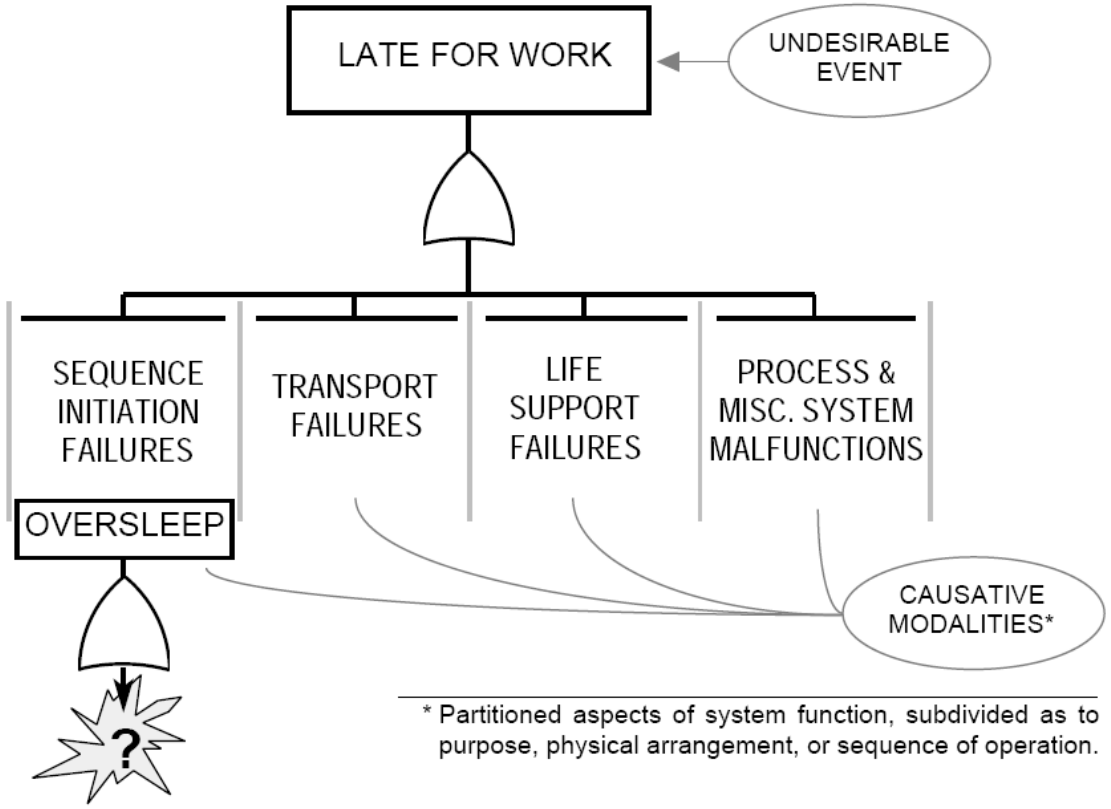
2. Identificar sus causas principales

Ir descomponiendo estas causas hasta llegar a las básicas

1. Root Cause Analysis

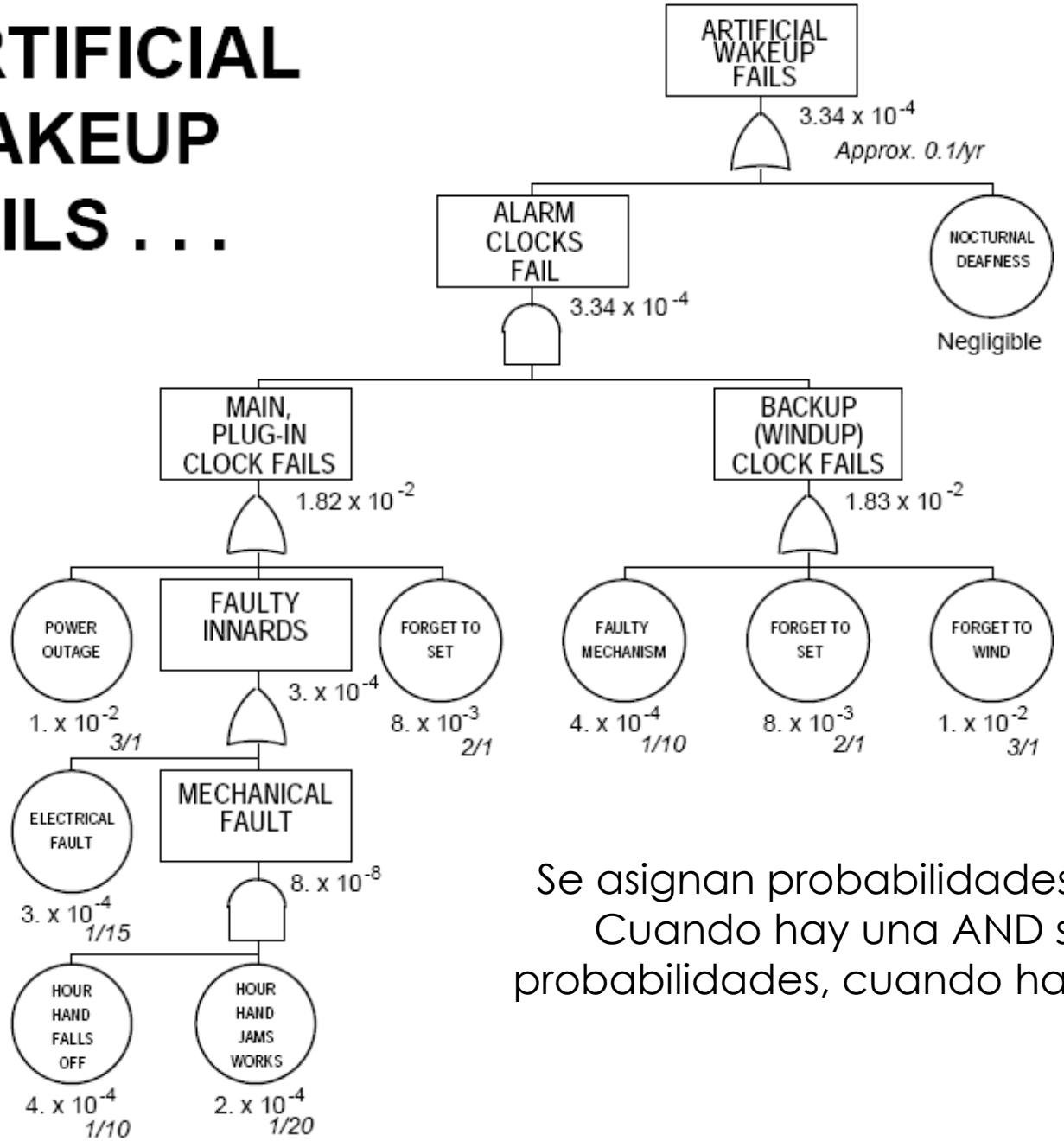
- Normas básicas:
  - Dividir la infraestructura analizada en dominios, redes, etc. para atacar problemas más sencillos.
  - Nunca alimentar una puerta desde otra puerta.
  - Utilizar nomenclatura clara y consistente para las causas y los eventos.
  - Ser realista y no esperar milagros.
  - Las causas básicas deben ser completamente independientes unas de otras.
  - Los fallos de partida (top events) deben ser muy probables o muy graves para que merezca la pena analizarlos.

