**Revisión posterior a un incidente**

Anteriormente, exploraste la fase de contención, erradicación y recuperación del ciclo de vida de respuesta a incidentes del NIST. Esta lectura explora las actividades involucradas en la fase final del ciclo de vida: la **actividad posterior a un incidente**. Como analista de seguridad, es importante que te familiarices con las tareas que deben llevarse a cabo en esta fase porque cada incidente de seguridad te dará la oportunidad de aprender y mejorar tus respuestas a incidentes futuros.

**Actividad posterior a un incidente**

La fase de actividad posterior a un incidente del ciclo de vida de respuesta a incidentes del NIST es el proceso de revisión que permite identificar áreas a mejorar durante el manejo de incidentes.

Diagrama

Descripción generada automáticamente

**Lecciones aprendidas**

Después de que una organización ha contenido un incidente, lo ha erradicado y se ha recuperado con éxito, el incidente llega a su fin. Sin embargo, esto no significa que haya terminado el trabajo de los profesionales de la seguridad. Los incidentes brindan a las organizaciones y sus equipos de seguridad la oportunidad de aprender de lo que sucedió y priorizar formas de mejorar el proceso de manejo de incidentes.

Esto se hace generalmente a través de una **reunión sobre lecciones aprendidas**, también conocida como análisis retrospectivo o revisión post incidente (post-mortem). Una reunión sobre lecciones aprendidas convoca a todas las partes involucradas luego de un incidente importante. Dependiendo del alcance que haya tenido, se pueden programar varias reuniones para recopilar datos suficientes. El propósito de esta reunión es analizar el incidente en su totalidad, evaluar las medidas de respuesta e identificar cualquier área a mejorar. Su objetivo no es echar culpas sino ofrecer a la organización y a su personal la oportunidad de aprender y mejorar. Esta reunión debe programarse a más tardar dos semanas después de que un incidente haya sido remediado con éxito.

No todos los incidentes requieren su propia reunión sobre lecciones aprendidas. El tamaño y la gravedad de un incidente dictarán si es necesario llevarla a cabo. Los incidentes importantes, como los ataques de ransomware, sí deben revisarse en una reunión sobre lecciones aprendidas específica, a la que asisten todas las partes que intervinieron en cualquier aspecto del proceso de respuesta al incidente. Algunos ejemplos de las preguntas que se tratan en esta reunión son:

* ¿Qué sucedió?
* ¿A qué hora ocurrió?
* ¿Quién lo descubrió?
* ¿Cómo se contuvo?
* ¿Cuáles fueron las medidas que se tomaron para la recuperación?
* ¿Qué pudo haberse hecho de otra manera?

Además de tener la oportunidad de aprender del incidente, existen beneficios adicionales de llevar a cabo una reunión sobre lecciones aprendidas. Para las grandes organizaciones, ofrecen una plataforma para que los miembros del equipo en todos los departamentos compartan información y recomendaciones para la prevención futura.

**Consejo profesional**: Antes de que un equipo organice una reunión sobre lecciones aprendidas, los organizadores deben asegurarse de que todos los asistentes lleguen preparados. Los organizadores de la reunión generalmente desarrollan y distribuyen una agenda de la reunión de antemano, la cual contiene los temas de discusión y garantiza que los asistentes estén informados y preparados. Además, se deben asignar con anticipación las funciones de quienes participarán en la reunión, incluido un moderador que dirija y facilite la discusión y un secretario que tome notas de la reunión.

**Recomendaciones**

Las reuniones sobre lecciones aprendidas brindan oportunidades para el crecimiento y la mejora. Por ejemplo, los equipos de seguridad pueden identificar errores en las acciones de respuesta, brechas en los procesos y procedimientos o controles de seguridad ineficaces. Una reunión sobre lecciones aprendidas debe dar como resultado una lista de acciones prioritarias o recomendaciones prácticas destinadas a mejorar los procesos de manejo de incidentes y la postura de seguridad general de una organización. Esto garantiza que las organizaciones estén implementando las lecciones que han aprendido después de un incidente, de modo que no estén expuestas a experimentar el mismo incidente en el futuro. Algunos cambios que pueden llevarse a cabo incluyen actualizar y mejorar las instrucciones del manual de estrategias o poner en práctica nuevas herramientas y tecnologías de seguridad.

**Informe final**

A lo largo de este curso, exploraste la importancia que tiene la documentación en el registro de detalles durante el ciclo de vida de respuesta a incidentes. Como punto de partida, la documentación de respuesta a incidentes debe describir el incidente teniendo en cuenta las cinco preguntas fundamentales a la hora de investigar un incidente: *quién* (who), *qué* (what), *dónde* (where), *por qué* (why) y *cuándo (where).* Los detalles plasmados durante la respuesta a incidentes son importantes para desarrollar documentos adicionales al final del ciclo de vida.

Uno de los documentos fundamentales que se crea al término de un incidente es el **informe final**.Este proporciona una revisión integral del incidente. Los informes finales no están estandarizados, y sus formatos pueden variar según las organizaciones. Además, se pueden crear varios informes finales dependiendo de los públicos para los que estén escritos. Algunos ejemplos de elementos comunes que pueden encontrarse en un informe final son:

* **Resumen ejecutivo**: Un resumen de alto nivel del informe que incluye las principales conclusiones y los hechos esenciales relacionados con el incidente
* **Línea de tiempo**: Un cronograma detallado del incidente que incluye marcas de tiempo que muestran la secuencia de eventos que llevaron al incidente
* **Investigación**: Una compilación de las medidas que se tomaron durante la detección y el análisis del incidente. Por ejemplo, el análisis de un artefacto de red, como una captura de paquetes, revela información sobre qué actividades ocurren en una red.
* **Recomendaciones**: Una lista de medidas sugeridas para la prevención futura

**Consejo profesional**: Al escribir el informe final posterior a un incidente, considera el público para quien lo estás escribiendo. A menudo, estos informes serán leídos por ejecutivos de negocios y otros profesionales no relacionados con la seguridad, que no tienen la pericia para comprender los detalles técnicos. Tener en cuenta al público al escribir un informe final te ayudará a comunicar de manera efectiva los detalles más importantes.

**Conclusiones clave**

Las acciones posteriores al incidente representan el final del ciclo de vida de respuesta a incidentes. Esta fase brinda la oportunidad para que los equipos de seguridad se reúnan, evalúen las acciones de respuesta, hagan recomendaciones para mejorar y desarrollen el informe final.