Integración de MITRE ATT&CK en la Detección de Ransomware

Camilo Andrés Quintero Rodríguez

Juan Sebastián Velasquez Rodríguez

Santiago Diaz Rojas

Ransomware: Definición y Características Esenciales

El ransomware es un tipo de malware que restringe el acceso a determinadas partes o archivos del sistema operativo infectado y pide un rescate a cambio de quitar esta restricción.

Mecanismo de Bloqueo

El software malicioso bloquea el acceso del usuario a sus archivos o dispositivo, impidiendo su uso normal.

Demanda de Rescate

Posteriormente, se exige un pago (generalmente en criptomonedas) para restaurar el acceso y descifrar los datos.

Secuestro de Datos

Según IBM, retiene como rehenes datos confidenciales o el dispositivo, amenazando con mantenerlos bloqueados o con publicarlos.

MITRE ATT&CK: Un Marco Común para la Ciberseguridad

MITRE ATT&CK es un marco de conocimiento abierto y actualizado que proporciona una base de datos exhaustiva sobre las tácticas, técnicas y procedimientos (TTP) utilizados por actores de amenazas.

Propósito Principal

Ayudar a las organizaciones a modelar, detectar, prevenir y mitigar amenazas basándose en comportamientos adversarios observados en el mundo real.

Lenguaje Común

Facilita la colaboración y el intercambio de información entre profesionales al establecer una taxonomía estructurada para describir las actividades de los atacantes.

Rol Estratégico de ATT&CK en la Defensa

Mapeo de Incidentes

Permite clasificar y entender los eventos de seguridad dentro de un contexto de ataque conocido.

Simulación de Ataques

Fundamental para ejercicios de equipo rojo (Red Team) y para evaluar la efectividad de las defensas existentes.

Optimización de Detección

Guía la creación de reglas de detección más precisas y basadas en el comportamiento real del adversario.

Mejora Continua

Herramienta estratégica que capacita para fortalecer las defensas y mejorar la postura de seguridad general de la organización.

Hipótesis Central del Proyecto (POC)

Hipótesis Principal (H1)

La integración de MITRE ATT&CK en un sistema modular de análisis de eventos simulados (como el desarrollado en este POC) permite identificar de manera efectiva secuencias de TTPs asociadas a ransomware.

Esto facilita la generación de alertas tempranas y la comprensión de patrones, mejorando la capacidad de respuesta en entornos controlados.

Hipótesis Nula

El mapeo sistemático con MITRE ATT&CK sobre eventos simulados no aporta mejoras relevantes en la detección, análisis o mitigación de ataques de ransomware respecto a métodos tradicionales.

Implementación del POC: Propósito y Resultados Esperados

1

¿Qué es un POC?

Un experimento rápido (*Proof of Concept*) para verificar la validez de una idea antes de invertir grandes recursos. No requiere perfección, solo demostrar el concepto.

2

Propósito en el Estudio

Evaluar si la matriz ATT&CK, integrada en un sistema modular, permite identificar y comprender mejor las técnicas de ransomware simulado.

3

Resultados Clave

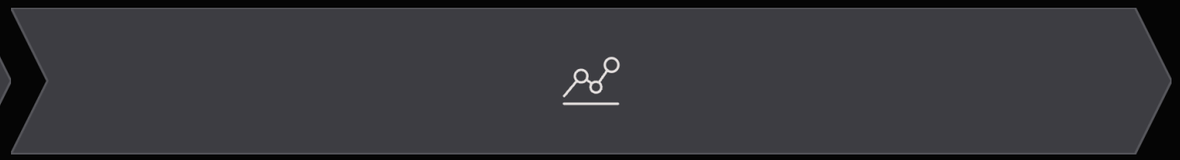
- Visualizar secuencias de técnicas de ransomware mediante mapeo ATT&CK.
- Validar la utilidad del enfoque modular para la correlación y alerta.
- Obtener evidencia para desarrollar soluciones de defensa adaptables.

Arquitectura Modular del POC: Flujo de Análisis

La arquitectura se diseñó para ser ligera y fácilmente adaptable, utilizando Python para el procesamiento central.

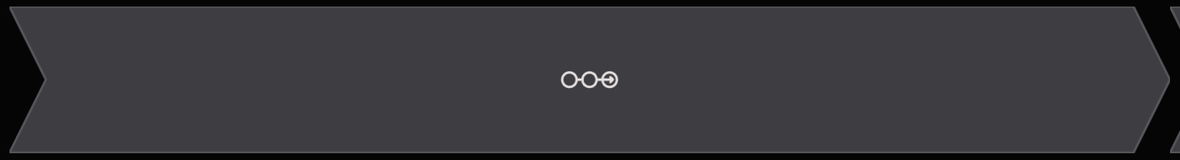
Módulo de Ingesta

Ingesta de eventos simulados (JSON) generados por Caldera desde la carpeta `data/`.



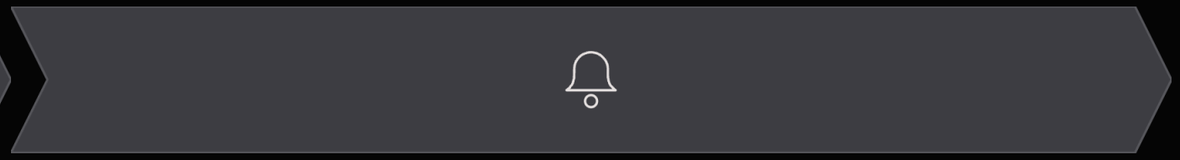
Procesamiento y Mapeo

Script que lee eventos, los mapea automáticamente a técnicas ATT&CK y los almacena en una base de datos ligera (SQLite).



Detección de Secuencias

Análisis de la base de datos para identificar secuencias de TTPs que indican patrones de ataque malicioso.



Visualización (Dashboard)

Aplicación web (Flask + Pandas) que muestra eventos, técnicas detectadas y alertas generadas de forma intuitiva.

Ventaja: La modularidad permite modificar o reemplazar fácilmente cada componente sin afectar el flujo general del sistema.

Caldera: La Plataforma de Simulación de Adversarios

Caldera, desarrollada por MITRE, es fundamental para nuestro POC. Permite automatizar la ejecución de técnicas de ataque cibernético en entornos controlados de forma segura.

Operación

Simulación completa que genera eventos.

Adversario

Perfil de atacante con un conjunto de habilidades.

Habilidad

Acción específica mapeada a una técnica ATT&CK (ej. T1083).

Agente

Programa ligero en el sistema objetivo que ejecuta las acciones.

Rol de Caldera y Generación de Datos

Caldera fue clave para obtener logs realistas y estructurados, validando el sistema de análisis.

1. Despliegue de Agente

Agente en entorno de laboratorio para ejecutar acciones simuladas.

2. Diseño del Adversario

Definición de habilidades personalizadas que cubren fases críticas del ataque (exfiltración, cifrado, evasión).

3. Ejecución de Operaciones

Simulaciones de ataque que generan eventos detallados.

4. Recolección de Logs

Eventos registrados en archivos JSON, sirviendo como datos base para el POC.

Estructura de los Datos Simulados para el Análisis

Cada registro JSON representa una acción adversaria con el contexto necesario para el mapeo y la detección de patrones de ransomware.

Campos Clave del Evento

- Comando Ejecutado (acción realizada por el agente).
- **Técnica ATT&CK Asociada** (ej. T1083 - File Discovery, T1486 - Data Encrypted).
- Metadatos del Agente (identificador, host, privilegios).
- Metadatos de la Operación y Adversario (contexto temporal y origen).
- Estado y Plataforma (resultado de la acción y SO).