# Threat Modeling

Transcribed on July 25, 2025 at 10:20 AM by Minutes AI

Speaker 1 (00:02)

Bienvenidos a esta nueva sesión.

En esta sesión vamos a hablar del modelado de amenazas o Threat Modeling.

Esta es una parte fundamental al iniciar cualquier proceso de hardening de redes de datos o prácticamente cualquier otro tipo de proyecto que requiera algún tipo de arquitectura.

Esta sesión se va a centrar principalmente en explicar qué es un modelo de amenazas y las diferentes herramientas que tenemos a nuestra disposición para poder implementar este modelo de la forma más eficiente posible, haciendo que nuestra arquitectura sea lo más segura desde el minuto cero de su planificación.

El modelado de amenazas es crucial para comprender y gestionar la seguridad de una arquitectura, ya que ofrece una representación estructurada de la información más relevante.

Este proceso implica capturar, organizar y analizar datos para tomar decisiones que sean informadas sobre los riesgos de la seguridad.

Además, aparte de crear el modelo, también se genera una lista priorizada de mejoras y requisitos de seguridad y esto es esencial para obtener una visión general de la aplicación y su entorno desde una perspectiva de seguridad y debe aplicarse de manera continua a lo largo del ciclo de vida de desarrollo de la aplicación o de la arquitectura de red que estemos implementando.

En la diapositiva podemos ver que hay unas seis preguntas que son las que nos debemos de hacer para poder identificar cómo afrontar este proceso del Threat Modeling o del modelado de amenazas.

La primera implica que las tareas, implica qué estamos haciendo.

Esto es importante para poder saber qué procesos necesitamos para implementar nuestro objetivo final que implica nuestra arquitectura.

El segundo punto es preguntarnos qué estamos construyendo.

Es vital, es importantísimo tener una visión muy clara de lo que estamos construyendo desde cero, ya sea una arquitectura o un software o lo que sea.

En la tercera pregunta nos haremos la pregunta de sí o cuáles son aquellos problemas o desafíos a los que nos vamos a enfrentar.

La cuarta pregunta es muy ¿Cómo vamos a enfrentarnos a ellos?

La quinta pregunta ya es parte de ese proceso cíclico, porque todo este organismo, este ciclo de procesos no es único, sino que tiene tiende a retroalimentarse y comenzar de nuevo.

Pues justo aquí, en este punto, en la pregunta número 5, nos haremos la pregunta ¿Lo hemos hecho bien?

¿Hemos ejecutado bien todos los procesos que implicaban esa aproximación a asegurar lo máximo posible nuestra arquitectura?

¿Y finalmente nos preguntaremos qué mejoras podemos hacer a la arquitectura para evitar esos riesgos de seguridad?

Para poder implementar todo este proceso de securización de la arquitectura o del modelado de amenazas es vital tener claras dos puntos.

El primero es tener muy muy claro cómo es nuestra arquitectura, eso es fundamental, al menos el esquema inicial, después sabemos que irá progresando, irá cambiando, pero inicialmente este punto es clave.

Pero no os preocupéis, tenemos herramientas que nos van a ayudar a esquematizar y a crear todo ese entorno o toda esa arquitectura de la manera más visible posible para poder crear después su Threat Modeling o su modelado de amenazas.

Una de ellas es PYTM que es la que podéis ver en la diapositiva, que nos va a permitir crear entre otras cosas, aparte de un informe muy completo de posibles vulnerabilidades, también nos podrá ayudar a crear lo que se llaman los dataflow.

Aquí tenéis un ejemplo en el que podemos ver un dataflow completo en el cual lo que hace es representar un tipo de arquitectura basada en una aplicación bancaria.

Como podéis observar, además de todos los puntos o elementos críticos que son representados por círculos, también podemos ver el flow, lo que es el flow de la información, tanto desde que el cliente hace la primera petición hasta la ejecución detrás en lo que es la parte del backend o de nuestra intranet.

Un dataflow tiene diferentes elementos que se representan muy parecido a los famosos diagramas de flujo que utilizábamos, en los cuales por ejemplo aquí vemos que un recuadro pertenece a un elemento externo.

Los círculos de representan básicamente a nuestra arquitectura, a nuestros elementos que son parte de la arquitectura.

Las líneas como es obvio representan el flow, lo que es el tráfico, lo que es el flujo de la información, incluso es direccional, como podéis ver se ve tanto la entrada como la salida.

Finalmente ese trazo de color rojo lo que hace es marcar la frontera, lo que hace es ir marcando lo que se llama en inglés la boundaries, que son las diferentes fronteras o de delimitaciones que fragmentan nuestra arquitectura.

