EVENT LOG MANAGER

blësk network monitoring

OBJECTIF : Gérer efficacement le flux massif de données provenant de sources différentes

Les employés d'une entreprise se connectent à multiple reprise sur des équipements du réseau interne, soit à distance soit au bureau. Mais comment savoir si un employé de l'organisation s'est fait pirater son compte et que son ordinateur se connecte d'un pays étranger alors qu'il se trouve physiquement en face de votre bureau ?

BLËSK Event Log Manager (ELM) permet d'identifier rapidement des évènements suspicieux à partir des Syslogs qu'il reçoit. L'Event Log Manager est un outil flexible et puissant qui permet de stocker des milliards de données, de filtrer en faisant de la recherche intelligente et en créant des tableaux qui permettent de mieux visualiser les évènements journaux (Syslogs). ELM peut fournir plusieurs informations selon les besoins. Les administrateurs peuvent donc être informés immédiatement d'une violation de sécurité potentielle.

Grâce à des outils Open source tel qu'Elasticsearch, Logstash et Kibana, ELM vous permet :

BÉNÉFICES

- Création de tableaux de bord, tableaux, etc.
- Effectuer et combiner de nombreux types de recherches – structurées, non structurées, géo, métriques.
- Faire un « *zoom out* » pour explorer les tendances et les modèles de vos données.
- Ingérer des données de toutes les formes, tailles et sources.
- Analyser et transformer vos données rapidement.

BLËSK VOUS AIDE :

Il est difficile et inintéressant pour une équipe TI de vérifier tous les logs de chaque machine. Cependant, les Syslogs sont extrêmement importants lorsqu'un appareil se fait pirater ou éprouve des problèmes. La masse des Logs issue des différentes machines doit être classée de sorte que l'interprétation soit facile à faire afin de ne pas faire d'erreur en faisant une recherche manuelle dans les données.

BLËSK a des tableaux prédéfinis colorés et faciles d'interprétation que vous pouvez utiliser et améliorer dans le but de pouvoir trouver le problème recherché en utilisant sa fonction de Drill Down.

Lorsqu'on clique sur un problème particulier, les graphiques changent pour ne montrer que l'information que l'équipe TI recherche.