Journalisation et SIEM

La **journalisation** informatique, également connue sous le nom de “**logging**”, est le processus d'enregistrement des **événements** et des activités qui se produisent sur un serveur. C'est un outil essentiel pour **surveiller**, dépanner et auditer les systèmes informatiques.

Un **log**, ou **journal**, est un **fichier** texte ou autre qui enregistre **chronologiquement** (**horodaté**) les événements et les activités qui se produisent sur un système informatique, une **application** ou un **service**.

Un **SIEM** (Security Information and Event Management) est un système de **gestion** de la sécurité des informations et des événements. C'est un outil **logiciel** qui **collecte**, **analyse** et **corrèle** les données de sécurité provenant de diverses sources au sein d'une organisation, telles que les journaux d'événements, les pare-feux, les systèmes de détection d'intrusion, les serveurs, les applications, etc.

Les produits les plus connues étant **Elastic Search** combiné à Kibana pour le monde **Open-Source** et **Splunk** une compagnie de **CISCO**.

Articles associés

- Les outils de journalisation
- Installation de ELK Stack : Elasticsearch, Kibana, Beats et Logstash