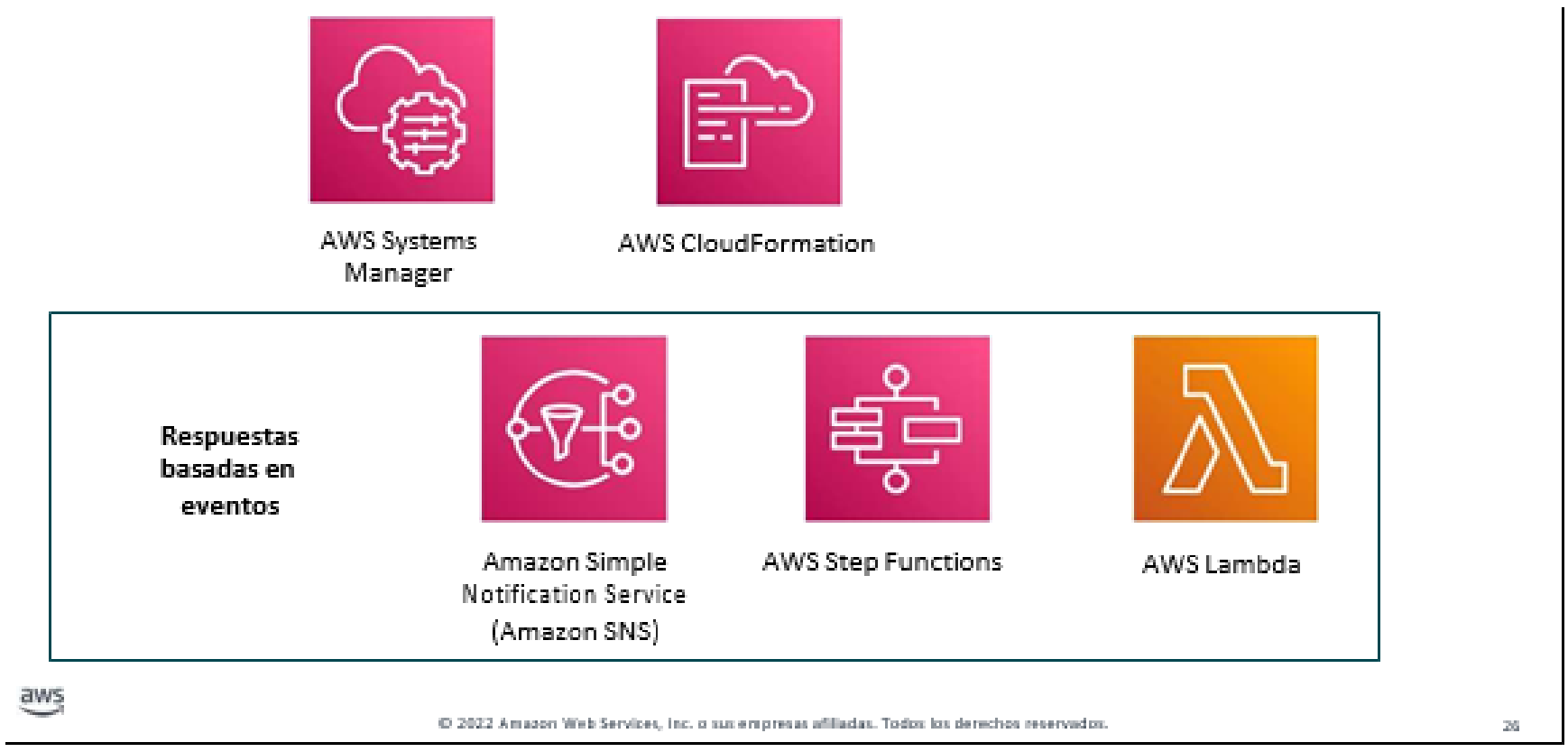
LECCIÓN 3: SERVICIOS QUE RESPALDAN LA FASE DE RESOLUCIÓN Y RECUPERACIÓN.

Observe que estos no son todos los servicios de AWS disponibles.

RESOLUCIÓN Y RECUPERACIÓN



AWS ofrece varios servicios diferentes que ayudan con la resolución y la recuperación.

