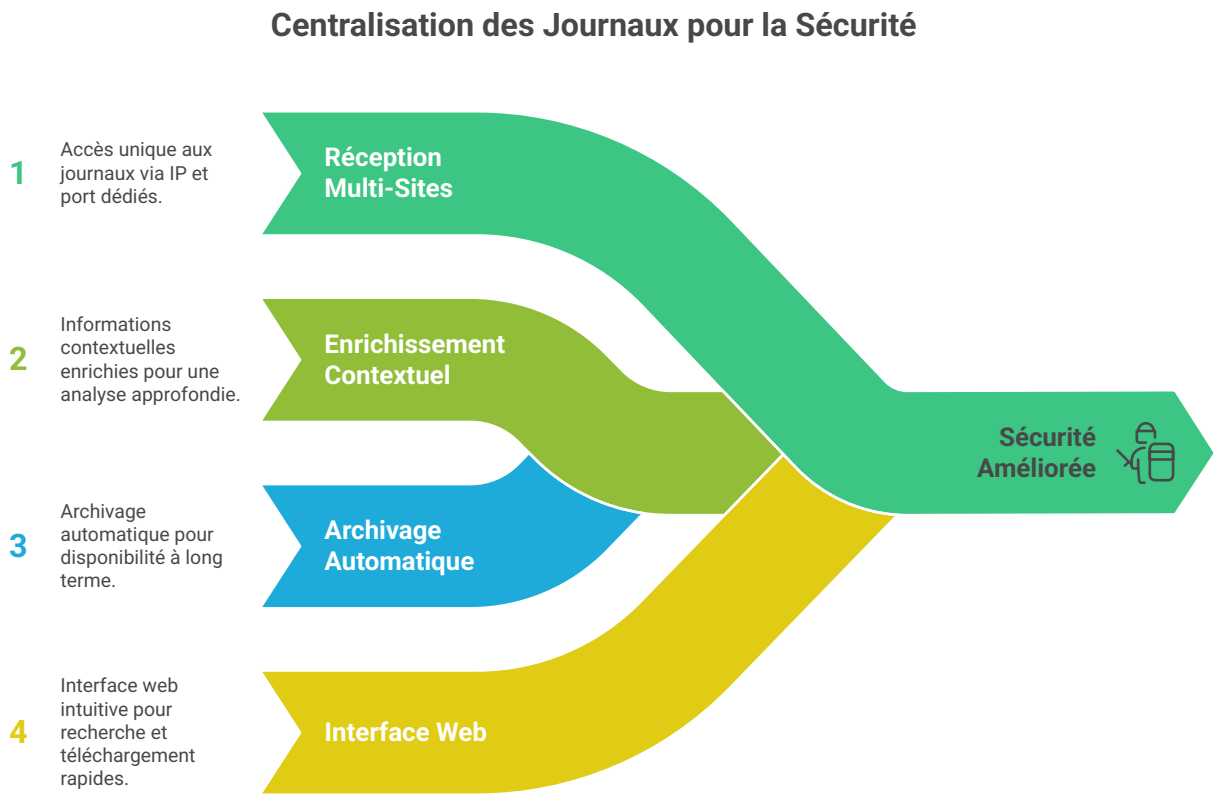
PAPIER BLANC

LOGCENTRAL

Logs et sécurité : mieux enquêter et réagir grâce à la centralisation



Résumé exécutif

Les journaux systèmes (syslogs) sont une source essentielle d'informations lors d'un incident de sécurité : tentative d'accès non autorisé, panne d'un équipement critique, configuration anormale… Mais lorsque ces logs sont dispersés sur différents sites ou équipements, les retrouver et les analyser rapidement devient un défi.

LogCentral centralise et archive les logs pour faciliter les investigations et réduire le temps nécessaire à réagir.

Logs et sécurité : mieux enquêter et réagir grâce à la centralisation

Contexte & enjeux

Les logs peuvent contenir des indices clés sur :

- Des connexions suspectes.
- Des modifications de configuration.
- Des comportements inhabituels d'un service ou d'un équipement.

- Dispersés sur plusieurs sites, ces logs :
  - Peuvent être **difficiles d'accès** au moment critique.
  - Risquent d'être **écrasés** ou perdus par rotation locale.
  - Allongent le temps d'investigation.

Problématique

Comment rendre les logs disponibles immédiatement et de manière centralisée pour soutenir les équipes de sécurité dans leurs investigations ?

Sans centralisation :

- Nécessité de **contacter plusieurs sites** pour récupérer les journaux.
- Risque de recevoir des fichiers incomplets ou déjà écrasés.
- Perte de temps lors des premières heures critiques d'un incident.

Solution : l'apport de LogCentral

LogCentral offre un point d'accès unique à tous vos journaux, quelle que soit leur origine, grâce à :

- **Réception multi-sites** via IP et port dédiés.
- **Enrichissement contextuel** (fournisseur d'accès, pays, parfois ville).
- **Archivage automatique** pour garantir la disponibilité même plusieurs mois après l'événement.
- **Interface web** avec recherche rapide et téléchargement direct des journaux pertinents.

Bénéfices pour la sécurité

- **Réactivité accrue** : accès immédiat aux journaux, même pour un site distant.
- **Meilleure exhaustivité** : logs conservés intacts selon la politique de rétention.
- **Traçabilité renforcée** : consultation possible de l'historique exact des événements.
- **Moins de dépendance** vis-à-vis des équipes locales pour extraire les données.

Cas d'usage concret

Un groupe de distribution constate un comportement anormal sur un serveur applicatif d'une succursale.

Grâce à LogCentral :

- Les journaux réseau et système de la succursale sont consultés **immédiatement** depuis le siège.
- L'équipe de sécurité identifie une configuration erronée ayant permis des connexions répétées non autorisées.
- Les mesures correctives sont appliquées le jour même, sans attendre l'envoi manuel des logs.

Conclusion

En centralisant les journaux, **LogCentral** permet aux équipes de sécurité et d'exploitation d'accéder rapidement à des informations fiables et complètes, indispensables pour réagir efficacement à un incident.

→ Contactez-nous pour découvrir comment LogCentral peut simplifier la gestion et l'accès à vos logs, quelle que soit la taille de votre réseau.