1. Root Cause Analysis



http://www.fault-tree.net/papers/clemens-fta-tutorial.pdf

ARTIFICIAL WAKEUP FAILS . . .



Se asignan probabilidades de abajo a arriba. Cuando hay una AND se multiplican las probabilidades, cuando hay una OR, se suman.

1. Root Cause Analysis

- Esta técnica deductiva emplea un enfoque de arriba-abajo (abstracto a concreto) que se combina muy a menudo con sistemas expertos y técnicas de inteligencia artificial.
- Sólo debe utilizarse cuando el esfuerzo merezca la pena.
  - Cuando hay pocos top events, graves y claramente identificados.
  - Evitar "matar moscas a cañonazos".
- De nuevo depende mucho de experiencia de los grupos encargados de construir los árboles.
- Y de los datos empleados para la estimación de probabilidades.
- Pero puede ser muy útil en algunos contextos.

1. Root Cause Analysis

Recuerda que ya estudiamos en la unidad 3 que hay muchas alternativas de este tipo, casi todas nos ayudan en la medida de probabilidad y en la gestión del riesgo (porque identifican sus causas, por ejemplo):

- FMEA (Failure Modes and Effects Analysis) y su extensión FMECA
- FMECA (Failure Mode, Effects, and Criticality Analysis)
- DRBFM (Design Review by Failure Mode)
- FTA (Fault Tree Analysis) y su extensión ETA (Event Tree Analysis)
- HAZOP (Hazard & Operability Studies)
- HACCP (Hazard Analysis and Critical Control Points)
- Structured What-If Technique (SWIFT)

2. Modelado de amenazas

- Estos modelos ayudan a identificar los escenarios de riesgo.
  - También ayudan en la fase de gestión/tratamiento.
- Se trata de hacer un "brainstorming" malicioso.
  - Pensar en todo lo que podría ir mal.
  - Qué amenazas se podrían materializar y cómo.
- El modelado de amenazas implica un enfoque proactivo en la gestión del riesgo, ya que no nos limitamos a esperar a que las amenazas se materialicen para saber cuáles nos pueden afectar, sino que intentamos anticiparnos a los incidentes, analizando cómo se podrían producir.

2. Modelado de amenazas

- ¿Recuerdas STRIDE de la asignatura de Introducción a la Ciberseguridad?
- STRIDE es el modelo de amenazas STRIDE propuesto por Microsoft y muy extendido.
  - Spoofing (suplantación de identidad).
  - Tampering (manipulación)
  - Repudiation (repudio).
  - Information disclosure (filtración de información sensible).
  - Denial of service (denegación de servicio).
  - Elevation of privilege (escalado de privilegios).

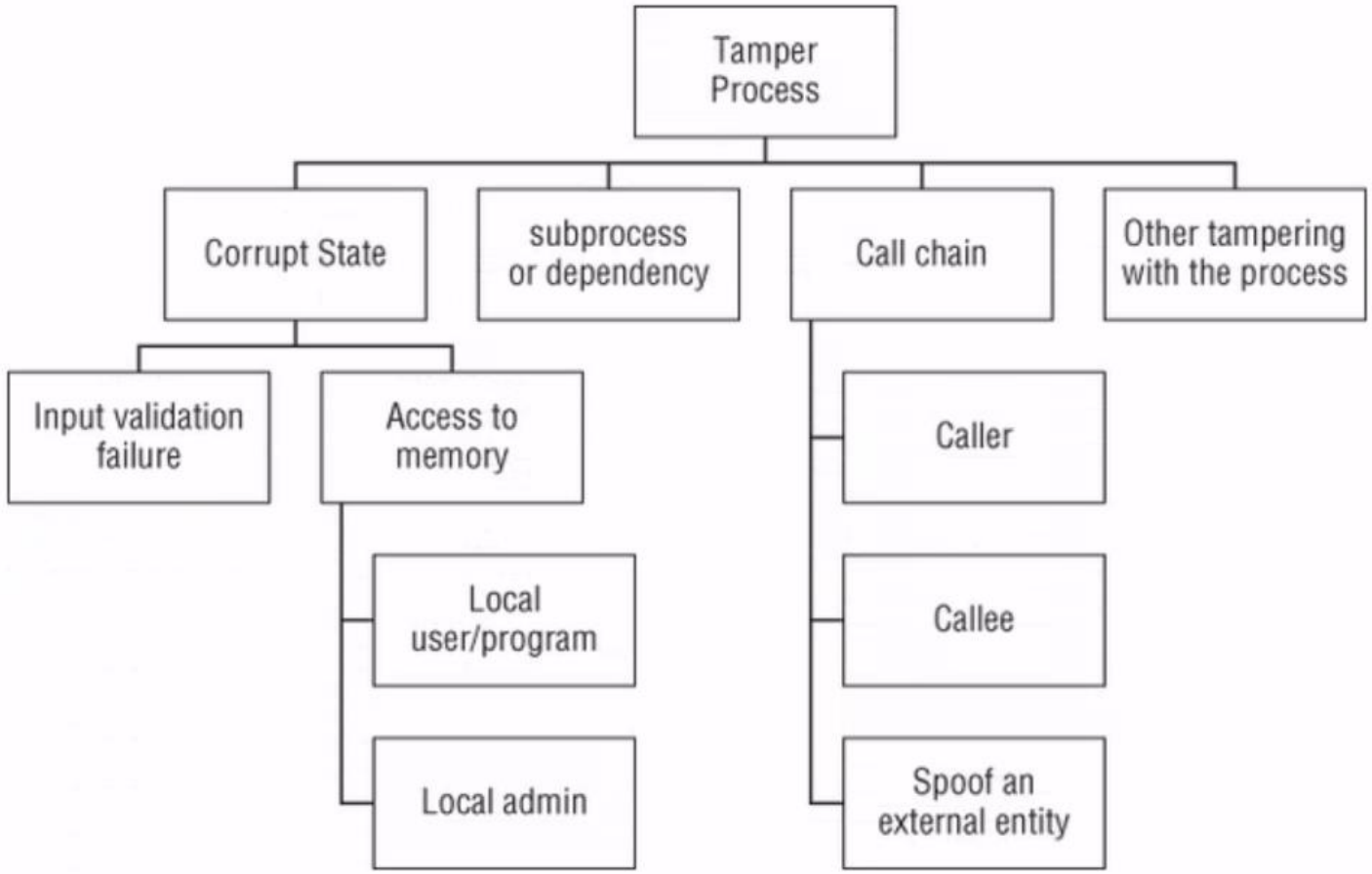
2. Modelado de amenazas

Amenaza	Pilar de la seguridad
Spoofing	Todos
Tampering	Integridad
Repudio	No repudio
Filtración de información	Confidencialidad
Denegación de servicio	Disponibilidad
Escalado de privilegios	Control de acceso