En esta lección, se describirán los siguientes servicios con más detalle y cómo respaldan esta fase de respuesta ante incidentes:

AWS Systems Manager

AWS CloudFormation

Amazon Simple Notification Service (Amazon SNS)

AWS Step Functions

AWS Lambda

Lambda, Amazon SNS y Step Functions son servicios de respuesta basados en eventos. Una respuesta basada en eventos es un programa informático escrito para responder a acciones generadas por el usuario o el sistema.

AWS SYSTEMS MANAGER

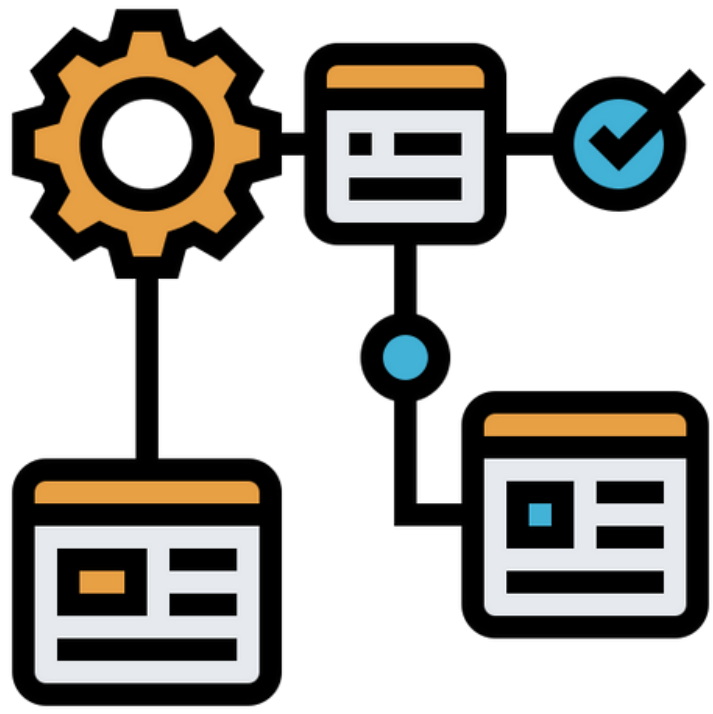
- **Le brinda visibilidad y control de su infraestructura en AWS.**

- **Proporciona una interfaz de usuario unificada para que pueda ver los datos operativos de varios servicios de AWS.**

- **Brinda la capacidad de agrupar recursos por aplicación y ver datos operativos para supervisar y solucionar problemas.**

- **Lo ayuda a mantener sus instancias en su estado definido y realizar cambios bajo demanda, como actualizar aplicaciones o ejecutar scripts de Shell.**

AWS Systems Manager le ofrece visibilidad y control de su infraestructura en AWS. Systems Manager proporciona una interfaz de usuario unificada para que pueda ver los datos operativos de varios servicios de AWS y automatizar tareas operativas en sus recursos de AWS. Con Systems Manager, puede agrupar recursos por aplicación, ver datos operativos para supervisar y solucionar problemas, y tomar medidas en sus grupos de recursos. Systems Manager puede ayudarlo a mantener sus instancias en su estado definido y realizar cambios a pedido, como actualizar aplicaciones o ejecutar scripts de shell. El servicio también puede ayudarlo a realizar otras tareas de automatización y aplicación de parches.



Para más información, consulte la Guía del usuario de AWS Systems Manager en **https://docs.aws.amazon.com/systems-manager/latest/userguide/what-is-systems-manager.html**.

AWS CLOUDFORMATION

- **Lo ayuda a modelar y configurar sus recursos de AWS para que pueda pasar menos tiempo administrando esos recursos y más tiempo centrándose en sus aplicaciones que se ejecutan en AWS.**

- **Ofrece la posibilidad de crear una plantilla que describa todos los recursos de AWS que desee.**

- **Se puede utilizar para recrear un entorno de prueba dentro de una nube virtual privada (VPC) aislada o forense.**

AWS CloudFormation es un servicio que le permite modelar y configurar los recursos de AWS para que pueda invertir menos tiempo administrando dichos recursos y más tiempo centrándose en las aplicaciones que se ejecutan en AWS. Usted crea una plantilla en la que se describen todos los recursos de AWS que desea y CloudFormation se encarga de aprovisionar y configurar esos recursos por usted. No necesita crear y configurar individualmente los recursos de AWS ni descubrir qué depende de qué; CloudFormation se encarga de eso.

