Uso de MITRE ATT&CK para Mapear Técnicas de Ransomware

Santiago Diaz Rojas, Camilo Andrés Quintero Rodríguez, Juan Sebastián Velásquez Rodríguez

Programa de Ingeniería de Sistemas
Escuela Colombiana de Ingeniería Julio Garavito
mail: {santiago.diaz-r, camilo.quintero-r, juan.velasquez-r}@mail.escuelaing.edu.co

Profesor: Ing. Diego Alexander López Correa

Materia: Seguridad y Privacidad de TI (SPTI)
Escuela Colombiana de Ingeniería Julio Garavito

***Abstract*—Este trabajo explora el uso de la matriz MITRE ATT&CK para mapear y analizar técnicas utilizadas por ransomware modernos. Se presenta un estudio del estado del arte sobre metodologías de ciberseguridad basadas en ATT&CK, se identifican patrones comunes de ataque, y se propone una hipótesis sobre la eficacia de este enfoque para anticipar y mitigar amenazas de ransomware. Además, se desarrolla un POC modular que ingiere eventos simulados, los mapea a técnicas ATT&CK, detecta secuencias de TTPs y genera alertas, visualizando los resultados en un dashboard. Los datos de simulación se generan mediante la plataforma Caldera, empleando agentes, adversarios y operaciones personalizadas.**

***Index Terms*—Ransomware, MITRE ATT&CK, Ciberseguridad, Técnicas de ataque, Mapeo de amenazas, Caldera, Simulación.**

I. Introducción

El ransomware se ha convertido en una de las principales amenazas en ciberseguridad debido a su capacidad de cifrar datos críticos y extorsionar a organizaciones. MITRE ATT&CK es un marco de conocimiento que documenta técnicas y tácticas de ciberataques, permitiendo a los defensores mapear comportamientos de atacantes y fortalecer estrategias de mitigación. En este trabajo se presenta un POC que integra la matriz ATT&CK y la plataforma Caldera para simular ataques, analizar eventos y validar la detección de técnicas de ransomware en un entorno controlado.

II. Estado del Arte

A. Ransomware

1) Definición y características: 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.

Este tipo de software malicioso bloquea al usuario el acceso a sus archivos o dispositivo, luego demanda un pago para restaurar el acceso.

Según IBM, el ransomware es un tipo de malware que retiene como rehenes los datos confidenciales o el dispositivo de una víctima, amenazando con mantenerlos bloqueados, o algo peor, a menos que la víctima pague un rescate al atacante

2) Evolución histórica:

a) Orígenes y primeras manifestaciones: El ransomware tiene sus raíces en los años 80 y 90. En 1989, el "Troyano del SIDA" marcó uno de los primeros intentos de extorsión digital, aunque en una forma rudimentaria. Sin embargo, fue en la década de 2000 cuando el ransomware comenzó a ganar notoriedad, con variantes como Gpcode y Gpcode.ak, que cifraban archivos y exigían un rescate. Estos primeros ejemplares eran relativamente sencillos y no se propagaban de manera autónoma.

b) Avances técnicos y expansión: A medida que avanzaba la tecnología, también lo hacían las capacidades del ransomware. A partir de 2013, comenzaron a surgir variantes más sofisticadas que empleaban técnicas de cifrado más robustas y métodos de propagación más eficientes. Además, se empezó a observar un cambio en el modelo de negocio, con el surgimiento de ransomware-as-a-service (RaaS), donde los desarrolladores ofrecían su malware como un servicio a otros ciberdelincuentes.

c) Auge de ataques masivos y sofisticación: Entre 2016 y 2017, el ransomware alcanzó su punto máximo de notoriedad con ataques de gran escala como WannaCry y NotPetya. Estos incidentes demostraron la capacidad del ransomware para propagarse rápidamente a través de redes vulnerables, afectando a miles de organizaciones en todo el mundo. Además, se evidenció la evolución hacia modelos de doble extorsión, donde los atacantes no solo cifraban los datos, sino que también amenazaban con su divulgación si no se pagaba el rescate.

d) Tendencias actuales y amenazas emergentes: En la actualidad, el ransomware sigue siendo una amenaza significativa. Los atacantes emplean técnicas avanzadas como el uso de vulnerabilidades de día cero, ataques dirigidos a la cadena de suministro y la explotación de sistemas de control industrial. Además, se observa una creciente profesionalización de los grupos de ciberdelincuentes, con estructuras organizativas complejas y modelos de negocio bien definidos.