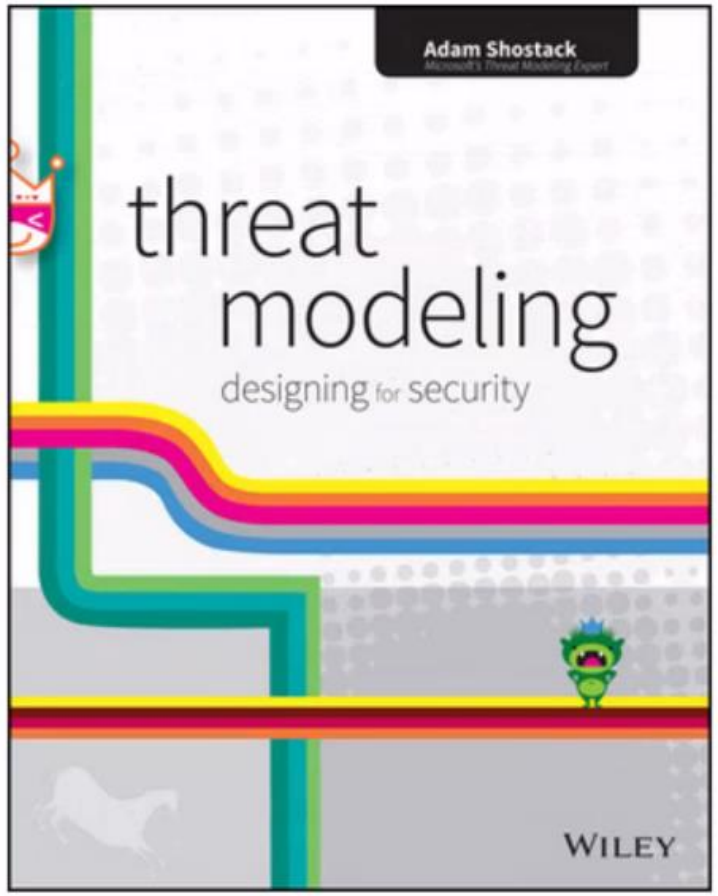
2. Modelado de amenazas

"Threat Modeling: Designing for Security", Adam Shostack

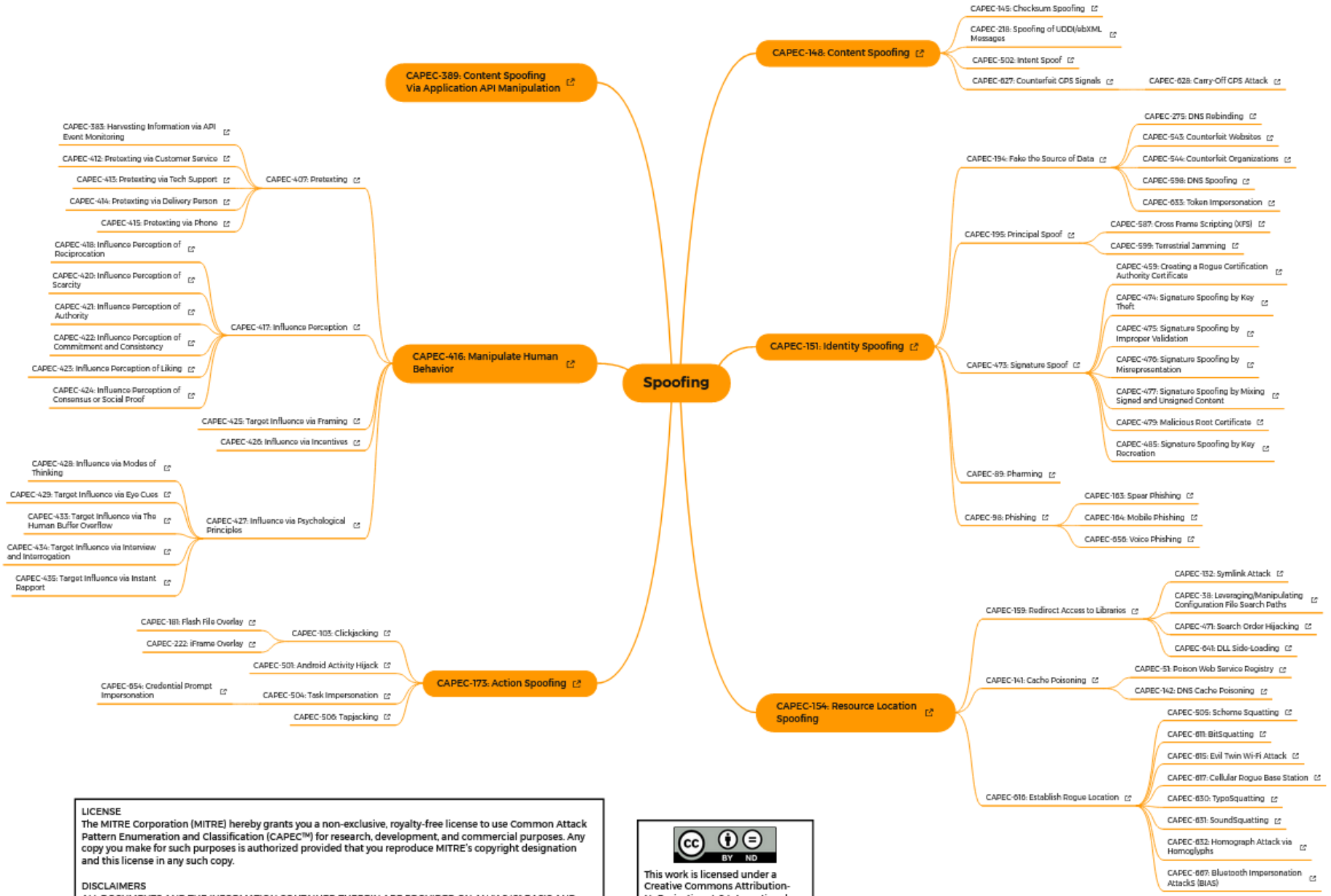
- STRIDE permite obtener modelos de amenazas muy completos mediante los árboles que se han propuesto a lo largo del tiempo.