Una empresa puede usar CloudFormation para recrear un entorno de prueba dentro de una nube virtual privada (VPC) aislada o forense. Una vez que el sistema está aislado, el equipo puede profundizar y descubrir el problema, si es posible reproducirlo, aplicar una solución y realizar pruebas. Luego, el equipo puede enviar cualquier infraestructura nueva, como código, o cualquier código de aplicación nuevo a producción.

Para más información, consulte la Guía del usuario de AWS CloudFormation en https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/Welcome.html.

AMAZON SIMPLE NOTIFICATION SERVICE (AMAZON SNS)

Es un servicio web basado en eventos que proporciona la capacidad para que las aplicaciones, los usuarios finales y los dispositivos envíen y reciban notificaciones instantáneamente desde la nube.

Amazon SNS y Lambda están integrados, por lo que puede invocar las funciones de Lambda con las notificaciones de Amazon SNS. Cuando se publica un mensaje en un tema de Amazon SNS que tiene suscrita una función de Lambda, se invoca la función de Lambda con la carga útil del mensaje publicado. La función de Lambda recibe la carga del mensaje como un parámetro de entrada y puede manipular la información del mensaje, publicar el mensaje en otros temas de SNS o enviar dicho mensaje a otros servicios de AWS.

Una empresa puede utilizar Amazon SNS para recibir notificaciones de posibles vulnerabilidades.

Para más información, consulte la Guía para desarrolladores de Amazon Simple Notification Service en https://docs.aws.amazon.com/sns/latest/dg/welcome.html.

AWS STEP FUNCTIONS

• Es un servicio de flujo de trabajo visual que los desarrolladores utilizan para crear aplicaciones distribuidas y automatizar los procesos empresariales y de TI.

• Brinda la capacidad de crear flujos de trabajo basados en eventos para administrar fallas, reintentos, paralelización, integraciones de servicios y observabilidad a fin de que los desarrolladores puedan concentrarse en la lógica comercial de mayor valor.

AWS Step Functions es un servicio de flujo de trabajo visual de código bajo que los desarrolladores utilizan para crear aplicaciones distribuidas, automatizar procesos comerciales y de TI, y crear canalizaciones de datos y machine learning mediante los servicios de AWS. Los flujos de trabajo basados en eventos gestionan errores, reintentos, paralelización, integraciones de servicios y observabilidad para que los desarrolladores puedan centrarse en la lógica empresarial de mayor valor.

Cuando una empresa experimenta anomalías, la implementación de Step Functions puede ayudarlo a crear una lógica empresarial compleja en flujos de trabajo basados en eventos que conectan servicios, sistemas o personas en cuestión de minutos.

Para más información, consulte la Guía para desarrolladores de AWS Step Functions en https://docs.aws.amazon.com/step-functions/latest/dg/welcome.html.

AWS LAMBDA

• Es un servicio informático basado en eventos y sin servidor que brinda la capacidad de ejecutar Código bajo demanda sin aprovisionar ni administrar servidores.

• Las funciones de Lambda no tienen estado.

AWS Lambda es un servicio informático basado en eventos sin servidor que brinda la capacidad de ejecutar código a pedido sin aprovisionar ni administrar servidores. Solo paga por el tiempo de cómputo que consume y no se le cobra cuando su código no se está ejecutando. Con Lambda, puede ejecutar código para prácticamente cualquier tipo de aplicación o servicio de backend, todo sin administración. Simplemente carga su código y Lambda se encargará de todo lo necesario para ejecutarlo y escalarlo con alta disponibilidad. Puede configurar el código para que se lo invoque automáticamente desde otros servicios de AWS o puede llamarlo directamente desde cualquier aplicación web o móvil.

Las funciones de Lambda son sin estado, no tienen afinidad con la infraestructura subyacente. Es decir que Lambda puede lanzar rápidamente tantas copias de la función como sea necesario para escalarse a la velocidad de los eventos entrantes. Después de cargar su código en Lambda, puede asociar su función con recursos específicos de AWS, como un bucket particular de Amazon Simple Storage Service (Amazon S3) o un tema de SNS. Luego, cuando el recurso cambie, Lambda ejecuta su función y administra los recursos de cómputo según sea necesario para las solicitudes entrantes.

