FICHE TECHNIQUE

WATCHGUARD ADVANCED REPORTING TOOL

Informations exploitables sur la sécurité et les systèmes d'information

RENFORCEZ VOTRE SÉCURITÉ PROACTIVEMENT

La hausse du volume des données de sécurité que gèrent les entreprises empêche généralement les services informatiques de se concentrer sur ce qui est vraiment important. Ces informations peuvent permettre de détecter des problèmes et des failles de sécurité imputables à des facteurs externes et à des employés internes.

Les professionnels de la sécurité sont désemparés face à l'explosion du volume de données. En raison du volume important d'informations gérées et de l'émergence de malwares de nouvelle génération, de nombreux détails sont négligés ou passent inaperçus, compromettant ainsi la sécurité du système tout entier.

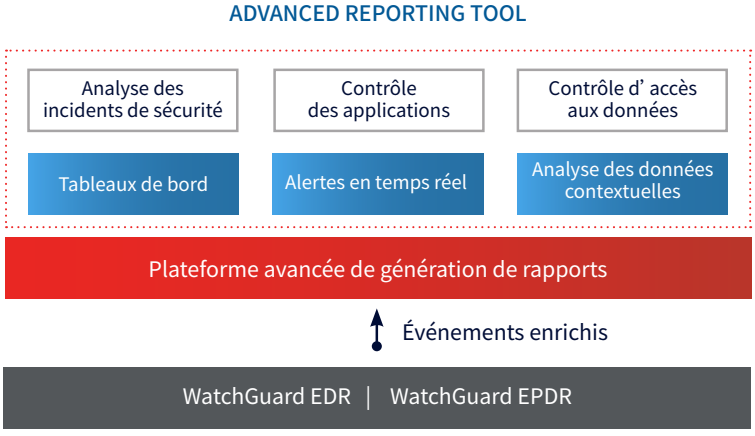
WATCHGUARD ADVANCED REPORTING TOOL

La plateforme Advanced Reporting Tool (ART) automatise le stockage et la mise en corrélation des données générées par l'exécution des processus et leur contexte, extraites au niveau des postes de travail par WatchGuard EPDR et WatchGuard EDR, sans avoir à investir dans l'infrastructure, les installations ou la maintenance.

Ces données permettent à **WatchGuard Advanced Reporting Tool** de générer automatiquement des informations de sécurité, ce qui donne aux entreprises les outils dont elles ont besoin pour identifier les attaques et les comportements inhabituels, quelle que soit leur origine, et pour détecter les abus internes susceptibles de survenir sur les réseaux et les systèmes de l'entreprise.

La plateforme **Advanced Reporting Tool** donne aux entreprises la capacité de rechercher, examiner et analyser, en fournissant des informations sur la sécurité et l'informatique telles que :

- Déterminer l'origine des incidents de sécurité et appliquer des mesures de sécurité pour prévenir de futures attaques.
- Mettre en œuvre des stratégies plus restrictives pour l'accès aux données stratégiques de l'entreprise.
- Surveiller et contrôler l'abus des ressources d'entreprise susceptibles d'avoir un impact sur les performances de l'entreprise et des employés.
- Rectifier les comportements d'employés qui ne sont pas conformes aux stratégies d'utilisation de l'entreprise.



PRINCIPAUX AVANTAGES

Accès aux données stratégiques

- Optimisez la visibilité sur tous les événements qui se produisent sur les appareils afin d'accroître l'efficacité et la productivité du service informatique.
- Accédez à l'historique des données pour analyser les indicateurs de sécurité et d'utilisation des ressources de l'entreprise.
- Obtenez des données approfondies pour identifier les risques de sécurité et les abus internes de l'infrastructure informatique.

Détecter les problèmes de réseau

- Identifiez des modèles d'utilisation de ressources et de comportements d'utilisateurs. Utilisez ces informations pour former les utilisateurs et mettre en œuvre des stratégies de réduction des coûts.
- Obtenez une visibilité sur les ordinateurs et les applications qui fonctionnent sur votre réseau pour améliorer la sécurité et renforcer le contrôle des actifs de votre entreprise.

Alerter et être alerté

- Transformez la détection des anomalies en alertes et en rapports en temps réel.
- Développez la confiance de l'entreprise en signalant les anomalies de sécurité et les abus de ressources informatiques commis par les employés en temps réel.

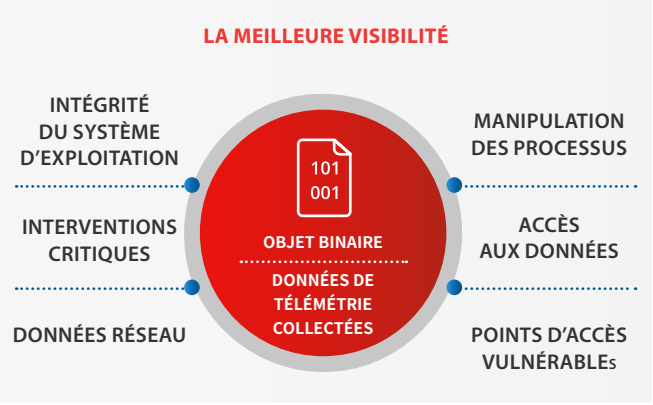
Être prêt à faire face aux incidents

- Générez des rapports configurables pour procéder à des analyses méthodiques de la posture de votre entreprise en matière de sécurité, identifiez toute mauvaise utilisation des actifs de l'entreprise et repérez les comportements anormaux.
- Affichez l'état des principaux indicateurs de sécurité et suivez leur évolution au fil du temps et de la mise en place de mesures correctives.

