**El proceso de triaje**

Anteriormente, aprendiste que el triaje se utiliza para evaluar alertas y asignar prioridad a incidentes. En esta lectura, explorarás el proceso de triaje y sus beneficios. Como analista de seguridad, serás responsable de analizar alertas de seguridad. Tener las habilidades para llevar a cabo el triaje de manera efectiva es importante porque te permite atender y resolver las alertas de seguridad de manera eficiente.

**El proceso de triaje**

Los incidentes pueden tener el potencial de causar un daño significativo a una organización. Los equipos de seguridad deben responder de manera rápida y eficiente para prevenir o limitar el impacto de un incidente antes de que sea demasiado tarde. **El triaje** es la priorización de incidentes en función de su nivel de importancia o urgencia. El proceso de triaje ayuda a los equipos de seguridad a evaluar y priorizar las alertas y asignar recursos de manera efectiva para que los problemas más críticos se atiendan primero.

El proceso de triaje consta de tres pasos:

1. Recibir y evaluar
2. Asignar prioridad
3. Recopilar y analizar

**Recibir y evaluar**

Durante esta primera etapa del proceso de triaje, un analista de seguridad recibe una alerta de, por ejemplo, un **sistema de detección de intrusiones** (IDS). Es posible que recuerdes que un IDS es una aplicación que monitorea la actividad del sistema y alerta sobre posibles intrusiones. Luego, el analista revisa la alerta para verificar su validez y asegurarse de que la entiende en su totalidad.

Esto implica recopilar la mayor cantidad de información posible sobre la alerta, incluidos, entre otros, los detalles sobre la actividad que desencadenó la alerta y los sistemas y activos involucrados. Aquí te presentamos algunas preguntas para tener en cuenta al verificar la validez de una alerta:

* **¿Es la alerta un falso positivo?** Los analistas de seguridad deben determinar si la alerta es un problema de seguridad genuino o un **falso positivo**, o sea, una alerta que detecta incorrectamente la presencia de una amenaza.
* **¿Se activó esta alerta en el pasado?** En caso afirmativo, ¿cómo se resolvió? El historial de una alerta puede ayudar a determinar si es un problema nuevo o recurrente.
* **¿La alerta se desencadena por una vulnerabilidad conocida?** Si una alerta es activada por una vulnerabilidad conocida, los analistas de seguridad pueden aprovechar los conocimientos existentes para determinar una respuesta adecuada y minimizar el impacto de la vulnerabilidad.
* **¿Cuál es la gravedad de la alerta?** La gravedad de una alerta puede ayudar a determinar la prioridad de la respuesta para que los problemas críticos se eleven rápidamente.

**Asignar prioridad**

Una vez que la alerta se ha evaluado y verificado adecuadamente como un problema de seguridad genuino, debe priorizarse en consecuencia. Los incidentes difieren en su impacto, tamaño y alcance, lo que afecta los intentos de respuesta. Para administrar el tiempo y los recursos, los equipos de seguridad deben priorizar la forma en que responden a varios incidentes, ya que no todos son iguales. A continuación, se detallan algunos factores a considerar al determinar la prioridad de un incide:

* **Impacto funcional:** Los incidentes de seguridad que tienen como objetivo sistemas de tecnología de la información impactan el servicio que estos sistemas brindan a sus usuarios. Por ejemplo, un incidente de ransomware puede afectar gravemente la confidencialidad, disponibilidad e integridad de los sistemas. Los datos pueden ser encriptados o eliminados, haciéndolos completamente inaccesibles para los usuarios. Considera cómo un incidente impacta en la funcionalidad existente para el negocio del sistema afectado.
* **Impacto de la información:** Los incidentes pueden afectar la confidencialidad, integridad y disponibilidad de los datos y la información de una organización. En un ataque de exfiltración de datos, los agentes de amenaza pueden robar datos confidenciales, que pueden pertenecer a organizaciones o usuarios externos. Considera los efectos que el compromiso de la información puede causar más allá de la organización.
* **Recuperabilidad:** La forma en que una organización se recupera de un incidente depende del tamaño y el alcance del incidente y de la cantidad de recursos disponibles. En algunos casos, la recuperación podría no ser posible, como cuando un agente de amenaza roba con éxito datos privados y los comparte públicamente. Dedicar tiempo, esfuerzo y recursos en un incidente sin recuperabilidad puede ser un desperdicio. Es importante considerar si la recuperación es posible y si merece el tiempo y el costo.

**Nota**: Las alertas de seguridad suelen llegar con un nivel de prioridad o gravedad asignado que clasifica la urgencia de la alerta en función de un nivel de priorización.

**Recopilar y analizar**

El paso final del proceso de triaje implica que el analista de seguridad realice un análisis exhaustivo del incidente. El análisis implica la recopilación de pruebas de diferentes fuentes, la realización de investigaciones externas y la documentación del proceso de investigación. El objetivo de este paso es recopilar suficiente información para tomar una decisión informada, a la hora de atender el incidente. Dependiendo de su gravedad, puede ser necesario elevarlo a un analista de nivel 2 o a un gerente. Los analistas y gerentes de nivel 2 podrían tener más conocimiento sobre el uso de técnicas avanzadas para atender el incidente.

**Beneficios del triaje**

Al priorizar los incidentes en función de su impacto potencial, puede reducirse el alcance del impacto en la organización, ya que garantiza una respuesta oportuna. Algunos de los beneficios que el triaje tiene para los equipos de seguridad son:

* **Gestión de recursos:** El triaje de las alertas permite a los equipos de seguridad enfocar sus recursos en las amenazas que requieren atención urgente. Esto ayuda a los miembros del equipo a evitar dedicar tiempo y recursos a tareas de menor prioridad y también podría reducir el tiempo de respuesta.
* **Enfoque estandarizado:** El triaje proporciona un enfoque estandarizado para el manejo de incidentes. La documentación del proceso, como los manuales de estrategias, ayuda a que las alertas pasen por un proceso iterativo, lo cual garantiza que se evalúen y validen correctamente. Esto hace que sean solo las alertas válidas las que pasen al siguiente nivel y sean investigadas.

**Conclusiones clave**

El triaje permite a los equipos de seguridad priorizar los incidentes según su nivel de importancia o urgencia. El proceso de triaje es importante para garantizar que una organización cumpla con sus objetivos de respuesta a incidentes. Como profesional de la seguridad, es probable que lo utilices para responder y resolver incidentes de manera efectiva.