3

CICLO DE VIDA DE LA GESTIÓN DE UN **INCIDENTE**

CONTENIDO

- *Etapas de la planificación*
- Diagrama de flujo de los incidentes

CICLO DE VIDA DE UN INCIDENTE

Para la mayoría de la gestión de los incidentes se describen una serie de etapas para un manejo adecuado de los mismos. Estas etapas se resumen en una etapa de preparación ante cualquier incidente, la etapa de detección y análisis de incidentes , la etapa de contención o recuperación y la etapa pos-incidente.

PREPARACIÓN - DETECCIÓN - CONTENCIÓN / RECUPERACIÓN - POS-INCIDENTE

ISO / IEC 27035
NORMA

ISO / IEC 27035:2011 Tecnología de la información – Técnicas de seguridad – gestión de incidentes de seguridad de la información, se trata de una guía para la localización, análisis y evaluación de vulnerabilidades e incidentes a los que puede estar expuesta una organización. Esta Norma puede ser usada para pequeñas, medianas y grandes empresas. Las pymes en función a su tamaño y tipo de negocio, pueden orientarse para la gestión de incidentes de seguridad por documentos y procesos explicados en esta Norma. Además, puede ser usada por empresas externas que se dedican a la gestión de incidentes de seguridad de la información a otras empresas.

1. PLANIFICACION Y PREPARACIÓN

En esta fase, se establecen meticulosamente los procesos, procedimientos y recursos necesarios para afrontar incidentes de ciberseguridad. Se elaboran planes de respuesta detallados, asignando roles y responsabilidades específicos a los miembros del equipo. Además, se llevan a cabo simulacros y entrenamientos periódicos para asegurar la eficacia y cohesión del equipo ante situaciones de amenaza.

2. DETECCIÓN Y REPORTE

Durante esta etapa, los sistemas de monitoreo se mantienen activos las 24 horas del día para identificar cualquier actividad inusual o indicador de compromiso. La detección de posibles amenazas desencadena el proceso de reporte, donde se recopilan datos relevantes, se documenta el incidente y se notifica de manera inmediata a los responsables, iniciando así el flujo de respuesta.

3. VALORACIÓN Y DECISIÓN

Tras la detección, se realiza una evaluación exhaustiva del incidente. Se determina la naturaleza y gravedad del evento, identificando las posibles amenazas y evaluando el impacto en la seguridad. Con esta información, se toman decisiones informadas sobre las medidas que deben implementarse para contener, mitigar y resolver el incidente.

4. RESPUESTA

En esta fase, se ejecutan las acciones delineadas en el plan de respuesta. Esto puede incluir la contención de la amenaza, la identificación y eliminación de malware, la restauración de sistemas desde copias de seguridad seguras, y la colaboración con equipos internos y externos para gestionar eficazmente la crisis.