DES ANALYSES FLEXIBLES ADAPTÉES À VOS BESOINS

Advanced Reporting Tool intègre des tableaux de bord avec des indicateurs clés, des options de recherche et des alertes par défaut dans trois domaines spécifiques :

- Incidents de sécurité
- Accès aux données stratégiques
- Utilisation des ressources du réseau et des applications
- Adaptez les recherches et les alertes sur des données clés relatives aux besoins de votre entreprise.



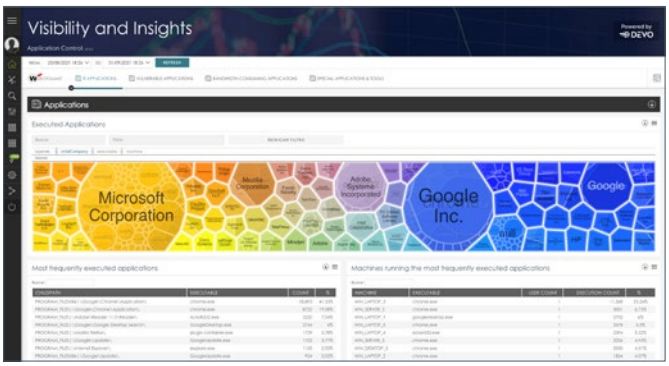
INFORMATIONS SUR LES INCIDENTS DE SÉCURITÉ

Générez des informations de sécurité, en traitant et en mettant en corrélation des événements générés lors de tentatives d'intrusion :

- Graphiques calendaires illustrant les malwares, les PUP (programmes potentiellement indésirables) et les exploits détectés au cours de l'année écoulée.
- Ordinateurs sur lesquels le plus grand nombre de malwares et de tentatives d'infection a été détecté.
- Ordinateurs contenant des applications vulnérables.
- Statut d'exécution des malwares, PUP et exploits.

DÉTECTION DES USAGES INFORMATIQUES PARALLÈLES (SHADOW IT)

- Applications les plus exécutées et les plus fréquemment exécutées.
- Script des applications exécutées (PowerShell, Linux shell, Windows cmd, etc.).
- Applications exécutées via un accès à distance (TeamViewer, VNC, etc.).
- Logiciels gratuits indésirables exécutés (Emule, torrent, etc.).



MODÈLES D'UTILISATION DES RESSOURCES RÉSEAU

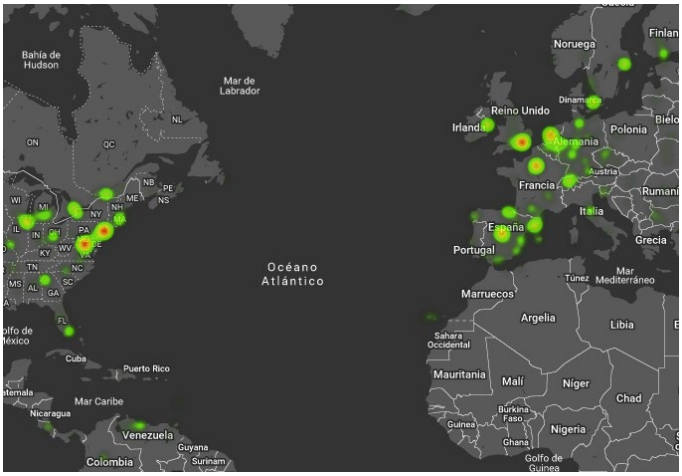
Identifiez les modèles d'utilisation des ressources informatiques pour définir et appliquer les stratégies de sécurité :

- Identification des applications internes à l'entreprise ou autres qui sont exécutées sur votre réseau.
- Identification des applications vulnérables qui sont exécutées ou installées sur le réseau et peuvent le contaminer ou affecter les performances de l'entreprise.
- Contrôle des licences MS Office, utilisées vs achetées.
- Applications les plus gourmandes en bande passante.

CONTRÔLEZ L'ACCÈS AUX DONNÉES D'ENTREPRISE

Montre l'accès aux fichiers contenant des données confidentielles sur le réseau :

- Fichiers les plus fréquemment consultés et exécutés par les utilisateurs du réseau.
- Graphiques calendaires et cartes illustrant les données envoyées au cours de l'année écoulée.
- Les utilisateurs ont accès à certains ordinateurs sur le réseau.
- Les pays qui reçoivent le plus de connexions de votre réseau.



ALERTES EN TEMPS RÉEL

Configurez des alertes en fonction d'événements susceptibles de signaler une faille de sécurité ou la violation d'une stratégie de gestion des données de l'entreprise :

- Alertes par défaut indiquant des situations à risque.
- Définissez des alertes personnalisées en fonction de requêtes créées par les utilisateurs.
- Sept méthodes de transmission (à l'écran et par email, JSON, Service Desk, Jira, Pushovery et PagerDuty).

Plateformes prises en charge et configuration système requise pour WatchGuard Advanced Reporting Tool

Compatible avec les solutions suivantes : WatchGuard EPDR et WatchGuard EDR

Liste des navigateurs compatibles :
Google Chrome et Mozilla Firefox (les autres navigateurs ne sont pas forcément compatibles).