Google Cloud
Security

Libro blanco

Más allá de marcar casillas: Aprovechar todo el potencial de MITRE ATT&CK con Google

Índice

Imagínese esto: Usted es un analista de seguridad que se enfrenta a un aluvión de alertas que señalan una posible brecha. Aparece un patrón familiar: spearphishing, inicios de sesión sospechosos, movimiento lateral. El adversario ya está en su red. Pero usted tiene una poderosa herramienta a su disposición: el marco MITRE ATT&CK® . Esta base de conocimientos actúa como su mapa de batalla en la guerra cibernética, estableciendo las tácticas y técnicas del enemigo. Con ATT&CK, puede identificar rápidamente la posición del atacante, predecir su próximo movimiento y desplegar contramedidas.

Desde 2013, esta base de conocimientos se ha convertido en el recurso de referencia para los equipos de seguridad de todo el mundo. Proporciona un lenguaje común para comprender las ciberamenazas, lo que permite a los defensores abordar las vulnerabilidades de forma proactiva y responder eficazmente a los ataques.

Pero aquí está el truco, simplemente hacer referencia al marco no es suficiente. Muchas organizaciones tienen dificultades para traducir los vastos conocimientos del ATT&CK en ideas prácticas. Puede que ajusten sus controles al marco, pero ¿después qué? ¿Cómo priorizan las amenazas? ¿Cómo proteger lo más importante?

En este informe técnico, profundizaremos en los retos a los que se enfrentan los equipos de operaciones de seguridad a la hora de aprovechar realmente la potencia de MITRE ATT&CK. Y lo que es más importante, desvelaremos la visión de Google para una nueva era de optimización de ATT&CK. Imagine un mundo en el que pueda:

- **Vaya más allá del mapeo básico:** Traduzca los conocimientos de ATT&CK en una estrategia de defensa a medida que se ajuste al perfil de riesgo exclusivo de su organización.
- **Priorizar estratégicamente las amenazas:** Céntrese en las amenazas más críticas y asigne los recursos estratégicamente.
- **Elimine los puntos ciegos:** Identifique y solucione proactivamente las brechas de seguridad antes de que los atacantes las exploten.
- **Optimice y agilice las operaciones:** Mejore la eficiencia y la colaboración mediante la automatización y la agilización de los flujos de trabajo.

Únase a nosotros en un viaje para redefinir cómo los equipos de SecOps aprovechan MITRE ATT&CK y construyen un futuro más seguro.

MITRE ATT&CK: un mapa dinámico de ciberamenazas

En el complejo panorama actual de amenazas, los equipos de SecOps necesitan una guía fiable para navegar por el mundo en constante evolución de los ciberataques. MITRE ATT&CK proporciona esa . Imagine una vasta biblioteca repleta de planos meticulosamente detallados de todos los ciberataques conocidos. Eso es básicamente lo que MITRE ATT&CK ofrece al mundo de la seguridad. Desarrollado por MITRE, una organización de investigación sin ánimo de lucro, este marco proporciona un catálogo estructurado y exhaustivo de las tácticas y técnicas de los adversarios.

Piénsalo de esta manera: cada "plano" de esta biblioteca describe una técnica de ataque específica, detallando las herramientas, procedimientos y comportamientos empleados por los actores maliciosos. Ya se trate de una estafa de phishing, el despliegue de malware o un sofisticado ataque de ransomware, ATT&CK desglosa la anatomía de estos ataques, proporcionando información valiosa sobre cómo se desarrollan.

Pero esta biblioteca no es estática; está en constante evolución, como el propio panorama de las amenazas. Cuando MITRE abrió sus por primera vez en 2013, se centró principalmente en los entornos empresariales tradicionales, es decir, en los sistemas Windows, macOS y Linux. Pero a medida que el mundo se desplazó hacia la nube, también lo hizo ATT&CK.

Reconociendo los desafíos únicos de la seguridad en la nube, MITRE amplió su biblioteca en 2019 para incluir planos de basados en la nube. Esta nueva ala de la biblioteca alberga esquemas detallados de ataques dirigidos a plataformas en la nube como Google Cloud, AWS y Microsoft Azure. Cubre todo, desde aplicaciones SaaS hasta infraestructura IaaS, proporcionando a los equipos de seguridad el conocimiento que necesitan para defenderse de las amenazas específicas de la nube.