2. Modelado de amenazas



CAPEC-STRIDE MAPPING



https://ostering.com/blog/2022/03/07/capec-stride-mapping/

2. Modelado de amenazas

- DREAD es otro acrónimo que nos ayuda a recordar los aspectos que tenemos que analizar y comprender para cada amenaza:
  - Damage o daño, es decir ¿qué impactos podría tener el ataque que materializa la amenaza?
  - Reproducibilidad o ¿cómo de sencillo es reproducir el ataque?
  - Explotabilidad, ¿cómo de sencillo es realizar el ataque, cuántos esfuerzos y recursos implica?
  - Afectación o ¿cuántos usuarios se verán afectados?
  - Descubrimiento, es decir ¿es sencillo descubrir que nuestra infraestructura es vulnerable?

2. Modelado de amenazas

- Hay otros muchos métodos/técnicas para realizar modelado:

PASTA	VAST	Persona Non Grata	Security Cards	Trike
OCTAVE	OWASP Cornucopia	MITRE ATT&CK	LINDDUN (privacidad)	

Marca en rojo lo que le funcionaría al adversario, en azul para lo que tienes contramedidas desplegadas, en verde para lo que tienes detecciones, etc.

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

What is LINDDUN?

LINDDUN is a privacy threat modeling methodology that supports analysts in systematically eliciting and mitigating privacy threats in software architectures.

LINDDUN provides support to guide you through the threat modeling process in a structured way.

In addition, **LINDDUN** provides privacy knowledge support to enable also non-privacy experts to reason about privacy threats. **LINDDUN** is a mnemonic for the privacy threat categories it supports:

https://www.linddun.org/

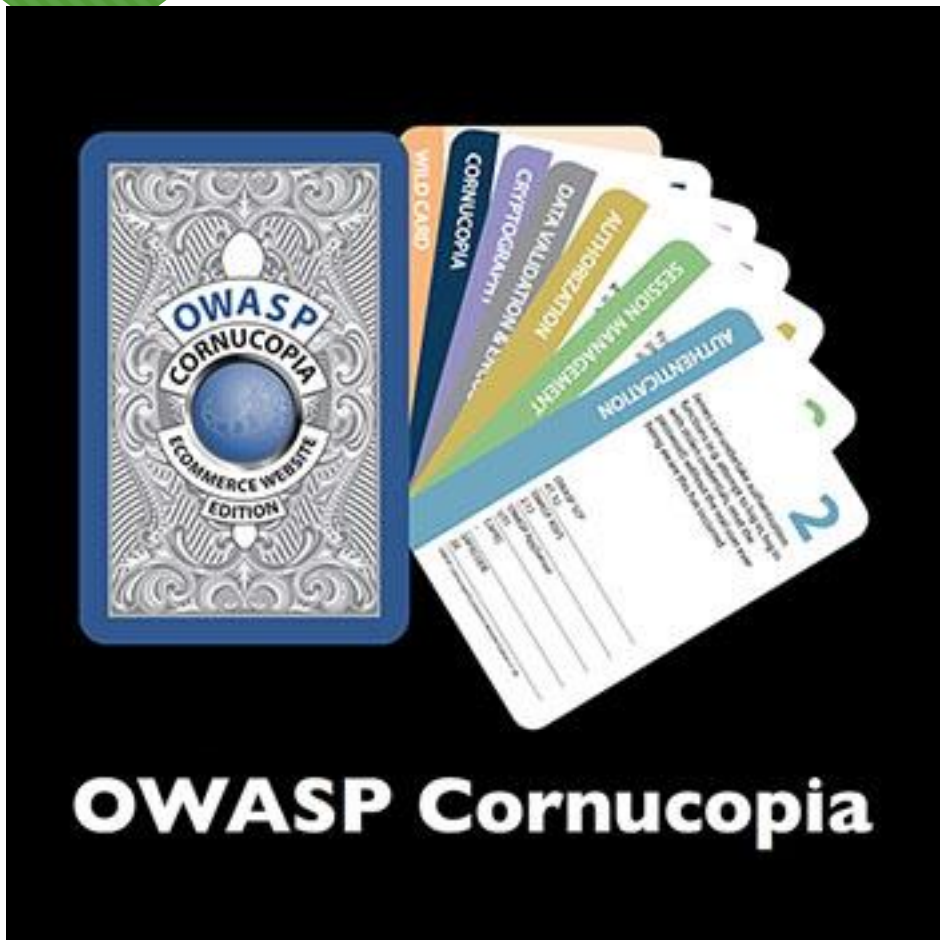
2. Modelado de amenazas

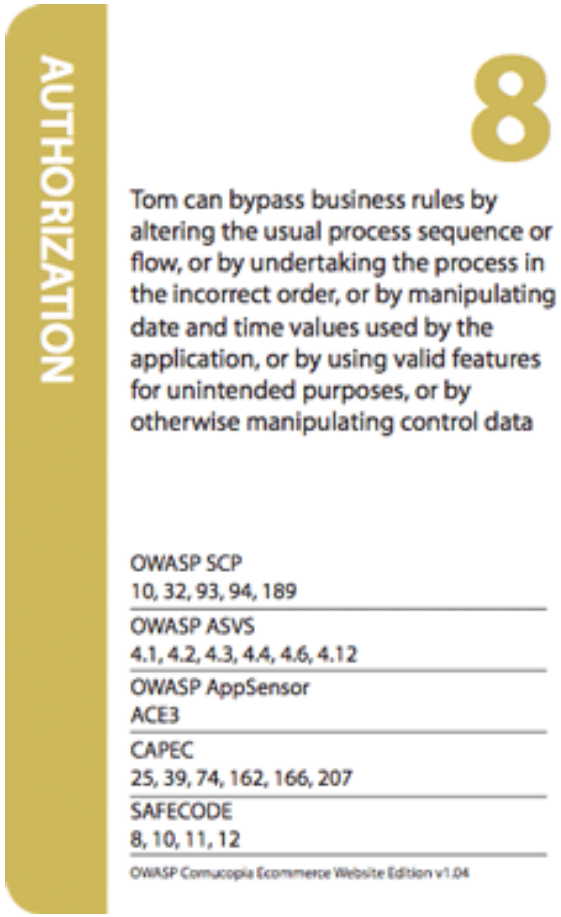
- Como siempre, hay que conocer sus ventajas e inconvenientes y valorar cuál es el adecuado en cada proyecto/organización.
- Algunos están muy orientados al software, otros a las amenazas para la privacidad.
- Lo importante es disponer de un proceso sistemático y que el modelo se pueda actualizar periódicamente.
  - Muy importante la representación gráfica y la documentación que la acompaña.
  - ¿Se añade algo más? ¿Recomendaciones para la mitigación, por ejemplo?

PRÁCTICA 1

- Vais a realizar vuestro primer proceso modelado de amenazas.
  - Para ello vamos a jugar una partida de Cornucopia.

