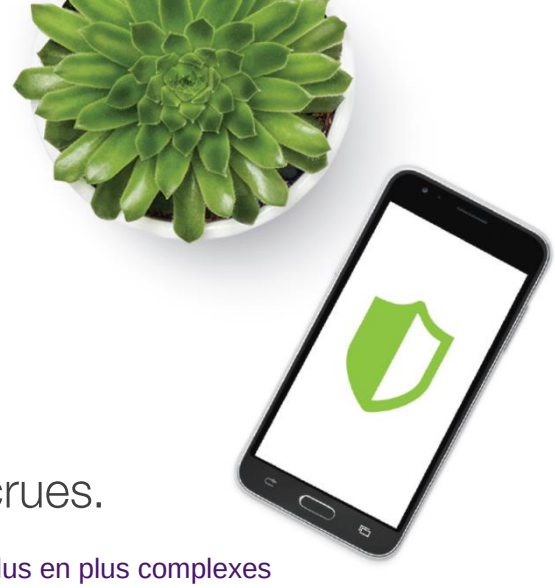


SIEM géré de TELUS

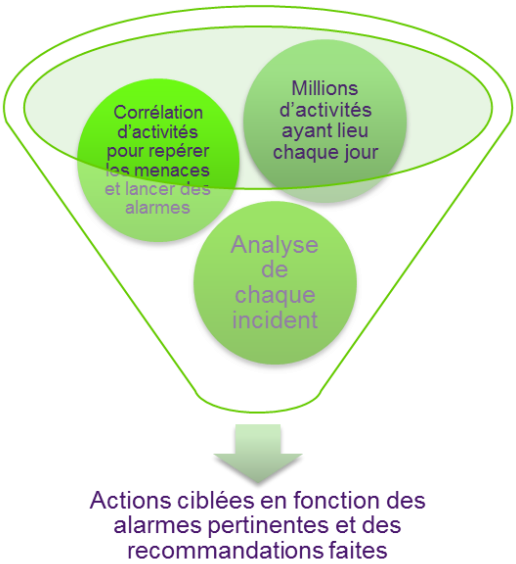
Pour une visibilité et une conformité accrues.

Les entreprises doivent protéger leurs réseaux des menaces de plus en plus complexes et difficiles à déceler, en plus de prouver qu'elles respectent la réglementation à cet égard. Or, face à la quantité phénoménale de données à prendre en compte pour y parvenir, la tâche s'apparente parfois à un obstacle infranchissable.

Un journal est un relevé des échanges de données entre les divers appareils d'un réseau. Il couvre toutes les opérations informatiques : des tentatives de connexion aux changements de configuration, en passant par les erreurs du système. Ces opérations sont repérées notamment par les routeurs, les serveurs et les applications du réseau, ainsi que par des solutions de sécurité comme des coupe-feu et des systèmes de prévention des intrusions.

Les journaux renferment des indices à propos des incidents de sécurité survenant sur le réseau. Cependant, comme ces incidents ne semblent pas interreliés de prime abord, les indices ne servent à rien tant que les données obtenues ne sont pas regroupées, corrélées, rationalisées et filtrées. Ce traitement est nécessaire pour déceler des menaces particulières, des comportements anormaux chez les utilisateurs ou d'autres interventions suspectes.

Dans de nombreux cas, les menaces à la sécurité laissent des traces tangibles (appelées parfois *Indicators of Compromise*). Cependant, les administrateurs de réseau et de TI doivent examiner et analyser une quantité de données variées si importante qu'ils n'ont pas le temps de passer les journaux au peigne fin et d'établir des liens entre les incidents importants. Par conséquent, bien des menaces à la sécurité passent inaperçues.



L'utilité d'un SIEM

Un système de gestion de l'information et des événements de sécurité (SIEM) optimise l'efficacité des activités de surveillance des menaces, en plus de les automatiser. Il recueille les données des systèmes de TI, fournisseurs et versions diverses confondus, et établit des corrélations entre elles. De plus, il permet au personnel des TI de se concentrer sur les menaces potentielles, les brèches de sécurité et les comportements suspects.

Défis liés aux SIEM traditionnels

Beaucoup d'organisations ayant consacré des sommes importantes aux technologies de SIEM ont réalisé trop tard qu'elles avaient investi dans une solution inefficace. De plus, dans bon nombre de cas, les SIEM ont été ignorés ou abandonnés pour diverses raisons :

- Dépense initiale en immobilisations trop élevée
- Investissement de temps et de ressources trop important concernant le réacheminement de l'information sur les incidents provenant de plusieurs sources. Déploiements plus lents que prévu
- Difficulté d'ajuster les alertes et les alarmes pour réduire le bruit et produire des conclusions pertinentes
- Aucun accès aux environnements infonuagiques publics ou privés
- Manque de personnel d'expérience pour gérer la solution

Pourquoi choisir le SIEM géré de TELUS?

TELUS propose des options de SIEM souples pour répondre à des besoins précis. Que vous choisissiez le service personnalisé sur les lieux ou la solution infonuagique hébergée au Canada, TELUS vous offre un niveau de visibilité suffisant pour détecter et prévenir les menaces potentielles et ainsi assurer la conformité réglementaire tout en évitant les longs déploiements et les défis associés aux technologies traditionnelles. Avec le SIEM géré de TELUS, vous profitez de nombreux avantages :

Journalisation, surveillance et réponse supérieures	▪ Grande visibilité dans une multitude de cas ▪ Surveillance de la journalisation et de l'infrastructure en tout temps et établissement de corrélations entre les journaux des Services de sécurité gérés de TELUS ▪ Avis transmis en temps réel par téléphone, par courriel ou dans des rapports en fonction de la gravité du problème
Surveillance évoluée des données	▪ Surveillance des alarmes ▪ Avis transmis en temps quasi réel au sujet des menaces à la sécurité et du triage ▪ Ajustements constants pour les divers cas d'utilisation ▪ Mesures à prendre fournies en réponse aux alertes ▪ Recommandations accompagnant les analyses et les alertes
Rapports ultrapersonnalisés dans le portail web des Services de sécurité gérés de TELUS	▪ Liste des principaux attaquants par hôte d'origine ▪ Relevé des ouvertures de session suspectes ▪ Activités de gestion de comptes ▪ Échecs des utilisateurs aux vérifications de conformité ▪ Activités liées aux nouveaux comptes ▪ Sommaire des activités des utilisateurs privilégiés
Modèles de service flexibles	▪ Sur les lieux ou dans le nuage ▪ Intégration aux ensembles de TELUS Sécurité améliorant les capacités d'analyse des journaux et la visibilité relative aux divers éléments
Soutien constant	▪ Réunions mensuelles pour faire des ajustements, des examens des interventions et des recommandations

L'équipe TELUS Sécurité a développé son expertise pendant les nombreuses années où elle a géré des solutions de SIEM non seulement pour des clients comme vous, mais aussi à l'interne. Profitez donc d'une surveillance constante de vos réseaux sans avoir à embaucher, à former et à maintenir en poste des experts en sécurité. De plus, le modèle de paiement de TELUS vous garantit des factures mensuelles prévisibles et vous évite de dépenser d'emblée des sommes importantes pour acheter et mettre en œuvre de l'équipement.

DÉCOUVREZ LES SOLUTIONS AU SERVICE DE VOTRE ENTREPRISE.

Apprenez-en davantage sur tout ce que le SIEM géré de TELUS peut faire pour vous. Communiquez avec votre directeur de comptes TELUS au 1-866-GO-TELUS ou visitez telus.com/SecuriteAffaires

TELUS | Affaires