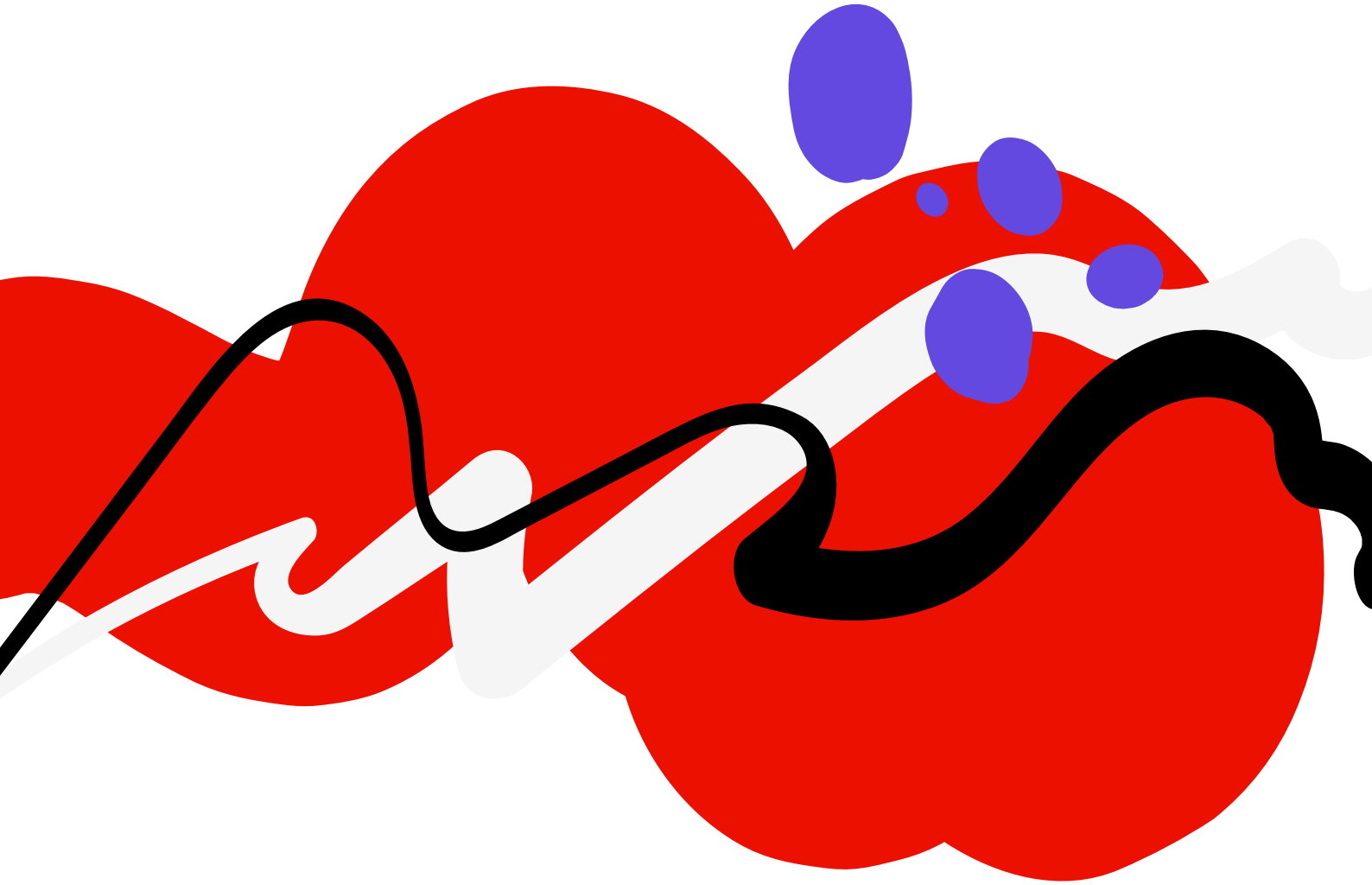
