LECCIÓN 5: PRÁCTICAS RECOMENDADAS PARA LA GENERACIÓN DE REGISTROS Y SUPERVISIÓN

• Defina los requisitos de su organización para los registros, las alertas y las métricas.

• Configure el registro de servicios y aplicaciones durante toda su carga de trabajo.

• Analice sus registros de forma centralizada.

El primer paso para usar las capacidades de registro y supervisión que proporciona AWS es definir sus requisitos. Identifique los recursos, las aplicaciones y los servicios para los que desea mantener registros. Los requisitos de registro y supervisión pueden variar ampliamente, por lo que debe definir cuáles son los requisitos organizacionales, legales y de cumplimiento para sus cargas de trabajo. A continuación, evalúe e identifique los recursos que AWS tiene disponibles para ayudarlo.

Cuando recopila métricas y define valores de referencia, puede obtener información sobre posibles amenazas a la seguridad. Defina quién debe recibir alertas y qué debe hacer con las alertas que recibe. Configure los registros en toda la carga de trabajo, incluidos los registros de aplicaciones, de servicios de AWS y de recursos.

Recopile sus registros de forma centralizada. Utilice la automatización de servicios como CloudWatch para analizar registros a fin de detectar cualquier anomalía o indicador de actividad malintencionada o peligro. Esta lección aborda los servicios adicionales de AWS para el registro y la supervisión.

AWS TRUSTED ADVISOR

- **Brinda recomendaciones basadas en cinco categorías de prácticas recomendadasde AWS: optimización de costos, seguridad, tolerancia a errores, límites de servicio y mejora del rendimiento.**

- **Evalúa su cuenta a fin de sugerir mejoras y optimizaciones para sus recursos.**

- **Es accesible a través de la consola de administración de AWS y está disponible para todos los niveles de soporte.**

AWS Trusted Advisor proporciona recomendaciones que lo ayudan a seguir las prácticas recomendadas de AWS, que se aprendieron luego de brindar servicios a cientos de miles de clientes de AWS. Trusted Advisor evalúa su cuenta mediante comprobaciones basadas en cinco categorías de prácticas recomendadas de AWS. Los controles identifican maneras de optimizar la infraestructura de AWS, mejorar la seguridad y el rendimiento, reducir los costos y supervisar las cuotas de servicio.

Suponga que es el administrador de la cuenta de AWS de su organización. Se encuentra buscando formas de optimizar los recursos de la cuenta y mejorar su posición de seguridad general, pero hacerlo manualmente le llevaría mucho tiempo. AWS Trusted Advisor puede automatizar este proceso por usted y brindarle recomendaciones de acciones que puede realizar para mejorar estas áreas. Después, puede seguir las recomendaciones para optimizar sus recursos y su posición de seguridad.

Trusted Advisor está disponible en todos los planes de AWS Support. Los clientes de AWS Basic Support y AWS Developer Support pueden acceder a comprobaciones de seguridad principales y a todas las comprobaciones para las cuotas de servicio. Los clientes de AWS Business Support y AWS Enterprise Support pueden acceder a todas las comprobaciones, incluidos la optimización de costos, la seguridad, la tolerancia a errores, el rendimiento y las cuotas de servicio.

Para más información, consulte AWS Trusted Advisor en la Guía del usuario de AWS Support en https://docs.aws.amazon.com/awssupport/latest/user/trusted-advisor.html.

AMAZON EVENTBRIDGE

• Es un servicio de bus de eventos sin servidor que se utiliza para conectar sus aplicaciones con datos de una variedad de orígenes.

• Proporciona un flujo de datos en tiempo real desde aplicaciones y servicios a objetivos, como AWS Lambda o buses de eventos.

• Se denominaba anteriormente Amazon CloudWatch Events.

Amazon EventBridge es un servicio de bus de eventos sin servidor que le facilita la creación de aplicaciones basadas en eventos al conectar esas aplicaciones con datos de una variedad de fuentes. El servicio conecta aplicaciones mediante el uso de eventos, que son señales de que el estado de un sistema ha cambiado. Para usar el servicio, no necesita aprovisionar, aplicar parches ni administrar servidores, y no necesita instalar ni mantener ningún software. EventBridge se escala automáticamente según la cantidad de eventos ingeridos y tiene tolerancia a errores incorporada.