Si necesita almacenar secretos para acceder a servicios externos, puede utilizar AWS Key Management Service (AWS KMS) para almacenar y recuperar los secretos en su función de Lambda.

La forma en que se invoca una función de Lambda depende del origen del evento que utilice con ella:

- **Para la invocación basada en eventos, algunos orígenes de eventos pueden publicar los eventos en Lambda e invocar directamente su función de Lambda. Esto se denomina modelo de inserción, donde los orígenes de eventos invocan su función de Lambda.**
- **Algunos orígenes de eventos publican eventos, pero Lambda debe sondear el origen del evento e invocar la función de Lambda cuando se producen eventos. Esto se denomina modelo de extracción.**

La invocación de solicitud/respuesta hace que Lambda ejecute la función de forma sincrónica y devuelva la respuesta de inmediato a la aplicación que realiza la llamada. Este tipo de invocación está disponible para aplicaciones personalizadas.

Para más información, consulte la Guía para desarrolladores de AWS Lambda en https://docs.aws.amazon.com/lambda/latest/dg/welcome.html.

LAMBDA PARA RESPUESTA A INCIDENTES

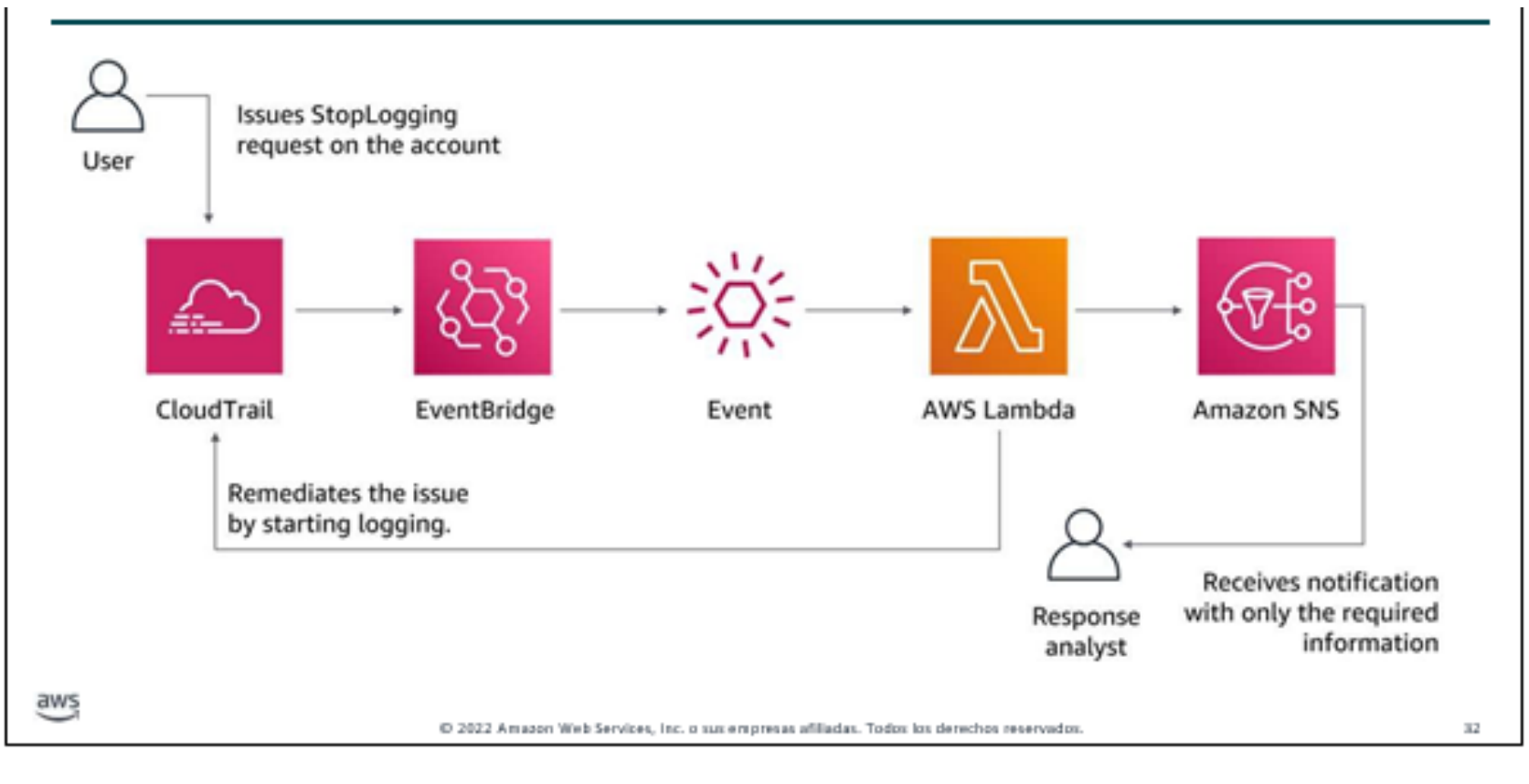
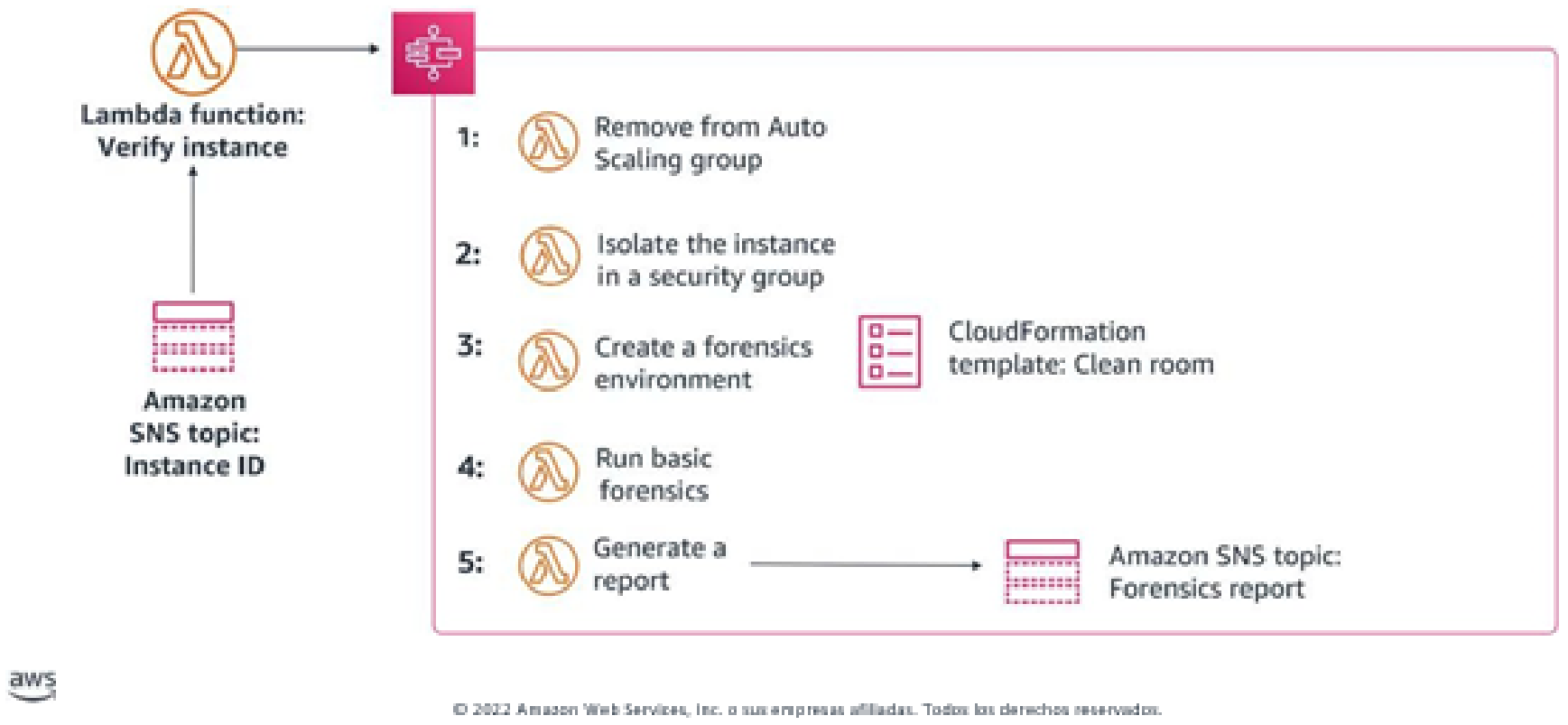


