**Prácticas adecuadas para una documentación eficaz**

**La documentación** es cualquier forma de contenido registrado que se utiliza para un propósito específico, y es esencial en el campo de la seguridad. Los equipos de seguridad utilizan la documentación para respaldar investigaciones, completar tareas y comunicar hallazgos. Esta lectura explora los beneficios de la documentación y te proporciona una lista de prácticas comunes para ayudarte a crear documentación efectiva en tu carrera en el campo de la seguridad.

**Beneficios de la documentación**

Anteriormente, has aprendido sobre distintos tipos de documentación de seguridad, entre ellos los manuales de estrategias y los informes finales. Además, sabes que la documentación efectiva tiene tres beneficios:

1. Transparencia
2. Estandarización
3. Claridad

**Transparencia**

En seguridad, la transparencia es fundamental para demostrar el cumplimiento de las normativas, regulaciones y procesos internos y dar cuenta de los requisitos vinculados con los seguros. Además, es esencial para los procedimientos legales. El proceso de documentar la posesión y el control de evidencia durante el ciclo de vida del incidente se denomina **cadena de custodia** y es un ejemplo de cómo la documentación genera transparencia y mejora la auditoría.

**Estandarización**

La estandarización a través de procesos y procedimientos repetibles ayuda a la mejora continua, a transferir conocimiento y a facilitar la incorporación de nuevos miembros al equipo. Los **estándares** son referencias que informan sobre cómo establecer políticas.

Previamente, has aprendido cómo NIST proporciona varios marcos de seguridad que se utilizan para mejorar las medidas de seguridad. Del mismo modo, las organizaciones establecen sus propios estándares para satisfacer las necesidades de sus negocios. El **plan de respuesta a incidentes** de una organización es un ejemplo de documentación que crea estandarización. Al describir y documentar paso a paso el proceso de respuesta a un incidente, antes de que este ocurra, el procedimiento queda estandarizado. De esta manera, ante un incidente, las personas pueden seguir el paso a paso, manteniendo, así, la consistencia con los procesos y procedimientos repetibles.

**Claridad**

Idealmente, la documentación debe proporcionar claridad. La documentación clara ayuda a las personas a acceder rápidamente a la información que necesitan y tomar las medidas necesarias. Los analistas de seguridad deben documentar el razonamiento que respalda cualquier medida que toman, y dejar en claro a su equipo por qué se elevó a superiores (escaló) o se cerró una alerta.

**Prácticas adecuadas**

En tu carrera como profesional de la seguridad, deberás aplicar las mejores prácticas de documentación. Aquí se detallan algunas pautas generales para que tengas en cuenta:

**Conoce a tu público**

Antes de que comiences a crear la documentación, considera a tu público y sus necesidades. Por ejemplo, un resumen de incidentes escrito para un gerente de un centro de operaciones de seguridad (SOC) estará redactado de manera diferente a uno que haya sido elaborado para un director ejecutivo (CEO). El gerente del SOC puede entender el lenguaje técnico del campo de la seguridad, pero un CEO podría no hacerlo. Por lo tanto, es necesario que adaptes tu documento para satisfacer las necesidades de tu público.

**Sé conciso**

Es posible que se te asigne la tarea de crear documentación larga, como un informe. Pero cuando resulta demasiado extensa, puede haber resistencia a utilizarla. Para asegurarte de que tu documentación sea útil, establece el propósito desde un comienzo. Esto ayuda a las personas a identificar rápidamente el objetivo del documento. Por ejemplo, los resúmenes ejecutivos describen los principales hechos de un incidente al comienzo de un informe final. Este resumen debe ser breve, de manera que pueda leerse por encima, fácilmente, para identificar los principales hallazgos.

**Actualízalo con frecuencia**

En seguridad, se descubren y explotan nuevas vulnerabilidades constantemente. La documentación debe revisarse y actualizarse regularmente para mantenerse al día con el panorama de amenazas en evolución. Por ejemplo, después de que se ha resuelto, una revisión integral de un incidente puede identificar brechas en los procesos y procedimientos que requieren cambios y actualizaciones. Al actualizar regularmente la documentación, los equipos de seguridad se mantienen bien informados y los planes de respuesta a incidentes permanecen actualizados.

**Conclusiones clave**

La documentación efectiva es beneficiosa para todas las personas de una organización. Saber cómo crear documentación es una habilidad esencial que debe tener un analista de seguridad. A medida que avanzas en tu proceso para convertirte en profesional de la ciberseguridad, asegúrate de considerar estas prácticas para crear documentación efectiva.