Advanced Reporting Tool

From Data to Actionable IT and Security Insight

L'augmentation des volumes de données de sécurité gérés par les entreprises empêche les départements informatiques de se concentrer sur les détails vraiment importants.

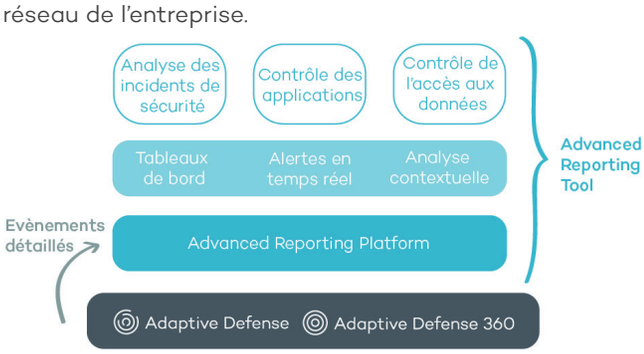
Ces informations peuvent être utilisées pour détecter les problèmes et violations de sécurité causés aussi bien par des facteurs externes que par des sources internes à l'entreprise.

Les départements informatiques sont submergés : les volumes importants de données manipulés et l'avènement d'une nouvelle génération de logiciels malveillants conduisent à négliger certains détails, voire à les ignorer totalement, ce qui fait courir un risque de sécurité au système tout entier.

La solution : Adaptive Defense et Advanced Reporting Tool.

La console Advanced Reporting Platform automatise l'enregistrement et la remise en contexte des informations relatives à l'exécution des processus, telles qu'elles sont recueillies par Adaptive Defense sur les postes clients..

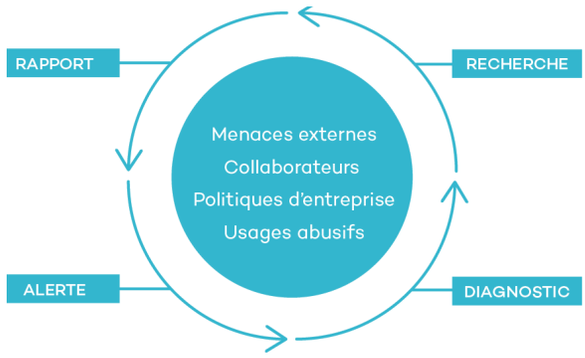
Advanced Reporting Tool est ainsi capable de générer automatiquement des informations de sécurité et de fournir des outils permettant aux entreprises de localiser avec précision les attaques et les comportements inhabituels, d'où qu'ils viennent, ainsi que de détecter toute utilisation interne abusive des systèmes et du réseau de l'entreprise.



Advanced Reporting Tool fournit les données permettant de prendre des décisions en toute connaissance de cause sur la gestion des systèmes informatiques et de la sécurité. Ces conclusions peuvent ensuite servir de base à un plan d'action visant à :

- Déterminer l'origine des menaces et appliquer des mesures de sécurité pour prévenir les attaques futures.
- Mettre en œuvre des stratégies plus restrictives pour l'accès aux informations métier critiques.
- Surveiller et contrôler les utilisations abusives de ressources de l'entreprise susceptibles d'influer sur les performances de l'entreprise et celles de ses employés.

Principaux avantages



1. Bénéficiez des informations appropriées

- Optimisez la visibilité de ce qui se passe sur chaque appareil et augmentez les performances et la productivité du département informatique.
- Accédez aux données historiques pour analyser les indicateurs de sécurité et d'utilisation des ressources IT.
- Profitez d'informations détaillées pour identifier les risques de sécurité et les utilisations internes abusives de l'infrastructure informatique.

2. Diagnostiquez les problèmes réseau

- Réduisez le nombre d'outils et de sources de données nécessaires à une compréhension totale de ce qui se passe sur les appareils de l'entreprise.
- Récupérez les modèles d'utilisation des ressources et de comportement des utilisateurs pour montrer leur impact professionnel potentiel.

3. Alertez et soyez alertés

- Transformez la détection d'anomalies en alertes temps réel et en rapports.

Améliorez la confiance dans votre entreprise en interceptant en temps réel les anomalies de sécurité et les utilisations abusives des ressources informatiques par les employés.

4. Créez des analyses horizontales et verticales

- Générez des rapports détaillés configurables pour analyser de façon méthodique la sécurité, identifier les utilisations abusives des actifs et découvrir les anomalies de comportement des utilisateurs.
- Montrez l'état des indicateurs de sécurité clés et suivez leur évolution à la suite des actions correctives réalisées.