2. Modelado de amenazas





https://owasp.org/www-project-cornucopia/

Data Validation and Encoding (VE)	
2	
3	
4	
5	
6	
7	
8	
9	
10	
J	
Q	
K	
A	

Session Management (SM)	
2	
3	
4	
5	
6	
7	
8	
9	
10	
J	
Q	
K	
A	

Cryptography (CR)	
2	
3	
4	
5	
6	
7	
8	
9	
10	
J	
Q	
K	
A	

Player Name	Tally			
	Requirements	Rounds/hands	Total	Rank
Example	*IIII*	*I*	*5*	

Authentication (AT)	
2	
3	
4	
5	
6	
7	
8	
9	
10	
J	
Q	
K	
A	

Authorization (AZ)	
2	
3	
4	
5	
6	
7	
8	
9	
10	
J	
Q	
K	
A	

Cornucopia (C)	
2	
3	
4	
5	
6	
7	
8	
9	
10	
J	
Q	
K	
A	

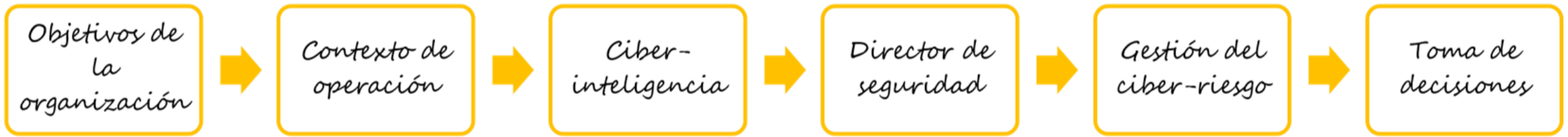
Application

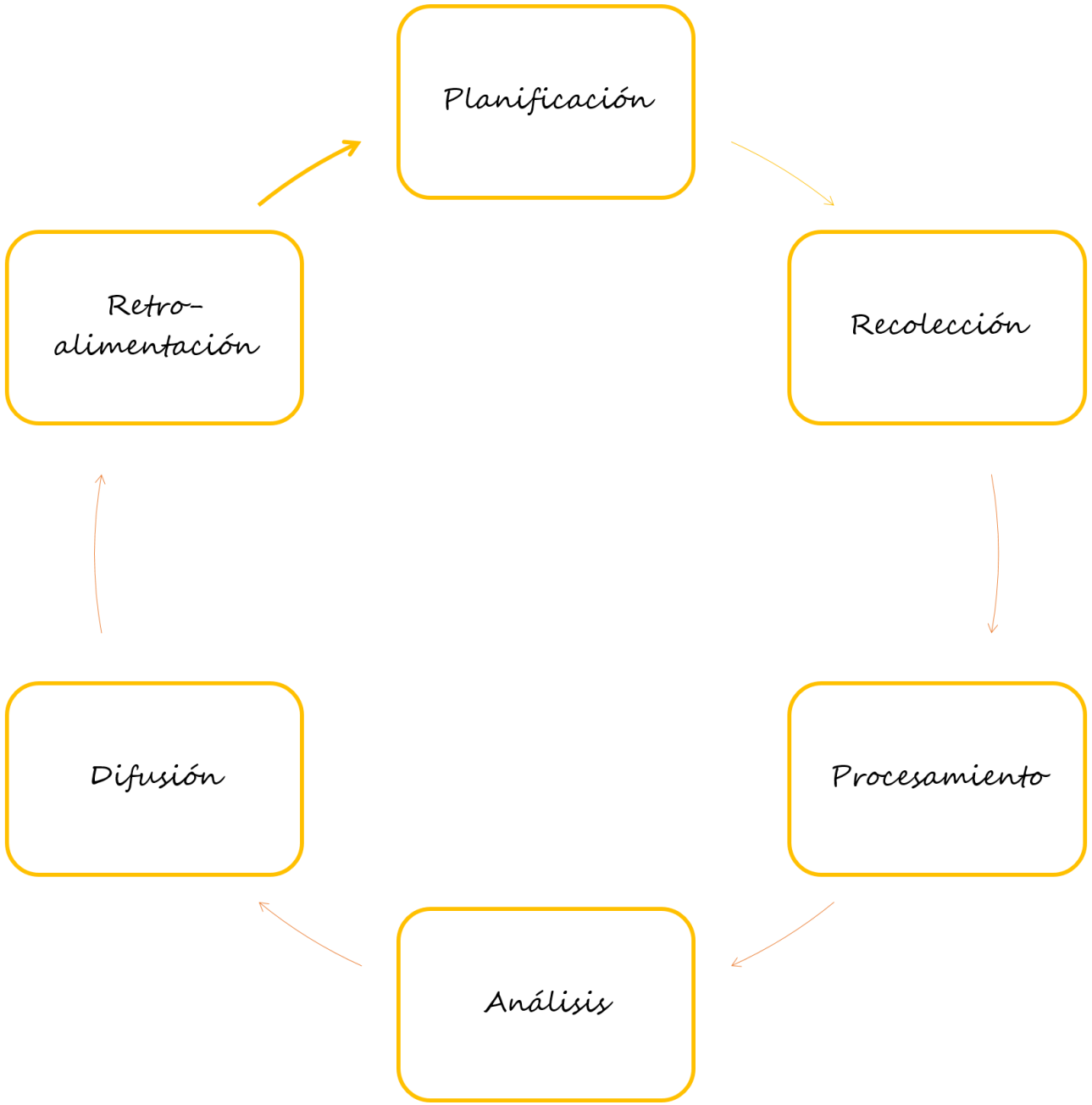
Aspect / Component / Function / Change

Date	Time	By

3. Inteligencia de amenazas

- La gestión del riesgo se realizará mejor cuanta más información se tenga sobre el adversario.
- Esta información o inteligencia permitirá reducir incertidumbre en los procesos de toma de decisiones y también se conoce en ocasiones como Threat Intelligence (inteligencia de amenazas).




Planificación
Recolección
Procesamiento
Análisis
Difusión
Retro-
alimentación

3. Inteligencia de amenazas

- Durante la fase de Planificación, los responsables del proceso de inteligencia identifican qué información es necesaria (IRs o Information Requirements), las posibles fuentes de las que se puede obtener y asignan responsabilidades a los miembros del equipo.
- Algunas fuentes externas pueden ser abiertas (OSINT u Open Source INTelligence) y otras pueden estar asociadas a la pertenencia a diferentes asociaciones, plataformas para la compartición de información, etc.
- También se deben utilizar fuentes internas como nuestros propios logs, capturas de tráfico de red, auditorías de accesos, evidencias relacionadas con incidentes de seguridad ocurridos en el pasado o informes producidos tras procesos de escaneo y análisis de vulnerabilidades o de ejercicios como tests de penetración o red team.
  - O de modelado de amenaza.