Veamos cómo se puede usar EventBridge para ayudarlo con la supervisión y la auditoría. Puede supervisar y auditar sus entornos de AWS y responder a cambios operativos en sus aplicaciones en tiempo real para evitar vulnerabilidades de infraestructura. Por ejemplo, cuando se accede a sus recursos a través de cuentas cruzadas o públicas, puede configurar un evento de Amazon Access Analyzer para que se genere y se envíe a una función de AWS Lambda mediante EventBridge a fin de eliminar los permisos no deseados.

EventBridge se denominaba anteriormente Amazon CloudWatch Events. CloudWatch Events y EventBridge usan la misma API, por lo que cualquier código que haya utilizado anteriormente con CloudWatch Events permanece igual. Si bien ambos servicios aún son compatibles, las nuevas funciones solo se agregan a EventBridge.

Para más información, consulte la Guía del usuario de Amazon EventBridge en https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-what-is.html.

AWS SECURIT HUB

- **Agrega alertas de seguridad de varios servicios de AWS y productos de socios en un formato estandarizado.**

- **Recopila datos entre cuentas y verifica la posición de seguridad de la nube con las prácticas recomendadas sobre seguridad de AWS.**

- **Lo ayuda a comprender su posición de seguridad general mediante el uso de una puntuación de seguridad unificada en todas sus cuentas de AWS.**

AWS Security Hub es un servicio que lo ayuda a supervisar su posición de seguridad en la nube mediante el uso de comprobaciones continuas y automatizadas de las prácticas recomendadas de seguridad, donde se las compara con sus recursos de AWS. Security Hub agrega alertas de seguridad de varios servicios de AWS y productos de socios externos y las presenta en un formato estandarizado, lo que le facilita actuar en función de ellas. También puede usar Security Hub para crear flujos de trabajo automatizados de respuesta, corrección y enriquecimiento al aprovechar la integración de Security Hub con EventBridge. Security Hub proporciona una puntuación de seguridad para cada estándar habilitado y una puntuación total para todas las cuentas asociadas con su cuenta de administrador. Esta información puede ayudarlo a supervisar su posición de seguridad general.

Un ejemplo de lo útil que es AWS Security Hub es su capacidad para ayudarlo a priorizar los esfuerzos de respuesta y corrección de los equipos de seguridad centrales y de DevSecOps al buscar, correlacionar y agregar diversos hallazgos de seguridad por cuentas y recursos.

Para más información, consulte AWS Security Hub en https://aws.amazon.com/security-hub.

AWS CONFIG

- **Ayuda a evaluar, auditar y analizar las configuraciones de sus recursos de AWS.**

- **Supervisa y registra de forma continua las configuraciones de los recursos de AWS.**

- **Brinda una evaluación automatizada de las configuraciones registradas en función de las configuraciones deseadas.**

Con el servicio AWS Config, puede examinar, auditar y evaluar las configuraciones de los recursos de AWS. AWS Config supervisa y registra de forma continua sus configuraciones de recursos de AWS, lo que le permite automatizar la evaluación de esas configuraciones comparándolas con las configuraciones deseadas. También puede usar AWS Config para ver las políticas de IAM que se asignan a usuarios, grupos o roles de IAM en cualquier momento en que AWS Config mantuvo un registro. Esta capacidad puede ayudarlo a determinar qué permisos pertenecían a qué usuario en ese momento específico. AWS Config puede ayudarlo a mantener el cumplimiento y la auditoría al brindar configuraciones históricas de recursos. Con la amplia gama de capacidades de AWS Config, puede simplificar la auditoría del cumplimiento, los análisis de seguridad,
la administración de cambios y la resolución de problemas operativos en su entorno de AWS.

Un ejemplo de un área en la que AWS Config es un activo valioso es la administración de cambios. Cuando se crean, actualizan o eliminan recursos, AWS Config transmite estos cambios de configuración a Amazon Simple Notification Service (SNS) para notificárselos. AWS Config representa relaciones entre recursos para que pueda evaluar cómo un cambio a un recurso podría afectar otros recursos.

Para más información, consulte AWS Config en https://aws.amazon.com/confi