LECCIÓN 4: PRÁCTICAS RECOMENDADAS PARA LA RESPUESTA Y ADMINISTRACIÓN DE UN INCIDENTE.

Veamos algunas de las prácticas recomendadas de la industria para el manejo de incidentes.

Para mejorar la respuesta a incidentes, comience identificando al personal clave en su organización. Mantenga una lista de contactos del personal dentro de su organización a los que necesitaría involucrar al responder y recuperarse ante un incidente. Involúcrese con socios externos, si es necesario, para que lo ayuden a responder y recuperarse ante un incidente. Además, investigue y pruebe herramientas que ayudarían a su organización a responder y recuperarse ante un incidente. La contención automatizada de un incidente puede reducir los tiempos de respuesta y el impacto organizacional.

La preparación es fundamental para minimizar la interrupción debido a un incidente. Cree manuales de procedimiento fáciles de implementar en los que se detallen los pasos a seguir para responder y recuperarse ante un incidente. Asegúrese de que sus planes de escalado y comunicaciones incluyan personal de su organización y partes externas a las que debe notificar en cada etapa durante un incidente. Tenga un proceso para identificar y documentar la causa raíz de un evento para que pueda desarrollar estrategias de mitigación a fin de limitar o prevenir la recurrencia y desarrollar procedimientos para respuestas rápidas y efectivas. Como parte de su planificación, asegúrese de que el personal de seguridad tenga las herramientas adecuadas implementadas previamente en AWS. Además, asegúrese de que el personal de seguridad tenga el acceso correcto preaprovisionado en AWS para que puedan responder adecuadamente a un incidente.

Ensaye con frecuencia la respuesta ante los incidentes y la recuperación. Ejecute eventos de respuesta a incidentes simulados, o días de juego, que involucren al personal clave y la administración para diferentes amenazas. Utilice las lecciones aprendidas de los días de juego como parte de un ciclo de retroalimentación para mejorar sus procesos.