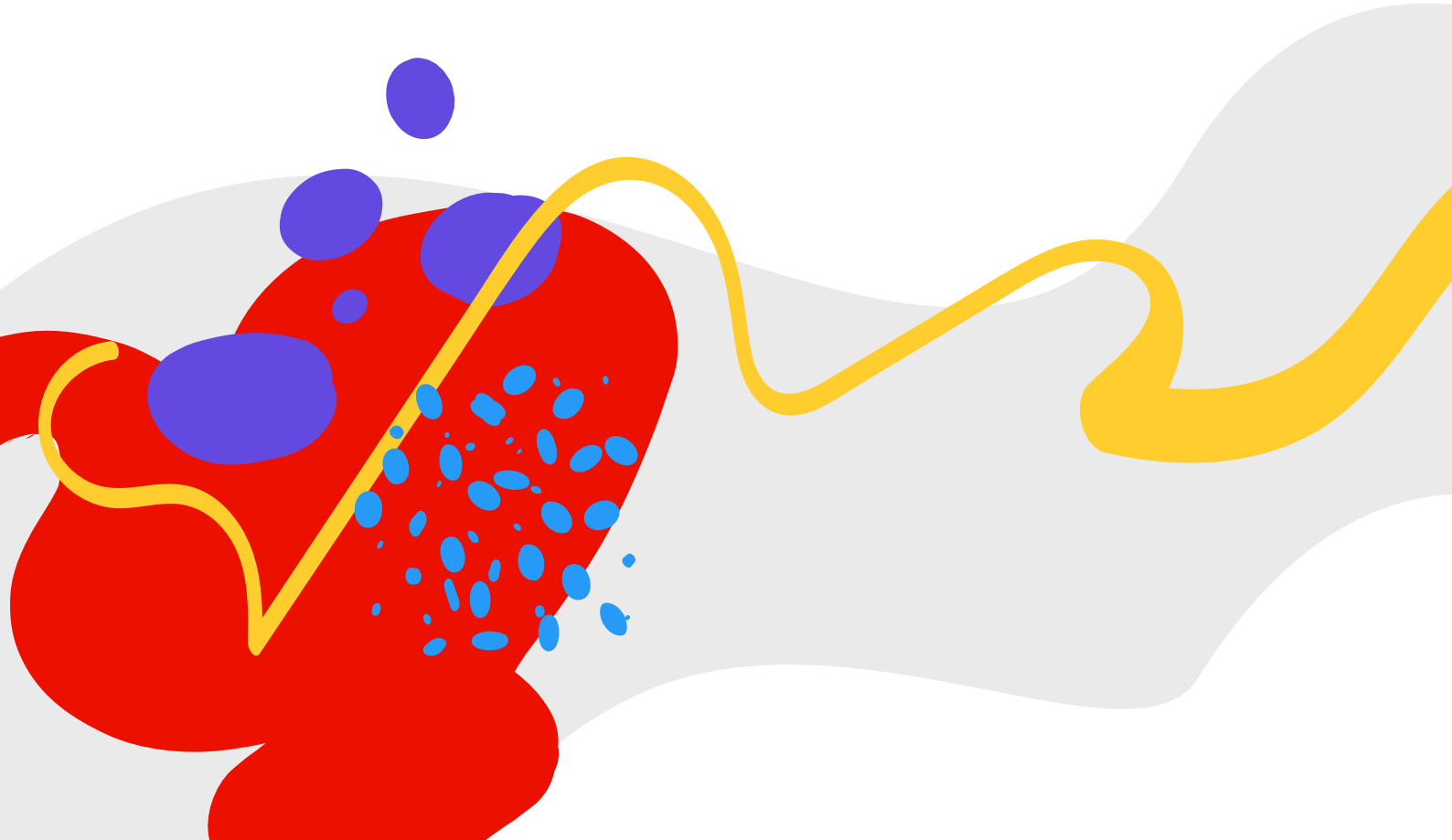
DOCUMENTO TÉCNICO

