Scénario

Vous êtes analyste cybersécurité et vous travaillez pour une entreprise multimédia qui propose aux petites entreprises des services de conception de sites web, de graphisme et des solutions de marketing pour les réseaux sociaux. Votre entreprise a récemment été victime d'une attaque DDoS qui a compromis le réseau interne pendant deux heures, jusqu'à ce que la situation soit résolue.

Au cours de l'attaque, les services réseau de votre entreprise ont soudainement cessé de répondre en raison d'un afflux de paquets ICMP. Le trafic normal du réseau interne ne pouvait accéder à aucune ressource du réseau. L'équipe de gestion des incidents a réagi en bloquant les paquets ICMP entrants, en arrêtant tous les services réseau non critiques et en rétablissant les services réseau critiques.

L'équipe de cybersécurité de l'entreprise a ensuite enquêté sur l'événement de sécurité. Elle a découvert qu'un acteur malveillant avait envoyé un flot de pings ICMP dans le réseau de l'entreprise par le biais d'un pare-feu non configuré. Cette vulnérabilité a permis à un attaquant malveillant de submerger le réseau de l'entreprise par le biais d'une attaque par déni de service distribué (DDoS).

Pour faire face à cet événement de sécurité, l'équipe chargée de la sécurité réseau a mis en œuvre :

- Une nouvelle règle de pare-feu pour limiter le taux de paquets ICMP entrants
- Une vérification de l'adresse IP source sur le pare-feu pour détecter les adresses IP usurpées dans les paquets ICMP entrants
- Un logiciel de surveillance du réseau pour détecter les tendances de trafic anormales
- Un système IDS/IPS pour filtrer une partie du trafic ICMP sur la base de caractéristiques suspectes

En tant qu'analyste cybersécurité, vous devez utiliser cet événement de sécurité pour créer un plan visant à améliorer la sécurité réseau de votre entreprise, conformément au Cyber Security Framework de l'Institut national des normes et de la technologie (NIST CSF). Vous utiliserez le CSF pour vous aider à réaliser les différentes étapes de l'analyse de cet incident de cybersécurité et à intégrer votre analyse dans une stratégie de sécurité générale :

- **Identifier** les risques de sécurité en établissant des audits réguliers des réseaux, systèmes, équipements et privilèges d'accès internes afin d'identifier les potentielles lacunes en matière de sécurité.
- **Protéger** les ressources internes grâce à la mise en œuvre de politiques, de procédures, de formations et d'outils qui contribuent à atténuer les menaces en matière de cybersécurité.
- **Détecter** les incidents de sécurité potentiels et améliorer les capacités de surveillance afin d'accroître la vitesse et l'efficacité des détections.
- **Répondre** pour contenir, neutraliser et analyser les incidents de sécurité, et pour mettre en œuvre des améliorations des processus de sécurité.
- **Récupérer** le fonctionnement normal des systèmes affectés et restaurer les données et/ou les ressources des systèmes affectés par un incident.