TAG

POR QUÉ ACRONIS LIDERA EL SECTOR DE LA CIBERRESILIENCIA EN TECNOLOGÍA OPERATIVA (OT)

DR. EDWARD AMOROSO,
CEO, TAG INFOSPHERE

Acronis

POR QUÉ ACRONIS LIDERA EL SECTOR DE LA CIBERRESILIENCIA EN TECNOLOGÍA OPERATIVA (OT)

EDWARD AMOROSO, CEO, TAG

INTRODUCCIÓN:

Durante décadas, la ciberseguridad ha sido sobre todo sinónimo de protección de la tecnología de la información (TI) frente a ataques maliciosos. En consecuencia, se han creado puestos de directores de Seguridad de la Información (CISO) para dirigir este enfoque. Sin embargo, más recientemente, el ámbito de la ciberseguridad se ha ampliado para incluir más sistemas operativos, industriales, físicos y tangibles. El resultado es un nuevo sector al que nos referimos como "seguridad de tecnología operativa" (OT).

Debido a que la seguridad de OT se desarrolló a raíz de la seguridad de TI, comparte muchos tipos de controles semejantes. La creación de visibilidad y el despliegue de medidas de mitigación, por ejemplo, son fundamentales tanto en las estrategias de seguridad de TI como en las de OT, y han resultado ser útiles a medida que la seguridad de OT se ha ido fusionando a nivel organizativo con iniciativas de TI más amplias. Esto lo demuestran los numerosos CISO a los que se les ha asignado hoy toda la responsabilidad de garantizar la seguridad de los entornos de OT.

No obstante, como era de esperar, muchas de las deficiencias que existen en los esquemas de seguridad de TI tradicionales también se heredan en los esquemas de protección de entornos industriales. Quizá la más evidente de estas deficiencias sea la escasa resiliencia que suelen mostrar los sistemas de OT cuando sufren un ataque. El ransomware, por ejemplo, ha sido eficaz a la hora de colapsar grandes entornos operativos, con graves consecuencias para los clientes.

Sin embargo, en el ámbito de la seguridad de OT surgen muchos problemas específicos. Dichos problemas suelen estar asociados a la falta de personal in situ con formación en seguridad en la mayoría de los entornos de OT, a la gran cantidad de sistemas antiguos y patentados que hay en estas redes, y a los entornos operativos, que dificultan en demasiadas ocasiones la implementación de actualizaciones o la instalación de parches, sin afectar a los objetivos del entorno en cuestión (como p. ej., una fábrica o planta de producción).

En este informe explicamos cómo los equipos de seguridad de OT, que en ocasiones están dirigidos por un CISO, pueden mejorar su resiliencia operativa al centrarse en funciones clave como la copia de seguridad y la recuperación. Este aspecto de la ciberprotección siempre ha sido un reto para los equipos de seguridad de TI, ya que las soluciones eficaces exigen un conocimiento exhaustivo de la infraestructura, y la mayoría de los proveedores que trabajan en este ámbito se han centrado tradicionalmente en las operaciones de TI más que en la seguridad.

En entornos de tecnología operativa (OT), creemos que la copia de seguridad y la recuperación son los elementos más importantes en cualquier iniciativa que persiga mejorar la seguridad. Sin duda, debe haber objetivos complementarios para formar mejor al personal de OT en materia de seguridad y reducir el número de sistemas heredados en uso. Sin embargo, nuestra opinión es que el mayor beneficio posible se obtendrá si los ingenieros de seguridad de OT se centran en este elemento clave del entorno de procesamiento.

Para ilustrar nuestra explicación, utilizaremos las soluciones de ciberresiliencia modernas del proveedor comercial Acronis. Su enfoque en torno a las copias de seguridad y la recuperación en cualquier tipo de infraestructura, ya sea de TI o de OT, parece ser muy adecuado para hacer frente a las crecientes ciberamenazas que afectan a las operaciones industriales en sectores como el de la fabricación, el transporte, la energía, la electricidad y el del ámbito militar, que no pueden tolerar ningún tipo de interrupción bajo ningún concepto.[1]

SEGURIDAD ACTUAL DE LOS SISTEMAS DE OT

Como se ha mencionado anteriormente, una de las principales diferencias de la falta de resiliencia entre la infraestructura de TI y la de OT es que, en muchos casos, los problemas de seguridad en los entornos de tecnología operativa pueden tener consecuencias más graves. Por ejemplo, los problemas de resiliencia en el control industrial podrían provocar fallos en los sistemas de seguridad, paralizar las líneas de producción o hacer que las centrales nucleares experimenten problemas operativos. No es difícil imaginar situaciones en las que la vida de las personas corra peligro.