Información general sobre la seguridad operativa de Adobe



Índice de contenidos



Introducción

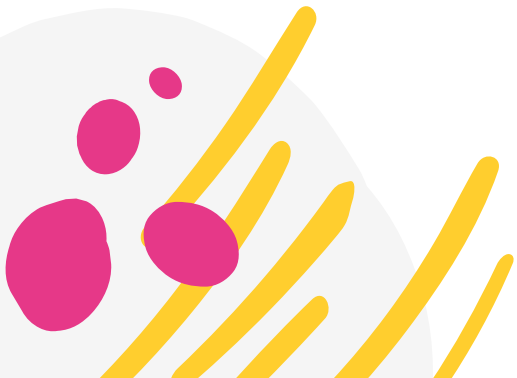
Con una presencia en la nube que incluye nubes públicas y privadas a través de diferentes proveedores, la estrategia de varias nubes de Adobe® requiere barreras de seguridad uniformes y repetibles que estén fácilmente disponibles para nuestros equipos de productos y servicios. Para ello, nuestro equipo especializado en seguridad operativa se centra en proteger los recursos de la nube a gran escala y en ayudar a garantizar la seguridad de las aplicaciones y los datos de los clientes dentro de nuestras operaciones de infraestructura en la nube en constante evolución.

En este informe técnico, se describe la estrategia de operaciones seguras en la nube de Adobe, así como los procesos y herramientas que hemos creado para ayudar a los desarrolladores e ingenieros de productos a mejorar su enfoque de seguridad, reducir el riesgo tanto para Adobe como para nuestros clientes e impulsar el respeto de todo Adobe al cumplimiento normativo, la privacidad y otros marcos de gobernanza.

La estrategia de operaciones seguras en la nube de Adobe

Al incorporar la seguridad en el núcleo de nuestros procesos en la nube, Adobe ayuda de forma proactiva a evitar posibles problemas que puedan surgir en el complejo panorama de la seguridad. A medida que nuestra presencia en la nube sigue creciendo e implicando entornos de varias nubes y tecnologías emergentes, como contenedores y orquestadores, las políticas y configuraciones estándar, así como las herramientas de automatización, nos permiten reducir los errores humanos y ofrecer garantías a nuestros clientes de que las distintas capas de la infraestructura están protegidas frente a posibles debilidades. La ampliación de la seguridad mediante la automatización, junto con la supervisión periódica de nuestro enfoque de seguridad y las revisiones trimestrales del cumplimiento normativo, ayudan a Adobe a detectar desviaciones de la seguridad y otros problemas antes de que se conviertan en críticos.

Para permitir que nuestros desarrolladores se centren en sus áreas de especialización y evitar errores accidentales de seguridad, hemos creado políticas de seguridad y configuraciones estándar que se aplican a todos los servicios que implementamos en la nube. La incorporación de controles de seguridad en las primeras fases del ciclo de vida de desarrollo contribuye a que Adobe no solo refuerce el enfoque de seguridad de nuestros servicios desde el diseño hasta la implementación, sino también a que reduzca la existencia de fallos de seguridad en las últimas fases de desarrollo, cuando resulta más complicado solucionarlos. La aplicación automatizada de nuestros controles y políticas de seguridad en la nube permite mejorar nuestro enfoque general de seguridad corporativa, así como garantizar a los clientes que su seguridad es nuestra máxima prioridad.