3. Inteligencia de amenazas

- Una buena fase de planificación debe intentar responder a una única pregunta, se debe enfocar en alimentar a un único proceso, función o actividad y debe proporcionar conocimiento para dar soporte a un único tipo de decisión. Si no, el ciclo de inteligencia no será efectivo.

3. Inteligencia de amenazas

- La fase de Recolección es en la que los miembros del equipo recurren a las fuentes identificadas en la fase anterior para cubrir los IRs con datos en bruto.
- Tras esta fase se produce la de Procesamiento, en la que todos estos datos se procesan para transformarlos en información útil, eliminando redundancias, integrando, transformando, etc.
- En esta fase son tremendamente útiles, por lo menos para procesar la información que proviene de fuentes internas, herramientas como los SIEM (Security Information and Event Management) o los TIPs (Threat Intelligence Plartforms).
  - Las primeras están más orientadas al procesamiento de distintos tipos de logs, las segundas son más flexibles y se pueden alimentar con otro tipo de datos, pero no son tan útiles para el tratamiento de logs en específico

3. Inteligencia de amenazas

- Esto permite pasar a una fase de Análisis en la que esta información produce conocimiento.
  - En nuestro caso, acerca de los escenarios que deben guiar el proceso de gestión del riesgo, es decir, tenemos un resultado del mismo tipo que con el modelado de amenazas.
- La fase de Difusión permite dar formato al conocimiento producido (no basta con generar un informe, este formato tiene que estar justificado y debe ser útil para su propósito) y hacerlo llegar a las personas adecuadas en el momento adecuado.
  - Dado que este conocimiento es información sensible para la organización, es una fase crítica que debe estar muy bien planificada si no queremos que este conocimiento no termine en las manos equivocadas.

3. Inteligencia de amenazas

- Por último, en la fase de Retroalimentación se analiza la cobertura real de las IRs establecidas en la fase de Planificación.
  - Y se recoge información sobre la eficacia y eficiencia del ciclo realizado, de manera que se pueda mejorar la siguiente vez que se repita.

3. Inteligencia de amenazas

- Hace unos años empezamos a ser conscientes de que nuestros adversarios estaban organizados, sin embargo, nosotros, que nos teníamos que proteger de ellos, no.
  - Es decir, nos intentábamos defender de sus ataques de manera individual y aislada, como mucho con la ayuda de los fabricantes de soluciones de seguridad, de consultoras o del CERT de referencia, pero sin cooperar ni colaborar en capacidades, como las de ciber-inteligencia, con otras potenciales víctimas.

3. Inteligencia de amenazas

- Surgen los:
  - ISACs (Information Sharing and Analysis Centers): entidades de confianza de tipo CERT gubernamental que pueden centralizar ciertas tareas de la compartición de inteligencia (almacenamiento, agregación y enriquecimiento, eliminación de falsos positivos, etc.).
  - ISAOs (Information Sharing and Analysis Organizations): distintos tipos de entidades y organizaciones que participan en estas iniciativas de compartición.

3. Inteligencia de amenazas

- Y el concepto de Threat Intelligence Sharing, modelo en el que los agentes que aporten nueva información deben hacerlo sin ánimo de lucro.
- Ya que han aparecido nuevos modelos de negocio alrededor de las herramientas y servicios que permiten a las organizaciones gestionar las iniciativas de ciber-inteligencia (bases de datos, motores de búsqueda, herramientas de análisis, cuadros de mando, información procesada, etc.).

3. Inteligencia de amenazas

- Lo esencial de estas iniciativas de compartición es que en el momento en el que un agente sufra un incidente u obtenga, por el medio que sea, nueva información sobre una amenaza de seguridad, pueda compartir todo su conocimiento con el resto de agentes colaborando en ellas.
  - En tiempo real y sin necesidad de intermediarios.
- ¿Qué tipo de información se comparte?
  - Artefactos, códigos, scripts, exploits y otras evidencias asociadas a las técnicas de explotación observadas, pruebas de concepto, informes, indicadores de compromiso (IoC), reglas de YARA o firmas para sistemas de detección de instrucciones, parches y herramientas, configuraciones de seguridad recomendadas, etc.

3. Inteligencia de amenazas

- Retos:

Capacidad de extraer valor de grandes volúmenes de información no estructurada

Establecimiento de relaciones de confianza y protección de datos

Aprobación de modelos, estándares y protocolos que todos los agentes que colaboran aprueben y utilicen