3) Familias más conocidas: Algunas de las familias de ransomware más relevantes en los últimos años incluyen:

- **WannaCry:** Es un ransomware que se propagó de manera masiva en mayo de 2017, afectando a miles de organizaciones en más de 150 países. Se propagaba como un gusano informático que cifraba los datos en sistemas Windows y exigía un rescate en Bitcoin para recuperarlos. Aprovechaba una vulnerabilidad no parcheada de Microsoft conocida como EternalBlue, filtrada por el grupo Shadow Brokers, y se cree que el grupo norcoreano Lazarus estuvo detrás del ataque.

- **Ryuk:** Apareció en 2018 y está especializado en atacar grandes organizaciones, incluyendo hospitales y gobiernos. Se cree que es operado por el grupo criminal ruso Wizard Spider. Ryuk suele propagarse a través del malware TrickBot y combina algoritmos de cifrado avanzados, haciendo inaccesibles los datos de la víctima y exigiendo rescates elevados.

- **Conti:** Fue una de las operaciones de ransomware como servicio (RaaS) más notorias, activa desde 2020 hasta su suspensión en 2022. También vinculada al grupo Wizard Spider, Conti se centraba en instituciones públicas y privadas, cifrando grandes volúmenes de datos de manera rápida y empleando técnicas sofisticadas para evadir detecciones, generando sumas significativas de dinero.

- **LockBit:** Es un ransomware que opera bajo el modelo RaaS y se dirige a organizaciones de todo el mundo, incluyendo empresas de tecnología e instituciones financieras. LockBit se especializa en cifrar sistemas de manera rápida y automatizada, y amenaza con filtrar la información de las víctimas si no se paga el rescate. Desde su aparición en enero de 2020, ha evolucionado con múltiples versiones y una red de afiliados que distribuyen su malware.

4) Tácticas y técnicas usadas: Según Arctic Wolf, los ataques de ransomware suelen seguir una serie de etapas bien definidas, cada una con tácticas y técnicas específicas:

a) Acceso Inicial (Initial Access): Técnicas comunes:

- **Phishing:** Envío de correos electrónicos fraudulentos para obtener credenciales o instalar malware.
- **Explotación de vulnerabilidades públicas:** Aprovechamiento de fallos conocidos en software sin parchear.
- **Acceso a través de RDP:** Uso de conexiones de escritorio remoto comprometidas.

b) Ejecución (Execution): Técnicas comunes:

- **Scripts maliciosos:** Uso de PowerShell o scripts por lotes para ejecutar el ransomware.
- **Carga útil de malware:** Descarga de componentes adicionales desde servidores remotos.

c) Persistencia (Persistence): Técnicas comunes:

- **Modificación de registros de inicio:** Alteración de claves del registro para asegurar la ejecución del malware al iniciar el sistema.
- **Instalación de servicios maliciosos:** Creación de servicios que permiten la ejecución continua del ransomware.

d) Escalamiento de Privilegios (Privilege Escalation): Técnicas comunes:

- **Explotación de vulnerabilidades locales:** Aprovechamiento de fallos en el sistema operativo para obtener mayores privilegios.
- **Uso de credenciales robadas:** Empleo de credenciales obtenidas para acceder a recursos restringidos.

e) Defensa Evasión (Defense Evasion): Técnicas comunes:

- **Desactivación de antivirus:** Inhabilitación de software de seguridad para evitar detección.
- **Encriptación de comunicaciones:** Uso de canales cifrados para ocultar la actividad maliciosa.

f) Movimiento Lateral (Lateral Movement): Técnicas comunes:

- **Uso de herramientas administrativas:** Empleo de herramientas como PsExec para moverse entre sistemas.
- **Acceso a través de credenciales compartidas:** Utilización de credenciales válidas para acceder a otros sistemas.

g) Recopilación (Collection): Técnicas comunes:

- **Acceso a archivos sensibles:** Identificación y recopilación de datos críticos para la organización.
- **Captura de pantallas:** Obtención de información visual del sistema afectado.