Esta evolución constante es lo que hace que ATT&CK sea tan potente. Es un recurso vivo que permite a los equipos de operaciones de seguridad:

- **Descifrar las tácticas de los atacantes:** Mediante el estudio de estos planos, los equipos de operaciones de seguridad pueden comprender mejor las metodologías de los atacantes, predecir sus próximos movimientos y reforzar de forma proactiva sus defensas en todos los entornos.
- **Desarrollar contramedidas:** Los equipos de operaciones de seguridad pueden aprovechar ATT&CK para identificar vulnerabilidades y aplicar controles de seguridad eficaces, ya sea en las instalaciones o en la nube.
- **Hable un común:** ATT&CK proporciona un lenguaje universal para los profesionales de la seguridad, fomentando la colaboración y el intercambio de conocimientos en todo el sector.
- **Construir una defensa proactiva:** Al comprender las tácticas y técnicas empleadas por los atacantes, los equipos de seguridad pueden pasar de una postura de seguridad reactiva a una proactiva, anticipándose a las amenazas antes de que se materialicen, independientemente de dónde ataquen.

En esencia, MITRE ATT&CK es el arma secreta del profesional de SecOps. Es la clave para desbloquear una comprensión más profunda del panorama de amenazas, permitiendo a las organizaciones construir una postura de seguridad robusta y resistente en un mundo digital en constante cambio. Exploraremos esto más a fondo en la siguiente sección, pero simplemente tener acceso a esta biblioteca no es suficiente. El verdadero poder reside en aprovechar eficazmente sus conocimientos para optimizar su estrategia de seguridad.

Los retos de la puesta en marcha de MITRE ATT&CK

Hemos establecido que MITRE ATT&CK es una herramienta poderosa, una vasta biblioteca de tácticas y técnicas de los adversarios. Pero incluso la biblioteca más completa puede tener sus limitaciones. Confiar únicamente en el marco ATT&CK para llevar a cabo operaciones de seguridad eficaces puede plantear problemas.

La ilusión del 100% de cobertura

El marco ATT&CK proporciona una visión general de las técnicas de ataque conocidas, pero no tiene en cuenta todas las posibles variaciones o amenazas emergentes. Es como tener un mapa que muestra las carreteras principales pero omite las carreteras más pequeñas y los callejones donde los atacantes podrían estar al acecho. Algunos proveedores de seguridad afirman tener una "cobertura del 100%" basándose en las pruebas de proveedores de MITRE, pero a menudo son engañosas. Aunque estas pruebas son útiles para evaluar el rendimiento de los proveedores frente a escenarios de ataque conocidos, no garantizan una protección completa en entornos reales.

El propio MITRE subraya que las evaluaciones ofrecen información sobre cómo las soluciones pueden abordar las necesidades de seguridad específicas de una organización frente a adversarios conocidos. Sin embargo, los equipos de operaciones de seguridad a veces malinterpretan esto como una garantía de cobertura completa dentro del dominio declarado del proveedor. En realidad, el diablo está en los detalles. Una mirada más atenta suele revelar lagunas en la protección cuando se aplica a las particularidades de un entorno informático único.

Por ejemplo, un proveedor que afirme que detecta completamente las técnicas de manipulación de cuentas puede quedarse corto cuando se enfrenta a los sistemas operativos o aplicaciones específicos utilizados en su organización. Esto crea una peligrosa ilusión de seguridad, dejando expuestas vulnerabilidades críticas. La verdadera cobertura integral sigue siendo un objetivo difícil de alcanzar debido a la naturaleza dinámica de las ciberamenazas y a las complejidades inherentes a los diversos entornos informáticos.

Marcar casillas frente a evaluar riesgos

Tratar la matriz ATT&CK como una simple lista de comprobación puede ser problemático. Los equipos de operaciones de seguridad deben ir más allá marcar casillas y priorizar sus defensas basándose en una evaluación de riesgos exhaustiva. Esto incluye la identificación de activos críticos, la comprensión de los actores de amenazas con más probabilidades de atacarlos y la adaptación de sus controles de seguridad en consecuencia.