Esto implica que la seguridad debe ser la máxima prioridad en los entornos de OT. Sin embargo, estos entornos han estado plagados de los problemas que plantean las tecnologías heterogéneas y patentadas, a menudo con hardware y sistemas operativos obsoletos. Esto limita la posibilidad de aplicar parches y actualizaciones, por no mencionar las escasas oportunidades para realizar copias de seguridad que existen en estos entornos, que a menudo no cuentan con suficientes recursos de TI ni con suficientes expertos cualificados.

Por otro lado, aislar los entornos de OT de los hackers mediante la inserción de un gateway entre los entornos de TI y OT nunca ha funcionado bien. El objetivo original de ocultar los sistemas de OT de internet mediante la creación de un perímetro de TI/OT ha fracasado por las mismas razones por las que siempre fallan los perímetros. No logran reconocer las amenazas internas, pasan por alto las rutas de acceso en torno al perímetro e incluso ignoran la naturaleza porosa de cualquier perímetro, etc.

La inserción de un gateway entre entornos de TI y OT tampoco aborda los problemas de seguridad de OT mencionados anteriormente, relacionados con sistemas patentados, dificultad para aplicar parches y personal sin formación en seguridad entre otros. La imagen siguiente muestra cómo estos problemas de seguridad no se solucionan con un gateway entre entornos de TI/OT. Tampoco aborda nuestro principal objetivo aquí, es decir, la resiliencia de la seguridad de OT, que requiere funciones de copia de seguridad y restauración.

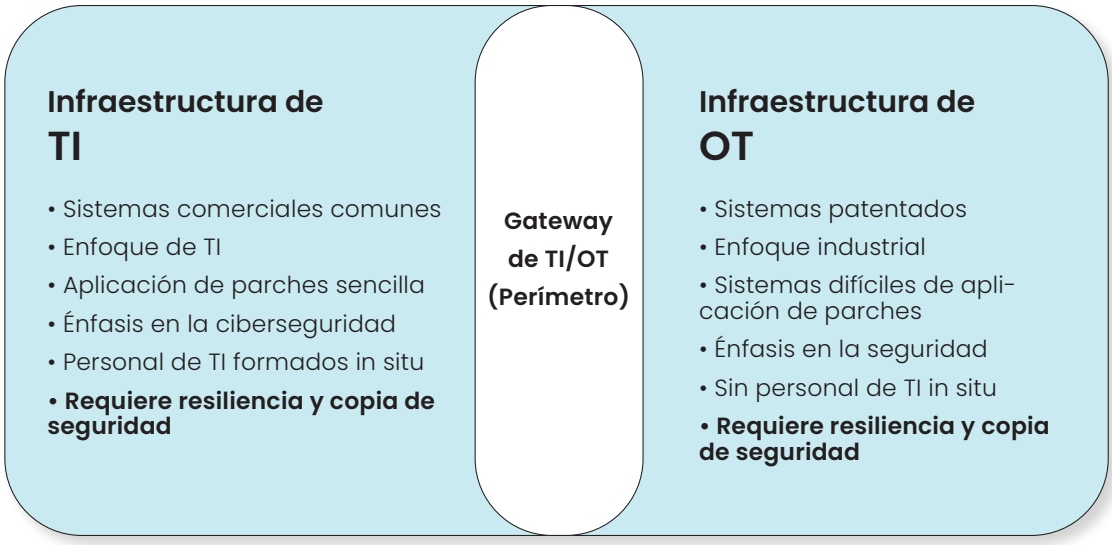

Figura 1. Desafíos de seguridad de los sistemas de OT

Como se ha sugerido, entendemos que la seguridad integral de OT requiere soluciones para todos estos problemas. No obstante, tal y como lo explicaremos a continuación, creemos que el objetivo principal de los despliegues de seguridad de OT modernos debe ser garantizar la continuidad de las operaciones frente al ransomware, el sabotaje o cualquier ciberataque destructivo. Vamos a plantear este caso en el contexto de la plataforma comercial de Acronis y el soporte que ofrece para la seguridad de OT.