h) Exfiltración (Exfiltration): Técnicas comunes:

- **Transferencia de archivos:** Envío de datos robados a servidores externos.
- **Uso de canales cifrados:** Empleo de protocolos seguros para ocultar la exfiltración.

i) Impacto (Impact): Técnicas comunes:

- **Cifrado de datos:** Encriptación de archivos para exigir un rescate.
- **Destrucción de datos:** Eliminación de información crítica para causar daño.
- **Interrupción de servicios:** Bloqueo de acceso a sistemas y servicios esenciales.

j) Tecnologías comunes utilizadas:

- Malware como servicio (RaaS): Plataformas que permiten a los ciberdelincuentes alquilar herramientas de ransomware.
- Exploits de día cero: Aprovechamiento de vulnerabilidades desconocidas en el software.
- Troyanos de acceso remoto (RATs): Herramientas que permiten el control remoto de sistemas infectados.
- Redes de bots (Botnets): Redes de dispositivos comprometidos utilizadas para distribuir el ransomware.
- Cifrado fuerte: Uso de algoritmos robustos para asegurar los archivos y dificultar su recuperación sin la clave de descifrado.

5) Impacto y consecuencias: El ransomware tiene consecuencias significativas en distintas dimensiones:

- **Económicas:** Una de las consecuencias más relevantes es la pérdida de ingresos debido a la paralización parcial o total de las operaciones. Además, las organizaciones deben asumir los costos adicionales para enfrentar el incidente, incluyendo la posibilidad de tener que pagar un rescate.

- **Tecnológicas:** La principal consecuencia tecnológica es la pérdida de información. Si una empresa no cuenta con copias de seguridad recientes o herramientas para descifrar el ransomware, es muy probable que la reconstrucción de los datos sea una tarea inviable.
- **Sociales:** Los ciberdelincuentes pueden revelar información confidencial de la empresa y de sus clientes, lo que podría resultar en multas, procesos legales y daños irreparables a la reputación. La pérdida de datos también puede afectar la confianza del cliente.

B. MITRE ATT&CK

1) Definición y propósito: MITRE ATT&CK es un marco de conocimiento abierto y en constante actualización que proporciona una base de datos exhaustiva sobre las tácticas, técnicas y procedimientos (TTP) utilizados por actores de amenazas en el ciberespacio. Su propósito principal es ayudar a las organizaciones a modelar, detectar, prevenir y mitigar amenazas de ciberseguridad basándose en comportamientos adversarios observados en el mundo real.

Este marco no es una herramienta de software, sino una taxonomía estructurada que permite a los equipos de seguridad mapear incidentes, realizar simulaciones de ataques (como ejercicios de equipo rojo), mejorar la detección de amenazas y optimizar las políticas de respuesta a incidentes. Además, facilita la colaboración y el intercambio de información entre profesionales de la seguridad al establecer un lenguaje común para describir las actividades de los atacantes.

En resumen, MITRE ATT&CK es una herramienta estratégica que capacita a las organizaciones para comprender mejor las tácticas y técnicas empleadas por los atacantes, permitiéndoles fortalecer sus defensas y mejorar su postura de seguridad general.

2) Estructura del marco: MITRE ATT&CK se organiza como una taxonomía estructurada que clasifica los comportamientos de los atacantes en distintos niveles:

a) Tácticas: Representan los objetivos de alto nivel que un atacante busca lograr durante un ciberataque, como el acceso inicial, la persistencia, el movimiento lateral o la exfiltración de datos.

b) Técnicas: Son las acciones específicas que los atacantes realizan para alcanzar cada táctica. Por ejemplo, para la táctica de acceso inicial, una técnica puede ser el phishing o la explotación de vulnerabilidades.

c) Sub-técnicas: Algunas técnicas se dividen en sub-técnicas que detallan métodos más específicos de ejecución, proporcionando un nivel de granularidad mayor para el análisis y la defensa.

d) Matrices por plataforma: Las tácticas y técnicas se representan en matrices categorizadas por plataforma, como Windows, Linux, macOS, dispositivos móviles o entornos en la nube. Esto permite a los equipos de seguridad visualizar y mapear las amenazas según el contexto tecnológico de su organización.

