Archiver et protéger les données et les preuves numériques

Akram, Thomas et Bastien

1-Cibeco dispose des moyens techniques nécessaires pour appliquer les recommandations en matière de collecte des preuves numériques :

Les journaux systèmes sont centralisés pour éviter les incohérences.
Deux serveurs de collecte en grappe redondée préviennent les pannes.
Un serveur de temps assure un horodatage précis.
La collecte se fait via un VLAN dédié, renforçant la sécurité.
Une bande passante garantie assure un transit efficace des journaux systèmes.
La consultation des journaux est simplifiée grâce à une interface web conviviale.

2-La liste des événements collectés par les journaux systèmes de Cibeco est fournie dans le document 2, incluant l'authentification, l'accès aux ressources, et les activités des programmes et systèmes. Le document 3 présente les catégories d'événements pouvant déclencher des alertes, allant des informations aux alertes liées à des actes malveillants comme les tentatives de force brute. Cette liste est en conformité avec les recommandations de l'ANSSI garantissant une couverture complète des événements pertinents pour la traçabilité.

3-La conservation durable des preuves collectées par Cibeco est assurée par l'utilisation de bandes magnétiques, éliminant ainsi le recours à des clés USB moins fiables. En prévention, les enregistrements sont effectués sur des disques durs configurés en RAID 5, garantissant une tolérance de panne. Avec l'utilisation de 10 bandes de 10 To chacune, et une copie en double, les capacités de stockage sont amplement suffisantes pour éviter tout problème lié à des capacités insuffisantes.

4-Le lieu de conservation des preuves numériques chez Cibeco est équipé pour faire face à des sinistres importants. La baie de stockage inclut un système anti-incendie, une copie en double, et une climatisation pour les périodes de canicule. Ces mesures, renforcées par un stockage d'archives dans un second bâtiment, attestent de la préparation du lieu face à d'éventuels sinistres.

Pour la synthèse, on l’a fait avec Gamma.app.