Detección automatizada

de fraudes, picos de facturación y alertas de vulnerabilidad con

Google Cloud Platform y Nuva Tecnología.

nuva
Tecnología Simple

CONTENIDO

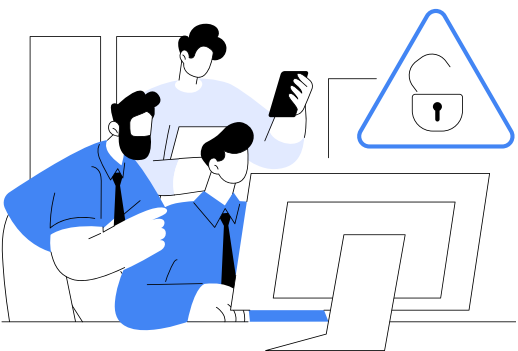
Introducción.....01

¿Cómo la detección automatizada puede ayudar a los líderes de IT?.....02

¿Cómo la detección automatizada puede ayudar a las organizaciones?.....04

¿Cómo implementar políticas de detección automatizada?.....05

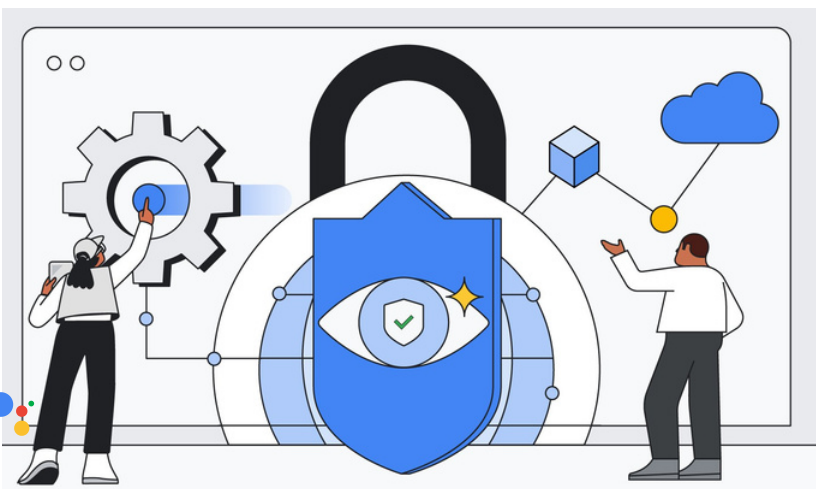
Conclusión.....06



nuva
Tecnología Simple

Introducción

En el panorama empresarial actual, las empresas se enfrentan a una serie de desafíos, entre ellos el fraude, los costos en tecnología y las vulnerabilidades de seguridad. Estos desafíos pueden tener un impacto significativo en la permanencia y el cumplimiento de las empresas ante entidades administrativas. Los líderes de infraestructura desempeñan un papel fundamental en la prevención y atención sobre estos desafíos.



En la actualidad es posible acceder a soluciones de detección automatizada para ayudarlos a proteger a sus organizaciones de pérdidas financieras, daños a la reputación y violaciones de datos.

¿Cómo la **detección automatizada** puede ayudar a los líderes de TI?

Muchos de los retos que se presentan en un área o equipo de TI son la cantidad de solicitudes de soporte; el cumplimiento, las muchas fuentes de datos y los tiempos de respuesta, ya que suelen ser áreas muy demandantes, esto deja como resultado la reducción del tiempo para desarrollar proyectos más innovadores en la organización. Basados en estos desafíos, Google ha desarrollado sus ecosistemas para que pueda ser de gran ayuda en temas vitales como:

Mejora la eficiencia: Las soluciones de detección automatizada pueden ayudar a los líderes de TI a automatizar tareas manuales, como la recopilación y el análisis de datos, esto al mismo tiempo permite liberar tiempo que pueda usarse para concentrarse en tareas estratégicas

Mejora la seguridad: El uso de soluciones de detección automatizada puede brindarle alertas para identificar amenazas de seguridad potenciales, picos altos en la facturación o identificar transacciones fraudulentas.