Esta estructura facilita la comprensión, la detección y la mitigación de ataques, así como la planificación de ejercicios de simulación y la mejora de políticas de seguridad.

3) Uso en estudios y análisis de ciberseguridad: El marco MITRE ATT&CK ha sido ampliamente adoptado en investigaciones académicas, reportes de la industria y prácticas de defensa cibernética debido a su capacidad para estandarizar la descripción de tácticas y técnicas de los atacantes.

En el ámbito académico, se ha utilizado para mapear ataques de ransomware y analizar la evolución de las técnicas empleadas por distintas familias de malware. Por ejemplo, estudios de la Universidad de Surrey (2021) y la Universidad de Oslo (2022) aplicaron ATT&CK para correlacionar eventos en incidentes de ransomware, identificando patrones recurrentes en fases de acceso inicial y movimiento lateral.

En la industria, empresas como IBM, CrowdStrike y Mandiant han empleado ATT&CK en informes de *threat intelligence* para mapear campañas de ransomware y *Advanced Persistent Threats* (APTs). Esto ha permitido a los analistas visualizar qué técnicas son más comunes y priorizar controles de seguridad en función de los riesgos más probables.

Además, organismos de ciberseguridad como CISA y ENISA han integrado ATT&CK en guías y marcos de referencia para la protección de infraestructuras críticas. Un ejemplo es la evaluación de seguridad en el sector de la salud, donde ATT&CK se utilizó para modelar escenarios de ataque contra hospitales y sistemas de historia clínica electrónica, mejorando las estrategias de detección y respuesta.

Finalmente, ATT&CK también se emplea en ejercicios de *red teaming* y *purple teaming*, permitiendo a los defensores comparar los resultados de simulaciones de ataque con las técnicas documentadas. Esto contribuye a evaluar la cobertura de detección de las organizaciones y a fortalecer sus capacidades defensivas frente a amenazas reales.

4) Ventajas y limitaciones: El marco MITRE ATT&CK presenta una serie de beneficios importantes que lo convierten en una referencia ampliamente utilizada en el ámbito de la ciberseguridad. Entre sus principales ventajas se encuentran la estandarización en la descripción de tácticas, técnicas y procedimientos (TTPs), lo que facilita la comunicación entre equipos de seguridad; su reconocimiento y adopción global, que lo consolida como un punto de referencia común para la industria; y su utilidad en actividades de Threat Intelligence, dado que permite mapear comportamientos adversarios de forma estructurada y consistente.

No obstante, ATT&CK también posee ciertas limitaciones. Una de ellas es que no provee mitigaciones técnicas exhaustivas ni específicas para cada técnica, por lo que requiere de interpretación y adaptación por parte de los analistas. Además,

su enfoque depende de la calidad de la información disponible, lo que puede generar vacíos en ciertos entornos o sectores. Finalmente, debido a la evolución constante de las amenazas, el marco debe actualizarse periódicamente, lo que implica que su aplicación nunca es definitiva y exige un seguimiento continuo por parte de las organizaciones.

C. Aplicaciones Previas

Diversos trabajos académicos y reportes de la industria han utilizado el marco MITRE ATT&CK para mapear ataques de malware y ransomware, lo que permite comprender mejor los patrones de amenaza y mejorar defensas. A continuación, algunos ejemplos relevantes:

- Fujii. (2022) realizaron un análisis sobre 26.078 muestras de malware en diferentes sandboxes en línea para observar cómo se mapeaban automáticamente comportamientos a técnicas ATT&CK, encontrando diferencias importantes según la sandbox usada.

- Rahman. (2024) analizaron más de 667 reportes de inteligencia de amenazas (CTI) para identificar cuáles técnicas ATT&CK aparecen con mayor frecuencia, qué pares de técnicas ocurren con más regularidad, y cómo esto puede servir para priorizar controles defensivos.

- Microsoft, en las evaluaciones MITRE Engenuity de 2022, demostró que su solución (Microsoft 365 Defender) cubre de forma comprehensiva muchas de las técnicas usadas por ransomware operado manualmente, mostrando cómo las defensas modernas pueden mapearse bien frente al marco.