La pila de seguridad operativa de Adobe

La pila de seguridad operativa de Adobe, desarrollada por nuestro equipo especializado en seguridad operativa, es un conjunto consolidado de herramientas que ayudan a garantizar que los productos y servicios de Adobe se diseñan pensando en las prácticas recomendadas de seguridad. Teniendo en cuenta las necesidades de seguridad de varias nubes de la empresa, este conjunto se basa en dos (2) principios fundamentales: estandarización y prevención. Para ello, esta pila incluye un conjunto estandarizado de soluciones de supervisión continua y flujo de trabajo que permite a los equipos de servicio diseñar sus entornos de nube privada y pública prestando atención a la seguridad, desde el principio, y ayuda a prevenir de forma proactiva los riesgos de seguridad.

La pila de seguridad operativa de Adobe funciona en una variedad de recursos en la nube, proporciona seguridad a gran escala, ofrece capacidades estandarizadas para toda la organización y ayuda a garantizar la visibilidad de la seguridad en los entornos operativos para los equipos de seguridad, auditoría y cumplimiento normativo de Adobe. Al adoptar el mismo conjunto de herramientas y procesos en todos nuestros equipos de productos y servicios, Adobe ayuda tanto a evitar errores de seguridad como a permitir que las aplicaciones se adapten a las soluciones de seguridad sin necesidad de reinventar la rueda.

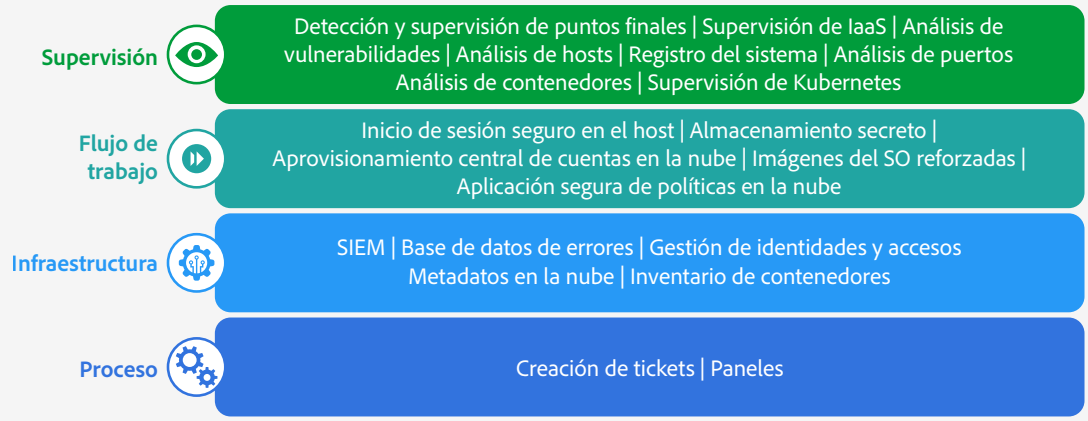


Figura 1: la pila de seguridad operativa de Adobe

Con el objetivo de hacer que la elección segura sea la elección predeterminada, la pila de seguridad operativa de Adobe incluye cuatro (4) capas distintas, cada una de las cuales incluye una amplia gama de herramientas y servicios comunes que cualquier equipo de producto de Adobe puede usar y que les brinda una forma de mantenerse al día de las prácticas recomendadas de seguridad tan cambiantes.

Supervisión

La capa de supervisión incluye herramientas para ayudar a introducir los datos de registro y configuración de todos los entornos y regiones de la nube de Adobe en un almacén de datos central. Una vez introducidos, los equipos de seguridad y cumplimiento normativo de Adobe, así como el centro de operaciones de seguridad (SOC, por sus siglas en inglés) de Adobe, pueden ponerse a analizar estos datos para ayudar a medir las desviaciones de seguridad y detectar las brechas de seguridad. Estas últimas se pueden encontrar a través de la revisión manual de los datos por parte del equipo de seguridad o mediante herramientas automatizadas de detección de seguridad.

Asimismo, nuestros equipos de seguridad realizan periódicamente análisis de hosts y contenedores en nuestros entornos en la nube, tanto desde la perspectiva de la aplicación como de la red, para ayudar a detectar vulnerabilidades. Cualquier vulnerabilidad descubierta a través de estos análisis y pruebas de penetración se evalúa, prioriza y asigna, en caso necesario, a un plan de corrección.

