DESCRIZIONE DELLA SOLUZIONE AKAMAI

Rilevamento delle violazioni multi-metodo in primo piano: uso delle policy di segmentazione per il rilevamento delle violazioni

Con le violazioni dei data center che non sembrano diminuire, è ora che i team addetti alla sicurezza concentrino maggiormente l'attenzione al centro del data center, dove le applicazioni comunicano tra loro ed eseguono funzioni mission-critical. Poiché sempre più organizzazioni distribuiscono le risorse del data center in più ambienti virtualizzati, i sistemi di difesa perimetrali non sono più adeguati. Gli amministratori della sicurezza necessitano di un mezzo efficiente per proteggere il traffico interno est-ovest da attacchi che sono già riusciti a violare i sistemi di difesa perimetrali.

L'utilizzo di firewall non è sufficiente

I firewall sono stati tradizionalmente utilizzati per proteggere le comunicazioni all'interno e all'esterno dei data center. Tuttavia, collocare i firewall al centro del data center è problematico. Non in grado di adattarsi a elevate quantità di traffico est-ovest, diventano un collo di bottiglia per le performance. L'utilizzo di Il firewall a livello di server consuma grandi quantità di risorse di calcolo dall'host, che è già molto gravato. Richiede inoltre l'implementazione di più soluzioni per essere efficace su diversi tipi e brand di sistemi operativi nel data center, rendendo difficile la gestione.

Fino a poco tempo fa, anche l'implementazione delle policy di sicurezza a livello di processo L7 rappresentava una sfida, poiché richiede la visibilità di tutte le applicazioni e i processi che comunicano nel vostro ambiente. Richiede inoltre una comprensione olistica del funzionamento congiunto previsto dei processi all'interno dell'applicazione e del data center. Senza queste informazioni, l'implementazione di policy di sicurezza a livello di processo può essere rischiosa e le possibilità di danneggiare qualcosa sono molto elevate.

Per proteggere le risorse critiche nel data center, migliorando contemporaneamente il rilevamento e la risposta alle violazioni, i team di sicurezza necessitano di strumenti per:

- Visualizzare tutte le applicazioni e i processi in esecuzione nei loro data center in tempo reale
- Implementare policy di sicurezza granulari senza ostacolare i processi critici
- Rilevare le comunicazioni non autorizzate che potrebbero indicare una violazione

La migliore difesa è l'attacco: rilevamento basato su policy con Akamai Guardicore Segmentation

Il rilevamento basato su policy può aiutare i team di sicurezza a rilevare, confermare e contenere più rapidamente le minacce per prevenire danni e ridurre al minimo le perdite. Questi controlli di sicurezza granulari svolgono una doppia funzione, impediscono agli intrusi di ottenere l'accesso dannoso a un'applicazione o a un processo, avvisando contemporaneamente gli amministratori della presenza di intrusi.

Le funzionalità delle policy di segmentazione all'interno di Akamai Guardicore Segmentation consentono ai professionisti della sicurezza di:

- Generare una mappa visiva completa di tutte le applicazioni e attività all'interno del data center, consentendo la visibilità di tutti i carichi di lavoro e una comprensione completa delle comunicazioni a livello di applicazione

Metodi di rilevamento multipli rilevano le violazioni più rapidamente

Elusione dinamica

Un'architettura di reindirizzamento e ambienti live generati in modo dinamico in grado di individuare gli autori di attacchi e identificare i loro metodi, senza influire sulle performance dei data center

Rilevamento basato sulle policy

Policy di sicurezza a livello di rete 4 e di processi 7 consente il riconoscimento immediato delle comunicazioni non autorizzate e del traffico non conforme

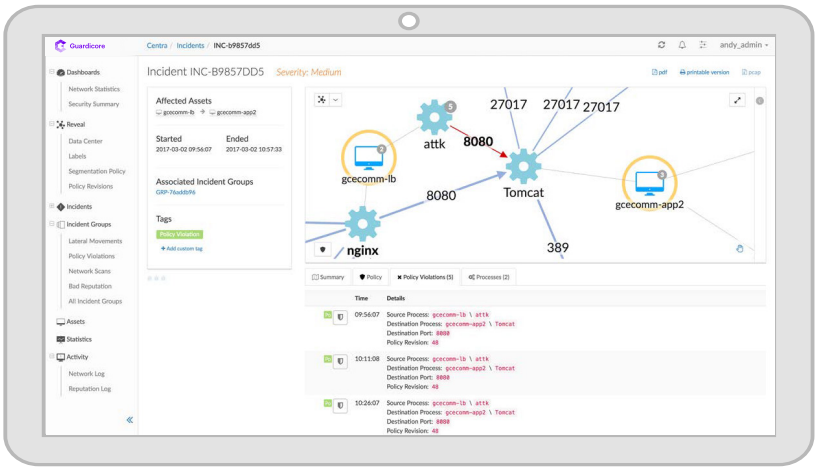
Analisi della reputazione

Rileva nomi di dominio, indirizzi IP e hash file sospetti all'interno dei flussi di traffico offrendo un rilevamento completo delle violazioni.

Akamai

- Filtrare e organizzare le applicazioni in gruppi ed etichettarle allo scopo di impostare policy di sicurezza comuni, ad esempio tutte le applicazioni relative a un particolare workflow o funzione aziendale
- Definire e creare regole che regolano comunicazioni autorizzate tra le applicazioni
- Testare e perfezionare queste regole per verificare che non interrompano il normale traffico autorizzato

Qualsiasi traffico non conforme, comunicazione non autorizzata o altra violazione delle policy attiva automaticamente un avviso che indica la possibile presenza di un intruso. Questo a sua volta avvia il processo di indagine per confermare e contenere la minaccia.



Akamai Guardicore Segmentation rileva una potenziale violazione riconoscendo e avvisando in caso di violazioni delle policy di segmentazione che coinvolgono processi non autorizzati che tentano di comunicare su porte autorizzate tra due host autorizzati.

Mettete all'angolo i vostri avversari con più metodi di rilevamento

Il rilevamento basato su policy è solo uno dei numerosi metodi utilizzati dalla nostra soluzione per migliorare il rilevamento e la risposta alle violazioni in tempo reale. Utilizzati congiuntamente, questi metodi complementari includono anche:

- **Elusione dinamica**, che utilizza server di data center, indirizzi IP, sistemi operativi e servizi reali come esche che cercano attivamente attività sospette alla prima indicazione, interagiscono con esse e le reindirizzano a un'area di contenimento per la conferma e l'indagine delle minacce
- **Analisi della reputazione**, che sfrutta la rete globale di sensori di minacce e feed di intelligence di Akamai per identificare processi negativi e indirizzi IP, nomi di dominio o hash di file sospetti associati alle minacce

L'implementazione simultanea di questi tre metodi costituisce una solida rete di sicurezza, praticamente garantendo il rilevamento in tempo reale di qualsiasi violazione nel data center, la mitigazione e il contenimento per un'indagine approfondita.

Ulteriori informazioni sulle funzioni di rilevamento completo delle violazioni di Akamai Guardicore Segmentation sono disponibili all'indirizzo akamai.com/guardicore.

 | Supporto | | Data di pubblicazione: 06/23