- MITRE publicó recientemente hallazgos sobre soluciones empresariales evaluadas frente a comportamientos de ransomware en plataformas Windows, evaluando no solo detección sino también tasas de falsos positivos, lo que revela los retos prácticos de usar ATT&CK para medir defensa real.

- Insikt Group (Recorded Future) identificó técnicas comunes de ransomware, las mapeó a ATT&CK y generó reglas Sigma para detección anticipada, subrayando cuánto pesa la táctica de *Defense Evasion* en estos ataques.

- Un estudio de caso de Microsoft describe un incidente real de ransomware, donde se rastreó cronológicamente cómo ocurrieron el acceso inicial, el movimiento lateral, la extracción de credenciales y el cifrado, y cómo se detectaron esas fases usando herramientas basadas en ATT&CK.

Estos ejemplos muestran que ATT&CK no sólo sirve para clasificación teórica, sino también para análisis práctico, evaluación de tecnologías, creación de reglas de detección y mejora de los procesos de respuesta a incidentes.

III. Hipótesis de trabajo

A. Hipótesis principal

La integración de la matriz 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 los patrones de ataque, mejorando la capacidad de respuesta ante incidentes en entornos controlados.

B. Hipótesis nula

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

C. Hipótesis secundarias

- H2: Los eventos generados por simulaciones con Caldera pueden ser mapeados eficientemente a un conjunto reducido de técnicas ATT&CK, representando fielmente el comportamiento de ransomware.
- H3: El análisis de secuencias de eventos simulados permite identificar combinaciones de técnicas que anticipan fases críticas del ataque, como la exfiltración o el cifrado de datos.
- H4: La visualización y correlación de eventos en el dashboard del POC, basada en ATT&CK, facilita la priorización de controles defensivos y la toma de decisiones informadas.

IV. Metodología

El estudio usa métodos cualitativos y cuantitativos. Las simulaciones y los datos los genero yo mediante Caldera.

A. Alcance y objetivos

Se analizan simulaciones de ransomware ejecutadas en Caldera. Objetivos principales:

- Detectar cadenas de técnicas ATT&CK asociadas a ransomware.
- Identificar patrones recurrentes y su frecuencia.
- Evaluar la capacidad de detectar variantes.

B. Datos

La fuente principal son los eventos exportados por Caldera (`events.json`) que ya incluyen las técnicas ATT&CK mapeadas. También se usan los artefactos generados en laboratorio.

C. Procedimiento

- Ejecutar operaciones en Caldera para cada variante de ataque que se quiera probar.
- Leer los eventos por host y ordenar cronológicamente las técnicas observadas.
- Detectar secuencias relevantes de técnicas.
- Guardar y listar las alertas generadas para su análisis.

D. Análisis

Se calcularán métricas sencillas:

- Frecuencia de cada técnica y de cada cadena detectada.
- Coocurrencias entre técnicas.
- Tiempos entre pasos dentro de una cadena.

V. Implementación del POC

A. ¿Qué es un POC?

Un POC (*Proof of Concept*) es un experimento rápido para comprobar si una idea funciona antes de invertir grandes recursos. Se asemeja a construir un prototipo: no tiene que ser perfecto, solo demostrar la validez de la idea.

B. Propósito del POC en este caso

Evaluar si la integración de la matriz MITRE ATT&CK en un sistema modular de análisis de eventos simulados permite identificar y comprender mejor las técnicas empleadas por ransomware, facilitando la detección y respuesta ante incidentes en entornos controlados.

C. Resultados esperados

- Visualizar y analizar secuencias de técnicas de ransomware mediante el mapeo ATT&CK, utilizando datos generados por simulaciones realistas con Caldera.
- Validar la utilidad del enfoque modular para correlacionar eventos, detectar patrones de ataque y generar alertas de forma más precisa.
- Obtener evidencia práctica sobre la capacidad del sistema para apoyar la investigación y el desarrollo de soluciones de defensa, considerando la posibilidad de adaptar el modelo a escenarios más complejos.

