|  |  |  |
| --- | --- | --- |
| logo | Journaux des événements | 1078 |

Responsable :

Mis à jour :

Les journaux servent à ce que les informations relatives aux activités liées à la sécurité soient reconnues, enregistrées, stockées et analysées et donc à répondre aux questions suivantes :

* quelle activité a été exercée
* qui a effectué l'activité
* sur quel système l'activité a-t-elle été effectuée
* quand l'activité a-t-elle été effectuée
* à quelle fréquence cette activité a-t-elle été réalisée
* avec quel outil l'activité a-t-elle été effectuée
* quel était le statut de l'activité (succès ou échec)

Les journaux sont de type :

* du proxy http sortant
* du pare-feu
* du système
* d’une application

Un journal est créé chaque fois que l'une des activités suivantes est effectuée par le système :

* créer, lire, mettre à jour ou supprimer des informations confidentielles, y compris l’authentification et les mots de passe
* créer, mettre à jour ou supprimer d’autres informations
* établir une connexion au réseau
* accepter une connexion réseau
* déconnecter l’utilisateur
* accorder, modifier ou révoquer les droits d'accès
* modifier les niveaux de privilèges
* modifier les règles de pare-feu et des mots de passe des utilisateurs
* modifier la configuration du système, du réseau ou des services, y compris l'installation de correctifs et mises à jour de logiciels installés
* démarrer, arrêter ou redémarrer le processus d'application
* abandonner ou finir anormalement le processus d'application suite à :
  + l'épuisement des ressources
  + l’atteinte d’une limite de ressources comme :
    - le CPU
    - la mémoire
    - le réseau les connexions
    - la bande passante du réseau
    - l'espace disque
  + la défaillance du réseau des services
  + une défaillance matérielle :
    - la détection d'activités suspectes
    - une détection d'intrusion du système :
      * + de prévention
        + anti-virus
        + anti-spyware

Les journaux nous permettent :

* de contrôler le volume d’utilisation des ressources
* de détecter des anomalies ou défaillances :
  + accidentelle ou volontaire
  + d’origine technique ou humaine
* de vérifier que les politiques de sécurité de l’information sont correctement appliquées
* de détecter :
  + toute violation de la loi
  + tout abus d’utilisation des moyens informatiques
* de fournir des preuves pour mener les enquêtes en cas d’incident de sécurité

La durée maximum de conservation des journaux est de 12 mois, sauf disposition contraire imposée par un texte de loi spécifique.

Exemple d’un journal (d’un pare-feu) :

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| N° | IP source et destination | Date et heure | Ports source et destination | Action entreprise par le pare-feu (relayé, bloqué, ignoré) | Remarque |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |