Processus de gestion des alertes de sécurité

2 types d'alertes sont à différencier :

1. Les alertes de sécurité qui sont patchées dans le cycle de vie normal et ne nécessitent pas la fermeture du service de manière urgente et non programmée de service
2. Les alertes critiques qui nécessitent une action rapide, la fermeture d'un service ou celles qui sont soumises à une injonction du ministère.

Dans le premier cas :

Le service concerné intègre à son planning l'application des correctifs de sécurité en y associant les services qui sont impactés.

Dans le second cas :

Dès que l'information est connue des RSSI (il est possible que l'alerte ne vienne pas des RSSI, mais elle doit impérativement leur être remontée), ceux-ci créeront un canal spécifique sur le chat pour cette alerte. Y seront inclus systématiquement :

- La direction
- Le responsable du service concerné (qui pourra ajouter les collaborateurs qu'il estime nécessaires sur le sujet).
- Le DPO si nécessaire

Ce canal permettra :

- D'exposer la problématique et les impacts éventuels de l'alerte
- D'informer sur les différentes phases de la remédiation
- D'informer sur la réception des correctifs et leur mise en application ainsi que sur les résultats obtenus après application du correctif.

Le service concerné par la mise à jour à réaliser, créera un ticket de type RFC pour assurer le suivi de/des mise(s) à jour nécessaire(s).

Le Directeur de la DGDNUM assurera la communication auprès de la direction métier.

Si un service a été fermé pour des raisons de sécurité, la décision de rouvrir le service ne pourra être autorisée que par la direction, en concertation avec les RSSI, le DPO si nécessaire et les équipes métier.

Le canal sur le chat, restera ouvert jusqu'à la résolution du problème et sera supprimé après le retour à une situation normale.