VI. Arquitectura del POC

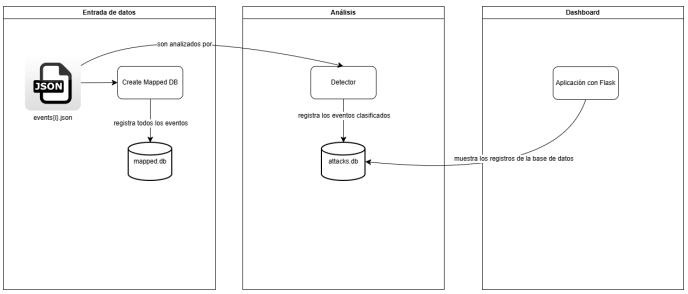

Figure 1. Diagrama general del sistema

A. Propósito

Implementar un POC ligero que:

- Ingesta eventos (json).
- Mapea eventos a técnicas ATT&CK.
- Detecta secuencias de TTPs.
- Genera alertas.
- Muestra resultados en un dashboard simple con Panda de Python.

B. Descripción extendida de la arquitectura

El proyecto está organizado en varios módulos que interactúan de forma secuencial y clara:

- Módulo de ingesta: los eventos simulados se almacenan en archivos JSON dentro de la carpeta `data/`. Cada evento representa una acción adversaria, incluyendo metadatos como comandos ejecutados, técnicas ATT&CK asociadas y contexto operacional.
- Procesamiento y mapeo: un script dedicado lee los eventos y los mapea automáticamente a técnicas ATT&CK, enriqueciendo la información con detalles relevantes para análisis posteriores. El resultado se almacena en una base de datos ligera.
- Detección de secuencias: otro script analiza la base de datos para identificar secuencias de TTPs (Tactics, Techniques, and Procedures) que puedan indicar actividades maliciosas o patrones de ataque.
- Generación de alertas: cuando se detectan patrones sospechosos, el sistema genera alertas que pueden ser consultadas por el usuario.
- Visualización en dashboard: una aplicación web construida con Flask y Pandas permite visualizar los eventos, las técnicas detectadas y las alertas generadas. El dashboard facilita la exploración y el análisis de los datos de forma intuitiva.

Tecnologías principales: Python (scripts y backend), Flask (dashboard web), Pandas (procesamiento de datos), SQLite (base de datos ligera), HTML (plantillas para la interfaz).

Ventajas: la arquitectura modular permite modificar, ampliar o reemplazar fácilmente cada componente. El uso de archivos JSON y una base de datos simple facilita la integración y el análisis rápido de los datos.

VII. Uso de Caldera en el POC

A. ¿Qué es Caldera?

Caldera es una plataforma de simulación de adversarios desarrollada por MITRE, diseñada para automatizar la ejecución de técnicas de ataque cibernético en entornos controlados. Su objetivo principal es ayudar a probar y mejorar las capacidades de detección y respuesta de los sistemas de defensa, permitiendo simular comportamientos de atacantes reales de manera segura.

B. Conceptos clave en Caldera

- Agente: es un programa ligero que se instala en el sistema objetivo y ejecuta las acciones simuladas. El agente reporta los resultados de cada acción a la plataforma Caldera.
- Adversario: representa un perfil de atacante, compuesto por una serie de habilidades (técnicas ATT&CK) que definen su comportamiento y estrategia.
- Habilidad: cada habilidad es una acción específica que el adversario puede ejecutar, como listar archivos, exfiltrar información o simular cifrado de datos. Las habilidades están asociadas a técnicas ATT&CK.
- Operación: es una simulación completa en la que uno o varios adversarios ejecutan sus habilidades a través de los agentes, generando una secuencia de eventos que pueden ser analizados posteriormente.

C. Rol de Caldera en el proyecto

En nuestro POC, Caldera fue fundamental para generar los datos de simulación que alimentan el sistema. Utilizamos la plataforma para crear agentes y adversarios personalizados, y ejecutamos varias operaciones que simulan ataques reales. El proceso fue el siguiente:

1) Se desplegó un agente en el entorno de laboratorio, encargado de ejecutar las acciones simuladas y reportar los resultados.
2) Cada integrante del equipo diseñó un adversario, definiendo un conjunto de habilidades que representaban diferentes tácticas y técnicas de ataque.
3) Las habilidades se seleccionaron y configuraron para cubrir distintas fases del ciclo de ataque, como descubrimiento, exfiltración, impacto y evasión.
4) Se ejecutaron varias operaciones, cada una representando una simulación de ataque distinta. Durante estas operaciones, los agentes ejecutaron las habilidades de los adversarios, generando eventos detallados que fueron registrados en archivos `JSON`.
5) Estos eventos sirvieron como base para el análisis y detección en el POC, permitiendo probar la capacidad del sistema para mapear técnicas ATT&CK, detectar secuencias de TTPs y generar alertas.

