Iteración TFG

Contexto y objetivo del trabajo:

Título: Motor de Respuesta Autónoma para Ciberdefensa en Escenarios Multidominio.

Descripción: Desarrollo de un motor capaz de identificar automáticamente contramedidas de ciberseguridad basadas en reglas doctrinales y fases operativas de la misión, con el objetivo de minimizar la interrupción operativa y optimizar la respuesta ante ciberamenazas en entornos multidominio.

Descripción general del enfoque

El motor propuesto se estructura en tres bloques claramente diferenciados:

- **Inputs**: información contextual sobre la misión, los activos implicados y el evento de amenaza.
- **Proceso intermedio**: análisis del impacto, propagación de efectos e identificación y evaluación de contramedidas.
- **Outputs**: recomendaciones priorizadas y explicables de cursos de acción defensivos.

Esta separación permite desacoplar la representación del contexto, el razonamiento del motor y la presentación de resultados

1.-Inputs del Motor

1.1 Modelo de activos y dependencias de la misión

El motor recibe como entrada un catálogo de activos presentes en la misión, así como las relaciones de dependencia existentes entre ellos. Por ejemplo, una página web puede depender de una base de datos, o una base de datos puede dar servicio a una aplicación concreta. Otro ejemplo más del contexto MDO sería un sistema de mando y control puede depender de enlaces de comunicaciones tácticas o satelitales, o un sistema de inteligencia puede dar servicio a capacidades de fuegos o maniobra en otros dominios. Este modelo creo que sería muy interesante representarlo como un grafo para poder visualizar de forma más clara la relación entre los activos y su importancia, de esta forma facilitando la propagación de impactos y la visualización de efectos colaterales.

Adicionalmente, para cada activo se define:

- su **tipo**
- la **importancia relativa de cada componente de la tríada CIA** (Confidencialidad, Integridad y Disponibilidad) dentro del contexto de la misión.

Estos valores se expresan como pesos normalizados (por ejemplo, 0.4, 0.4, 0.2), cuya suma es igual a 1

1.2 Evento de amenaza

El motor recibe un evento de amenaza previamente procesado, con una estructura similar a la siguiente:

- **technique_id:** identificador de la técnica de ataque (TTP).
- **target_assets:** activos que se consideran directamente afectados.
- **confidence:** nivel de confianza asociado a la identificación del TTP.

El parámetro confidence permite modular el comportamiento del motor y evitar respuestas excesivamente disruptivas ante hipótesis con bajo grado de certeza.

Las técnicas de ataque, las mitigaciones y las contramedidas se representan mediante un modelo estructurado de conocimiento alineado con estándares de intercambio de inteligencia de amenazas como STIX, lo que permite mantener identificadores consistentes y relaciones bien definidas entre ataques y acciones defensivas a lo largo de todo el proceso del motor.

1.3 Fase operativa de la misión

El sistema recibe también la fase operativa actual de la misión, ya que esta condiciona qué tipos de contramedidas son aceptables. En fases iniciales o de reconocimiento pueden permitirse acciones más disruptivas que en fases críticas de ejecución de la misión.

2. Proceso Intermedio del Motor

2.1 Validación inicial

Una vez recibidos los inputs, el motor realiza una validación inicial que incluye la verificación de que el technique_id existe y la comprobación de que los activos están definidos en el modelo de la misión.

2.2 Cálculo del impacto del ataque

Para cada activo afectado, el motor obtiene un impacto base del TTP, que representa cómo suele afectar dicha técnica a cada componente de la tríada CIA para ese tipo de activo. Este impacto se ajusta posteriormente multiplicándolo por los pesos CIA definidos para el activo (en los inputs), obteniendo así el impacto realmente crítico para la misión. Finalmente, el valor resultante se modula mediante el parámetro confidence, de forma que ataques con baja certeza generan estimaciones de impacto más conservadoras.

El resultado es un vector de impacto que describe cómo el ataque afecta a la confidencialidad, integridad y disponibilidad de cada activo dentro del contexto específico de la misión.

2.3 Propagación del impacto por dependencias

El impacto calculado se propaga a otros activos relacionados mediante las dependencias definidas en el modelo. Por ejemplo, una degradación en la base de datos puede afectar indirectamente a la disponibilidad de la página web que depende de ella. Más específicamente en el contexto MDO se puede traducir a, por ejemplo, una degradación en un sistema de comunicaciones puede afectar indirectamente a la disponibilidad de las capacidades de mando y control que dependen de dicho enlace.

Este proceso de propagación tiene en cuenta la dependencia y cómo de crítica es la misma y se ajusta según el nivel de confidence (propagación más agresiva con alta confianza y más conservadora con baja confianza).

El resultado es una estimación del impacto total inicial sobre la misión, que servirá como referencia para el cálculo posterior del riesgo residual.

2.4 Identificación de cursos de acción (COAs)

A partir del technique_id, el motor identifica las mitigaciones asociadas y las traduce a contramedidas concretas (COAs) mediante un catálogo defensivo de bajo nivel (por ejemplo, alineado con D3FEND).

Para cada COA se obtiene:

- su **coste operacional**, es decir, cómo afecta temporalmente a la tríada CIA.

- el **tiempo estimado de ejecución**.
- su **impacto propagado** sobre otros activos dependientes.

Por ejemplo, reiniciar una base de datos puede degradar su disponibilidad y, durante ese tiempo, afectar también a la disponibilidad de los servicios que dependen de ella. (MDO) Por ejemplo, aislar temporalmente un nodo de comunicaciones o reconfigurar un sistema de mando y control puede degradar su disponibilidad y, durante ese periodo, afectar a las capacidades operativas que dependen de dicho sistema.

2.5 Beneficio de las contramedidas y riesgo residual

Además del coste, cada COA tiene asociado un beneficio defensivo esperado, que representa en qué medida reduce el impacto del ataque actual.

Con esta información, el motor calcula el riesgo residual estimado tras aplicar cada contramedida, comparándolo con el riesgo inicial.

El nivel de confidence vuelve a desempeñar un papel clave, ya que penaliza contramedidas muy disruptivas cuando la certeza del ataque es baja y las permite cuando es alta.

2.6 Ranking por estrategias

Finalmente, el motor genera un ranking de contramedidas en función de distintas estrategias u objetivos, tales como minimizar el riesgo residual, maximizar la protección de un componente de la tríada CIA...

3. Outputs del Motor

El sistema devuelve, para cada estrategia, las N mejores contramedidas, proporcionando para cada una:

- un **score global**,
- el **coste operacional**,
- el **beneficio esperado**,
- el **riesgo residual estimado**,
- la **fase operativa considerada**,
- una **explicación contextual** que justifica la recomendación.

Adicionalmente, se muestra:

- qué activos han sido impactados directamente por el ataque,
- qué activos han sido impactados de forma colateral por propagación,
- el efecto equivalente producido por la contramedida.

Finalmente, se incluye una comparativa visual y resumida del estado de la misión antes y después de aplicar la contramedida, facilitando una comprensión global del resultado.