Evaluación de MITRE ATT&CK

IBM Security ReaQta muestra las mejores prestaciones de su clase

Características más importantes

Promueve la continuidad de negocio al tiempo que libera al equipo de seguridad del análisis manual de ciberamenazas

Reduce la fatiga de alertas y simplifica la ciberseguridad generando el mínimo número de alertas de amenaza necesarias

Proporciona visibilidad completa de los endpoints para permitir una respuesta rápida en todas las etapas

Acerca del informe

ReaQta, una empresa de IBM, ha completado con éxito la evaluación de MITRE ATT&CK. Este informe muestra que ReaQta proporciona cobertura completa frente a ataques sofisticados, prácticamente sin intervención humana, al tiempo que genera alertas de primera calidad.

¿Qué es una evaluación de MITRE ATT&CK?

MITRE ATT&CK define un conjunto de etapas durante un ciberataque y evalúa la capacidad de las soluciones para detectar amenazas. Cada una de las etapas especificadas representa una “táctica” en la cadena de interrupción:

- Acceso inicial
- Ejecución
- Persistencia
- Elevación de privilegios
- Evasión de defensa
- Acceso con credencial
- Descubrimiento
- Movimiento lateral
- Recopilación
- Exfiltración
- Mandato y control

Cómo ayuda la evaluación de MITRE a las organizaciones

La evaluación no puntúa las soluciones y está diseñada para ayudar a las organizaciones a identificar la solución más adecuada que se ajuste a sus desafíos de seguridad específicos. Las organizaciones deben tener en cuenta que la evaluación se realiza en entornos aislados y tiene limitaciones. A veces algunas características de una solución están inhabilitadas porque no dan soporte a esa infraestructura de laboratorio específica, como en el caso de ReaQta NanoOS, en el que no se pudo utilizar el hipervisor en directo que se utiliza para detectar comportamientos maliciosos de alto nivel. No obstante, la plataforma funcionó bien, incluso sin su componente principal.

MITRE tiene un conjunto de técnicas identificadas, cada una de las cuales pertenece a un grupo de tácticas basado en el actor de amenaza seleccionado para la evaluación. MITRE eligió APT29 para esta ronda de evaluación.

Compromiso

Recopilación y evasión

Reconocimiento

Ampliación del acceso

Exfiltración

Limpieza

Promueve la continuidad de negocio al tiempo que libera al equipo de seguridad del análisis manual de ciberamenazas

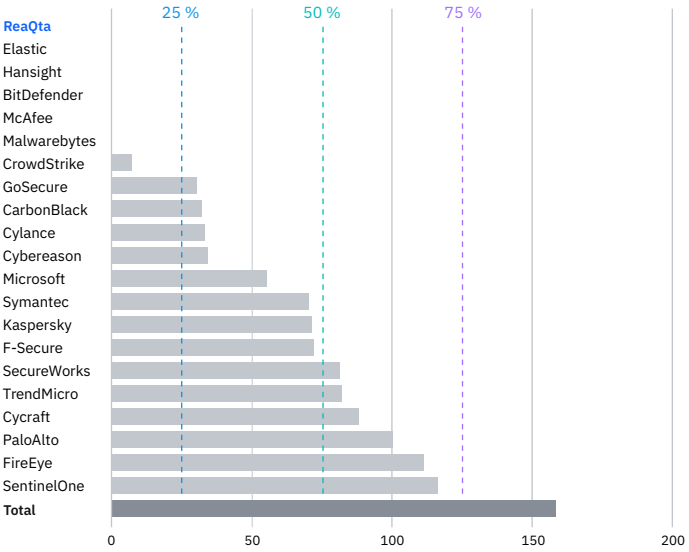
Antes de iniciar la evaluación, ReaQta decidió participar sin un proveedor de servicio de seguridad gestionado (MSSP), es decir, sin interacción humana durante el ataque. MITRE es una infraestructura de evaluación de tecnología, y parecía deshonesto que intervinieran personas en el proceso. Además, la contribución de las detecciones de los MSSP sesga considerablemente la evaluación. El equipo del centro de operaciones de seguridad (SOC) sabe que se está produciendo un ataque y exactamente dónde y cómo.

El método de MSSP no hubiera proporcionado a los clientes de ReaQta una evaluación justa de la tecnología. MITRE ha sido muy receptivo a los comentarios y, a partir de la tercera ronda, todas las empresas se evaluarán sin intervención humana.