Advanced Reporting Tool

Des analyses flexibles adaptées aux besoins de votre entreprise

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

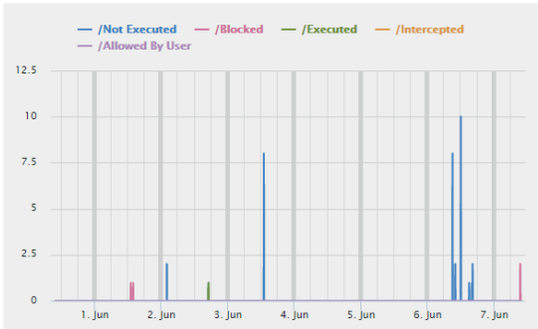
- Incidents de sécurité.
- Accès aux informations critiques.
- Utilisation des applications et des ressources réseau.

Adaptez les recherches et les alertes d'informations clés à vos besoins professionnels.

Informations sur les incidents de sécurité

Générez des informations sur la sécurité, en traitant et en mettant en corrélation les événements déclenchés lors des tentatives d'intrusion.

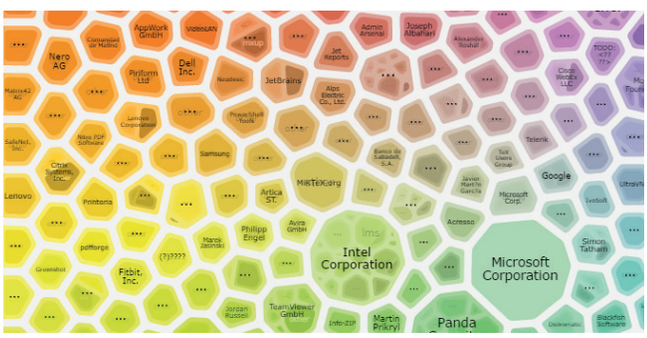
- Diagrammes calendaires montrant les logiciels malveillants et les programmes potentiellement indésirables détectés durant l'année écoulée.
- Ordinateurs avec le plus grand nombre de tentatives d'infection et le plus grand nombre de spécimens de logiciels malveillants détectés.
- État d'exécution des logiciels malveillants sur les ordinateurs en réseau.
- Désignation des ordinateurs présentant des applications vulnérables.



Réduction des coûts

Découvrez les modèles d'utilisation des ressources informatiques pour définir et mettre en vigueur des stratégies de réduction des coûts.

- Recherchez les applications d'entreprise et les autres applications qui s'exécutent dans votre réseau.

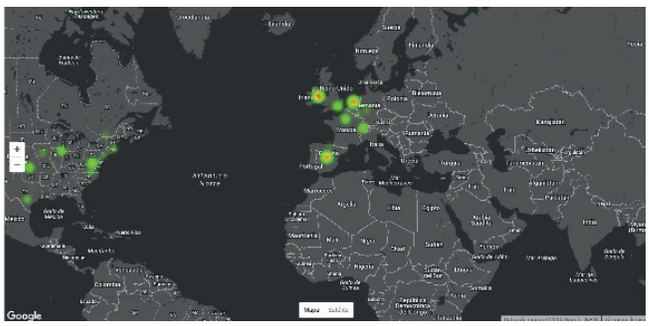


- Comparez les licences bureautiques utilisées par rapport à celles achetées.
- Applications avec la plus grande consommation de bande passante.
- Applications vulnérables exécutées ou installées dans le réseau qui peuvent conduire à des infections, ont un effet sur les performances métier ou entraînent des coûts de résolution.

Contrôle de l'accès aux données sensibles

Visualisez l'accès aux fichiers de données confidentiels et les fuites de données dans le réseau.

- Pays ayant reçu le plus de connexions de la part de votre réseau.
- Fichiers les plus lus et les plus exécutés par les utilisateurs réseau.
- Découvrez quels utilisateurs ont accédé à certains ordinateurs dans le réseau.
- Diagrammes calendaires montrant les données envoyées durant l'année écoulée.



Alertes en temps réel

Configurez des alertes pour les événements pouvant révéler une faille de sécurité ou la violation d'une stratégie de gestion de données de l'entreprise :

- Alertes par défaut indiquant des situations à risque.
- Définissez des alertes personnalisées au moyen de requêtes créées par l'utilisateur.
- Sept méthodes de présentation disponibles (affichage écran et e-mail, JSON, Service Desk, Jira, Pushovery et PagerDuty).

CONFIGURATION MINIMALE REQUISE

Navigateur pris en charge (liste non exhaustive) :

- Mozilla Firefox.
- Google Chrome.

Connexion Internet et communication sécurisée via le port 443.

Résolution d'écran minimale: 1280x1024 (1920x1080 recommandé).