El ecosistema de GCP y el acompañamiento de Nuva Tecnología en estas implementaciones facilita la detección automática, tarea que puede complicarse cuando hay tantos ecosistemas que conviven y requieren actualizaciones constantes, como es el caso de los sistemas on-premise.

Estas funcionalidades de la mano de un acompañamiento experto permiten ayudar a proteger a las organizaciones de pérdidas financieras, daños a la reputación y violaciones de datos.

Mejorar el cumplimiento: Cumplir con las regulaciones internas y políticas sobre el manejo de los datos y la información es algo que los líderes de las empresas tienen muy presente.

En este caso la IA puede ayudar a identificar patrones y anomalías que podrían indicar un incumplimiento normativo, lo que permite a las organizaciones tomar medidas preventivas, también ayuda a las organizaciones a ser más transparentes en sus prácticas de tratamiento de la información, proporcionando información clara y accesible sobre cómo se recopilan, utilizan y protegen los datos.

Toda la **infraestructura de Google Cloud Platform (GCP)** cuenta con las certificaciones **ISO 27001, ISO 27017, ISO 27018, SOC 2 y SOC 3** y cumple las normativas de la **HIPAA y el Reglamento General de Protección de Datos.**

¿Cómo la **detección automatizada** puede ayudar a las organizaciones?

Las soluciones de detección de fraudes pueden analizar datos históricos y en tiempo real para identificar patrones sospechosos. Esto puede ayudar a las organizaciones a detectar fraudes antes de que causen daños financieros.

Botón de pánico para Google Cloud; un desarrollo de Nuva Tecnología para GCP; con este servicio logramos darle una herramienta a nuestros clientes que pueda permitirles tener un mayor control y reducir drásticamente las probabilidades de que sufran facturaciones desbordadas.

- El aprendizaje basado en datos permite integrarse a soluciones de detección de vulnerabilidades; ya que estos datos pueden ser analizados para identificar vulnerabilidades en los sistemas y aplicaciones. Esto logra ayudar a las organizaciones a proteger sus datos y sistemas de ataques que puedan hacerles perder mucho dinero o su reputación.

¿Cómo implementar **políticas de detección automatizada**?

Para implementar un plan de políticas de ciberseguridad automatizada se debe tener en cuenta lo siguiente:

Se debe determinar qué datos necesitan para sus soluciones de detección automatizada. Estos pueden ser, datos de transacciones, datos de clientes y datos de seguridad.

Se debe establecer cuáles serán los objetivos de sus soluciones de detección automatizada. Estos objetivos pueden incluir la detección de fraudes, la detección de picos de facturación y la detección de vulnerabilidades.

Elección de la solución de detección automatizada; es necesario elegir cuál será la herramienta que mejor se adapte a las necesidades de su organización o de los datos que necesita controlar.

Google Cloud Platform (GCP) tiene disponible gran variedad de potentes herramientas y servicios para la detección automatizada.

Google Cloud Security Command Center (SCC): proporciona una vista unificada de la seguridad y el cumplimiento normativo en la nube.

Cloud Monitoring: permite recopilar y analizar métricas, registros y eventos de GCP.

Cloud Logging: ofrece un servicio de registro centralizado para GCP.

Cloud Security Scanner: ayuda a identificar vulnerabilidades de seguridad en aplicaciones web.

Cloud Armor: protege las aplicaciones web de ataques DDoS y otras amenazas.

Conclusión

La detección automatizada es una herramienta poderosa que, con los pasos correctos y con el acompañamiento de un partner experto en la herramienta, puede ayudar a los líderes áreas IT a mejorar la eficiencia de su equipo de trabajo, la seguridad de los sistemas y el cumplimiento frente a las normativas y blindar sus ecosistemas contra ataques que puedan vulnerar información privada.

nuva®
Tecnología Simple

Contáctanos para potenciar el crecimiento de tu empresa

Colombia:
www.nuva.co
+57 3016177677

México:
www.nuvatecnologia.mx
+52 5541644805