Los MSSP aportan un gran valor, y los clientes deberían poder elegir libremente entre las implementaciones autónomas o con MSSP.

Como se muestra en el siguiente gráfico, el número de detecciones realizadas por personas afectó considerablemente a las detecciones generadas. En varios casos, más del 50 % de las detecciones, y hasta el 73 %, se crearon manualmente. Solo 6 empresas decidieron participar sin intervención humana.

Detecciones de MSSP (generadas manualmente)



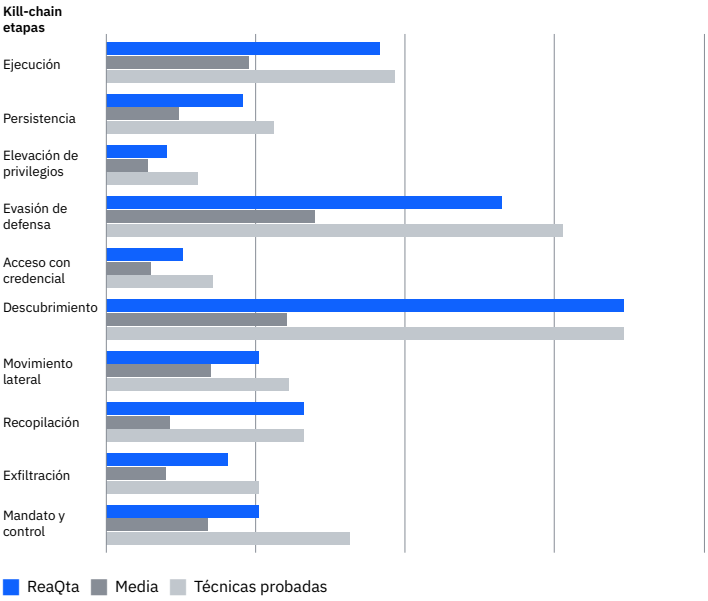
Detecciones manuales generadas por cada proveedor

Evaluación de MITRE Segunda ronda: APT29

Se probó la capacidad de los proveedores para detectar las tácticas y técnicas utilizadas por APT29 (también conocido como The Dukes, Cozy Bear y CozyDuke), un sofisticado adversario a nivel nacional conocido por su sigilosidad. APT29 es conocido por estar detrás de destacados ataques: el Pentágono en 2015, el Comité Nacional Demócrata en 2016 y los gobiernos de Noruega y Holanda en 2017.

El cambio respecto a la ronda anterior fue importante: APT3 (Primera ronda) es un actor de amenaza ruidoso, que utiliza distintas herramientas importándole mucho menos mantener un perfil bajo. Por otro lado, APT29 es extremadamente sigiloso, opera con un perfil muy bajo y depende en gran medida de LOLBins y de un programa malicioso sin archivos.

Cobertura de detección de técnicas (automatizada)



Cobertura de detección automática de ReaQta en comparación con la media

Resultados de la evaluación de ReaQta

El ataque se desarrolló durante dos días en los que los atacantes se adentraron progresivamente en la red tras obtener el acceso inicial. La gran mayoría de las operaciones se realizaron utilizando Microsoft PowerShell, en lugar de herramientas personalizadas y malware, a fin de mantener un perfil de detección bajo. El objetivo de la evaluación es mostrar cómo las soluciones probadas responden al ataque y qué tipo de visibilidad se proporciona durante toda la cyber kill chain

Como se desprende del resumen de los resultados de la evaluación, ReaQta proporciona visibilidad completa en toda la cyber kill chain. ReaQta detectó el 90 % de las tácticas y técnicas probadas, demostrando su capacidad para responder a las amenazas y remediarlas en cada etapa del ataque.

