**Manual De Estrategias**

Un manual de estrategias es un manual que proporciona detalles sobre cualquier acción operativa. Los manuales también aclaran qué herramientas deben usarse en respuesta a un incidente de Seguridad. En el campo de la Seguridad, los manuales de estrategias son esenciales. Urgencia, eficiencia y precisión son necesarias para identificar y mitigar rápidamente una amenaza de Seguridad a fin de reducir el riesgo potencial. Los manuales garantizan que las personas sigan una lista coherente de acciones de una manera prescrita, independientemente de quién esté trabajando en el caso.

Se utilizan diferentes tipos de libros de jugadas. Estos incluyen guías para la respuesta a incidentes, alertas de Seguridad y propósitos específicos de los equipos y de los productos. Aquí, nos centraremos en un manual que se usa comúnmente en ciberseguridad, llamado manual de respuesta a incidentes.

**Respuesta ante incidentes** es el intento rápido de una organización de identificar un ataque, contener el daño y corregir los efectos de una brecha de Seguridad. Un manual de respuesta a incidentes es una guía con seis fases que se utiliza para ayudar a mitigar y gestionar los incidentes de Seguridad de principio a fin.

Hablemos de cada fase.

La primera fase es la **preparación**. Las organizaciones deben prepararse para mitigar la probabilidad, el riesgo y el impacto de un incidente de Seguridad documentando los procedimientos, estableciendo planes de personal y educando a los usuarios. La preparación sienta las bases para una respuesta exitosa a los incidentes. Por ejemplo, las organizaciones pueden crear planes y procedimientos de respuesta a incidentes que describan las funciones y responsabilidades de cada miembro del equipo de Seguridad.

La segunda fase es **la detección y el análisis**. El objetivo de esta fase es detectar y analizar eventos utilizando procesos y tecnología definidos. El uso de las herramientas y estrategias adecuadas durante esta fase ayuda a los analistas de Seguridad a determinar si se ha producido una violación y a analizar su posible magnitud.

La tercera fase es **la contención**. El objetivo de la contención es evitar daños mayores y reducir el impacto inmediato de un incidente de Seguridad. Durante esta fase, los profesionales de la Seguridad utilizan herramientas y estrategias para determinar si se ha producido una violación y evaluar su magnitud potencial de Seguridad toman medidas para contener un incidente y minimizar los daños. La contención es una alta prioridad para las organizaciones porque ayuda a prevenir los riesgos continuos para los activos y datos críticos.

La cuarta fase de un manual de respuesta a incidentes es **la erradicación y la recuperación**. Esta fase implica la eliminación completa de los artefactos de un incidente para que la organización pueda volver a sus operaciones normales. Durante esta fase, los profesionales de Seguridad eliminan los artefactos del incidente al eliminar el código malicioso y mitigar las vulnerabilidades. Una vez que hayan ejercido la debida diligencia, pueden empezar a restaurar el entorno afectado a un estado seguro. Esto también se conoce como restauración de TI.

La quinta fase es **la actividad posterior al incidente**. Esta fase incluye documentar el incidente, informar a los líderes de la organización y aplicar las lecciones aprendidas para garantizar que la organización esté mejor preparada para gestionar futuros incidentes. Según la gravedad del incidente, las organizaciones pueden realizar un análisis de incidentes a gran escala para determinar la causa raíz del incidente e implementar varias actualizaciones o mejoras para mejorar su postura general de Seguridad.

La sexta y última fase de un manual de respuesta a incidentes es **la coordinación**. La coordinación implica denunciar los incidentes y compartir información durante todo el proceso de respuesta a los incidentes, según los estándares establecidos por la organización. La coordinación es importante por muchos motivos. Garantiza que las organizaciones cumplan con los requisitos de cumplimiento y permite una respuesta y resolución coordinadas.