SOLUCIONES DE RECUPERACIÓN Y DE COPIA DE SEGURIDAD DE ACRONIS PARA OT Y SISTEMAS DE CONTROL INDUSTRIAL (ICS)

Nuestra experiencia sugiere que los programas de seguridad de OT deben abordar tres áreas complementarias. En primer lugar, deben garantizar la visibilidad en los entornos de OT, que suele obtenerse mediante plataformas comerciales como Claroty y Dragos. Obtener visibilidad es esencial, y hay que invertir en mejorar su funcionamiento en la práctica. Por ejemplo, se debería impartir mejor formación a los usuarios, y quizá hacer más hincapié en las simulaciones de ciberataques a entornos de OT.

En segundo lugar, creemos que los directivos deberían desafiar a sus equipos de seguridad de TI para que desarrollen más controles convergentes a medida que los sistemas de OT se vayan integrando con los de TI. Por ejemplo, deberían adoptarse las tendencias de OT de "confianza cero" (Zero Trust), lo que implica que más sistemas operativos se conecten con la nube y con otros sistemas de TI tradicionales. Esto permite ampliar los controles de TI, como las plataformas de protección de aplicaciones nativas de la nube (CNAPP), para abarcar toda la infraestructura de OT.

En tercer lugar, y lo que es más importante, recomendamos que los equipos de seguridad de OT empiecen a centrarse más en la resiliencia operativa. En la práctica, esto implica la necesidad de garantizar la continuidad operativa mediante soluciones de copia de seguridad y recuperación automatizadas. Esto se aplica obviamente a los sistemas de TI, pero como se ha sugerido anteriormente, la interrupción del soporte de OT puede tener consecuencias mucho más graves, como poner en riesgo la seguridad de las personas, y la solución de Acronis puede ayudar a evitar estos problemas.

La plataforma de Acronis cubre perfectamente los requisitos de seguridad y resiliencia más aplicables a la infraestructura de OT. Esto es una buena noticia, ya que los equipos de las empresas no deberían tener que desarrollar su propia solución de copia de seguridad y recuperación local, aunque su hardware y software estén obsoletos y sean patentados. En concreto, las funciones clave incluidas en la suite de Acronis que son esenciales para la resiliencia en entornos de OT son las siguientes:

1. **Recuperación rápida de sistemas de OT**: Acronis ofrece protección de alto rendimiento para ordenadores de OT, lo que permite una restauración rápida para evitar costosas interrupciones en las plantas de producción. La función de recuperación rápida es crucial para minimizar el tiempo de inactividad y mantener la continuidad de la actividad empresarial.
2. **Recuperación universal de ordenadores**: Acronis Cyber Protect garantiza una recuperación rápida y fiable para cualquier ordenador, incluidos los sistemas heredados más antiguos, como los de la época de Windows XP, con opciones de restauración desde cero. Esta función es esencial para mantener la continuidad con los sistemas heredados que se van volviendo cada vez más antiguos y que son habituales en los entornos de OT.
3. **Planes de copia de seguridad personalizables**: Acronis permite crear planes de copia de seguridad personalizables adaptados a los requisitos específicos de los entornos de OT y de sistemas de control industrial (ICS), con el fin de garantizar que los datos y sistemas críticos queden protegidos de forma adecuada. La necesidad de personalizar los planes de copia de seguridad aumenta a medida que la infraestructura de OT se vaya modernizando con la IA y con métodos de entrega más sostenibles.
4. **Integración con herramientas de terceros**: Acronis ofrece una vista unificada de copia de seguridad y recuperación con control centralizado y opciones de integración con herramientas de terceros, lo que no solo simplifica la gestión, sino que también mejora la eficacia operativa. Los entornos de OT son especialmente difíciles de integrar en términos de seguridad, por lo que esta capacidad es de vital importancia.
5. **Opciones de soberanía de datos**: las organizaciones pueden elegir entre almacenamiento interno o utilizar los centros de datos globales de Acronis, e incluso otras opciones como Amazon S3 y Microsoft Azure, lo que garantiza el cumplimiento de los requisitos en materia de soberanía de datos. Acronis ayudará a los clientes a desarrollar el acuerdo de alojamiento de datos más adecuado.

6. **Recuperación con autoservicio para teletrabajadores**: Acronis proporciona opciones de recuperación con autoservicio para teletrabajadores, lo que permite al personal sin alta cualificación técnica iniciar procesos de recuperación, descentralizar eficazmente las cargas de trabajo de TI y retomar la actividad empresarial con mayor rapidez tras sufrir un incidente.

