

## L'audit de sécurité des réseaux Windows<sup>™</sup> avec WinReporter<sup>®</sup>

---

*Ce document présente comment les administrateurs réseaux et système peuvent tirer le meilleur parti de WinReporter<sup>®</sup>, édité par IS Decisions, pour réaliser les contrôles de sécurité suivants :*

- ▶ *Détection de vulnérabilités*
- ▶ *Détection d'intrusions système*
- ▶ *Recherche de preuves et analyses a posteriori*

## WinReporter® : un outil d'audit polyvalent

---

WinReporter® est un logiciel permettant d'obtenir une vision globale et exhaustive d'un réseau Windows™.

Il collecte l'information relative aux serveurs et aux postes de travail du réseau, et propose 58 rapports prédéfinis concernant par exemple les matériels, les mises à jour logicielles, la gestion des licences, ou les contrôles de sécurité, ... L'exploitation de ces rapports permet une administration rigoureuse des systèmes et du réseau.

WinReporter® va plus loin et offre la possibilité d'exploiter plus finement toute information collectée au moyen de requêtes SQL personnalisées.

Enfin, et bien que WinReporter® soit un outil d'administration généraliste, l'étendue de ses possibilités lui permet de réaliser de véritables audits de sécurité.

Ce document a pour objectif de mettre en évidence les fonctionnalités de WinReporter® permettant de mener à bien ces tâches bien particulières de sécurisation des systèmes et du réseau.

## Les principales menaces viennent de l'intérieur

---

Toutes les études disponibles prouvent que 80% des attaques réseaux sont perpétrées par des membres de l'entreprise ou de l'organisation victimes, agissant à partir d'un poste de travail interne.

Ceci est souvent la conséquence d'une politique de sécurité interne laxiste ou inadaptée, voire inexistante : droits excessifs attribués aux utilisateurs, systèmes non « patchés », absence d'audits de sécurité, etc.

Cette situation rend les réseaux vulnérables à tout type d'attaques, même les plus triviales.

Un dicton fameux dans la communauté des hackers qualifie d'ailleurs les réseaux d'entreprise de *“durs à la périphérie et perméables à l'intérieur”*.

Afin de ramener ces risques à un niveau acceptable, des mesures particulières doivent être prises pour sécuriser le réseau. WinReporter® peut aisément s'acquitter de ces tâches.

## La valeur ajoutée de WinReporter®

---

La totalité de l'information relative à la configuration des ordinateurs du réseau est collectée par WinReporter®. Il est donc possible de connaître dans les moindres détails la configuration matériel et logiciel de chaque ordinateur membre du réseau.

De plus, WinReporter® peut aussi rapatrier l'ensemble des données des journaux d'événements.

L'analyse des journaux d'événements est la base de la surveillance du système, et cette procédure doit être clairement formalisée et régulièrement testée.

Cependant la quantité d'information à traiter est telle que peu d'administrateurs consacrent le temps nécessaire à une inspection minutieuse des journaux d'événements.

Si Windows produit une quantité impressionnante d'informations sur le fonctionnement du système, il ne propose en revanche que très peu de moyens efficaces pour retrouver rapidement l'information critique :

- ▶ Les informations pertinentes sont éparpillées sur l'ensemble des machines du réseau.
- ▶ L'information disponible n'est pas suffisamment précise et explicite.
- ▶ En cas de perte d'intégrité d'une machine, l'information propre à cette machine est perdue.
- ▶ Les possibilités de filtrage d'événements et d'édition de rapports sont insuffisantes.

WinReporter® comble ces lacunes, en offrant un moyen rapide et efficace pour consigner la totalité de l'information dans une base de données centrale, l'exploiter et éditer des rapports pertinents, et immédiatement exploitables.

## WinReporter® et l'audit sécurité

La grande polyvalence de WinReporter® en fait un outil extrêmement puissant, capable de mener à bien les tâches suivantes :

- ▶ Détection de vulnérabilités
- ▶ Détection d'intrusions système
- ▶ Recherche de preuves

## Gestion des vulnérabilités avec WinReporter®

La détection de vulnérabilités est le pilier central de la gestion du risque informatique.

