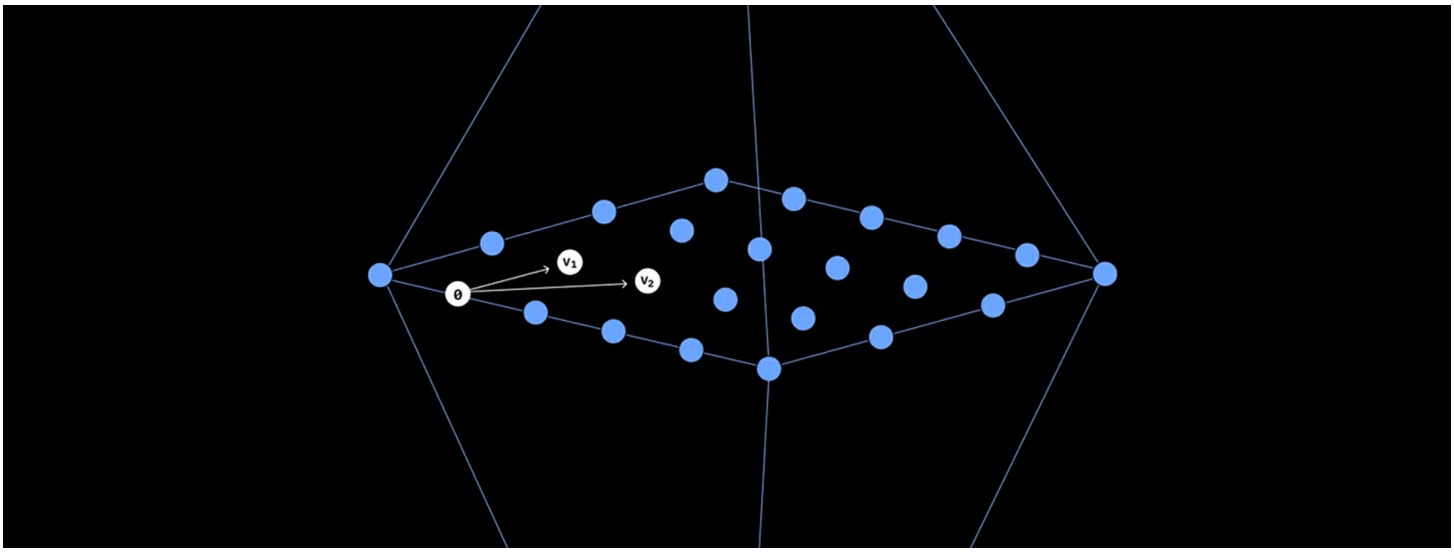
Comunicados

IBM anuncia la tecnología Quantum-Safe para salvaguardar los datos más valiosos de los gobiernos y las empresas

-La compañía lanza el IBM Quantum Safe Roadmap junto con un portafolio de tecnologías para simplificar y permitir una migración completa, protegiendo los datos críticos contra posibles ataques futuros



ARMONK, NY, 10 de mayo de 2023 **-** IBM (NYSE: IBM) anunció hoy en su conferencia anual Think en Orlando, Florida, la nueva tecnología IBM Quantum Safe: un conjunto completo de herramientas y recursos que combinan la profunda experiencia en seguridad de IBM, diseñado como una solución de punta a punta para ser disponibilizada a medida que las organizaciones, incluyendo agencias gubernamentales, preparan su viaje de seguridad cuántica en dirección a la era post-cuántica.

La tecnología cuántica está avanzando rápidamente. Los sistemas cuánticos están en un camino para resolver problemas empresariales o científicos previamente sin solución, pero este progreso también plantea riesgos de seguridad. A medida que las computadoras cuánticas continúen avanzando, alcanzarán la habilidad de superar los protocolos de seguridad más utilizados en el mundo.

Reconociendo este riesgo, IBM ha aprovechado su amplia experiencia en criptografía, computación cuántica e infraestructura crítica para desarrollar la tecnología IBM Quantum Safe, en otras palabras, tecnología con criptografía resistente a la computación cuántica. Este conjunto de capacidades está diseñado para ayudar a los clientes a prepararse para la era post-cuántica a través de:

- **IBM Quantum Safe Explorer** que le permite a las organizaciones analizar el código fuente y de objetos para localizar activos criptográficos, dependencias, vulnerabilidades y crear una lista de materiales criptográficos (CBOM). Esto permite que los equipos puedan ver y agregar los riesgos potenciales en una ubicación central.

