

One Identity Safeguard for Privileged Analytics

Detecte y evite infracciones de seguridad relacionadas con el acceso con privilegios

Beneficios

- Proporciona información sobre lo que ocurre en su sistema del área de TI al rastrear y visualizar la actividad del usuario.
- Autenticación continua por medio del análisis constante de la dinámica de las pulsaciones de teclas y los movimientos del mouse.
- Identifica desviaciones inusuales de la actividad de la línea de base con aprendizaje automático.
- Acorta el tiempo para detectar un incidente de seguridad con información contextual y priorización basada en riesgos de sesiones grabadas.
- Reduce el ruido de las alertas de seguridad, así se puede enfocar en lo que importa.
- Mejora la seguridad al finalizar conexiones cuando se lanza un alerta sobre actividad potencialmente nefaria.

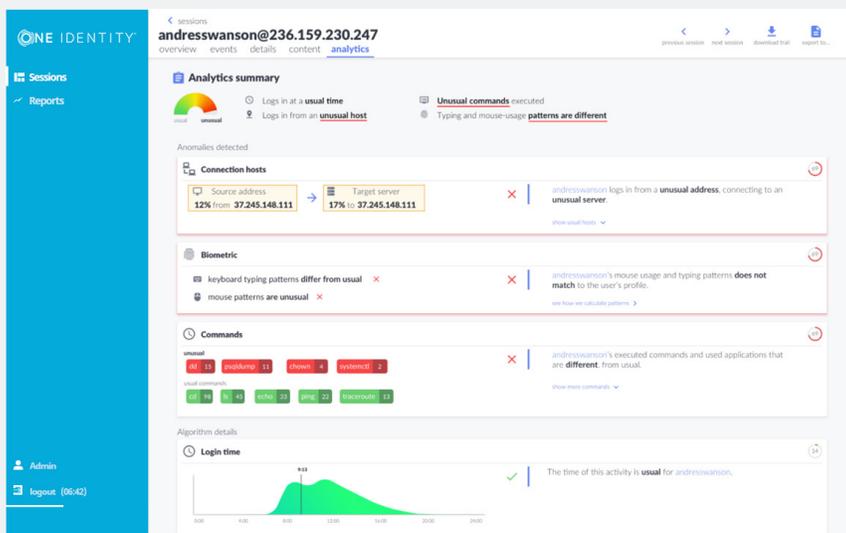
Información general

Como gerente de seguridad del área de TI, sabe que no debe pensar que su empresa nunca experimentará una infracción de cuenta con privilegios. Hoy en día, a las empresas les lleva un promedio de 206 días para identificar una infracción. Y el tiempo es dinero y riesgo. Así, ya sea una infracción de una cuenta con privilegios que fue apropiada o un administrador no autorizado, cuanto más se demore en descubrirla, más tiempo tendrán los infiltrados para encontrar datos y robarlos, y para que se sumen multas y más gastos forenses.

Probablemente tuvo que otorgar acceso con privilegios más allá de sus administradores confiables. Se puede haber expandido para incluir administradores externos de consultores externos que pueden estar ubicados en cualquier parte del mundo. ¿Cómo puede asegurarse de que los administradores que tienen acceso con privilegios lo utilizan para hacer el bien y no el mal?

Con la Protección de One Identity para análisis con privilegios, usted sabe quiénes son sus usuarios más riesgosos, mantiene una vigilancia constante de nuevas amenazas internas y externas, y puede detectar comportamiento con privilegios inusual. Esta solución poderosa le da visibilidad completa a sus usuarios con privilegios y sus actividades, y si hay un problema, puede tomar medidas inmediatas y estar bien posicionado para evitar filtraciones de datos.

¹ Ponemon's 2017 Cost of Data Breach Study (Estudio sobre el costo de la filtración de datos de 2017 de Ponemon).



Determine con facilidad el comportamiento y los usuarios riesgosos

Vea con rapidez si la actividad de un usuario es inusual y potencialmente riesgosa con la vista de resumen del análisis. Contiene un resumen de comandos inusuales, actividad biométrica y hosts de conexión.