ARQUITECTURA DE LA PLATAFORMA DE ACRONIS

La plataforma de Acronis Cyber Protect se basa en un almacén de datos que albergará y protegerá las fuentes de datos clave de la empresa de OT actuales, históricas y de otros tipos. En un entorno de OT se pueden instalar varias instancias de la consola de la plataforma de Acronis Cyber Protect, con varios agentes asociados desplegados en el entorno para recopilar y restaurar datos. Los metadatos se transmiten desde las consolas al almacén.

Además, se proporcionan paneles de control y consolas para supervisar todos los aspectos del proceso de copia de seguridad y recuperación, tanto para cada despliegue de Cyber Protect como para el Centro de supervisión centralizada de Acronis (Acronis Centralized Monitoring Hub). Este centro proporciona vistas históricas, con opciones de generación de informes y supervisión personalizables, mientras la tarea de copia de seguridad y recuperación esté en curso. El objetivo, obviamente, es garantizar la continuidad de la actividad empresarial tras sufrir incidentes, ataques y cualquier otro tipo de problema relacionado con la resiliencia (véase la Figura 2).

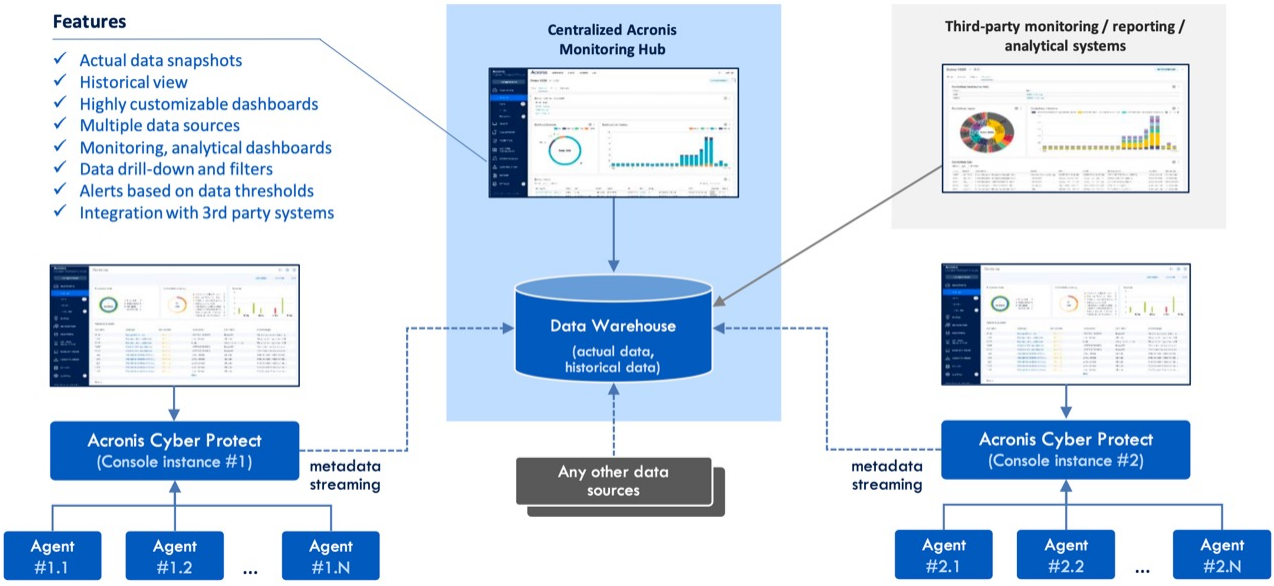

Figura 2. Arquitectura de sistemas de Acronis

INTEGRACIONES DE ACRONIS

Acronis Cyber Protect (observe las dos instancias representadas en el diagrama) admite la integración mediante la unificación de funciones de copia de seguridad, recuperación ante desastres, protección contra el malware basada en IA, asistencia remota y herramientas de seguridad en una única plataforma para el equipo de seguridad, incluso en entornos de OT. Esta consolidación permite a cualquier empresa, incluidos los equipos de seguridad de OT, gestionar varios aspectos de la ciberprotección a través de una única interfaz, lo que reduce la complejidad y mejora la eficacia.