Las siguientes herramientas se incluyen en la capa de supervisión de la pila de seguridad operativa de Adobe:

- **Detección y respuesta de puntos finales**: CrowdStrike Falcon, un agente de detección y respuesta de puntos finales (EDR, por sus siglas en inglés) ligero y de última generación que se instala en todos los puntos finales —incluidos los servidores— de Adobe, protege nuestros datos y sistemas con una supervisión y recopilación continuas en tiempo real que nos permiten identificar y responder rápidamente a las amenazas.
- **Supervisión de IaaS**: MAVLink, una herramienta de recopilación de datos de la nube pública desarrollada por Adobe, consulta las API de Amazon Web Services (AWS) y Microsoft Azure para obtener datos de registro y configuración del entorno y, después, introduce esta información en un almacén de datos de Splunk. Al utilizar MAVLink, los desarrolladores permiten a los equipos de ingeniería de seguridad de Adobe ver el estado de la nube pública en un momento determinado desde la perspectiva de seguridad. Los equipos de cumplimiento normativo y auditoría interna de Adobe también pueden utilizar estos datos para determinar el cumplimiento normativo con muchos elementos de los estándares de seguridad tanto de AWS como de Azure.
- **Análisis de vulnerabilidades**: gracias a una variedad de herramientas comerciales y desarrolladas internamente, escaneamos de forma periódica los centros de datos de Adobe, así como toda nuestra presencia en la nube, lo que permite detectar posibles vulnerabilidades antes de que surjan.
- **Análisis de hosts**: mediante Hubble, un marco modular de cumplimiento normativo de seguridad basado en Python, desarrollado internamente y de código abierto para la comunidad externa, Adobe lleva a cabo las tres (3) actividades siguientes:
  - Auditoría: comprueba los sistemas host con los archivos de políticas basados en el estándar del Centro de Seguridad de Internet (CSI).
  - Consulta: recopila información del sistema mediante osquery para detectar intrusiones.
  - Integridad de archivos: realiza un seguimiento de los cambios de archivos en directorios clave.
- **Registro del sistema**: Adobe recopila registros del sistema y mensajes de eventos de diferentes máquinas y los almacena en Splunk para su supervisión y revisión.

- **Análisis de puertos**: analizamos continuamente cientos de miles de direcciones IP de Adobe, lo que permite reducir el intervalo de tiempo entre la exposición inicial y la corrección. Gracias a la canalización de análisis mediante Nmap, los equipos pueden detectar rápidamente la exposición de puertos en el perímetro.
- **Análisis de contenedores**: Adobe registra y analiza imágenes de contenedores en busca de vulnerabilidades y exposiciones comunes (CVE, por sus siglas en inglés) conocidas tanto en la creación como en el tiempo de ejecución. Esos análisis los cargamos en Splunk, mientras que los equipos reciben un ticket de Jira para las incidencias que requieren solución.
- **Supervisión de Kubernetes**: mediante una herramienta de seguridad interna diseñada para supervisar los clústeres de Kubernetes, los ingenieros de seguridad de Adobe pueden obtener una instantánea de configuración de solo lectura de cualquier clúster en un momento predefinido y ejecutar evaluadores personalizados para detectar brechas de seguridad. Después, enviamos los resultados a Splunk para analizarlos y crear tickets.