L'administrateur doit évaluer de manière fiable et exhaustive les vulnérabilités de son réseau afin de les ramener à un niveau acceptable, ce qui est en général passablement complexe.

Partant du principe qu'un attaquant exploitera le maillon le plus faible dans la chaîne de la sécurité, l'administrateur doit en effet considérer toutes les failles possibles, matérielles et logicielles, pouvant mettre en péril ses systèmes.

L'une des fonctionnalités cruciales de WinReporter® est qu'il récupère toutes les données de configuration des systèmes.

Correctement interprétée, cette information permet ainsi de découvrir les failles exposant le système. Autrement dit, WinReporter® donne une opportunité unique à l'administrateur de prendre les mesures nécessaires avant qu'un attaquant ne puisse exploiter les vulnérabilités de son réseau.

WinReporter® donne accès à toute l'information sur la configuration des systèmes, en particulier dans les domaines suivants :

- ▶ Mises à jour manquantes : Service Packs et hotfixes installés  
**Comment procéder** : Reporter > Rapports > Windows > Versions & mise à jour > Versions & mise à jour de Windows
- ▶ Logiciels suspects : scanners, outils de chiffrement, logiciels d'échange de fichiers  
**Comment procéder** : Reporter > Rapports > Logiciel > Politique Logicielle
- ▶ Comptes utilisateurs ou groupes suspects  
**Comment procéder** : Reporter > Rapports > Windows > Utilisateurs et groupes
- ▶ Reporter > Rapports > Windows > Analyse des comptes locaux
- ▶ Reporter > Rapports > Windows > Analyse des administrateurs locaux
- ▶ Découverte de périphériques non autorisés : modems, NIC, cartes sans fils, lecteurs de disquette  
**Comment procéder** : Reporter > Périphériques > Périphériques > carte réseau | modem | lecteur de disquette
- ▶ Répertoires partagés sans contrôle  
**Comment procéder** : Reporter > Rapports > Windows > Analyse des partages
- ▶ Reporter > Rapports > Windows > Permissions des partages
- ▶ Partitions de type FAT, pas de contrôle d'accès  
**Comment procéder** : Reporter > Rapports > Général > Rapport Global > Partitions disques
- ▶ Services atypiques et/ou dangereux  
**Comment procéder** : Reporter > Rapports > Windows > Analyse des services

WinReporter® permet aussi de contrôler le nombre de licences installées, et la présence de logiciels posant des problèmes potentiels de respect du copyright présents sur le réseau :

- ▶ Nombre de logiciels installés  
**Comment procéder :** Reporter > Rapports > Logiciel > Statistiques d'installation
- ▶ Logiciels d'échange de fichiers abusant des ressources réseau et important des fichiers illicites  
**Comment procéder :** Reporter > Rapports > Logiciel > Politique Logicielle

Ces quelques exemples montrent bien que WinReporter® a été conçu pour offrir une grande souplesse d'utilisation afin de répondre au mieux à tous types d'interrogations.

## Détection d'intrusion système avec WinReporter®

Dans un système distribué, les journaux d'événements sont répartis sur l'ensemble des ordinateurs du réseau, ce qui rend leur analyse difficile et laborieuse.

WinReporter® comble également cette lacune, et tire le meilleur parti du système de journalisation d'événements de Windows™, en permettant d'implémenter une efficace méthode de détection d'intrusion système (HIDS).

Il est nécessaire de rappeler qu'un firewall ne constitue que la première ligne de défense d'un réseau, et que, bien que nécessaire, celui-ci est à lui seul incapable d'assurer totalement la sécurité du réseau. Une politique de sécurité sérieuse impose l'utilisation de deux types de systèmes de détection d'intrusion (réseaux et système), en plus du firewall.

WinReporter® peut efficacement implémenter la détection d'intrusion système.

Grâce à la souplesse de WinReporter®, l'administrateur peut aisément contrôler tous les événements survenus en local sur chaque ordinateur du réseau.

De plus, ceci étant réalisé via l'exploitation des mécanismes de journalisation standard de Windows™, cette détection d'intrusion n'a pas d'impact négatif sur les performances du système.