Pues bien, como decía antes, disponemos de herramientas y una de ellas es Python.

Pythm nos permite implementar nuestro data flow usando un framework llamado PYTM, el cual nos permite definir cada elemento de la arquitectura como si fuera un objeto.

Ahí puedes ver un ejemplo de código en el cual tú puedes ir definiendo los diferentes elementos como si fueran parte de una clase de Python en programación orientada a objeto.

Esto no nos da la ventaja de que podemos personalizar y añadir diferentes parámetros para cada elemento de la arquitectura y al ser código ya os podéis imaginar que podemos hacer prácticamente cualquier cosa con esos elementos para organizarlos, analizarlos, etc.

Pero posiblemente, aparte de de presentarte de una forma gráfica muy elegante la arquitectura que tienes que proteger o que hacer ese análisis de amenazas, quizás lo mejor que tiene PYTM es que es capaz de generarte un informe en el cual te van a aparecer todas aquellas vulnerabilidades que puedan afectar a tu arquitectura.

Y fijaros que esto es importante, que aún ni siquiera hemos comenzado a implementarla.

Estamos todavía definiéndola, planificándola, pero ya al menos tenemos una visión lateral de qué posibles problemas podríamos tener en la arquitectura que estamos diseñando.

También Microsoft tiene una solución ya implementada que se llama el Microsoft Threat Modeling Tool, el cual se encarga de procesar todas las diferentes fases que tiene el modelado de amenazas de una forma muy dinámica y muy práctica.

La mejor forma de entender cómo funciona una aplicación que está destinada al modelo de amenazas es verlo en la práctica.

Así que vamos a ver por encima cómo funciona esta herramienta del Microsoft Tree Modeling Tool dentro de un entorno que es una máquina de Windows 11.

El primer paso será buscar la aplicación para instalarla, así que directamente ponemos Microsoft Three Modeling 2 download y buscamos la página principal que debe estar por aquí abajo.

Aquí está.

Aquí nos hace una pequeña introducción a cómo funciona la aplicación que se adapta a un modelo que es el SDL, que es el Microsoft Security Development Lifecycle y que es muy estándar.

Realmente la mayoría de los modelos de amenazas se basan en este ciclo que se va repitiendo.

Pero aquí lo que nos interesa es buscar en la descarga que está aquí abajo con Download, la bajamos, la ejecutamos y la instalamos.

Y ya finalmente lo que obtendremos será este icono que es el que ya directamente abre la aplicación.

Bien, aquí es importante elegir bien la plantilla, porque fijaros, podemos decidir qué plantilla utilizar.

Aquí incluso hay una específica creada por la comunidad que está destinada a dispositivos médicos, pero nos iremos a la cole que es la principal, que es la base.

Pues nada, la seleccionamos, esto es primordial porque es lo que nos dará los stencils que son los diferentes elementos que vamos a utilizar para construir la arquitectura.

Después nada, pinchamos en Crear un modelo y ya se abrirá lo que es la interfaz principal.

Bien, aquí tenemos varias zonas, la que nos interesa ahora mismo es esta de aquí, que es la zona en la que vamos a ir dibujando la arquitectura y la otra es la parte en la que están los diferentes elementos que podemos utilizar para corto.

En un dataflow diagrama tenemos varios objetos que representan diferentes tipos de acciones y elementos.

Por ejemplo tenemos el círculo, el círculo representa un proceso, que son los que podéis ver aquí directamente si cogemos por ejemplo un servidor web, por ejemplo si lo ponemos fuera, veis cómo aparece con un círculo, un círculo implica un proceso.

Ahora imaginad por un momento que buscamos una base de datos database, por ejemplo esta de aquí y la ponemos fuera, fijaros que ahora cambia a dos líneas paralelas, esto es un datastore, que es un sitio de almacenamiento.

Después también tenemos cuando es un recuadro, es una entidad externa, por ejemplo un cliente que se conecta a la aplicación.

También tenemos las flechas que son las que hacen la conexión, que es el dataflow en sí.

Y finalmente tenemos las líneas discontinuas que marca lo que se llama el boundary.

Si yo pincho aquí y pongo boundary, se nos pondrá por ejemplo estas para Internet, pues fijaros que aparece la línea, esto marcará la separación, por ejemplo si este servidor web se conectara esta base de datos hacia Internet, pues directamente pondríamos aquí lo que es la separación a Internet y haríamos la conexión entre ellos.