3. Inteligencia de amenazas

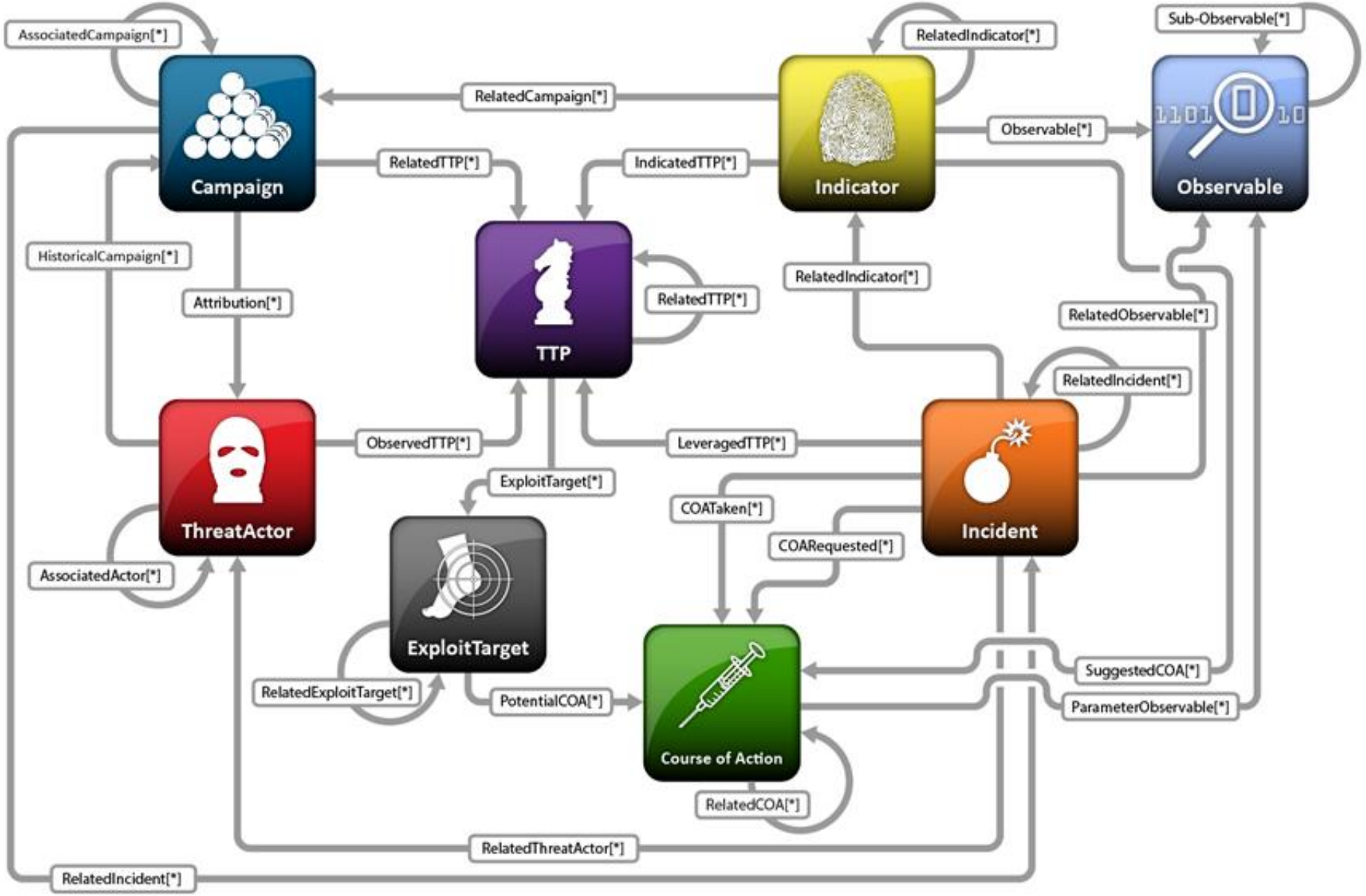
- En esta asignatura vamos a explorar un poco el tercer reto, aunque habréis estudiado algo en la asignatura de Inteligencia de Seguridad.
- STIX (Structured Threat Information Expression) es un lenguaje estándar para describir amenazas de ciberseguridad como formato serializado.
  - Actualmente en su versión 2.1, mantenido por OASIS.
- Con STIX se trabaja con piezas de información, la unidad más pequeña es un objeto con unos atributos asociados.
  - Cada objeto puede relacionarse con otros objetos y estas relaciones pueden visualizarse por analistas de manera sencilla (en forma de grafos) o se pueden almacenar con JSON.

3. Inteligencia de amenazas

- STIX distingue distintos tipos de domain objects o SDOs:
  - Patrón de ataque, campaña, línea de acción, identidad, indicador, intrusión, malware, observable, informe, agente de amenaza, herramienta, vulnerabilidad, grupo, infraestructura, idioma, ubicación, análisis de malware, nota y opinión.
- Además, se pueden crear nuevos tipos de objeto si se necesitan.
- Los observables tienen su propio formato estándar, CYBOX, que antes era independiente pero se integró en la anterior versión de STIX.
- Y existen dos tipos de relación estándar: la genérica y la que implica que se ha observado un domain object.

3. Inteligencia de amenazas


```
{
"type": "campaign",
"id": "campaign--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
"created": "2019-04-06T20:03:00.000Z",
"name": "Green Group Attacks Against World Leaders",
"description": "Campaign by Green Group against targets at DAVOS."
}
```



https://oasis-open.github.io/cti-documentation/

3. Inteligencia de amenazas

- El propósito de STIX es tener un lenguaje común para compartir información sobre amenazas entre diferentes entidades y organizaciones.
- Esta compartición se resuelve con documentos JSON, que se denominan bundles.
- Un bundle comienza con el atributo type indicando que es un bundle y con un id, pero no es un objeto, sino una colección de objetos que se quieren compartir y que no tienen que estar relacionados entre sí.
  - Es decir, no tienen por qué conformar un grafo, en un mismo bundle pueden aparecer objetos de grafos diferentes, que no están relacionados entre ellos.