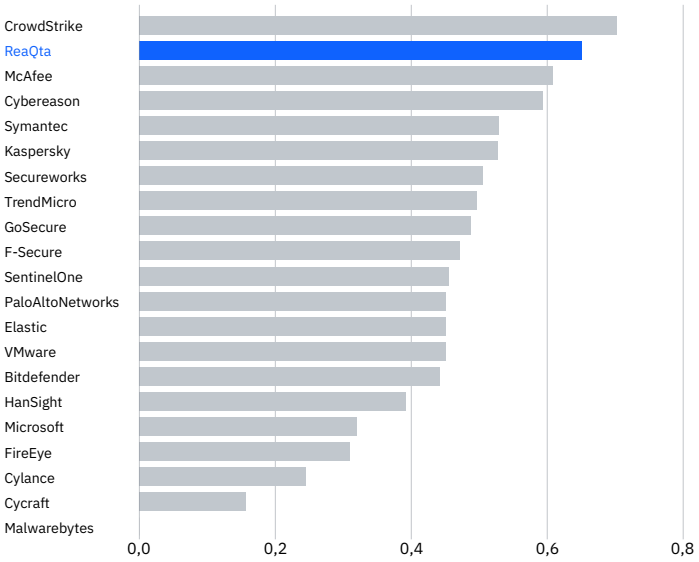
ReaQta muestra uno de los mejores índices de capacidad de acción del mundo, incluso cuando se compara con los proveedores que confían en las detecciones manuales de los MSSP.

Reduce la fatiga de alertas y simplifica la ciberseguridad generando el mínimo número de alertas de amenaza necesarias

La plataforma detectó y generó alertas en las etapas de ejecución, persistencia, elevación de privilegios y evasión de defensa, lo que permitió al equipo de seguridad realizar el seguimiento de APT29 y de sus acciones. Las alertas de la plataforma fueron coherentes durante las últimas etapas de la cadena de interrupción: movimiento lateral, recopilación, exfiltración y mandato y control, lo que muestra la capacidad de respuesta de ReaQta y limita los daños también en las últimas etapas de un ciberataque.

El índice de capacidad de acción destacó la funcionalidad de la plataforma para reducir el ruido al reducir el número de alertas generado. La plataforma capturó todas las tácticas y técnicas en unas pocas alertas correlacionadas, en comparación con una única alerta por táctica y técnica, lo que supondría un número de alertas excesivo para que los equipos del SOC pudieran examinarlas y responder a ellas.

Capacidad de acción de alertas

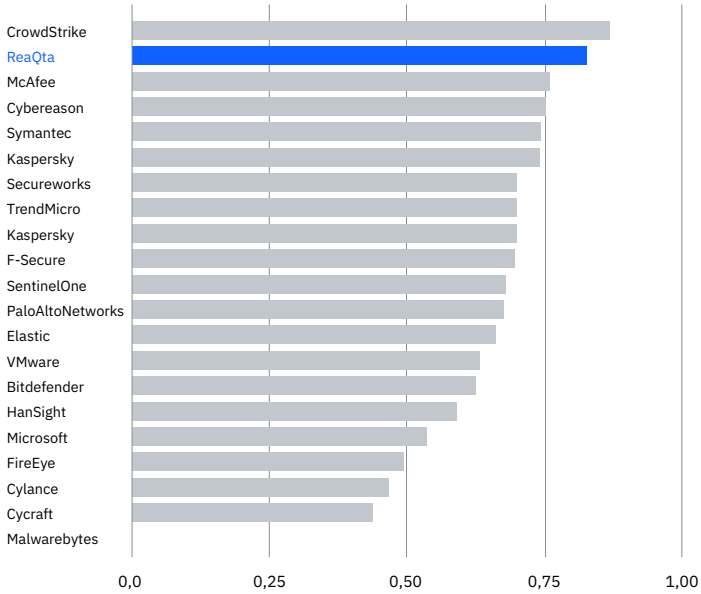


Índices de capacidad de acción (los datos incluyen detecciones manuales para los proveedores que dependen de los MSSP)

Una vez más, ReaQta proporciona alertas de gran calidad sin intervención humana, mientras que tanto el primer como el tercer proveedor confiaron en el análisis manual durante la evaluación.

La visibilidad que proporciona ReaQta hace necesario filtrar los datos, correlacionarlos y generar el menor número posible de alertas, donde cada una de ellas contiene la mayor cantidad posible de información relacionada. Esta es la finalidad de los motores de IA de ReaQta: recopilar, correlacionar y resumir la telemetría. La calidad de las alertas también la confirma el análisis de Forrester en el gráfico siguiente.