Por ejemplo si la conexión fuera una conexión HTTPs, buscamos, la sacamos fuera y ya sólo queda poner la dirección de esa conexión, por ejemplo si es bidireccional, pues conectaríamos primero la primera conexión sería adaptarla aquí a la base de datos y haríamos otra más en sentido contrario, por ejemplo podría ser desde la base de datos al servidor web, por ejemplo aquí.

De esta forma lo que ya tenemos es muy bien indicado todo lo que es el flujo de datos y los diferentes elementos.

Por un lado tenemos un datastore, que es la base de datos, el servidor web y las conexiones HTTP.

También hemos marcado la conexión hacia Internet o lo que separa las diferentes fronteras tanto de la red interna como de la red externa, en este caso Internet.

Y como decía, por ejemplo si hubiera un cliente que va a conectar con este servidor web, pues directamente pondríamos aquí external, nos va a indicar todos los diferentes objetos que podemos utilizar, por ejemplo un usuario o un servicio externo web, en este caso alguien con un navegador podría estar desde Internet aquí y se podría conectar al servidor web y de esta forma ya tendríamos esta interacción.

La conexión pues directamente lo mismo, HTTPs o bueno, o cualquier otra que pensemos que podemos utilizar otra vez la misma.

Para que lo veáis directamente, pues el browser, esto es de prueba, pinchamos aquí una prueba para que veáis cómo se va montando.

Es importante hacer bien las conexiones y que todo esté bien comprobado para después poder hacer lo que es el informe del modelado de amenazas, porque si no está bien conectado, no está bien indicado.

Por ejemplo aquí la frontera, fijaros, la frontera está cortando en este punto y en estos puntos quiere decir que todo esto está en Internet y esto está en la red interna nuestra.

Es importantísimo.

Para comprobar si todo está correcto pinchamos aquí en Diagram Reader y Readful Diagram y aquí nos hará un análisis escrito de todo lo que se está viendo en el esquema, la conexión de un sitio a otro, el tipo de conexión, cuál es, etc.

Si esto funciona bien ya podríamos ir directamente a hacer el equipo desde aquí.

En este caso si le damos nos dirá que lo genere.

Este es un caso muy específico, muy de prueba, pero de todas formas podemos ver una prueba.

Veremos una prueba de cómo se genera, si todo ha ido bien, ha empezado a coger todos los elementos que hay y nos va a hacer una pequeña simulación de los posibles problemas que tiene esta arquitectura.

Entonces aquí se irán viendo todos los posibles problemas.

Spoofing, Tampering Como podéis ver también recordar que cada elemento tiene sus propiedades, botón derecho propiedades y aquí tenemos una gran cantidad de opciones para poder customizarlo y personalizarlo al nivel que queramos.

En principio os recomiendo coger siempre los stencils porque ya vienen con una preconfiguración que nos va a facilitar mucho el trabajo.

Prácticamente todas o por no decir la mayoría del modelado de amenazas se basa en un concepto llamado stride.

La descripción de stride es la que podéis ver en pantalla, son diferentes siglas, las cuales corresponden a un tipo de ataque, un tipo de amenaza.

Podemos ver la primera que es spoofing, que realmente significa falsificación de identidad o de información, que lo que implica es un engaño hacia un sistema o hacia un.

Después tenemos el Tampering que es la modificación no autorizada de datos o sistemas, lo cual compromete su integridad.

Después tenemos el que es la negación o rechazo por parte del usuario de haber realizado una acción concreta, incluso cuando fue ese usuario quien lo hizo.

Después tenemos el Information Disclosure, esto es la divulgación no autorizada de información con confidencial.

Básicamente es eso.

Después tenemos el Daniel of Service, este ya seguro que os suena más, que es el 2.

Esto es un ataque que lo que busca es inutilizar un sistema o recurso impidiendo su uso legítimo.

Y finalmente la e pertenece a Elevation of Privilege, esto es la obtención de privilegios o permisos adicionales más allá de los que se te otorgó de una forma inicial.

También existen unas formas un poco más amenas que nos pueden ayudar a crear ese modelado de amenazas.

Aquí podéis ver dos otros ejemplos que se basan básicamente en un juego de cartas.

El que ves a la izquierda es el Microsoft Elevation of Privilege, el cual es una herramienta que está creada por el equipo de Microsoft que tiene el objetivo de facilitar todo ese proceso de modelado de amenazas en el desarrollo de software o la implementación de una arquitectura.

Aquí tenéis un ejemplo de cómo sería ese formato de las cartas son las instrucciones y aquí también podemos ver un ejemplo de los diferentes ataques.

