Intégration avec les systèmes SIEM d'entreprise

Ajoutez à votre SIEM les informations détaillées et contextuelles de tout ce qui s'exécute sur votre réseau

panda

Une nouvelle source d'informations : les programmes utilisateur

Les solutions de gestion des informations et des événements système (System Information and Event Management, SIEM) sont devenues une nécessité pour gérer la sécurité des infrastructures informatiques grandes et moyennes. Leurs capacités à recueillir et à corréler les états des différents systèmes informatiques permettent aux entreprises de transformer de gros volumes de données en informations utiles à la prise de décisions.

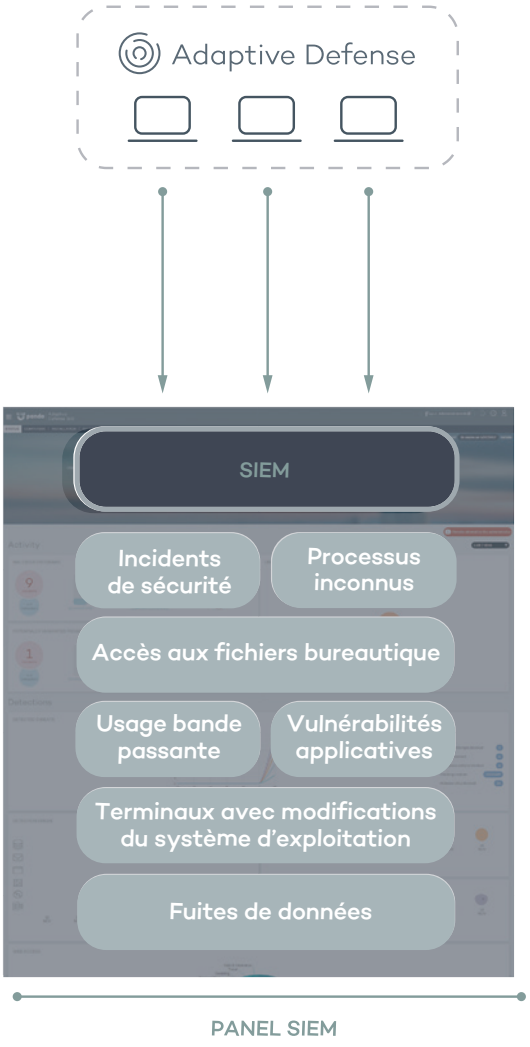
Intégrez une nouvelle source d'informations critiques dans les informations de sécurité recueillies et corrélées par votre système SIEM : tous les processus et les programmes s'exécutant sur vos appareils et surveillés en continu par Adaptive Defense.

Un nouvel état de la sécurité

Les départements informatiques ont besoin de niveaux élevés de visibilité et de maîtrise pour être en mesure d'anticiper les problèmes de sécurité causés par les logiciels malveillants de nouvelle génération.

Adaptive Defense aide les administrateurs à filtrer les énormes volumes de données gérés par les systèmes SIEM et à se concentrer sur ce qui compte vraiment :

- Quels nouveaux programmes en cours d'exécution n'ont pas encore été classifiés comme logiciels légitimes ou logiciels malveillants ?
- Comment ces programmes ont-ils pu accéder au réseau ?
- Quelles activités suspectes entreprennent-ils sur les appareils utilisateur (modifications du Registre, connexions, installation de pilotes, etc.) ?
- Quels logiciels légitimes présentant des vulnérabilités connues et exploitables sont utilisés ?
- Quels processus accèdent aux documents utilisateur et envoient des informations à l'extérieur ?
- Quel usage chaque processus qui s'exécute sur le réseau informatique fait-il des accès au réseau ?



PANEL SIEM

Intégration et fonctionnement transparents

Adaptive Defense s'intègre de façon transparente avec les solutions SIEM d'entreprise existantes sans nécessiter de déploiement supplémentaire sur les appareils des utilisateurs. Les événements surveillés sont envoyés en toute sécurité dans un format LEEF/CEF compatible avec la plupart des systèmes SIEM du marché, soit directement, soit indirectement par l'intermédiaire de plug-ins.

Disponible avec les solutions

- Adaptive Defense
- Adaptive Defense 360

Compatible avec :

ALIEN VAULT · ArcSight An HP Company · QRadar · bitacora · lookwise

Également compatible avec les formats LEEF et CEF