- **IBM Quantum Safe Advisor** permite crear una vista dinámica u operativa del inventario criptográfico para guiar la corrección, analizar la postura criptográfica y la conformidad para priorizar los riesgos.

- **IBM Quantum Safe Remediator** permite a las organizaciones implementar y probar patrones de

corrección de criptografía resistente a la computación cuántica, basados en mejores prácticas, para entender posibles impactos en los sistemas y activos a medida que se preparan para desplegar soluciones Quantum-Safe.

IBM también está anunciando su **IBM Quantum Safe Roadmap** para apoyar a los clientes y ayudarles a comprender la transición de seguridad. Este es el primer modelo de IBM que lleva los hitos de la tecnología hacia otras tecnologías con criptografía resistente a la computación cuántica cada vez más avanzadas, diseñada para ayudar a las organizaciones a abordar anticipadamente los requisitos y los estándares criptográficos a través de la cripto-agilidad y proteger los sistemas contra las vulnerabilidades emergentes.

Este proceso consta de tres acciones claves:

1. **Descubrir:** identificar el uso de criptografía, analizar las dependencias y generar un CBOM.

2. **Observar:** Analizar la postura criptográfica de las vulnerabilidades y priorizar la corrección basada en riesgos.

3. **Transformar:** Corregir y mitigar con la cripto-agilidad y la automatización integrada.

"Como líder en computación cuántica, IBM reconoce la importancia de abordar de forma integral las necesidades críticas de nuestros clientes, pues ellos también consideran la transformación de su criptografía para la era cuántica", dijo Ray Harishankar, IBM Fellow y Líder de tecnología IBM Quantum Safe. "Nuestro nuevo conjunto de tecnologías Quantum-Safe e hitos establecidos en nuestra hoja de ruta están diseñados para la continua evolución de la seguridad post-cuántica en conjunto con computación cuántica útil, incluyendo soluciones para ayudar a las industrias a navegar por este cambio de forma eficaz y fácil".

El año pasado, el gobierno de los Estados Unidos dio a conocer nuevos requisitos y directrices que piden a las agencias federales que comiencen la transición hacia Quantum-Safe. El Instituto Nacional de Estándares y Tecnología (NIST) seleccionó cuatro algoritmos con criptografía resistente a la computación cuántica para la estandarización, tres de ellos fueron desarrollados por IBM, junto a colaboradores de la academia e industria.

Luego, la Agencia de Seguridad Nacional (NSA) anunció nuevos requisitos para que los sistemas de seguridad nacional hagan una transición hacia algoritmos resistentes a la computación cuántica para 2025, y la Casa Blanca dio a conocer los requisitos para que las agencias federales presenten un inventario criptográfico de sistemas que podrían ser vulnerables a computadores cuánticos relevantes criptográficamente.

"A medida que la era de la computación cuántica se acerca rápidamente a la realidad, es imperativo que las tecnologías de criptografía resistentes a la computación cuántica también se desplieguen para proteger los datos y los sistemas clásicos de hoy", dijo Patrick Moorhead, CEO y fundador de Moor Insights & Strategy. "Lo que el mundo necesita para asegurar los datos en la era de la computación cuántica es experiencia en tecnología cuántica y criptografía avanzada de clase mundial, junto con décadas de experiencia en el desarrollo de productos para infraestructura crítica. Creo que en estos pilares se destaca IBM, y ahora con un *roadmap* de criptografía resistente a la computación cuántica para guiar la industria y las nuevas tecnologías para simplificar la migración, me emociona ver el avance hacia la criptografía resistente a la computación cuántica en el mundo".

El IBM Quantum Safe Roadmap y la tecnología, mostrarán a las empresas su contexto criptográfico existente para que puedan empezar a abordar los cambios que pueden ser necesarios para progresar en la era post-cuántica.

Para obtener más información sobre la tecnología IBM Quantum Safe o para solicitar un demo, visite:

https://www.ibm.com/quantum/quantum-safe .