Aquí podéis ver el spoofing que hemos comentado antes, pero además con diferentes niveles.

Es una forma muy amena y muy directa de poder poner sobre la mesa los diferentes problemas que pueden afectar, pero sobre todo es ver cómo se pueden solucionar.

Esa es un poco la clave de este tipo de juegos, fomentar ese networking, esa comunicación con el resto de equipos para mostrar los posibles problemas, pero sobre todo mostrar lo que tenemos implementado y si es seguro para esa vulnerabilidad.

Bien, pues una vez que ya tenemos una primera aproximación a las posibles vulnerabilidades que nos pueden afectar ten tenemos que tomar algunas decisiones.

Aquí podéis ver cinco de ellas que son las básicas, las cuales podemos optar según veamos qué tipo de fallo de seguridad o de vulnerabilidad nos tenemos que afrontar.

Básicamente hay sólo dos que son los aceptables, el resto tenemos que evitarlo como sea.

La primera que es ignorar el riesgo, esa por supuesto nunca tenemos que hacerlo, no podemos obviar que hay un problema en nuestra arquitectura, tenemos que afrontarlo de una forma u otra.

La siguiente es evitarlo.

Esta quizás puede sonar que es una buena opción, pero implica un coste quizás demasiado alto.

Y hablo de coste económico y desde cursos porque implicaría quizás una implementación o un rediseño completo de la arquitectura y eso como podéis imaginar puede acabar en un coste demasiado alto para nuestra empresa u organismo.

El tercer punto es el más lógico y es aceptar el riesgo, saber que esto te va a pasar de alguna forma u otra y tener siempre alguna técnica para poder evadirlo o que el impacto sea mínimo.

Como podéis imaginar es imposible tener en cuenta todos los posibles riesgos que hay en el mundo o en Internet, con lo cual aquí lo que tenemos que hacer es elegir aquellos que nuestro modelado de amenaza nos ha dado como principales y al menos, por lo menos tenerlos documentados como posibles fallos de seguridad que nos pueden afectar.

El cuarto punto, que es quizás uno de los que más hemos hecho durante toda nuestra vida, es transferir el riesgo a otra persona o a otro departamento.

Pues bien, esto conviene no hacerlo si no es estrictamente necesario.

Por supuesto habrá situaciones en las que error o el fallo que puede provocar esa vulnerabilidad de seguridad no está en nuestra mano poder subordinarlo, con lo cual es obvio que tengamos que pasarlo a otro departamento.

Y finalmente, este también es un punto que es bastante claro, es confrontar el tenemos que hacer además de aceptarlo, que es el punto 3, tenemos que confrontar.

Y por último, este punto es muy importante, aunque casi nunca se le da la relevancia que realmente tiene y es la parte de la generación de informes.

Crear informes sólidos es crucial cuando creamos un modelo de amenazas, ya que estos informes son la base para tomar las decisiones, una base informada sobre la seguridad de una aplicación o de una arquitectura.

Un informe detallado y bien estructurado proporciona una visión muy clara de los posibles fallos de seguridad y amenazas que nos enfrentan al sistema.

Entonces esto nos permite priorizar y abordar aquellos riesgos que son más complejos o que nos pueden afectar de una forma más efectiva.

Además, estos informes sirven como base para documentar todo lo que ha pasado durante el ciclo de desarrollo o de implementación de la arquitectura para futuras interacciones que haya con la misma implementación.

Si presentamos una información que es precisa y comprensible sobre estos fallos de seguridad, estos informes nos van a ayudar a generar una confianza tanto dentro de nuestra empresa o de nuestra organización como entre los usuarios finales y esto contribuye a la creación tanto de aplicaciones, arquitecturas mucho más seguras y robustas en un entorno que estamos viendo que cada vez es más amenazante y muy complejo.

La importancia del modelado de amenazas dentro de la arquitectura de datos es un tema que tenemos que tomarnos muy en serio Este enfoque no sólo destaca las vulnerabilidades y amenazas potenciales, sino que también permite a las organizaciones abordar y mitigar proactivamente los riesgos antes de que puedan ser explotados.

Al integrar el modelo de amenazas en el proceso de diseño arquitectónico, las empresas pueden asegurar una infraestructura de red más segura y, sobre todo, resiliente.

Esta postura proactiva no solo protege datos y activos valiosos, sino que también refuerza el compromiso de una organización con la ciberseguridad, mejorando así nuestra reputación y confiabilidad en un mundo cada vez más digital y más peligroso.

Llegamos al final de la sesión.

Os esperamos en el siguiente vídeo.