WinReporter® permet d'avoir une vision globale et précise sur le fonctionnement du système, et des scans réguliers permettent de détecter tous types d'événements sensibles tels que :

- ▶ Les événements de connexion et de déconnexion  
**Comment procéder :** Reporter > Rapports > Rapports d'événement > Historique des sessions.
- ▶ Le suivi des processus  
**Comment procéder :** Reporter > Rapports > Rapports d'événement > Suivi des processus
- ▶ Les événements d'accès aux fichiers  
**Comment procéder :** Reporter > Rapports > Rapports d'événement > Accès aux fichiers
- ▶ Les événements d'arrêts et de démarrage  
**Comment procéder :** Reporter > Rapports > Rapports d'événement > Arrêt et démarrages des machines
- ▶ Un suivi détaillé des événements de sécurité  
**Comment procéder :** Reporter > Rapports > Rapports d'événement > Rapport générique

Même les attaques les plus sophistiquées laissent des traces, et WinReporter® est par conséquent l'outil idéal pour rapidement détecter toutes intrusions ou tentatives d'intrusions système.

Il faut cependant souligner que les ordinateurs très sensibles exigent un contrôle en temps réel, et que WinReporter® ne permet de détecter les événements suspects que lors des scans.

EvenTrigger®, autre logiciel édité par IS Decisions, répond spécifiquement à ce type de besoin, tous les événements suspects au niveau local est immédiatement notifiés au serveur central.

## Recherche de preuves avec WinReporter®

Aucun réseau n'est sécurisé à 100%.

La sécurité des systèmes d'information est un compromis délicat entre protection et facilité d'usage, et tout système est donc susceptible d'être tôt ou tard victime d'une attaque.

Une politique de sécurité efficace impose de prévoir des procédures à mettre en place après l'occurrence d'un problème de sécurité.

Dans cette situation aussi WinReporter® trouve sa place dans la trousse à outils de l'administrateur, car il se révèle d'une grande utilité pour analyser l'attaque ayant déjà eu lieu.

Scanner le réseau et sauvegarder l'information régulièrement est indispensable pour identifier les responsabilités des utilisateurs, et obtenir des preuves recevables pour d'éventuelles actions en justice.

A titre d'exemple, WinReporter® permet à l'administrateur de découvrir les détails des actions réalisées par un utilisateur donné :

- ▶ Quand et où il se connecta.  
**Comment procéder:** Reporter > Rapports > Rapport d'événement > Historique des sessions
- ▶ Quels processus furent lancés  
**Comment procéder:** Reporter > Rapports > Rapport d'événement > Suivi des processus
- ▶ Quels fichiers furent accédés, et de quelle manière  
**Comment procéder:** Reporter > Rapports > Rapport d'événement > Accès aux fichiers

L'existence connue de ce type de contrôles responsabilise tous les utilisateurs, en particulier les membres du groupe administrateur.

## Recherche de preuves avec WinReporter®

Jusqu'ici nous avons vu comment utiliser les rapports prédéfinis de WinReporter® dans un contexte de sécurité informatique. Il faut cependant noter que les administrateurs avancés pourront réaliser des recherches beaucoup plus pointues.

L'administrateur a accès à la base de données non propriétaire de WinReporter® : des requêtes SQL précises lui permettront à coup sûr de rapidement trouver l'information critique dont il a besoin :

- ▶ Par exemple, un administrateur peut avoir besoin d'identifier l'utilisateur qui a exécuté le programme démarrant un service précis sur un ordinateur donné.  
Il s'agit en effet d'un moyen efficace de découvrir qui a installé une *backdoor* sur l'ordinateur en question.  
WinReporter® rend cette recherche triviale :  
*Reporter > Tables > services et trouver le service suspect.*
- ▶ La présence de fichiers ne respectant pas le copyright est un problème moins critique mais plus commun. Pour s'assurer qu'aucun fichier de type MP3 ne se trouve sur le réseau, l'administrateur peut simplement exécuter la commande suivante :  
*Reporter > Tables > Logiciel > realfiles, et chercher les fichiers de type \*mp3.*
- ▶ WinReporter® peut étroitement collaborer avec des logiciels dédiés à la sécurité. La table *netcards* informe l'administrateur de toutes les adresses MAC autorisées.  
Si un sniffer réseau détecte des paquets contenant des adresses MAC non conformes, il est très probable qu'une attaque est en cours ...