Incident report analysis

Summary	Mi organización ha sufrido un ataque DDoS, que ha puesto en peligro la red interna durante dos horas hasta que se ha resuelto
Identify	Ataque DDos, avalancha de paquetes ICMP entrantes.
Protect	El equipo de gestión de incidentes respondió bloqueando los paquetes ICMP entrantes, deteniendo todos los servicios de red no críticos de línea y restableciendo los servicios de red críticos
Detect	Descubrieron que un actor malicioso había enviado una avalancha de pings ICMP a la red de la empresa a través de un cortafuegos no configurado, esto permitió al agresor abrumar la red de la empresa mediante un ataque de denegación de servicio.
Respond	Se implementaron una nueva regla de cortafuegos para limitar la tasa de paquetes ICMP entrantes, verificación de la dirección IP de origen en el cortafuegos para comprobar si hay direcciones IP falsificadas en los paquetes ICMP entrantes, y por último, un sistema IDS/IPS para filtrar parte del tráfico ICMP basado en características sospechosas.
Recover	Para recuperarse de un ataque DDoS por inundación de ICMP, es necesario restablecer el acceso a los servicios de red a un estado de funcionamiento normal. En el futuro, los ataques externos de inundación de ICMP se podrán bloquear en el cortafuegos. A continuación, se deben detener todos los servicios de red no críticos para reducir el tráfico interno de la red. A continuación, se deben restablecer primero los servicios de red críticos. Por último, una vez que la inundación de paquetes ICMP haya expirado, todos los sistemas y servicios de red no críticos se pueden volver a conectar.