Calidad de las alertas



Calidad de las alertas (los datos incluyen detecciones manuales para los proveedores que dependen de los MSSP)

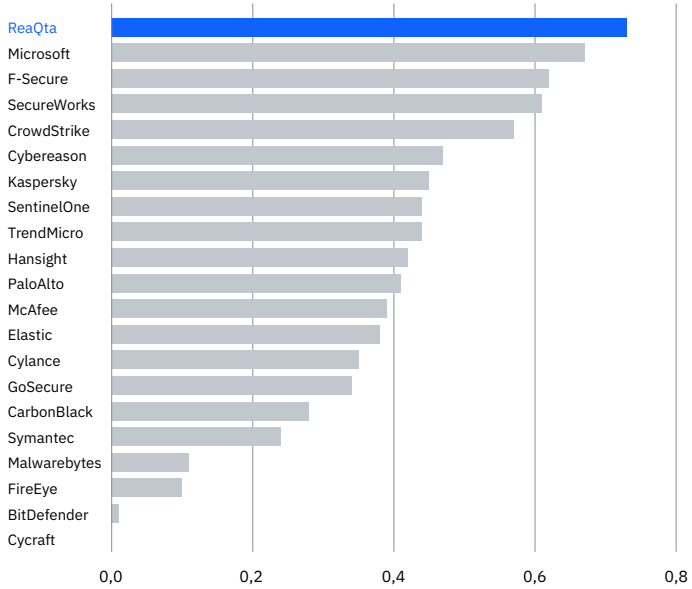
“La capacidad de acción es el resultado de la eficiencia y calidad de las alertas [...] la eficiencia de las alertas (no demasiadas) y la calidad de las alertas (cómo ayudan a comprender la trama) están relacionadas y son críticas para comprender la utilidad que tendrá una alerta determinada”.

Forrester[2]

Lo que distingue a una buena plataforma de los meros generadores de ruido es proporcionar alertas completas y de alta fidelidad.

El siguiente gráfico muestra cómo se comportó ReaQta en comparación con otras soluciones cuando se eliminaron las detecciones manuales. Cada barra representa la cantidad de información relacionada con incidentes capturada con cada alerta generada. Los motores de ReaQta capturaron la mayor cantidad de información, lo que se traduce en una considerable reducción de la carga de trabajo en entornos reales.

Cobertura de ataque por alerta generada (relación señal/ruido)



Porcentaje de cobertura de ataque proporcionado por alerta

ReaQta generó solo 25 alertas y recopiló correctamente toda la información necesaria para realizar el seguimiento de los atacantes en cada una de ellas, en lugar de crear 158 alertas, una para cada técnica probada.

La capacidad de proporcionar un flujo de trabajo unificado de resolución de incidentes es fundamental para reducir la fatiga de alertas.

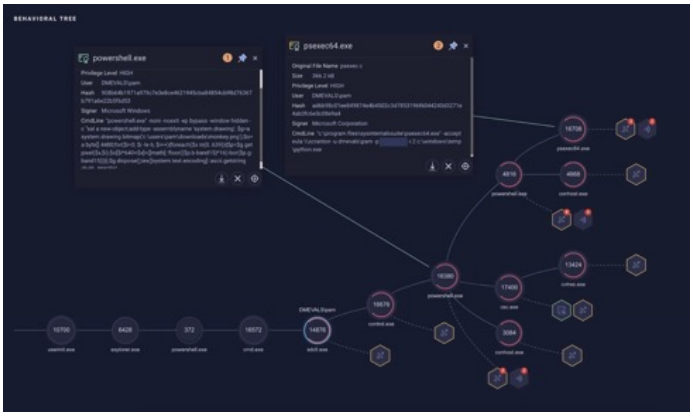
ReaQta correlacionó el argumento durante la evaluación de MITRE. Esto permitió a los analistas entender y estudiar fácilmente a un atacante activo, sin la distracción de cientos de alertas generadas sin ninguna correlación directa con el incidente original. Esto habría sido mucho más difícil de gestionar durante un análisis real.

El método de ReaQta redujo la fatiga de alertas en un 85 % al tiempo que mantuvo completa visibilidad durante todo el ataque. ReaQta está específicamente diseñado para generar el mínimo número de alertas por incidente, facilitando una experiencia de análisis fluida e ininterrumpida. La capacidad de mantener todo en una única vista ayuda a los analistas a responder más rápido, sin necesidad de cambiar entre distintas vistas de pantalla para comprender los sucesos a nivel global.