D. Ventajas de usar Caldera

El uso de Caldera permitió simular ataques de forma controlada y reproducible, generando logs realistas y estructurados. Esto facilitó el desarrollo y la validación del sistema, asegurando que los eventos procesados representaran escenarios relevantes y variados. Además, la flexibilidad de Caldera permitió adaptar las simulaciones a las necesidades del equipo, personalizando adversarios y habilidades según los objetivos del laboratorio.

E. Descripción de los datos simulados

Los datos simulados utilizados en el POC fueron generados mediante la plataforma Caldera, ejecutando operaciones de adversarios personalizados en un entorno controlado. Cada evento se almacena en archivos JSON y representa una acción adversaria, incluyendo información relevante para el análisis y la detección.

Cada registro de evento contiene, entre otros campos:

- Comando ejecutado: acción realizada por el agente.
- Técnica ATT&CK asociada: cada evento está mapeado a una técnica específica, como File and Directory Discovery (T1083) o Data Encrypted for Impact (T1486).
- Metadatos del agente: información sobre el agente que ejecutó la acción (identificador, grupo, privilegios, host, etc.).
- Metadatos de la operación y adversario: nombre de la operación, adversario responsable y contexto temporal.
- Estado y plataforma: resultado de la acción, sistema operativo y tipo de ejecutor.

Estos datos permiten analizar el comportamiento de los adversarios simulados, identificar patrones de ataque y validar la capacidad del sistema para mapear y detectar técnicas de ransomware. La estructura clara y detallada de los eventos facilita su procesamiento y visualización en el dashboard del POC.

VIII. Resultados Obtenidos

El desarrollo y ejecución del POC permitió simular escenarios de ataque de ransomware y analizar cómo se comportan estos incidentes cuando se mapean con la matriz MITRE ATT&CK. Se logró visualizar las técnicas empleadas por los adversarios, identificar patrones de ataque y generar alertas de manera intuitiva. El sistema demostró que es posible correlacionar eventos y entender mejor el ciclo de ataque, facilitando la toma de decisiones y el aprendizaje sobre cómo defenderse ante amenazas similares.

Además, el uso de Caldera permitió crear diferentes adversarios y operaciones, generando datos variados y realistas que enriquecieron el análisis. El dashboard desarrollado facilitó la exploración de los eventos y técnicas detectadas, mostrando de forma clara cómo evolucionan los ataques y qué tácticas son más frecuentes. El equipo pudo experimentar con la simulación de incidentes, observar el impacto de cada técnica y comprender la importancia de mapear los eventos para anticipar fases críticas del ataque.

IX. Conclusiones

El POC mostró que integrar MITRE ATT&CK en el análisis de eventos simulados ayuda a comprender y detectar mejor las técnicas de ransomware. La experiencia permitió al equipo familiarizarse con herramientas de simulación y mapeo, y evidenció que un enfoque modular y visual puede ser útil para fortalecer la defensa en ciberseguridad.

El proceso de simulación y análisis ayudó a identificar la utilidad de correlacionar eventos y técnicas, mostrando que el mapeo sistemático facilita la priorización de controles y la respuesta ante incidentes. El uso de Caldera resultó clave para generar escenarios diversos y realistas, permitiendo validar el funcionamiento del sistema en diferentes contextos. En resumen, el POC sirvió como una herramienta de aprendizaje y experimentación, demostrando el valor de combinar simulación y mapeo de amenazas para mejorar la preparación ante ataques de ransomware.

X. Repositorio del POC

El código fuente, scripts y documentación del POC están disponibles en el siguiente repositorio de GitHub:

https://github.com/CamiloQuinteroR/ransom-lab.git

References

[1] "Ransomware," *Wikipedia*, [En línea]. Disponible en: https://es.wikipedia.org/wiki/Ransomware. [Consultado: 16 de septiembre de 2025].

