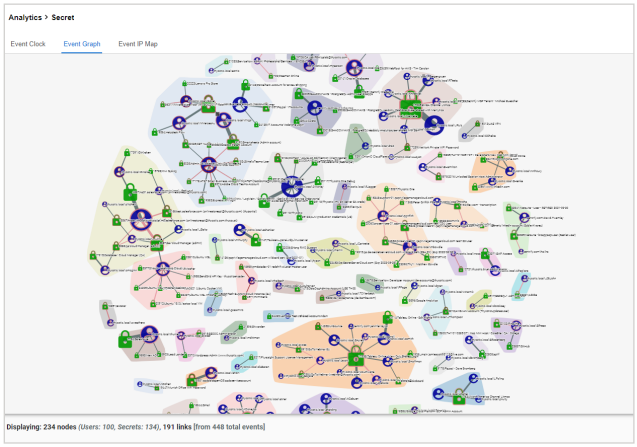
Privileged Behavior Analytics

Detección de vulneraciones y robos de datos antes de que se produzcan

Reduce los riesgos de seguridad

La reducción de los riesgos de seguridad en una organización mediante la mejora de la seguridad ahorra tiempo, dinero y recursos a cada departamento, al tiempo que maximiza la inversión en Secret Server y Privilege Manager.

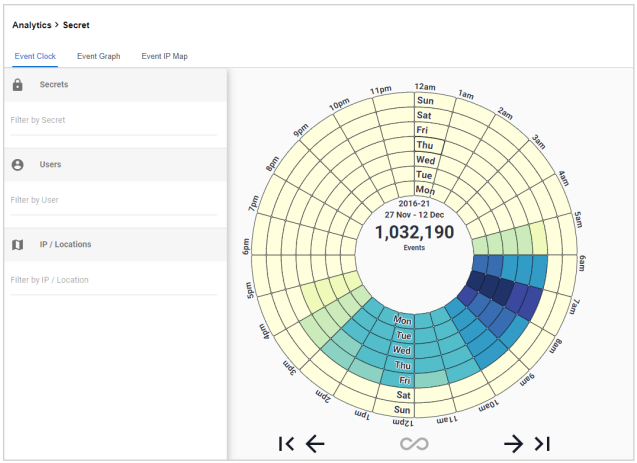
Privileged Behavior Analytics permite a los administradores de IT y de seguridad detectar rápidamente cualquier brecha de seguridad antes de que se produzca, analizar la distribución y el acceso de las cuentas con privilegios en toda la organización y añadir una capa de seguridad a los despliegues de Secret Server y Privilege Manager.



Detecta los primeros indicios de vulneración

¿Acceder a las 3:00 de la madrugada a una importante cuenta con privilegios es un comportamiento adecuado en una organización?

Un comportamiento poco habitual y repentino de un usuario puede ser un indicio temprano de una vulneración de datos o de una amenaza interna. Privileged Behavior Analytics puede detectar rápidamente este comportamiento anómalo y alertar al instante al equipo de seguridad sobre un posible ciberataque o una amenaza interna antes de que se produzca.



Prioriza las alertas más importantes

¿Cómo saber en qué alerta o actividad relacionada con seguridad es importante centrarse primero?

El aprendizaje automático y el reconocimiento de patrones de conducta ayudan a priorizar las actividades en el sistema, alertando al usuario de lo que más importa. Por ello, permite conocer el instante en que se produce una actividad sospechosa y así poder adoptar medidas rápidamente. Además, clasifica las alertas por valoración de la amenaza y permite enfocarse en primer lugar en las más críticas.

Detección de las vulneraciones antes de que se produzcan

Según Forrester, se estima que el 80 % de las vulneraciones están relacionadas con las cuentas con privilegios. Estas brechas de seguridad vienen dadas por cuentas con privilegios que han sido comprometidas o atacadas por amenazas internas. Además de proteger todas las cuentas con privilegios, es vital rastrear y analizar quién tiene acceso a cada una de ellas, así como saber cuándo y cómo las utilizan.

Privileged Behavior Analytics de Delinea ayuda a detectar una posible vulneración antes de que se lleve a cabo. Se trata de una solución en la nube, que utiliza tecnología de aprendizaje automático para analizar el comportamiento de las cuentas con privilegios en Secret Server -la solución de gestión de accesos con privilegios de Delinea. De esta forma, puede alertar rápidamente al equipo de seguridad sobre comportamientos anómalos, o lo que es lo mismo, sobre cualquier indicio temprano de ataque o abuso de privilegios.

Con Privileged Behavior Analytics y Secret Server, una empresa puede analizar el comportamiento temporal de sus usuarios, lo que permite identificar rápidamente si se produce alguna actividad poco habitual. Asimismo, la solución incluye un reloj de acceso secreto que permite a los equipos de seguridad analizar rápidamente cada comportamiento. Estas herramientas de análisis pueden filtrarse aún más para centrarse en un secreto específico o en la conducta de un usuario en un período de tiempo determinado.

Delinea se centra en el vector de ataque más vulnerable: las cuentas con privilegios. Con Delinea es posible adoptar una estrategia multicapa que cubra las necesidades de seguridad de los privilegios de una organización, desde los endpoints hasta las credenciales, garantizando la protección en cada paso.

¿Quién tiene acceso a qué cuentas?

Con Privileged Behavior Analytics, se puede ver un mapa de las cuentas con privilegios y de todos los usuarios que tienen acceso a ellas. Tanto los usuarios como los secretos se agrupan en «comunidades» que actúan como miniecosistemas, y permiten ver si un secreto está contenido en un grupo de personas, o si hay usuarios accediendo a secretos que se encuentran en otros departamentos.

¿Qué alertas son las más importantes?

Privileged Behavior Analytics utiliza una base de comportamiento para el acceso de los usuarios, basada en algoritmos de aprendizaje automático que tienen en cuenta la conducta temporal, el comportamiento de acceso, la sensibilidad de las credenciales y otros comportamientos de usuarios similares. Cuando uno de ellos se desvía de esta base, dependiendo de los algoritmos, se le asigna una valoración de amenaza. De ese modo, el sistema prioriza las valoraciones de amenaza para que la empresa pueda centrarse primero en las alertas con mayor riesgo potencial para la organización.

Delinea

Delinea es un proveedor líder de soluciones de gestión de accesos con privilegios (PAM) que proporciona una seguridad sin fisuras para la empresas híbridas y modernas. Nuestras soluciones consiguen que el acceso privilegiado sea más accesible eliminando la complejidad y definiendo los límites de acceso para reducir el riesgo, garantizar el cumplimiento y simplificar la seguridad. Delinea elimina la complejidad y define los límites del acceso para miles de clientes en todo el mundo, incluyendo más de la mitad de las empresas Fortune 100. Nuestros clientes van desde pequeñas empresas hasta las mayores instituciones financieras del mundo, agencias de inteligencia y empresas de infraestructuras críticas. **delinea.com**