Analyse Incident du rapport

Résumé	L'entreprise a subi un incident de sécurité entraînant l'arrêt brutal de tous ses services réseau. L'équipe de cybersécurité a identifié la cause de cette interruption : une attaque par déni de service distribué (DDoS) provoquée par un afflux massif de paquets ICMP. En réponse, l'équipe a bloqué l'attaque et mis hors service tous les services réseau non critiques, permettant ainsi le rétablissement des services essentiels.
Identifier	Attaque par déni de service (DoS) / Inondation ICMP
Protéger	Nouvelle règle de pare-feu pour limiter le taux des paquets ICMP. Vérification des adresses IP sources pour détecter l'usurpation d'IP (spoofing).
Détecter	Mise en place d'un logiciel de surveillance pour surveiller les trafic anormaux. Mise en place d'un système IDS.
Répondre	Utilisation du plan de réponse pour contenir l'inondation et neutraliser la source via le filtrage.
Rétablir	Restauration du fonctionnement normal des systèmes affectés après s'être assuré que le trafic malveillant est bloqué.

Réflexions/Notes :