[2] IBM, "Ransomware," *IBM Think*, [En línea]. Disponible en: https://www.ibm.com/es-es/think/topics/ransomware. [Consultado: 16 de septiembre de 2025].

[3] Malwarebytes, "Ransomware," *Malwarebytes*, [En línea]. Disponible en: https://www.malwarebytes.com/es/ransomware. [Consultado: 16 de septiembre de 2025].

[4] Check Point Software Technologies, "Evolución del Ransomware," *Check Point Cyber Hub*, [En línea]. Disponible en: https://www.checkpoint.com/es/cyber-hub/ransomware/evolution-of-ransomware/. [Consultado: 16 de septiembre de 2025].

[5] Varonis, "A Brief History of Ransomware," *Varonis Blog*, [En línea]. Disponible en: https://www.varonis.com/blog/a-brief-history-of-ransomware. [Consultado: 16 de septiembre de 2025].

[6] Arctic Wolf, "The History of Ransomware," *Arctic Wolf Blog*, [En línea]. Disponible en: https://arcticwolf.com/resources/blog/the-history-of-ransomware/. [Consultado: 16 de septiembre de 2025].
[7] Sangfor Technologies, "Ransomware Evolution," *Sangfor*, [En línea]. Disponible en: https://www.sangfor.com/es/cybersecurity/innovations/ransomware-evolution. [Consultado: 16 de septiembre de 2025].
[8] "Ryuk (ransomware)," *Wikipedia*, [En línea]. Disponible en: https://es.wikipedia.org/wiki/Ryuk_(ransomware). [Consultado: 16 de septiembre de 2025].
[9] Cloudflare, "Ryuk ransomware," *Cloudflare*, [En línea]. Disponible en: https://www.cloudflare.com/es-es/learning/security/ransomware/ryuk-ransomware/. [Consultado: 16 de septiembre de 2025].
[10] Akamai, "What is Conti ransomware," *Akamai Glossary*, [En línea]. Disponible en: https://www.akamai.com/es/glossary/what-is-conti-ransomware. [Consultado: 16 de septiembre de 2025].
[11] "Conti (ransomware)," *Wikipedia*, [En línea]. Disponible en: https://en.wikipedia.org/wiki/Conti_(ransomware). [Consultado: 16 de septiembre de 2025].
[12] Kaspersky, "LockBit ransomware," *Kaspersky Resource Center*, [En línea]. Disponible en: https://latam.kaspersky.com/resource-center/threats/lockbit-ransomware. [Consultado: 16 de septiembre de 2025].
[13] "LockBit," *Wikipedia*, [En línea]. Disponible en: https://en.wikipedia.org/wiki/LockBit. [Consultado: 16 de septiembre de 2025].
[14] Arctic Wolf, "The Top 10 Ransomware TTPs," *Arctic Wolf Blog*, [En línea]. Disponible en: https://arcticwolf.com/resources/blog/the-top-10-ransomware-ttps/. [Consultado: 16 de septiembre de 2025].
[15] PwC, "El ransomware: más allá de una amenaza persistente," *PwC*, [En línea]. Disponible en: https://www.pwc.com/ia/es/publicaciones/perspectivas-pwc/El-ransomware-mas-alla-de-una-amenaza-persistente.html. [Consultado: 16 de septiembre de 2025].
[16] MITRE, "MITRE ATT&CK," [En línea]. Disponible en: https://attack.mitre.org/. [Último acceso: 16-sep-2025].
[17] IBM, "MITRE ATT&CK," [En línea]. Disponible en: https://www.ibm.com/es-es/think/topics/mitre-attack. [Último acceso: 16-sep-2025].
[18] Fortinet, "MITRE ATT&CK," [En línea]. Disponible en: https://www.fortinet.com/lat/resources/cyberglossary/mitre-attck. [Último acceso: 16-sep-2025].
[19] D3 Security, "Top MITRE ATT&CK Tactics and Techniques," [En línea]. Disponible en: https://d3security.com/blog/top-mitre-attack-tactics-and-techniques/#:~:text=Ejecuci%C3%B3n:%20Int%C3%A9rprete%20de%20comandos%20y,y%20el%20control%20no%20autorizados.. [Último acceso: 16-sep-2025].