La arquitectura flexible de la plataforma, así como sus interfaces de programación de aplicaciones y de línea de comandos, permite a Acronis y a terceros desarrollar e integrar aplicaciones (véase en la Figura 2 las fuentes de terceros que se conectan al almacén de datos centralizado). Este diseño promueve un ecosistema dinámico en el que se pueden incorporar servicios adicionales de protección, administración y automatización, lo que garantiza que la plataforma pueda seguir adaptándose a los entornos de ciberseguridad en constante evolución. Esta flexibilidad

garantiza que las organizaciones puedan integrar las soluciones de Acronis en sus infraestructuras existentes, lo que mejora la resiliencia y la seguridad en general, especialmente en entornos de OT.

COPIA DE SEGURIDAD FORENSE DE ACRONIS

Acronis Cyber Protect incluye una función de copia de seguridad forense que permite recopilar pruebas digitales a partir de las copias de seguridad a nivel del disco, con el fin de simplificar los análisis posteriores. Esta función es fundamental para las organizaciones que necesiten gestionar los requisitos de cumplimiento normativo y llevar a cabo investigaciones internas de forma eficaz. También es esencial para los entornos de OT, donde el análisis forense puede ayudar a identificar los ataques dirigidos a infraestructuras críticas y servicios esenciales.

El proceso de copia de seguridad forense de Acronis implica la captura de imágenes del disco completas, incluidos los datos activos, el espacio libre y los volcados de memoria. Este enfoque exhaustivo, que cada vez se impone más como requisito de seguridad en entornos de OT, garantiza que se conserven adecuadamente todas las pruebas digitales potenciales, lo que no solo permite realizar análisis detallados posteriores al incidente de forma más fácil, sino también respaldar las obligaciones legales y normativas.

Al integrar la recopilación de datos forenses con las rutinas de copia de seguridad habituales, Acronis permite a las organizaciones de entornos de TI y OT mantener la continuidad de su actividad empresarial, a la vez que garantiza que la información forense crítica esté disponible cuando se necesite. Esta integración elimina la necesidad de realizar procesos de recopilación de datos forenses por separado, optimiza las operaciones y reduce el riesgo de pérdida de datos durante los incidentes.

ACRONIS DISASTER RECOVERY INTEGRADO

Acronis Cyber Protect ofrece una solución de recuperación ante desastres integrada que minimiza la complejidad y los costes. Al combinar las funciones de copia de seguridad y recuperación ante desastres, la plataforma garantiza que las empresas puedan restaurar rápidamente los recursos informáticos tras incidentes como desastres naturales, errores humanos, ciberataques o fallos de hardware. Como se ha sugerido anteriormente, en el contexto de los sistemas de OT, estos incidentes pueden tener consecuencias devastadoras.

Las funciones de recuperación ante desastres incluyen la posibilidad de poner en marcha rápidamente recursos informáticos de TI o de OT en caso de desastre, runbooks para automatizar los procesos de recuperación y pruebas de conmutación por error para garantizar que los sistemas funcionen como cabría esperar durante un incidente real. Estas funciones son esenciales para mantener la continuidad de la actividad empresarial y minimizar el tiempo de inactividad, especialmente en el caso de las aplicaciones en tiempo real, que son muy habituales en entornos de OT.

Al integrar la recuperación ante desastres con la ciberseguridad y la administración de endpoints, Acronis ofrece un enfoque integral de la ciberprotección. Esta integración garantiza que todos los aspectos de la infraestructura de TI de una organización estén bien protegidos, con el fin de promover la resiliencia frente a una amplia variedad de posibles interrupciones. Además, simplifica la gestión para los CISO que sean responsables de los sistemas de producción de TI y OT.

ALINEACIÓN CON LOS REQUISITOS NORMATIVOS

Además de la necesidad operativa de disponer de copias de seguridad y resiliencia, los equipos de seguridad de OT se ven sometidos cada vez más a una variedad de nuevos marcos normativos y de cumplimiento externos. Como consecuencia, el cumplimiento normativo en materia de ciberseguridad para entornos de OT se ha convertido en un componente mucho más difícil de los programas de seguridad empresarial, ya que incluye requisitos convergentes que evolucionan con el aumento de las amenazas.