5. LECCIONES APRENDIDAS

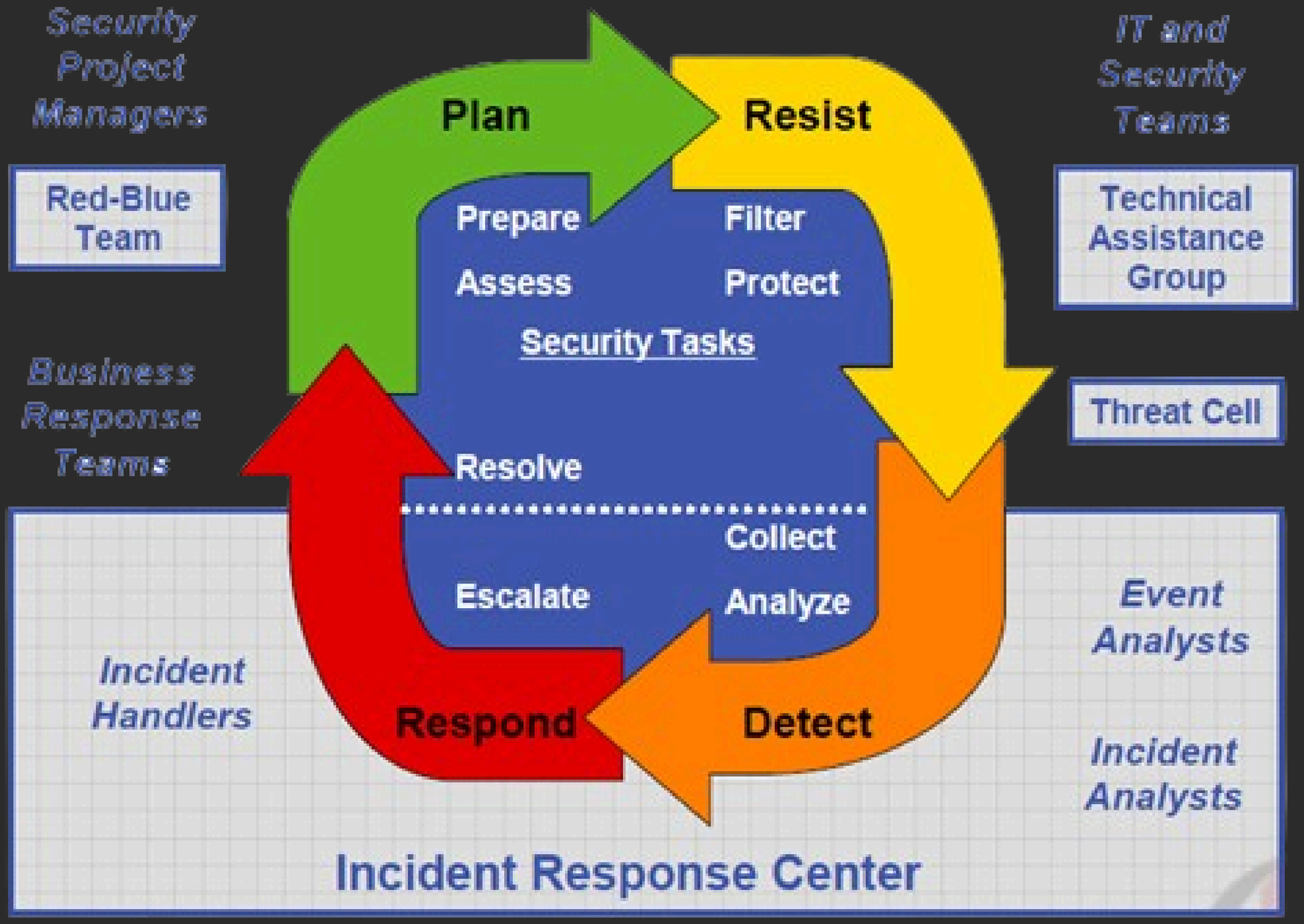
Después de manejar el incidente, se realiza un análisis en profundidad. Se revisan las acciones tomadas, se evalúa la eficacia de la respuesta y se identifican áreas de mejora. Las lecciones aprendidas se documentan meticulosamente, proporcionando valiosos conocimientos que se incorporarán al proceso de mejora continua de la gestión de incidentes.

6. ACTIVIDAD POST-INCIDENTE

En la fase final, se llevan a cabo actividades destinadas a la normalización de las operaciones. Se actualizan registros y documentación, se comunican las lecciones aprendidas a todo el equipo, se implementan ajustes en los procedimientos según sea necesario y se completa un informe detallado del incidente para fines regulatorios y referencia futura. Esta fase cierra el ciclo de gestión de incidentes, pero también alimenta la fase de planificación y preparación para futuros eventos.

6. ACTIVIDAD POST-INCIDENTE

En la fase final, se llevan a cabo actividades destinadas a la normalización de las operaciones. Se actualizan registros y documentación, se comunican las lecciones aprendidas a todo el equipo, se implementan ajustes en los procedimientos según sea necesario y se completa un informe detallado del incidente para fines regulatorios y referencia futura. Esta fase cierra el ciclo de gestión de incidentes, pero también alimenta la fase de planificación y preparación para futuros eventos.


Security Project Managers
Red-Blue Team
Business Response Teams
Plan
Resist
Prepare
Filter
Assess
Protect
Security Tasks
Resolve
Collect
Escalate
Analyze
Respond
Detect
IT and Security Teams
Technical Assistance Group
Threat Cell
Incident Handlers
Event Analysts
Incident Analysts
Incident Response Center


';--have i been pwned?