Análisis del Caso: Incidente de CrowdStrike 2024

Integrantes: Erick Alpusig, Claudio Peñaherrera, Saul Tualombo

1. Resumen del Caso

- El incidente de CrowdStrike de 2024 ocurrió el 19 de julio de 2024, cuando una actualización defectuosa del software de seguridad Falcon, distribuida a sistemas Windows, provocó fallos masivos en millones de computadoras a nivel global. Esta actualización, destinada a mejorar la detección de amenazas mediante la recopilación de telemetría, generó errores de 'pantalla azul de la muerte' (BSOD) en aproximadamente 8.5 millones de dispositivos, afectando sectores como aerolíneas, bancos, hospitales y aeropuertos en países como Estados Unidos, Australia y el Reino Unido. El problema se debió a un archivo de configuración (canal 291) con un formato de datos antiguo que causó una lectura de memoria fuera de límites en el sensor Falcon versión 7.11 o superior, llevando a bucles de reinicio o modo de recuperación.

Fuente principal: Informe preliminar posterior al incidente (PIR) de CrowdStrike
https://www.crowdstrike.com/wp-content/uploads/2024/07/CrowdStrike-PIR-Executive-Summary_es-ES.pdf

---

2. Clasificación del Mantenimiento

- Este mantenimiento fue principalmente correctivo, ya que se trató de una corrección urgente de un defecto en el software existente que provocó fallos catastróficos en producción, como el BSOD en sistemas operativos Windows. Sin embargo, también incorporó elementos preventivos, puesto que la actualización buscaba anticiparse a nuevas técnicas de amenazas mediante mejoras en la detección, aunque falló en las validaciones previas.
- La justificación radica en que el incidente surgió de un error no detectado en el contenido de respuesta rápida, requiriendo una reversión inmediata para mitigar daños, lo que alineó con la definición de mantenimiento correctivo al restaurar la funcionalidad básica; el aspecto preventivo se evidencia en las pruebas de telemetría planeadas para evitar vulnerabilidades futuras, pero la falta de pruebas exhaustivas lo convirtió en una mezcla reactiva-preactiva.

---

3. Procesos SCM Involucrados

- Los procesos de Software Configuration Management (SCM) fueron cruciales para contener el incidente, permitiendo una reversión rápida de la actualización defectuosa a las 05:27 UTC del 19 de julio, lo que evitó que más sistemas en línea

se vieran afectados. En cuanto al Control de Versiones, es probable que el equipo de CrowdStrike utilizara herramientas como Git para crear una rama de emergencia (hotfix branch) dedicada al análisis del archivo de canal defectuoso, aislando los cambios y permitiendo pruebas rápidas antes de fusionar la corrección a la rama principal.

- Para la Gestión de Cambios, se implementó un proceso de aprobación urgente y escalonado post-incidente, notificando a clientes y coordinando con proveedores como Microsoft para herramientas de recuperación, aunque inicialmente careció de validaciones independientes que hubieran detectado el error en el formato de matriz de 20 campos en lugar de 21 esperados.

---

4. Impacto en el Ciclo de Vida (SDLC)

- El incidente afectó principalmente las fases de Pruebas y Despliegue del SDLC, ya que las pruebas unitarias y manuales solo cubrieron la 'ruta feliz' sin validar formatos de datos antiguos ni regresiones, lo que permitió que el error pasara a producción sin detección. Hubo una re-planificación de emergencia en la fase de Mantenimiento, con despliegues manuales en modo seguro para eliminar archivos .sys problemáticos en cada dispositivo, saltando pruebas automatizadas completas y requiriendo intervención física en millones de hosts, lo que extendió la recuperación por días.
- Además, el Desarrollo se vio impactado retroactivamente al necesitar fortalecer controles de errores en el sensor Falcon, mientras que el despliegue inicial sin implementación escalonada (canary releases) amplificó el alcance global, afectando la fase de Implementación al no proporcionar opciones para retrasar actualizaciones en infraestructuras críticas.

---

5. Beneficios del SCM

- Un buen SCM permitió la trazabilidad completa del problema, identificando rápidamente el archivo de canal 291 como culpable y facilitando la reversión sin propagar daños adicionales a sistemas Mac o Linux, lo que redujo el tiempo de inactividad global. Esto también habilitó auditorías post-mortem detalladas, como el PIR de CrowdStrike, que reveló fallos en validaciones Regex y pruebas de estrés, permitiendo mejoras como revisiones de código por terceros y estrategias de despliegue escalonado para futuras actualizaciones.
- En última instancia, la estabilidad proporcionada por el SCM evitó un colapso total, mitigando pérdidas estimadas en 5.4 mil millones de dólares y restaurando operaciones en sectores críticos mediante copias de seguridad y herramientas de recuperación compartidas con clientes.