Flujo de trabajo

La capa de flujo de trabajo de la pila de seguridad operativa de Adobe está formada por herramientas que ayudan a los desarrolladores e ingenieros de productos a ofrecer la seguridad integral de los productos de Adobe y de la infraestructura de la empresa. Las herramientas disponibles en esta capa, que permiten a nuestros equipos aplicar de forma eficaz las políticas de seguridad, facilitan la realización de operaciones seguras, entre las que se incluyen las siguientes:

- **Inicio de sesión seguro en el host**: la gestión centralizada de credenciales y acceso ayuda a Adobe a mantener un control estricto sobre las máquinas virtuales en la nube mediante la aplicación de políticas de autenticación multifactor (MFA, por sus siglas en inglés) y principios de privilegio mínimo. Además, registramos todas las sesiones administrativas con fines de auditoría.
- **Almacenamiento secreto**: Adobe utiliza un producto líder de bóveda segura de terceros para proteger, almacenar y controlar estrictamente el acceso a tokens, contraseñas, certificados, claves API y otros secretos.
- **Aprovisionamiento central de cuentas en la nube**: los equipos de productos, a fin de agilizar la gestión y la gobernanza de la presencia en la nube de Adobe, pueden crear y administrar cuentas en la nube a través de un servicio central, lo que permite al equipo de gobernanza de Adobe gestionar con mayor facilidad la facturación de las cuentas en la nube, así como aplicar de forma centralizada las políticas operativas y de seguridad. Contar con una única fuente de confianza para los metadatos de cuentas en la nube resulta fundamental para comprender el tamaño y el enfoque de seguridad de nuestra presencia en la nube, mientras que el aprovisionamiento de cuentas centralizado nos permite conocer la propiedad correcta de las cuentas y su finalidad prevista.
- **Imágenes del sistema operativo reforzadas**: al proporcionar imágenes reforzadas centralizadas que se adhieren a los puntos de referencia del Centro de Seguridad en Internet (CSI) y aplican tanto las actualizaciones de seguridad aprobadas por el CSI como las herramientas de seguridad más recientes, Adobe ofrece una experiencia segura e inmediata a todos nuestros equipos de productos. Nuestras herramientas de seguridad internas analizan las imágenes, almacenadas en una aplicación desarrollada internamente llamada Image Factory, antes de liberarlas para que las usen nuestros equipos de ingeniería. Asimismo, los equipos de productos pueden utilizar la API de Image Factory para integrar la última imagen de la máquina directamente en su proceso de creación.

- **Aplicación segura de políticas en la nube**: mientras que la mayoría de los proveedores de servicios en la nube ofrecen políticas seguras predeterminadas, Adobe utiliza una herramienta complementaria desarrollada internamente para automatizar la aplicación y corrección de políticas, así como para proporcionar una capa adicional de protección contra las desviaciones accidentales de seguridad y los servicios inseguros implementados en la nube. La herramienta emplea servicios nativos de la nube, como Azure Policy, las políticas de control de servicios de AWS y AWS Config Rules, para aplicar los requisitos de cumplimiento normativo de políticas y recursos en todas las cuentas de nube pública de Adobe. Cualquier recurso que no cumpla con los requisitos en una cuenta de nube pública desencadena automáticamente las medidas de política adecuadas. La herramienta, después, registra la acción y notifica al equipo o equipos afectados para que puedan identificar lo que ha desencadenado el evento de corrección.

Con el fin de ofrecer protección frente a los errores de configuración más comunes, nuestras políticas se centran en un conjunto de categorías que incluyen las vías de compromiso más utilizadas por los atacantes:

- Identidad y privilegios en la nube
- Integridad y privacidad de los datos
- Exposición de los extremos de redes
- Integridad de DNS

Asimismo, nuestro modelo operativo de políticas en la nube establece que las cuentas nuevas incluyan todas las políticas activas actuales en el momento del aprovisionamiento. Cuando Adobe publica una nueva política, nuestro proceso de aplicación automatizada aplica las cuentas existentes a medida que cumplen con dicha política. Para acelerar el proceso de aplicación tras la publicación de una nueva política, aplicamos automáticamente las cuentas después de un periodo de reposo (unos 30 días) tras la publicación. Las cuentas que no cumplan con lo establecido reciben automáticamente un ticket para que se rectifiquen, incluida una fecha límite para que se ajusten a la nueva política.