Incluso con este enfoque, el gran volumen de técnicas de la matriz ATT&CK puede abrumar a los equipos con pocos recursos. Intentar detectar todas y cada una de las técnicas es poco práctico.

Por ejemplo, evaluar las afirmaciones de los proveedores puede ser un campo minado. Un proveedor puede prometer protección contra la manipulación de cuentas en todos los sistemas operativos y aplicaciones SaaS. Pero luego, si se examina más de cerca, se descubre que Linux no es compatible y que ningún proveedor puede cubrir todas las SaaS. Sin una investigación cuidadosa, los equipos de operaciones de seguridad pueden caer en una falsa sensación de seguridad.

El carácter estático del marco

Aunque el marco ATT&CK se actualiza periódicamente, no siempre puede seguir el ritmo de la rápida evolución de los ciberataques. Constantemente surgen nuevas técnicas y tácticas, y los atacantes a menudo encuentran formas creativas de eludir las defensas conocidas.

Confiar únicamente en el marco ATT&CK puede crear una falsa sensación de seguridad, ya que es posible que no capte las amenazas más recientes ni tenga en cuenta los matices específicos de su entorno.

El eslabón perdido: Automatización e integración

Por último, la puesta en práctica del marco ATT&CK a menudo requiere un esfuerzo manual, transfiriendo información de la matriz a otras herramientas y flujos de trabajo de seguridad. Esta falta de automatización puede dar lugar a ineficiencias, errores y retrasos en la respuesta a las amenazas. Es como tener un mapa pero tener que calcular manualmente las distancias y las direcciones en lugar de utilizar un GPS.

Para optimizar realmente el uso de ATT&CK, las organizaciones necesitan una integración perfecta y procesos automatizados que traduzcan sus conocimientos en medidas prácticas dentro de sus operaciones de seguridad.

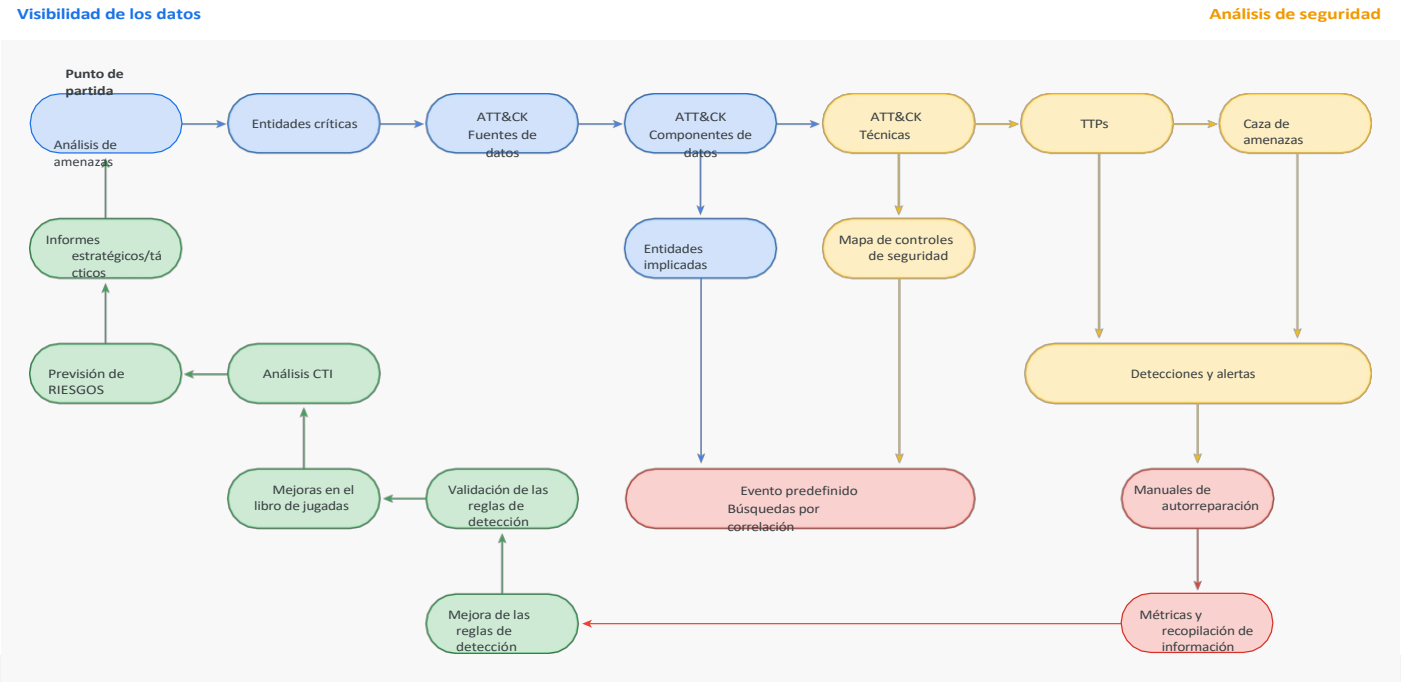
La visión de Google: Una nueva era de optimización MITRE ATT&CK

