(Les plans d'action pour chaque alerte sont détaillés dans les rapports correspondants, et le regroupement des alertes est présenté dans ce PDF en raison des problèmes de connexions incessants sur la plateforme Kali.)

Activités Malveillantes Ciblant les Comptes Privilégiés et le Contrôleur de Domaine FR-SRV-DC04

Alertes analysées :

- Multiple Authentication Failures Followed by Success
- Privileged User Created
- Potential Dump Memory

2. Indices similaires identifiés :

1. **Adresses IP communes :**
    - **10.11.2.12 (FR-SRV-DC04) :**
        - Mentionnée dans les trois alertes comme un serveur impliqué.
        - Utilisée dans "Multiple Authentication Failures Followed by Success" pour des tentatives d'authentification suspectes.
        - Identifiée dans "Privileged User Created" comme faisant partie des serveurs de domaine affectés.
        - Impliquée dans "Potential Dump Memory" comme un serveur critique lié aux activités suspectes.
2. **Serveur critique commun :**
    - **FR-SRV-DC04 (Contrôleur de domaine) :**
        - Présent dans les trois rapports, impliquant des activités suspectes liées à la gestion des comptes et des privilèges.
        - Décrit comme une cible ou un point central pour des manipulations dans les trois cas.
3. **Risque lié aux utilisateurs privilégiés :**
    - **Les trois alertes signalent des actions impliquant des utilisateurs ou des comptes à hauts privilèges :**
        - Compte Carter dans "Multiple Authentication Failures Followed by Success".
        - Compte Local Service (NT AUTHORITY) et création suspecte de comptes dans "Privileged User Created".
        - Compte Vagrant dans "Potential Dump Memory", impliqué dans des manipulations de comptes.

4. **Activité suspecte autour des ressources critiques :**
    - **Modifications ou accès à des ressources sensibles dans les trois alertes :**
        - Authentifications bruteforce dans "Multiple Authentication Failures Followed by Success".
        - Tentatives d'accès avec le privilège SeSecurityPrivilege dans "Privileged User Created".
        - Tentative de dump mémoire de lsass.exe pour extraire des informations sensibles dans "Potential Dump Memory".

Résumé du regroupement :

Ces trois alertes partagent des adresses IP communes, notamment 10.11.2.12 (FR-SRV-DC04), qui est un serveur clé dans toutes les activités suspectes. Elles mettent également en évidence des activités suspectes autour de comptes utilisateurs privilégiés (Carter, Local Service, Vagrant) et des ressources critiques comme lsass.exe.

Les incidents signalent une menace coordonnée ciblant les contrôleurs de domaine, les utilisateurs privilégiés et les ressources système sensibles. Ce regroupement est pertinent pour investiguer une compromission potentielle systémique au sein de l'infrastructure du domaine.