Surveillance des données dans le PLM Digital Thread

Les parcours de transformation numérique des entreprises englobent de plus en plus la conception et la fabrication des produits. Dans les environnements complexes de gestion du cycle de vie des produits (PLM), le fil numérique englobe des centaines d'appareils, d'outils et d'applications. Il inclut des milliers d'utilisateurs et des dizaines de partenaires tiers. Et il supporte des pétaoctets de données, dont la propriété intellectuelle est le joyau de la couronne.

Les mesures de sécurité PLM se sont traditionnellement concentrées sur la protection de la propriété intellectuelle. Mais aujourd'hui, les méthodes de contrôle d'accès basées sur les rôles et les départements ne suffisent plus. Il ne suffit plus de sécuriser les systèmes et les dispositifs qui stockent, transportent et traitent la propriété intellectuelle. Tout d'abord, ils ne protègent pas les données elles-mêmes au niveau binaire. Ensuite, les données IP ne sont même pas la première cible des attaquants.

40%
Pourcentage d'infractions commises à l'aide d'informations d'identification volées[1]

112% augmentation
Les courtiers en accès vendent des informations d'identification volées en 2022 par rapport à 2021

4th
Les courtiers en accès vendent des informations d'identification volées en 2022 par rapport à 2021[2]

Nouvelles Priorités en Matière de Protection

Il est plus rapide, plus facile et plus efficace pour les attaquants de prendre pied dans un réseau par le biais de l'ingénierie sociale et de la compromission par courrier électronique que d'essayer d'attaquer de front un système de gestion du cycle de vie des produits (PLM). L'espionnage industriel reste une motivation d'attaque, mais en 2023, les données les plus ciblées par les cyber-attaquants sont les données entourant la propriété intellectuelle elle-même - les données personnelles et les identifiants des utilisateurs. Pourquoi ?
Les données personnelles sont financièrement lucratives, et les informations d'identification des utilisateurs permettent à des acteurs malveillants de pénétrer dans le réseau sans être détectés et d'y persister. Les attaquants exploitent les données personnelles et les informations d'identification des utilisateurs à partir des outils de communication couramment utilisés dans l'entreprise et dans le PLM :

- Courriel
- Canaux de collaboration
- Applications de productivité
- Documents de planification
- Images
- Recherches sur Internet
- SaaS et connexions de tiers

Les systèmes PLM n'ont jamais été conçus pour protéger ce type de données. C'est pourquoi il ne suffit pas de se concentrer sur les données de propriété intellectuelle elles-mêmes. Vous devez être en mesure de voir, de suivre et de défendre les données qui les entourent a fin de prévenir efficacement les incidents de sécurité et les violations.

[1] Data Breach Investigations Report 2022, Verizon
[2] 2023 Global Threat Report, Crowdstrike

© Flying Cloud Technology 2023

Surveillance des Données—Protection des données du Digital Thread

La surveillance des données brevetée Flying Cloud CrowsNest vous permet de visualiser les données au fur et à mesure qu'elles sont créées, déplacées et consommées dans votre environnement. Pour la première fois, vous pouvez voir les données de manière analytique et légale, et contrôler où elles vont.

Voir les Données en Temps Réel

CrowsNest identifie et prend l'empreinte des données structurées et non structurées. Contrairement aux solutions de gestion des droits numériques (DRM), CrowsNest prend l'empreinte des données sans les toucher ni les modifier. Une fois les données identifiées, vous bénéficiez d'une visibilité complète sur les types de données, les adresses IP, les relations et le contenu en temps réel.