La aplicación automatizada permite a nuestros desarrolladores centrarse en el trabajo de mayor nivel para cumplir con la política, mientras que el proceso garantiza la aplicación de la propia política. El proceso automatizado, de forma periódica, comprueba si hay cuentas nuevas que cumplan con los requisitos y aplica automáticamente las políticas.

Infraestructura

Los metadatos sofisticados y actualizados periódicamente son un componente clave de la capa de infraestructura de la pila de seguridad operativa de Adobe, que constituye la base de las capas de supervisión y flujo de trabajo. Mediante estos metadatos, la pila puede asignar automáticamente las brechas de seguridad descubiertas al equipo que posee el recurso en la nube infractor. Otras herramientas de la capa de infraestructura son:

- **Gestión de eventos e información de seguridad (SIEM, por sus siglas en inglés)**: al usar Splunk para buscar, supervisar, visualizar y analizar los datos de registro agregados recopilados en la capa de supervisión, el centro de operaciones de seguridad de Adobe puede llevar a cabo un análisis más exhaustivo de los sucesos e incidentes relacionados con la seguridad.

- **Base de datos de errores**: Adobe, a fin de ayudar a proporcionar una única fuente de atribución, registra los errores en Jira mediante su sistema automatizado de creación de tickets para la responsabilidad y el seguimiento.
- **Gestión de acceso e identidades (IAM, por sus siglas en inglés)**: Adobe utiliza Active Directory de Microsoft junto con otras herramientas estándar para gestionar la autenticación.
- **Metadatos en la nube**: Adobe realiza un seguimiento y auditoría de los metadatos de todas las cuentas de nube pública y audita estos datos con una periodicidad trimestral para ayudar a proteger las cuentas y garantizar la gobernanza de las políticas. El portal de metadatos en la nube permite a los equipos de productos y seguridad incorporar nuevas cuentas en la nube según los flujos de trabajo establecidos. Además, los equipos pueden acceder a los metadatos del almacén de datos para filtrar el ruido, eliminar los falsos positivos y ayudar a dar la prioridad adecuada a las amenazas críticas.
- **Inventario de contenedores**: un amplio conjunto de metadatos para todo el ecosistema de contenedores de Adobe que ayuda a nuestros equipos de productos a obtener información más detallada sobre la orquestación de contenedores. Además, los equipos pueden utilizar los metadatos de contenedores para supervisar y visualizar métricas, así como para conseguir una visibilidad completa de cualquier entorno de Kubernetes.

Proceso

La capa de proceso permite a Adobe mejorar continuamente nuestro enfoque de seguridad e implementar las prácticas recomendadas de seguridad. Los datos de las otras tres capas de la pila de seguridad operativa de Adobe se almacenan en un almacén de datos centralizado y se incorporan a Jira (para mitigar y resolver las brechas de seguridad), a los paneles (para aumentar la visibilidad de la gestión) y a otros partners internos.

Utilizamos indicadores clave de rendimiento (KPI, por sus siglas en inglés) para medir la eficacia de la implementación de la pila de seguridad operativa de Adobe en toda la empresa, así como para identificar valores atípicos. La creación automatizada de tickets de Jira notifica a los equipos de productos cuando su servicio se desvía de un estado de seguridad reforzado y ayuda a nuestros equipos de ingeniería y operaciones a cumplir varios dominios de control en el marco común de controles (CCF, por sus siglas en inglés) de Adobe, como la gestión de configuración y de activos.

La pila de seguridad operativa de Adobe en acción

Cada capa de la pila de seguridad operativa de Adobe, que aprovecha la automatización, los controles en el nivel del sistema y la estandarización, funciona conjuntamente con las demás para ayudar a proporcionar seguridad a nuestros recursos en la nube implementados.

