PRÉSENTATION DE LA SOLUTION AKAMAI

Analyse de la détection de violations par plusieurs méthodes : utiliser des règles de segmentation pour détecter les violations de centre de données

Les nombre de violations de centre de données ne montrant aucun signe de diminution, il est temps que les équipes de sécurité se concentrent davantage sur le cœur du centre de données, où les applications communiquent entre elles et exécutent des fonctions stratégiques. Étant donné que de plus en plus d'entreprises distribuent des ressources de centre de données sur plusieurs environnements virtualisés, les défenses de périmètre ne sont plus adaptées. Les administrateurs de sécurité ont besoin de moyens efficaces pour protéger le trafic interne est-ouest contre les attaques qui ont déjà réussi à percer les défenses de périmètre.

Les pare-feu ont atteint leurs limites

Les pare-feu sont traditionnellement utilisés pour sécuriser les communications entrantes et sortantes des centres de données. Toutefois, placer des pare-feu au cœur du centre de données pose une série de problèmes. Incapables de s'adapter aux énormes quantités de trafic est-ouest, ils entravent les performances. Un pare-feu au niveau du serveur consomme de nombreuses ressources informatiques de l'hôte, qui est déjà fortement mis à l'épreuve. Par ailleurs, il est nécessaire de déployer plusieurs solutions pour couvrir les nombreux types et marques de systèmes d'exploitation du centre de données, ce qui en rend la gestion difficile.

Jusqu'à récemment, la mise en œuvre de règles de sécurité au niveau des processus (couche 7) représentait également un défi. En effet, cela nécessite une visibilité sur toutes les applications et tous les processus communiquant dans votre environnement. Cela exige en outre une compréhension globale de la façon dont les processus doivent fonctionner ensemble au sein des applications et du centre de données. Sans ces informations, la mise en œuvre de règles de sécurité au niveau des processus peut s'avérer risquée, et les probabilités de violation sont considérablement plus élevées.

Pour protéger les ressources critiques du centre de données tout en améliorant la détection et le traitement des violations, les équipes de sécurité doivent disposer de moyens pour :

- visualiser en temps réel toutes les applications et tous les processus exécutés dans leurs centres de données ;
- mettre en œuvre des règles de sécurité granulaires sans entraver les processus critiques ;
- détecter les communications non autorisées qui peuvent indiquer une violation.

La meilleure défense est l'attaque : détection basée sur les règles avec Akamai Guardicore Segmentation

La détection basée sur les règles peut aider les équipes de sécurité à détecter, confirmer et contenir plus rapidement les menaces afin d'éviter les dommages et de minimiser les pertes. Ces contrôles de sécurité granulaires ont une double fonction : empêcher un intrus d'accéder de manière malveillante à une application ou à un processus, tout en alertant simultanément les administrateurs de sa présence.

Grâce aux capacités de règles de segmentation d'Akamai Guardicore Segmentation, les professionnels de la sécurité pourront :

- générer une carte visuelle complète de toutes les applications et activités au sein du centre de données, assurant ainsi une visibilité sur toutes les charges de travail et une compréhension complète des communications au niveau de la couche applicative ;

Plusieurs méthodes de détection détectent les violations plus rapidement

Leurres dynamiques

Une architecture de redirection et des environnements connectés générés de manière dynamique mobilisent les attaquants et identifient leurs méthodes, sans perturber les performances du centre de données

Détection basée sur les règles

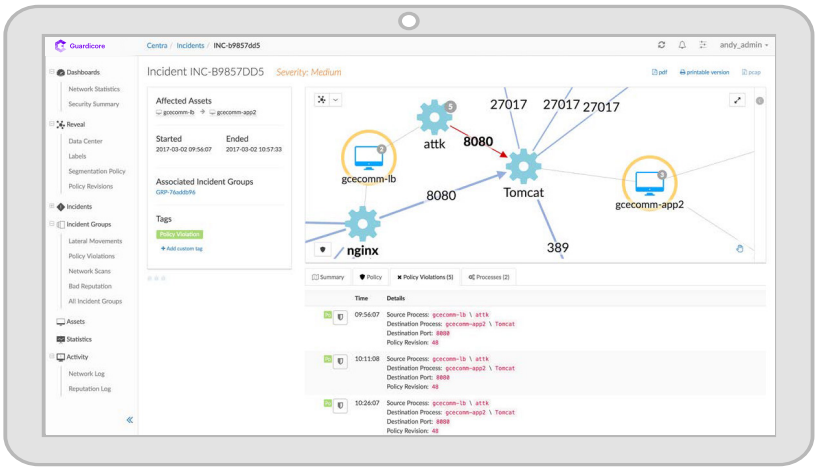
Les règles de sécurité au niveau du réseau (couche 4) et des processus (couche 7) permettent de reconnaître instantanément les communications non autorisées et le trafic non conforme

Analyse de la réputation

Détecte les noms de domaine, les adresses IP et les hachages de fichiers suspects dans les flux de trafic, assurant ainsi une détection complète des violations

- filtrer et organiser les applications en groupes, et les étiqueter, afin de définir des règles de sécurité communes (par exemple, toutes les applications liées à un flux de travail ou à une fonction métier spécifique) ;
- définir et créer des règles régissant les communications autorisées entre les applications ;
- tester et affiner ces règles pour veiller à ce qu'elles ne perturbent pas le trafic autorisé normal.

Tout trafic non conforme, toute communication non autorisée ou toute autre violation de règle déclenche automatiquement une alerte indiquant la présence éventuelle d'un intrus. Cela déclenche à son tour le processus d'investigation visant à confirmer et à contenir la menace.



Akamai Guardicore Segmentation détecte une violation potentielle en reconnaissant et en signalant les violations de règle de segmentation qui impliquent des processus non autorisés tentant de communiquer sur des ports autorisés entre deux hôtes autorisés.

Acculez vos adversaires avec plusieurs méthodes de détection

La détection basée sur les règles n'est que l'une des nombreuses méthodes utilisées par notre solution pour améliorer la détection et le traitement des violations en temps réel. Ces méthodes complémentaires, compatibles les unes avec les autres, sont les suivantes :

- **Leurres dynamiques :** méthode consistant à utiliser des services, systèmes d'exploitation, adresses IP et serveurs de centres de données réels comme leurres qui recherchent activement des activités suspectes dès l'apparition des premiers signes, les mobilisent et les redirigent vers une zone de confinement pour confirmer les menaces et mener une enquête sur ces dernières.
- **Analyse de la réputation :** méthode consistant à exploiter le réseau mondial de capteurs de menaces et de flux de renseignements d'Akamai pour identifier les processus négatifs et les adresses IP, noms de domaine ou hachages de fichiers suspects associés à des menaces.

Le déploiement simultané de ces trois méthodes constitue un solide filet de sécurité, qui assure pratiquement de détecter, d'atténuer et de confiner toutes les violations en direct dans le centre de données pour pouvoir mener une enquête approfondie.

Pour en savoir plus sur les capacités de détection complète des violations de la solution Akamai Guardicore Segmentation, consultez le site akamai.com/guardicore.