Basándose en el poder fundacional de MITRE ATT&CK, explorado en secciones anteriores, Google imagina un futuro que trasciende las limitaciones convencionales del marco. Creemos que mediante la integración de ATT&CK con otras prácticas recomendadas de ciberseguridad y el aprovechamiento de tecnologías de vanguardia, los equipos de operaciones de seguridad pueden superar los retos existentes y abrir una nueva era de eficiencia operativa, creando una postura de seguridad verdaderamente proactiva y resistente.

Cinco estrategias clave para los equipos de SecOps

1. **De la cobertura a la postura:** Como hemos comentado antes, no con marcar casillas en la matriz ATT&CK. Para defender realmente el entorno informático de su empresa, los equipos de operaciones de seguridad deben pasar de la mera cobertura a la evaluación y el perfeccionamiento continuos de su postura de seguridad. Esto implica varios pasos cruciales:

    - **Perfiles de amenazas:** Genere perfiles detallados de amenazas basados en comportamientos conocidos de adversarios prevalentes en su sector y área geográfica.
    - **Evaluación de la postura:** Evalúe la solidez de su postura de seguridad frente a estos perfiles de amenaza, identificando las Tácticas, Técnicas y Procedimientos (TTP) que requieren priorización.
    - **Primero las** joyas de la corona**:** Identifique sus activos de alto valor ("joyas de la corona") y combine este conocimiento con la priorización TTP para determinar las áreas más críticas para la defensa.
    - **Análisis de brechas:** Filtre sus hallazgos con la cobertura ATT&CK existente para descubrir cualquier brecha de seguridad.
    - **Mejora de los controles:** Desarrolle o mejore los controles de seguridad para subsanar las deficiencias detectadas y reforzar su postura general en materia de seguridad.
    - **Pruebas continuas:** Utilice plantillas preconfiguradas diseñadas en torno a técnicas específicas o cadenas de técnicas para probar la eficacia de sus controles de seguridad. Estas plantillas pueden ampliarse con el tiempo para incorporar nuevos procedimientos y garantizar la exhaustividad de las pruebas.
    - **Integración y medición:** Asigne cada caso de uso al marco ATT&CK de MITRE e integre la lógica de detección para cuantificar las mejoras cuantificables de sus capacidades de detección y corrección.



2. Priorizar es la clave: En el dinámico mundo de los ciberataques, no todas las amenazas son iguales. La inteligencia sobre amenazas en tiempo real le permite priorizar sus respuestas en función de las amenazas con más probabilidades de afectar a sus sistemas de misión crítica. Esto incluye:

- **Analizar la actividad de los actores de amenazas:** Observe la actividad de los actores de amenazas dentro de su entorno empresarial a través de la lente de ATT&CK, identificando dónde se concentra la actividad de amenazas y qué están haciendo los actores maliciosos internos y externos.
- **Identificación de desajustes:** Detecte desajustes entre su cartera de reglas y la actividad observada de los actores de amenazas. Esto pondrá de relieve las áreas del mapa ATT&CK en las que la densidad de reglas es desproporcionada en relación con el nivel de actividad de las amenazas, lo que le permitirá priorizar la implementación de nuevas reglas de detección.
- **Desarrollar perfiles de amenazas:** Cree perfiles de amenazas detallados que describan con precisión su empresa y generen una lista priorizada de técnicas de ATT&CK en las que centrarse. Esto le ayuda a identificar y defenderse contra las amenazas que tienen más probabilidades de dirigirse a su organización.