Las herramientas de control de acceso y credenciales permiten aplicar de forma uniforme las políticas de gestión de acceso e identidades en todos nuestros servicios gestionados en la nube, mientras que el registro de las actividades de los usuarios ofrece información

más detallada sobre las áreas potenciales para la mejora de las políticas de aplicación. Los desarrolladores, por tanto, crean, implementan y gestionan servicios en la nube seguros de forma predeterminada empleando imágenes del sistema operativo reforzadas de nuestra infraestructura de Image Factory.

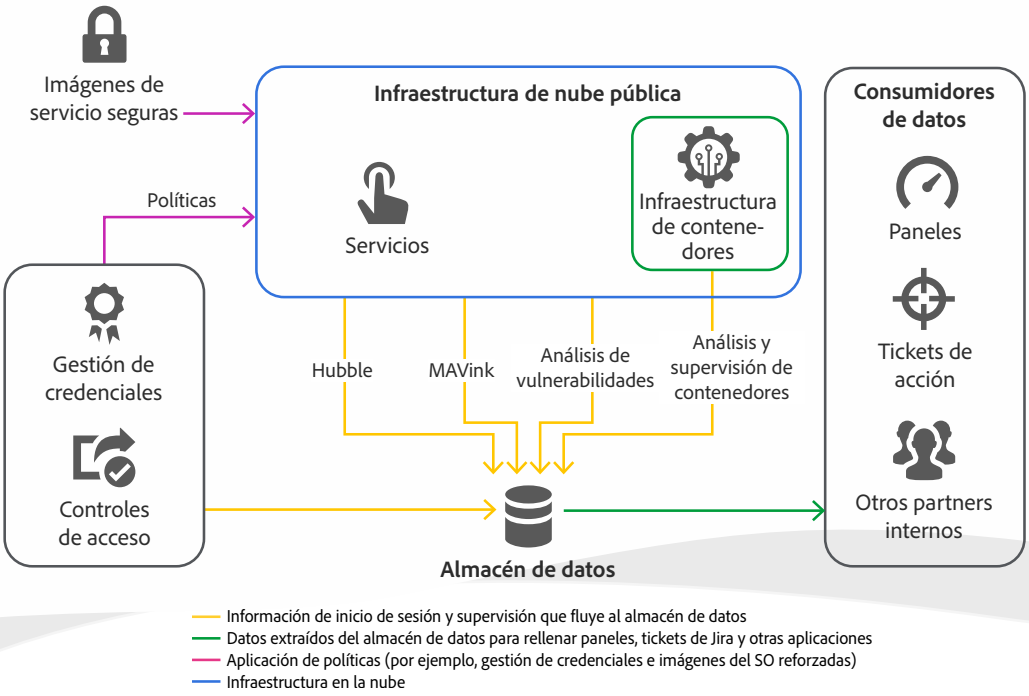


Figura 2: el flujo de datos de la pila de seguridad operativa de Adobe

Tras la implementación, nuestras herramientas de supervisión vigilan continuamente los servicios —ya estén implementados en la nube o en nuestra plataforma de contenedores— y envían registros y otra información pertinente a un almacén central de datos. Los paneles, los tickets de Jira y otras aplicaciones de toda la empresa extraen datos de este almacén para rellenar sus aplicaciones de cara al usuario.

Conclusión

La estrategia de seguridad operativa de Adobe brinda a nuestros equipos de productos y servicios barreras de seguridad uniformes y repetibles para ayudar a garantizar que las ofertas de los clientes de Adobe se creen teniendo en cuenta la seguridad y se adhieran a nuestro cumplimiento normativo, privacidad y otros marcos de gobernanza. La automatización de la seguridad junto con la supervisión continua de nuestro enfoque de seguridad mediante informes, paneles y revisiones trimestrales del cumplimiento normativo ayudan a Adobe a prevenir de forma proactiva los riesgos de seguridad y a mantener la seguridad integral tanto de nuestros productos como de la infraestructura de la empresa.