Diagrama del uso de Lambda para respuesta ante incidentes. El usuario emite una solicitud StopLogging a CloudTrail. CloudTrail y EventBridge invocan una función de Lambda para corregir automáticamente el evento. La información procesada se envía como una notificación SNS a un analista de respuestas. Otra función de Lambda se invoca automáticamente para reiniciar el registro.

Con un sistema de respuesta dirigido por eventos, un mecanismo de detección invoca un mecanismo de respuesta para solucionar automáticamente el evento. Puede utilizar las capacidades de respuesta dirigidas por eventos para reducir el tiempo de obtención de valor entre los mecanismos de detección y los mecanismos de respuesta. Para crear esta arquitectura basada en eventos, puede usar Lambda.

Por ejemplo, suponga que tiene una cuenta de AWS con el servicio AWS CloudTrail habilitado. Si CloudTrail alguna vez está deshabilitado, el procedimiento de respuesta consiste en habilitar el servicio de nuevo e investigar al usuario que deshabilitó el registro de CloudTrail. Puede usar EventBridge para supervisar el evento “cloudtrail:StopLogging” específico e invocar la función si ocurre. Cuando EventBridge invoca esta función de Lambda, la función recopila los detalles del evento específico. Los detalles incluyen información como la identidad de la entidad principal que deshabilitó CloudTrail, cuándo se deshabilitó y el recurso específico que se vio afectado. Esta información procesada podría luego enviarse como una notificación a través de Amazon SNS. Puede usar esta información para profundizar en el registro y luego generar una alerta o notificación solo con los valores específicos que necesita su analista de respuestas. También se podría invocar otra función de Lambda para reiniciar automáticamente el registro.

TRABAJO CONJUNTO PARA LA RESPUESTA ANTE INCIDENTES



En esta diapositiva, se proporciona un ejemplo de cómo usar Step Functions, Lambda, CloudFormation y Amazon SNS para reparar una instancia comprometida. Primero, una secuencia de comandos o una herramienta de terceros envía una ID de instancia a un tema de SNS. Luego, una función de Lambda verifica la ID y, si se ve comprometida, inicia el siguiente flujo de trabajo de Step Functions:

1. **La instancia se elimina de su grupo de Auto Scaling y se crea una instantánea de cualquier volumen adjunto de Amazon Elastic Block Store (Amazon EBS).**
2. **La instancia se aísla mediante la eliminación de todos los grupos de seguridad asociados anteriormente. A continuación, se asigna un nuevo grupo de seguridad forense a la instancia sin permisos de entrada ni salida.**
3. **Se utiliza una plantilla de CloudFormation para crear un nuevo entorno, incluida una nueva VPC que contiene una instancia de análisis forense con herramientas prediseñadas adjuntas a una copia de cualquier volumen de las instantáneas.**
4. **Se realiza una investigación forense básica en los volúmenes asociados.**
5. **Luego se genera un informe con los resultados de la investigación y se envía al equipo a través de un tema SNS.**

Una conclusión clave de esta lección es que AWS ofrece varios servicios que respaldan la fase de resolución y recuperación, incluidos los siguientes:

- **Systems Manager le ofrece visibilidad y control de su infraestructura en AWS.**

- **Con CloudFormation, puede crear y aprovisionar implementaciones de infraestructura de AWS de manera predecible y repetida.**

- **Lambda es un servicio de respuesta basado en eventos que brinda la capacidad de ejecutar código sin aprovisionar ni administrar servidores.**

- **Amazon SNS es un servicio web de respuesta basado en eventos que coordina y administra la entrega o el envío de mensajes a puntos finales o clientes suscritos.**

- **Step Functions facilita la coordinación de componentes de aplicaciones distribuidas como una serie de pasos en un flujo de trabajo visual.**