3. Aprovechar el poder de la inferencia: Imagine una herramienta capaz de predecir el próximo movimiento de un atacante basándose en sus tácticas actuales. El Technique Inference Engine, desarrollado por el Center for Threat Informed Defense, hace exactamente eso. Al aprovechar el aprendizaje automático y la inteligencia sobre amenazas, este motor permite a los equipos de operaciones de seguridad:

- **Priorizar la caza de amenazas:** Céntrese en los métodos de intrusión más probables durante los eventos de triaje cibernético.
- **Mejorar el análisis de incidentes:** Mejorar el análisis post mortem de los incidentes de seguridad.
- **Identifique lagunas:** Destaque las posibles lagunas de detección, detección y notificación en su dispositivo de seguridad.

- **Descubrir ataques relacionados:** Identificar vectores de ataque similares o relacionados.
- **Planifique la emulación de adversarios:** Cree planes eficaces de emulación de adversarios para probar y mejorar sus defensas.

El motor de inferencia utiliza un modelo de aprendizaje automático entrenado en inteligencia sobre ciberamenazas para recomendar probables TTP basadas en TTP de entrada conocidas. A que se detectan nuevas actividades, el modelo se puede volver a entrenar para incorporar TTPs de adversarios no vistas anteriormente, lo que garantiza que su equipo de seguridad se mantenga a la vanguardia.

4. Adoptar la matriz de la nube: A medida que las organizaciones migran cada vez más a la nube, la necesidad de un enfoque de ATT&CK específico para la nube se vuelve primordial. Las herramientas de seguridad tradicionales suelen tener dificultades con el volumen de registros de la nube y la naturaleza dinámica de los entornos de nube. La matriz de la nube proporciona una visión completa de las tácticas y técnicas empleadas en los ataques basados en la nube, aborda estos retos y ofrece orientación para mitigar las amenazas específicas de la nube.

- **El compromiso de Google:** Cuando MITRE presentó por primera vez las matrices de la nube en 2019, Google reconoció inmediatamente su importancia y patrocinó un proyecto para mapear controles de seguridad de Google Cloud Platform a ATT&CK. Este esfuerzo de colaboración con el Center for Threat Informed Defense (CTID), una organización de MITRE Engenuity, ha dado como resultado mapeos exhaustivos de técnicas en la nube a los controles de seguridad de AWS, Azure y GCP.
- **Amenazas únicas en la nube:** El uso del marco de ATT&CK para la nube es vital porque las vulnerabilidades de la nube a menudo difieren de las vulnerabilidades tradicionales en las instalaciones y pueden no estar incluidas en bases de datos como CVE. Las matrices de la nube ofrecen visibilidad de una amplia gama de ataques específicos de la nube, entre ellos:

  i. Acceso inicial a la cuenta
  ii. Comandos de ejecución
  iii. Persistencia para manipular cuentas
  iv. Escalada de privilegios
  v. Evasión de la defensa
  vi. Acceso con credenciales
  vii. Descubrimiento de servicios y cuentas
  viii. Movimiento lateral
  ix. Recogida de datos y correo electrónico
  x. Exfiltración de datos
  xi. Destrucción de datos
  xii. Ataques a datos cifrados
  xiii. Denegación de servicio
  xiv. Robo financiero
  xv. Secuestro de recursos

- **Visibilidad y entornos dinámicos:** La matriz de nube aborda el reto crítico de la visibilidad en entornos de nube en los que las herramientas tradicionales pueden ser menos eficaces. Al asignar fuentes de registro y controles de seguridad específicos a ATT&CK, se obtiene una comprensión más clara de la postura de seguridad de la nube. Esto es especialmente importante en entornos de nube dinámicos con prácticas DevOps, donde los entornos de desarrollo pueden ser más vulnerables a los ataques. La matriz de la nube ofrece orientación para mitigar estas amenazas únicas.