Proporciona completa visibilidad de los puntos finales para permitir una respuesta rápida en todas las etapas

La plataforma pudo mantener la correlación entre acciones en todas las etapas de la de ATT&CK. La correlación automática de sucesos reduce el tiempo necesario para reconstruir las distintas acciones ejecutadas por los atacantes y, en última instancia, reduce el tiempo de respuesta en caso de ataques reales.

Árbol de comportamiento



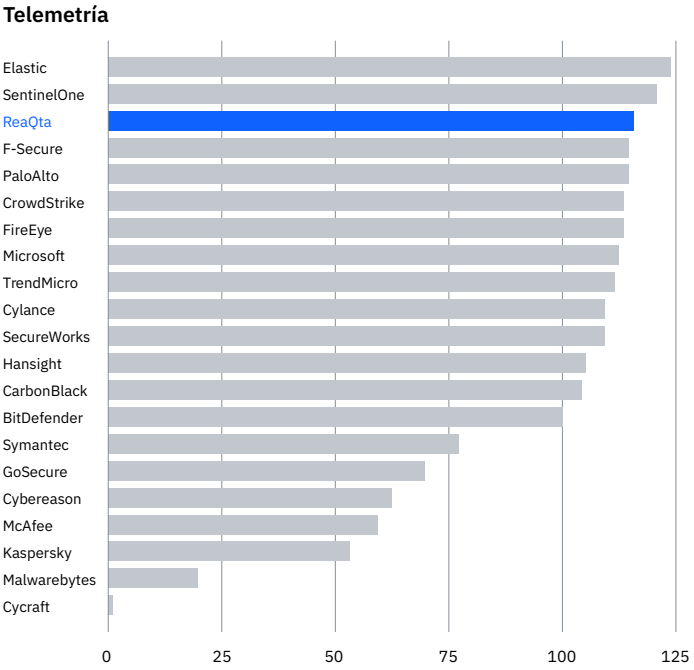
ReaQta correlacionó la trama durante la evaluación de MITRE

Para proporcionar un ejemplo relacionado con la evaluación, el gráfico anterior muestra cómo se capturó una etapa completa del ataque en una alerta individual. ReaQta correlacionó toda la información en una trama fácil de entender, proporcionando así a un equipo del SOC toda la información para el triaje correspondiente. No se requirió interacción humana y se explicó claramente el ataque, y su riesgo se evaluó, sin necesidad de ninguna actividad manual.

Analizando más detalladamente la detección de las tácticas y técnicas de APT29, ReaQta proporcionó visibilidad desde las primeras etapas de la cyber kill chain hasta las etapas más sofisticadas, que a menudo son más difíciles de detectar. Lo que destaca aquí es la capacidad de la plataforma para detectar amenazas de manera uniforme en cada una de las etapas, proporcionando así oportunidades de respuesta y remediación en cada una de ellas.

ReaQta mostró una de las mejores telemetrías, junto con un impresionante motor de IA capaz de condensar la información y evaluar el riesgo. Resultará una potente herramienta en manos de cualquier SOC o equipo que quiera dedicar su tiempo a la detección de amenazas y no a la gestión constante de alertas.

ReaQta mostró una de las mejores telemetrías.



Cantidad de telemetría proporcionada por ReaQta

Conclusión

La plataforma basada en IA de ReaQta proporciona a los equipos de seguridad prestaciones de detección avanzada y respuesta rápida, minimizando la intervención humana, simplificando todo el proceso de ciberseguridad y promoviendo la continuidad de negocio para organizaciones de cualquier tamaño.

Esta evaluación validó el método de ReaQta para la detección de sofisticados actores de amenaza. ReaQta continuará participando en pruebas independientes de terceros en el futuro.

ReaQta agradece y aplaude el trabajo de MITRE para ayudar a las organizaciones a tomar decisiones informadas con estas evaluaciones.

Para obtener más información, visite:
ibm.com/products/reaqta

IBM España, S.A
Tel.: +34-91-397-6611
Santa Hortensia, 26-28
28002 Madrid
Spain

Fabricado en Estados Unidos de América
Marzo de 2022

1 MITRE ATT&CK evaluation, The MITRE Corporation and MITRE Engenuity, 2020.
2 Further Down the Rabbit Hole With MITRE’s ATT&CK Eval Data, blog de Forrester, 4 de mayo de 2020.