

TGDetect

En un coup d'oeil

TGDetect est une solution de surveillance des événements de sécurité qui fournit des capacités d'alerte flexibles pour IBM i.

Doté d'un moteur de filtrage de règles entièrement personnalisable, TGDetect vous donne une vision rapide de l'activité du système dont vous avez besoin pour vous assurer que vous êtes protégé contre les failles de sécurité.

ADVANTAGES :

- Surveillance des principaux événements liés à la sécurité, notamment le journal historique, le journal de sécurité, les files d'attente de messages et les commandes sensibles
- Les événements critiques en matière de sécurité sont transmis au sommet de la hiérarchie
- Gain de temps – Plus besoin d'examiner d'innombrables enregistrements de données d'événements intégrés à TGSecurity Suite
- Facilité d'installation et de configuration
- Envoi d'alertes au courrier électronique, SIEM, MSGQ

Surveiller les événements de sécurité IBM i

PROBLÈME :

Il existe de **nombreuses sources de données sur les événements de sécurité** sur IBM i et il n'y a jamais assez de temps pour tout examiner.

SOLUTION:

TGDetect surveille de nombreuses sources de données d'événements de sécurité sur IBM i et **vous permet de contrôler la façon dont vous souhaitez être alerté au sujet de ces données**. QHST, les files de messages (y compris QSYSOPR), QAUDJRN et la surveillance des commandes sensibles sont tous couverts.

Alertes de sécurité en temps réel

PROBLÈME :

Les menaces à la sécurité sont réelles. Vous devez savoir qu'un problème se pose au moment où il se produit. Plus un problème passe inaperçu, plus il est difficile de le résoudre et d'en corriger ensuite les effets.

SOLUTION:

TGDetect vous alerte sur les événements de sécurité potentiellement critiques au moment où ils se produisent afin que vous puissiez y remédier rapidement. De plus, les alertes TGDetect vous aident à vous **prémunir contre d'éventuelles failles de sécurité** en vous signalant toute activité suspecte au moment où elle se produit, afin que vous puissiez prendre les mesures nécessaires.

Voir ce qui est important pour vous

PROBLÈME :

S'il y a un volume important d'événements système, il est difficile de distinguer les événements de sécurité critiques des utilisations acceptables.

SOLUTION :

TGDetect est incroyablement personnalisable, ce qui vous permet de filtrer les alertes en fonction de ce qui est important pour vous. Voyez des éléments tels que les tentatives de connexion qui ont échoué pour des utilisateurs puissants précis et les événements du journal en temps réel. Utilisez également les alertes de TGSecurity Suite pour les événements tels que les tentatives de connexion à distance, les changements de profil d'utilisateur douteux et les problèmes d'autorité de la bibliothèque de production.

Alertes de sécurité pour votre IBM i

La quantité de données liées à la sécurité sur votre IBM i peut souvent en rendre accablante la gestion. Les règles de conformité et les auditeurs ont de vastes exigences en matière de journalisation et de critères de rapport. Comment savoir sur quels événements de sécurité se concentrer?

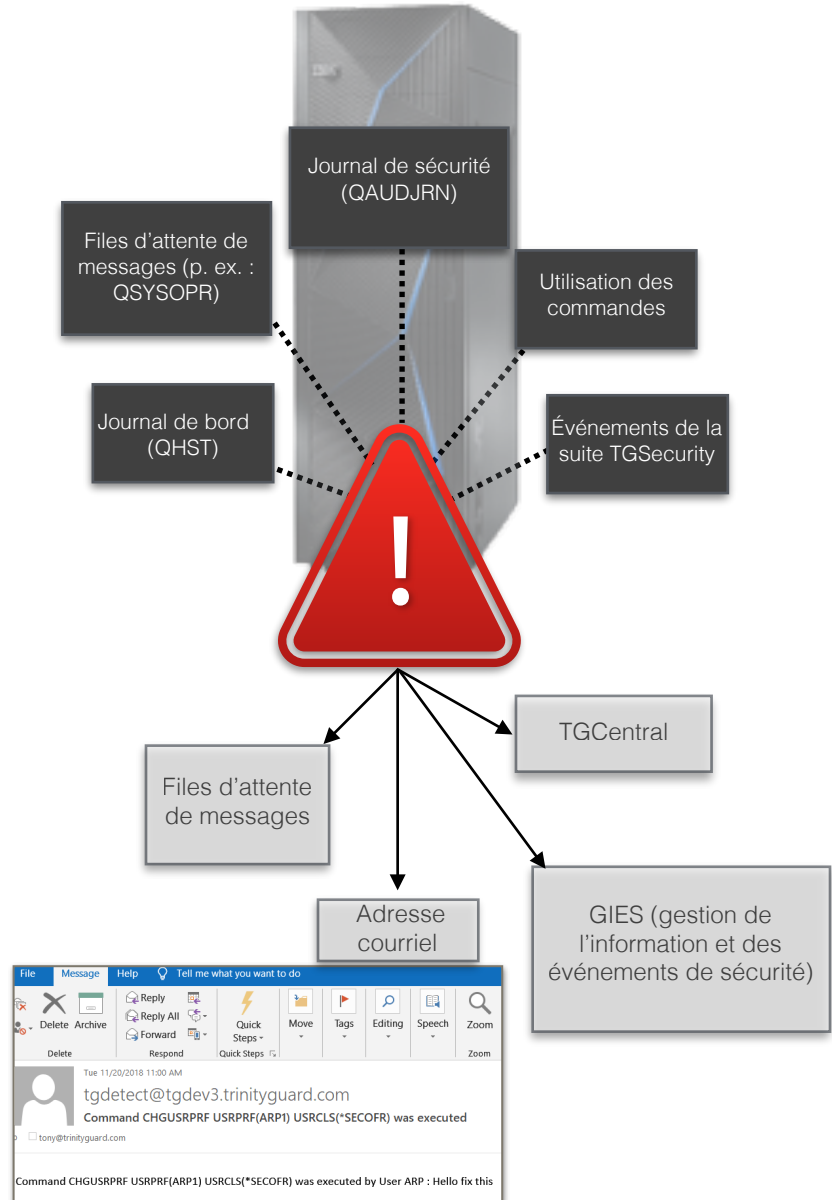
TGDetect vous avertit des événements de sécurité critiques au moment où ils se produisent, ce qui vous évite de passer des heures à examiner les données d'audit. Surveillance rigoureuse et ses capacités d'alerte flexibles, vous simplifie le processus de détermination des comportements suspects sur votre IBM i.

Avantages

- Alertes en temps réel en cas d'activité suspecte du système
- Gain de temps précieux dans l'examen des rapports d'audit
- Réception d'alertes pour les événements de sécurité critiques au moment où ils se produisent
- Facilité de signaler à un responsable les événements critiques en matière de sécurité
- Utilisation de votre solution GIES existante pour recevoir des alertes et des données de journal

Principales caractéristiques

- Alertes de sécurité IBM i envoyées à votre boîte de réception
- Surveillance des principales sources de renseignements sur la sécurité, notamment QHST, QAUDJRN, l'utilisation des commandes et les files d'attente des messages
- Intégré pour travailler efficacement avec TGAudit et TGSecure, et pour en recevoir des alertes
- Intégration avec n'importe quel GIES, y compris Splunk, Graylog, ArcSight, QRadar et ELK Stack



TG Security Suite est une solution de sécurité fiable pour les clients du monde entier.

Nous sommes heureux de discuter avec vous et de vous fournir un plan gratuit de mise en oeuvre de la sécurité IBM i. Visitez notre site Web ou appelez-nous. N'hésitez pas à communiquer avec nous!