5. **Colaboración e intercambio de información:** En la lucha contra la ciberdelincuencia, la información es poder. Al fomentar la colaboración tanto interna como con colegas del sector, los equipos de SecOps pueden obtener una perspectiva más amplia del panorama de las amenazas y compartir las mejores prácticas de defensa.

- **Colaboración interna:** Implique a las partes interesadas de todos los departamentos en los debates sobre estrategias de seguridad, fomentando una cultura de responsabilidad compartida y comunicación abierta.
- **Acabar con los silos:** fomente el uso de herramientas de seguridad comunes y automatice los procesos para eliminar los silos de flujo de trabajo y reducir la carga de su equipo de SecOps.
- **Colaboración externa:** Aproveche recursos como los Centros de Análisis e Intercambio de Información (ISAC, por sus siglas en inglés) y el Centro de Defensa Informada contra Amenazas () CTID, por sus siglas en inglésspara conocer mejor las amenazas específicas del sector y colaborar con sus homólogos en estrategias de defensa.

Ventajas del enfoque de Google

Al adoptar la visión de Google para la optimización de ATT&CK, los equipos de SecOps pueden:

- **Vaya más allá de una postura de seguridad reactiva** e identifique y mitigue proactivamente las amenazas antes de que se materialicen.
- **Conocer mejor las tácticas de los adversarios** y adaptar sus defensas al perfil de riesgo específico de su organización.
- **Priorizar sus respuestas** basándose en la información sobre amenazas en tiempo real y centrarse en las amenazas que un mayor peligro.
- **Mejore la eficacia operativa** mediante la automatización y la agilización de los flujos de trabajo.
- **Fomentar la colaboración y el intercambio de información** para construir una defensa colectiva más sólida contra los ciberataques.

Mejore su seguridad con la visión de Google para MITRE ATT&CK

A lo largo de este libro blanco, hemos recorrido los entresijos del marco ATT&CK de MITRE, explorando sus puntos fuertes y sus limitaciones. Hemos visto cómo permite a los equipos de seguridad comprender las tácticas de los adversarios, predecir sus próximos movimientos y construir una defensa proactiva. Pero también hemos descubierto los desafíos: las limitaciones de los marcos estáticos, la ilusión de una cobertura del 100% y la necesidad crítica de priorización y automatización.

Ahora, es el momento de dar el siguiente paso.

Imagine un mundo en el que pueda integrar ATT&CK a la perfección en sus operaciones de seguridad, transformándolo de una guía de referencia en un arma dinámica contra las ciberamenazas. Esta es la visión de la que Google es pionero.

Principales conclusiones

- **Vaya más allá de la cartografía básica:** No se limite a marcar casillas. Traduzca los conocimientos de ATT&CK en una estrategia de defensa a medida, priorizando las amenazas en función de su perfil de riesgo único y centrándose en sus "joyas de la corona": sus activos más críticos.

- **Priorice como un profesional**: Aproveche la información sobre amenazas en tiempo real y la potencia del motor de inferencia de técnicas para anticiparse a las acciones de los atacantes y asignar los recursos de forma estratégica.
- **Adopte la matriz de la nube:** Navegue por los desafíos únicos de la seguridad en la nube con el marco específico para la nube de ATT&CK, obteniendo visibilidad y control en entornos de nube dinámicos.
- **Colaborar y vencer:** rompa los compartimentos estancos, fomente el intercambio de información y construya una defensa colectiva más sólida mediante la colaboración interna y externa.

La ventaja de Google

El enfoque de Google para la optimización de ATT&CK le permite:

- **Mitigue proactivamente las amenazas** antes de que perturben su negocio.
- **Conozca mejor las tácticas del adversario** y adapte sus defensas en consecuencia.
- **Mejore la eficacia operativa** mediante la automatización y la agilización de los flujos de trabajo.
- **Cree una postura de seguridad más resistente** mediante la evaluación y la mejora continuas.

¿Está preparado para liberar todo el potencial de MITRE ATT&CK y transformar sus operaciones de seguridad? Póngase en contacto con el equipo de Google Cloud Security hoy mismo para obtener más información sobre nuestras soluciones innovadoras y emprender un viaje hacia un futuro más seguro. Juntos, cambiemos las tornas contra los ciberataques.