Más concretamente, observamos que los organismos reguladores mundiales están haciendo hincapié en la resiliencia operativa, a través de marcos como el Digital Operational Resilience Act (DORA) en la Unión Europea y de las directrices del Comité de Supervisión Bancaria de Basilea, que destacan la necesidad de contar con una ciberseguridad sólida en los sectores de infraestructuras críticas. Las soluciones de Acronis ayudan a cumplir estos requisitos normativos, ya que ofrecen soporte en los siguientes ámbitos:

1. **Marcos integrales de gestión de riesgos:** las soluciones de Acronis permiten a las organizaciones de seguridad implementar marcos adaptables de gestión de riesgos, probar la resiliencia con regularidad y mantener una comunicación abierta con las partes interesadas y las entidades reguladoras, con el fin de alinearse con los marcos de resiliencia operativa global tanto para entornos de TI como de OT.
2. **Planificación de la respuesta ante incidentes:** Acronis ayuda a desarrollar planes de respuesta ante incidentes por escrito, ya sea de forma autónoma o como parte de un plan de continuidad de la actividad empresarial, con el fin de garantizar la preparación frente a posibles ciberamenazas. Se trata de una tarea nueva para muchos equipos de seguridad de OT, por lo que el soporte de Acronis es especialmente útil en este caso.
3. **Gestión de riesgos de terceros:** la posibilidad de integrar las soluciones de Acronis facilita una supervisión sólida por parte de terceros, un componente crítico de la resiliencia operativa, como destacan los organismos reguladores. Como se ha sugerido anteriormente, la ciberintegración con terceros puede ser complicada, ya que hasta ahora se ha ignorado o no se le ha dado la importancia que merece.

LOS PROVEEDORES LÍDERES DE AUTOMATIZACIÓN DE OT E ICS CONFÍAN EN ACRONIS

La adopción de las soluciones de copia de seguridad y recuperación de Acronis por parte de los mayores proveedores de plataformas de OT e ICS del mundo pone de manifiesto el papel crítico que desempeñan estas soluciones a la hora de garantizar la resiliencia en entornos industriales y de OT. Líderes del sector como ABB, Emerson, Siemens, Schneider Electric, Rockwell Automation y Yokogawa integran Acronis Cyber Protect en sus plataformas, ya sea como una solución de marca blanca o de marca conjunta, para ofrecer a sus clientes una mayor resiliencia operativa. El hecho de que estas grandes empresas hayan optado por Acronis demuestra la fiabilidad, flexibilidad y liderazgo de la plataforma en el ámbito de las copias de seguridad y de las opciones de recuperación en entornos de OT.

CONCLUSIÓN Y PLAN DE ACCIÓN PARA LOS EQUIPOS DE SEGURIDAD DE OT

Creemos que las soluciones de copia de seguridad y recuperación de Acronis son idóneas para los clientes que deseen reforzar la resiliencia y la seguridad de sus infraestructuras de OT. Al ofrecer funciones de recuperación rápida, soporte para sistemas heredados, planes de copia de seguridad personalizables y alineación con los requisitos normativos, Acronis permite a las organizaciones mantener la continuidad de su actividad empresarial y cumplir con los estándares mundiales de resiliencia operativa en constante evolución.

Nuestro consejo para los CISO que sean responsables de acometer esta tarea, o para cualquier otro equipo de gestión o dirección que trabaje para abordar la ciberresiliencia en el ámbito de la OT, es que se pongan en contacto cuanto antes con Acronis para obtener más información sobre sus soluciones. Nuestro equipo de TAG también está disponible en todo momento para ayudar a los lectores a profundizar en este tema o en cualquier otro relacionado con la ciberseguridad y la inteligencia artificial. Esperamos tener noticias suyas.

[1] Estamos muy agradecidos a los equipos técnicos y directivos de Acronis por ayudarnos a comprender los distintos riesgos a los que se ven expuestos los entornos de OT de sus clientes. El equipo de Acronis nos dio acceso a su documentación de productos y nos ayudó a obtener información útil sobre sus hojas de ruta de productos tanto para la seguridad de entornos de TI como de OT.

ACERCA DE TAG

TAG es una empresa de investigación y asesoramiento de confianza que proporciona información y recomendaciones en ciberseguridad, inteligencia artificial y ciencias climáticas a miles de proveedores de soluciones comerciales y empresas de la lista Fortune 500. Fundada en 2016 y con sede en Nueva York, TAG rompe con la tendencia de la investigación de pago al ofrecer orientación imparcial y exhaustiva, análisis de mercado, consultoría de proyectos y contenido personalizado, todo desde una perspectiva profesional.