

PLANS D'ACTION

Compromission du domaine d'Echelon

CELLULE SOC

Septembre 2024

Version	Date	Propriétaire	Rédacteur / Autorité
1.0	30/09/2024	Cellule SOC	Nicolas Clerbout
Finale			

Table des matières

Liste des figures	. 3
1. Remédiations pour l'extraction de données	. 4
2. Remédiations pour la compromission initiale	. 5
3. Remédiations pour l'escalade de privilèges	. 6
4. Remédiations pour les actions de persistance	. 7
5. Synthèse des actions à mettre en œuvre	. 8
Tâches du case restant à effectuer :	. 8

Liste des figures

Section 1:	
Figure 1 - Réaction immédiate : règle SNORT	4
Figure 2 - Actions à réaliser suite à la fuite de données	4
Section 2:	
Figure 3 - Plan d'action contre la compromission initiale	5
Section 3:	
Figure 4 - Plan d'action contre l'escalade de privilèges	6
Section 4:	
Figure 5 - Plan d'action face aux actions de persistance	7
Section 5:	
Figure 6 - Tâches à réaliser (TheHive)	8

1. Remédiations pour l'extraction de données

A Echelon/Analyst

Mise en place d'une règle de blocage sur SNORT

block tcp \$HOME_NET any -> 103.251.167.20 53 (msg:"trafic DNS vers IP malveillante"; sid:10001; rev:1;)

Figure 1 - Réaction immédiate : règle SNORT

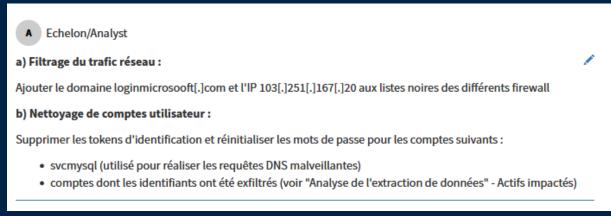


Figure 2 - Actions à réaliser suite à la fuite de données

2. Remédiations pour la compromission initiale

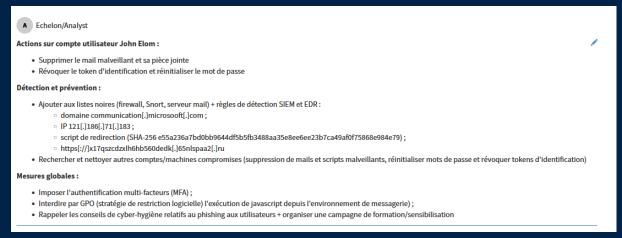


Figure 3 - Plan d'action contre la compromission initiale

3. Remédiations pour l'escalade de privilèges



A Echelon/Analyst

Nettoyage de comptes

Révoquer les tokens d'identification et réinitialiser les mots de passe des comptes svcmysql et john.elom (cf. remédiations concernant la compromission initiale et l'extraction de données)

Sécuriser les mots de passe

- · Supprimer les fichiers contenant des mots de passe
- · Interdire le stockage des mots de passe dans des fichiers en clair

Sécuriser les comptes de service

Interdire les connexions interactives aux comptes de service

Figure 4 - Plan d'action contre l'escalade de privilèges

4. Remédiations pour les actions de persistance

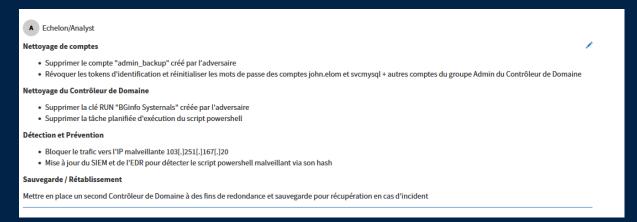


Figure 5 - Plan d'action face aux actions de persistance

5. Synthèse des actions à mettre en œuvre

Tâches du case restant à effectuer :



Figure 6 - Tâches à réaliser (TheHive)