Características

Detecte amenazas desconocidas en tiempo real

La seguridad basada en reglas no detectará nuevos métodos de ataques externos ni personas maliciosas con información privilegiada. La Protección para análisis con privilegios rastrea y visualiza la actividad del usuario en tiempo real para una mejor comprensión de lo que ocurre realmente en su entorno del área de TI. No requiere reglas de correlación predefinidas; simplemente funciona con sus datos de sesión existentes.

Operación sin patrones

En lugar de usar la coincidencia basada en patrones para detectar comportamiento "malo conocido" (lo que a menudo es incorrecto), la Protección para análisis con privilegios usa datos recopilados de su entorno del área de TI. Crea una línea de base de comportamiento "normal" y detecta desviaciones al usar varios algoritmos de aprendizaje automático.

Análisis del contenido de la pantalla

Al analizar el contenido de la pantalla de sesiones con privilegios y comprender los títulos de ventanas y los comandos emitidos, la Protección para análisis con privilegios puede enriquecer el perfil del comportamiento de la línea de base de las aplicaciones y comandos de sus usuarios con privilegios usados periódicamente. Este análisis granular facilita la identificación del comportamiento típico y la detección de robos de identidad con privilegios.

El enfoque de One Identity hacia la administración del acceso con privilegios

El portafolio de One Identity incluye el conjunto más completo de soluciones de administración de acceso con privilegios. Puede tomar como base las capacidades de Safeguard for Privileged Analytics de One Identity con soluciones para la administración de sesiones y contraseñas, la delegación granular de la cuenta raíz de UNIX y la cuenta de administrador de Active Directory, funciones adicionales para sudo de código abierto preparado para uso empresarial y registro de pulsaciones de tecla para las actividades raíz de UNIX, todo perfectamente integrado en la solución de puente de Active Directory, líder del sector.

Biometría del comportamiento

Cada usuario tiene su propio patrón idiosincrásico de comportamiento, incluso cuando realiza acciones idénticas, como escribir o mover un mouse. Los algoritmos integrados en la Protección para análisis con privilegios inspeccionan estas características del comportamiento capturadas por la Protección para sesiones con privilegios. Los análisis del movimiento del mouse y la dinámica de las pulsaciones de teclas no solo lo ayudan a identificar filtraciones, sino que también sirven como autenticación biométrica continua.

Reduzca los ruidos de alerta

Privileged Analytics reduce los ruidos de alerta generados por las SIEM al categorizar los eventos de usuario basados en los niveles de desviación y riesgo, y al resaltar los eventos más sospechosos. Las alertas se pueden enviar a las SIEM o sus analistas de seguridad pueden ver una lista priorizada de eventos en la interfaz de usuario intuitiva, lo que les permite enfocarse en los más importantes.

Respuesta automatizada

En la mayoría de las situaciones de ataques, los eventos de alto impacto a menudo son precedidos por una fase de reconocimiento. Así que la detección y la respuesta durante esta fase es crucial para prevenir actividades dañinas. La integración sin problemas en la Protección para sesiones con privilegios permite la finalización de sesión de forma automática cada vez que ocurre un evento altamente sospechoso o se detecta un comportamiento malicioso.

Acerca de One Identity

One Identity ayuda a las empresas a tener una buena administración de identidades y accesos (IAM). Con nuestra combinación exclusiva de ofertas, que incluyen un portafolio de gestión de identidades, administración de accesos, administración de cuentas con privilegios e identidad como soluciones de servicios, las empresas puede alcanzar su máxima potencial, sin impedimentos de seguridad, pero con protección contra amenazas. Obtenga más información en [OneIdentity.com](https://www.oneidentity.com)

© 2019 One Identity LLC TODOS LOS DERECHOS RESERVADOS. One Identity y el logotipo de One Identity son marcas comerciales y marcas comerciales registradas de One Identity LLC en Estados Unidos y otros países. Para obtener una lista completa de las marcas comerciales de One Identity, visite nuestro sitio web en www.oneidentity.com/legal. Todas las demás marcas comerciales, marcas de servicio, marcas comerciales registradas y marcas de servicio registradas son propiedad de sus respectivos dueños.

Datasheet_2019_PAM-Privileged-Analytics_US_RS_41021