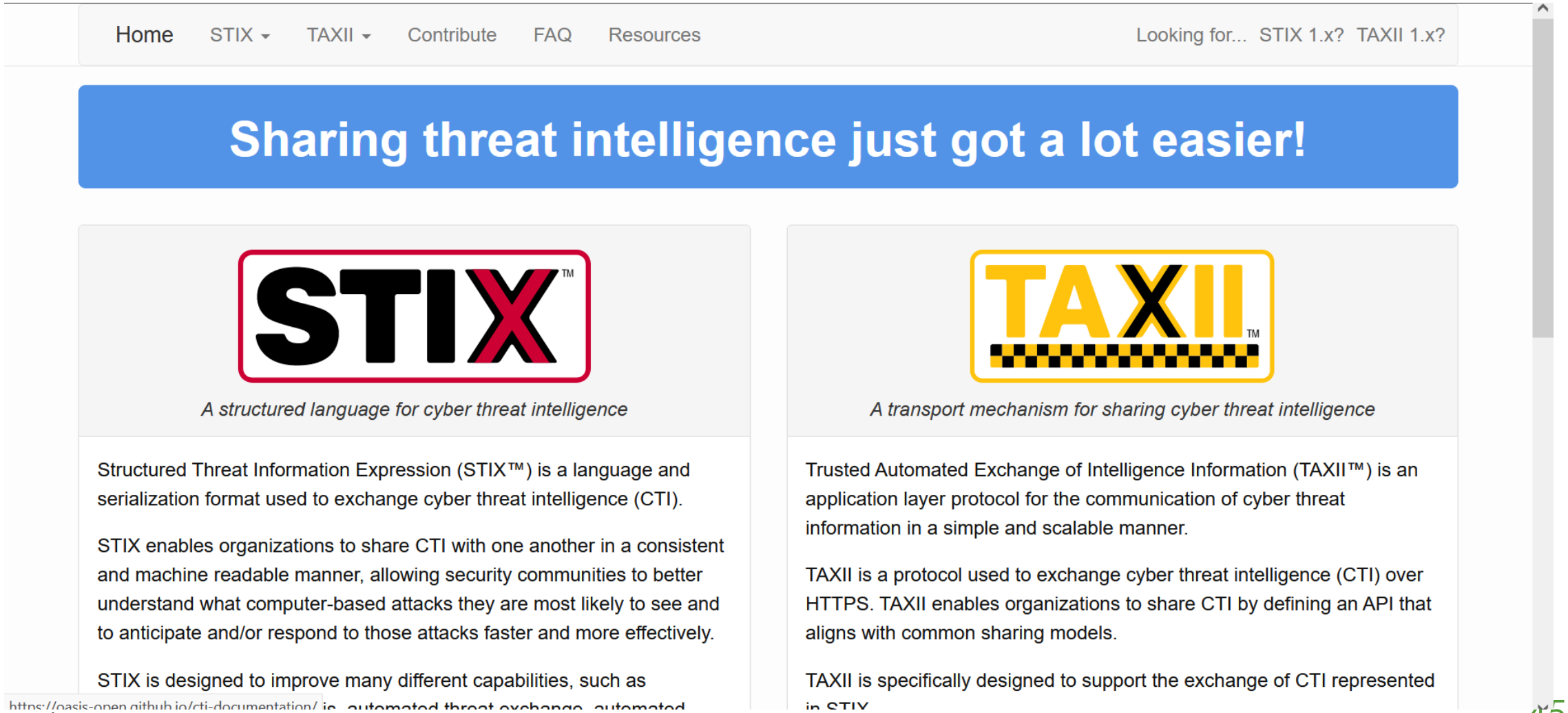
3. Inteligencia de amenazas

- En este punto ya sabemos cómo debemos representar la información acerca de amenazas de seguridad si deseamos compartirla. ¿Pero cómo la compartimos?
- Construimos el bundle y ¿después qué?
- TAXII (Trusted Automated Exchange of Intelligence Information) nos proporciona un protocolo para estandarizar la compartición, de manera que se resuelve con un esquema cliente-servidor y se utiliza HTTPS.
  - En concreto TAXII define una API RESTful y especifica unos requisitos que deben cumplir los servidores y los clientes.

3. Inteligencia de amenazas

- TAXII soporta dos tipos de modelos de compartición:
  - Las colecciones, de manera que un servidor TAXII pueda almacenar un repositorio local de objetos que son servidos a los clientes que los solicitan.
  - Y los canales, que en lugar de basarse en un modelo petición/respuesta, se basa en uno de publicación/suscripción. De manera que el cliente que genera un objeto lo puede publicar en un servidor para compartirlo con otros clientes que están suscritos.

https://oasis-open.github.io/cti-documentation/



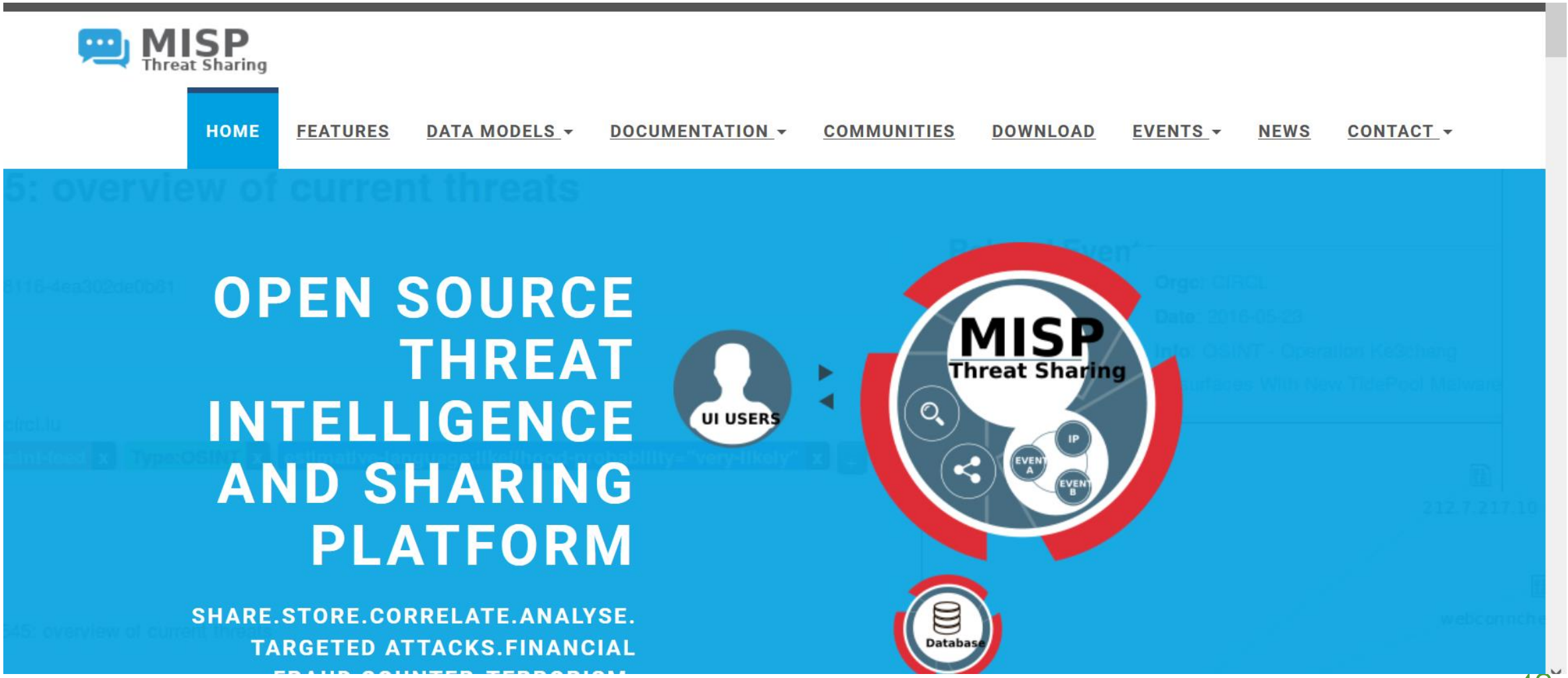
3. Inteligencia de amenazas

- Ni STIX ni TAXII proporcionan herramientas ni software específicos, son especificaciones.
  - Diferentes organizaciones y empresas han comenzado a desarrollar validadores, visualizadores y otras herramientas que pueden ser muy útiles en la compartición de inteligencia de amenazas.
- El problema, como ocurre con muchos esfuerzos de estandarización, es que ambas especificaciones tienen competencia, han surgido muchos estándares con el mismo objetivo.
  - Y la fragmentación de los esfuerzos ha hecho que ninguno esté ahora mismo especialmente maduro

3. Inteligencia de amenazas

- Una de las que más está evolucionando es MISP (Malware Information Sharing Platform), ya que organizaciones como FIRST (Forum of Incident Response and Security Teams) lo están impulsando y adoptando.
- También basado en JSON, su objetivo es el mismo, facilitar la compartición de inteligencia de manera estándar y automática.

https://www.misp-project.org/



Para leer e investigar…

- "THREAT MODELING: A SUMMARY OF AVAILABLE METHODS". Nataliya Shevchenko, Timothy A. Chick, Paige O'Riordan, Thomas Patrick Scanlon, PhD, & Carol Woody, PhD (2018).
- NIST SP 800-150 "Guide to Cyber Threat Information Sharing" (2016).

Referencias

- Fotografías
  - https://unsplash.com
- Iconos
  - https://www.flaticon.es/
- Figuras:
  - "Dirección de seguridad y gestión del ciberriesgo" Fernando Sevillano y Marta Beltrán. Colección Ciberseguridad, editorial RaMa. 2021