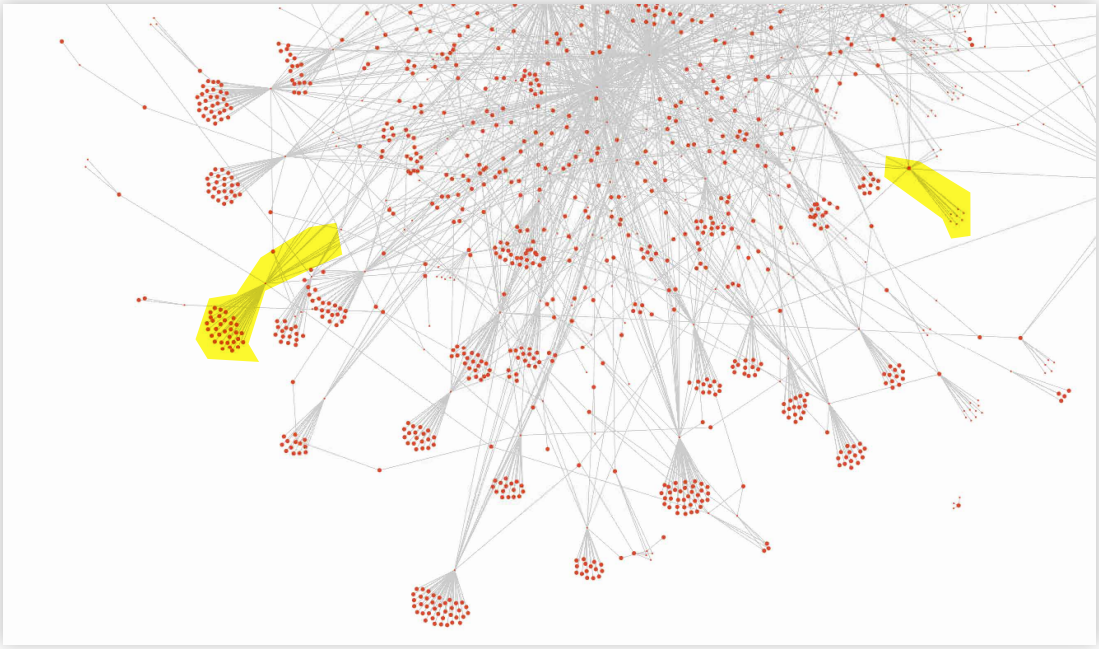

Figure 1. Voyez où les données proviennent, voyagent et prolifèrent dans l'environnement grâce à la possibilité d'analyser les détails au niveau des paquets.

Classer automatiquement les données, en éliminant les méthodes manuelles de marquage des données ou en s'appuyant sur les utilisateurs. Utilisez les règles préconfigurées prêtes à l'emploi de CrowsNest. Importez des règles d'autres sources. Ou créez vos propres règles. Contrairement aux technologies traditionnelles basées sur l'adresse IP, l'empreinte digitale des données de CrowsNest vous permet même de géo-clôturer les données dans des espaces physiques en fonction de leur contenu.

© Flying Cloud Technology 2023

Suivre Vos Données

CrowsNest établit une base roulante d'activité normale pour vos données et suit les données à empreintes digitales partout où elles vont. La ligne de base est continuellement mise à jour en temps réel au fur et à mesure que du nouveau contenu est ajouté, que l'infrastructure change et que les utilisateurs vont et viennent. CrowsNest vous avertit lorsque les données saisies par empreintes digitales ne correspondent pas à la ligne de base.

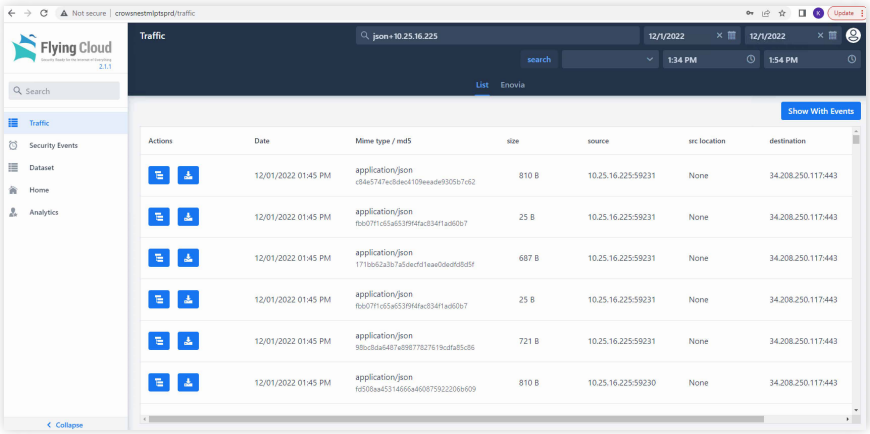

Figure 2. Suivi des types de fichiers, de l'activité, des événements ayant fait l'objet d'une alerte et d'autres attributs. Pour chaque donnée, vous pouvez obtenir des informations détaillées au niveau des paquets.

Défendre Vos Données

C'est vous qui décidez comment CrowsNest doit suivre vos données et les défendre. Définissez les paramètres des événements en fonction de vos critères et recevez des alertes en temps réel en cas de violation de la politique. Vous pouvez également déclencher automatiquement d'autres contrôles de sécurité pour réagir. Une fois créées, les règles s'appliquent non seulement aux données ayant fait l'objet d'une empreinte digitale, mais aussi à toutes les données circulant sur le réseau.

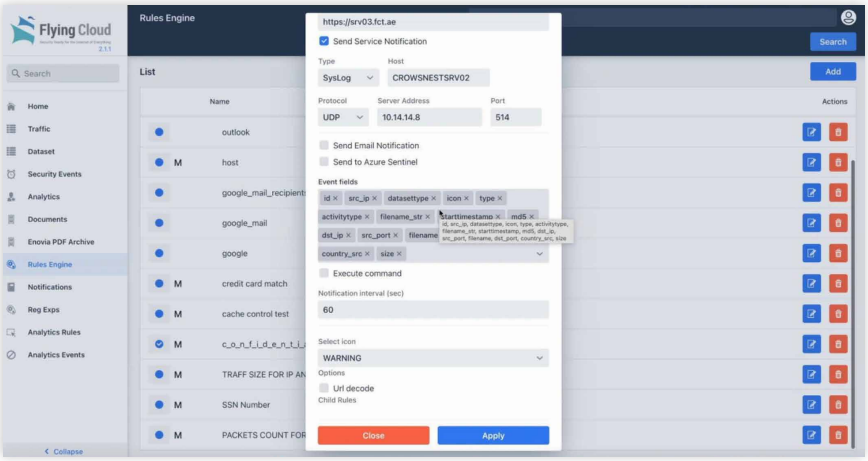

Figure 3. Notre moteur de règles facile à utiliser vous permet d'appliquer une politique aux données elles-mêmes, en fonction de leur contenu, de leur niveau de sensibilité ou de tout autre paramètre.

