Análisis del informe del incidente

Resumen	La organización experimentó un ataque DDoS, que comprometió la red interna durante dos horas hasta que se resolvió. Durante el ataque, los servicios de red de tu organización dejaron de responder repentinamente debido a una avalancha de paquetes ICMP entrantes. El tráfico normal de la red interna no pudo acceder a ningún recurso de la red. El equipo de gestión de incidentes respondió bloqueando los paquetes ICMP entrantes, deteniendo todos los servicios de red no críticos fuera de línea y restableciendo los servicios de red críticos.
Identificar	La red dejo de funcionar al recibir un ataque DDoS, específicamente un ataque de inundación ICMP, por parte de un agente de amenaza. Todos los servicios críticos de la red ser vieron afectados.
Proteger	El equipo de seguridad de red implementó una nueva regla de firewall para limitar la tasa de paquetes ICMP entrantes y un sistema IDS/IPS para filtrar parte del tráfico ICMP basándose en características sospechosas.
Detectar	El equipo de seguridad de red implementó la verificación de la dirección IP de origen en el firewall para comprobar si hay direcciones IP falsas en los paquetes ICMP entrantes y un software de monitoreo de red para detectar patrones de tráfico anómalos.
Responder	Para futuros incidentes de ciberseguridad, se aislará los sistemas que se vean comprometidos para evitar detener todos los servicios de red. Si hubiera estragos se restaurarían sistemas y/o servicios que se vieran afectados. Consecuentemente se deben analizar los registros de red para ver las causas. Por último, se reportarían los sucesos a las autoridades correspondientes.

Recuperar	Los servicios de red se deben restaurar cuanto antes, tras aplicar las medias de protección y detección por parte del equipo de seguridad se podrían evitar ataques DDoS. Los servicios de red no críticos deben detenerse para reducir el tráfico de red interno y restaurar los servicios de red críticos. Por último, tras el bloqueo de los paquetes ICMP entrantes se debería restaurar los servicios no críticos.

Reflexiones/Notas: Este ataque DDoS destaca la importancia de contar con protocolos de respuesta estructurados y personal capacitado para gestionar crisis de ciberseguridad en tiempo real.