INFORME SOBRE LA SOLUCIÓN DE AKAMAI

Detección de filtraciones de datos con varios métodos: Uso de políticas de segmentación para la detección de filtraciones en centros de datos

Las filtraciones en el centro de datos no parecen disminuir: es hora de que los equipos de seguridad centren más la atención en el núcleo del centro de datos, donde las aplicaciones se comunican entre sí y realizan funciones críticas. Los administradores de seguridad necesitan un medio eficaz para proteger el tráfico de este a oeste interno de los ataques que ya han logrado eludir esas defensas perimetrales. Los administradores de seguridad necesitan un medio eficaz para proteger el tráfico de este a oeste interno de los ataques que ya han logrado eludir las defensas perimetrales.

El firewall ha llegado a un callejón sin salida

Tradicionalmente, los firewalls se han utilizado para proteger las comunicaciones dentro y fuera de los centros de datos. Sin embargo, colocar los firewalls en el núcleo del centro de datos es problemático. Al ser incapaces de adaptarse a grandes cantidades de tráfico de este a oeste, se convierten en un cuello de botella para el rendimiento. El firewall en el nivel de servidor consume grandes cantidades de recursos informáticos del host, que ya está muy sobrecargado. Además, obliga a implementar varias soluciones para abarcar los distintos tipos y marcas de sistemas operativos del centro de datos, lo que dificulta la gestión.

Hasta hace poco, la implementación de políticas de seguridad en el nivel de proceso L7 representaba también un desafío. Esto se debe a que requiere tener visibilidad de todas las aplicaciones y procesos que se comunican en su entorno. Además, exige una comprensión integral de cómo deben funcionar conjuntamente los procesos dentro de la aplicación y el centro de datos. Sin esa información, la implementación de políticas de seguridad en el nivel de proceso puede ser arriesgada, y las probabilidades de provocar algún daño son mucho más altas.

Para proteger los activos críticos en el centro de datos y, al mismo tiempo, mejorar la detección y la respuesta a filtraciones, los equipos de seguridad necesitan los medios para:

- Visualizar todos los procesos y aplicaciones que se ejecutan en sus centros de datos en tiempo real
- Implementar políticas de seguridad detalladas sin obstaculizar los procesos críticos
- Detectar comunicaciones no autorizadas que puedan indicar una filtración

La mejor defensa es el ataque: detección basada en políticas con Guardicore Segmentation de Akamai

La detección basada en políticas puede ayudar a los equipos de seguridad a detectar, confirmar y contener las amenazas con mayor rapidez para prevenir daños y minimizar las pérdidas. Estos controles de seguridad detallados tienen una doble función: por un lado, impiden que un intruso acceda a una aplicación o un proceso y, por otro, alertan a los administradores de su presencia.

Las políticas de segmentación de Akamai Guardicore Segmentation permiten a los profesionales de la seguridad:

- Generar un mapa visual completo de todas las aplicaciones y la actividad dentro del centro de datos, lo que permite ver todas las cargas de trabajo y comprender en su totalidad las comunicaciones que se producen en el nivel de aplicación.

Varios métodos de detección detectan filtraciones con mayor rapidez

Engaño dinámico
Una arquitectura de redirección y entornos activos generados de forma dinámica atraen a los hackers e identifican sus métodos sin interrumpir el rendimiento del centro de datos.

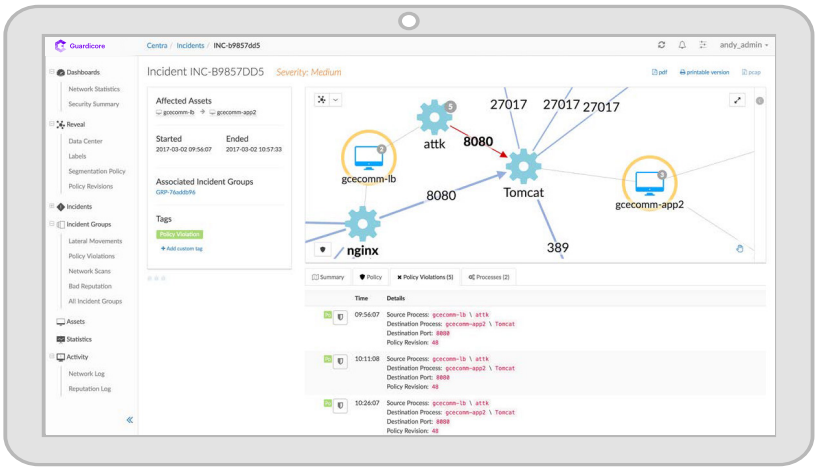
Detección basada en políticas
Las políticas de seguridad en los niveles de red de capa 4 y de proceso de capa 7 permiten reconocer de forma instantánea las comunicaciones no autorizadas y el tráfico que incumple los estándares.

Análisis de reputación
Analiza nombres de dominio, direcciones IP y hashes de archivos sospechosos en los flujos de tráfico para garantizar una detección exhaustiva de las infracciones.

Akamai

- Filtrar y organizar las aplicaciones en grupos, y etiquetarlas con el fin de establecer políticas de seguridad comunes; por ejemplo, todas las aplicaciones relacionadas con un flujo de trabajo o una función empresarial concretos.
- Definir y crear reglas que rijan las comunicaciones autorizadas entre aplicaciones.
- Probar y perfeccionar esas reglas para asegurarse de que no interrumpen el tráfico autorizado normal.

Cualquier tráfico que incumpla los estándares, comunicación no autorizada u otra infracción de políticas activa automáticamente una alerta que indica la presencia de un intruso. Esto, a su vez, inicia el proceso de investigación para confirmar y contener la amenaza.



Guardicore Segmentation de Akamai detecta una posible filtración al reconocer y alertar sobre infracciones de la política de segmentación que implican procesos no autorizados que intentan comunicarse en puertos autorizados entre dos hosts permitidos.

Arrincone a sus adversarios con varios métodos de detección

La detección basada en políticas es solo uno de los diversos métodos que utiliza nuestra solución para mejorar la detección y la respuesta a las filtraciones en tiempo real. Cuando funcionan conjuntamente, estos métodos complementarios también incluyen:

- **Engaño dinámico**, que emplea servidores de centros de datos reales, direcciones IP, sistemas operativos y servicios como señuelos que buscan activamente la primera indicación de actividades sospechosas, interactúan con ellas y las redirigen a un área de contención para la confirmación e investigación de amenazas.
- **Análisis de reputación**, que aprovecha la red global de sensores de amenazas y fuentes de inteligencia de Akamai para identificar procesos negativos y direcciones IP, nombres de dominio o hashes de archivos sospechosos asociados a las amenazas.

La implementación simultánea de estos tres métodos constituye una sólida red de seguridad que garantiza que prácticamente cualquier filtración activa en el centro de datos se detecte, mitigue y contenga para una investigación detallada.

Obtenga más información sobre las completas funciones de detección de filtraciones de Guardicore Segmentation de Akamai en akamai.com/guardicore.