CrowsNest offre un contrôle beaucoup plus puissant sur vos données que les solutions DLP. Il peut également identifier et isoler les comportements de données caractéristiques des ransomwares, des botnets, des logiciels malveillants, de Bitcoin, des portes dérobées et des logiciels de commande et de contrôle.

© Flying Cloud Technology 2023

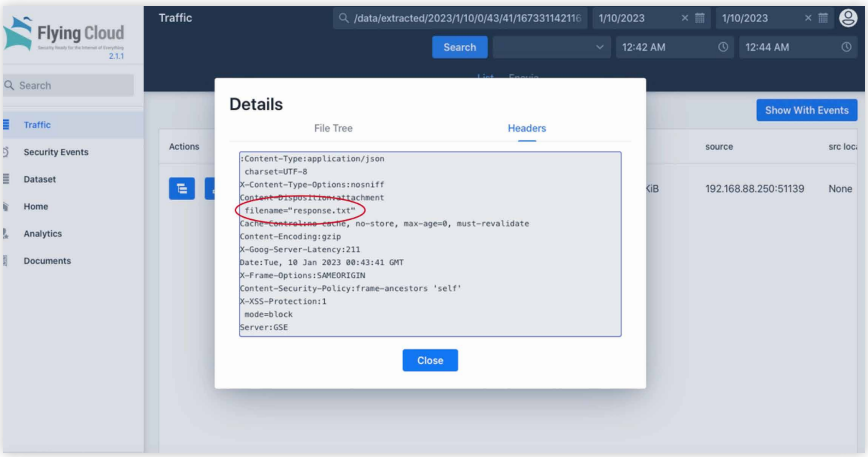

Figure 4. Visualisez les données de session au niveau des paquets et exportez le fichier PCAP vers d'autres outils d'analyse de la sécurité.

Allez plus loin avec la criminalistique des données. CrowsNest fournit un contexte d'événement complet au niveau du paquet. Vous pouvez rejouer les anomalies de données pour les analyser et les stocker à des fins réglementaires.

Avantages

Soutenir la Conformité et la Prise de Décision Exécutive

CrowsNest fournit une chaîne de contrôle pour toutes les données, de la personne qui les crée à celle qui les consomme, en passant par l'endroit où ces données vont et la façon dont elles changent. Si un événement se produit, vous disposez d'un enregistrement qui montre exactement ce qui s'est passé, comment cela s'est passé et quelles données ont été affectées. Une chaîne de contrôle vous fournit la documentation nécessaire pour soutenir la prise de décision au niveau de la direction et du conseil d'administration, ainsi que les initiatives de conformité.

Renforcer la Sécurité du PLM

Suivre les données à travers les systèmes, les interfaces et les utilisateurs sur le réseau de l'entreprise, à l'intérieur et à l'extérieur du PLM. Grâce à des données de session détaillées, vous pouvez rendre compte de toutes les données qui quittent et entrent dans l'environnement PLM. Si un utilisateur autorisé laisse des données quitter le réseau, vous le saurez et pourrez prendre des mesures d'atténuation.

Améliorer la Posture de Sécurité Globale

CrowsNest vous permet de sécuriser et de défendre les données non IP qui sont toujours essentielles dans le monde numérique. Il s'agit notamment des données opérationnelles, financières, marketing, RH, d'identification informatique et de planification. Ces fonctions essentielles dépendent toujours de données critiques pour assurer la continuité et la résilience de l'entreprise.

S'assurer que les Autres Contrôles Fonctionnent Comme Prévu

Assurez-vous que les autres contrôles de sécurité, tels que la DMZ et la segmentation du réseau, fonctionnent comme prévu. CrowsNest vous signalera les empreintes digitales et autres données sensibles qui se déplacent là où elles ne devraient pas.

© Flying Cloud Technology 2023

Pour plus d'informations, demandez une réunion. Vous pouvez également nous rendre visite sur le site www.flyingcloudtech.com.

A Propos de Flying Cloud

Flying Cloud sécurise ce qui compte le plus : les données. Nous permettons aux organisations de voir leurs données lorsqu'elles sont créées, déplacées et consommées sur le réseau. Fondée en 2014, Flying Cloud détient neuf brevets de surveillance des données. Notre solution de surveillance des données CrowsNest donne aux clients la possibilité, pour la première fois, d'examiner leurs données de manière analytique et légale, ainsi que de contrôler où elles vont. Flying Cloud e st une société privée.

© Flying Cloud Technology 2023