Servicio de análisis de amenazas para accesos con privilegios de Centrify

Controles de aprendizaje automático para el panorama de amenazas actual

Los controles de Zero Trust Privilege deben poder adaptarse al contexto de riesgo. Gartner promueve CARTA (acrónimo en inglés de Continuous, Adaptive, Risk, and Trust Assessment, evaluación adaptable y continua de los riesgos y la confianza), que es absolutamente imprescindible para el acceso con privilegios. Zero Trust Privilege implica saber que, incluso cuando un usuario con privilegios ha introducido las credenciales correctas, si la solicitud proviene de un contexto de riesgo, se necesita una verificación más sólida para permitir el acceso. Actualmente se utilizan algoritmos de aprendizaje automático para analizar minuciosamente el comportamiento de los usuarios con privilegios e identificar cualquier actividad «anómala» o «fuera de lo normal» (y por consiguiente arriesgada) y aplicar el nivel adecuado de control según el riesgo correspondiente.

El panorama de amenazas actual requiere controles adaptables

Los adversarios cibernéticos son cada vez más sofisticados y, por consiguiente, es muy recomendable aplicar varias capas de seguridad a la hora de protegerse contra el uso indebido del acceso con privilegios. El panorama de amenazas actual requiere que los controles de seguridad puedan adaptarse al contexto de riesgo y utilizar el aprendizaje automático para analizar minuciosamente el comportamiento de los usuarios con privilegios.

Adaptar el control no significa únicamente notificar una actividad de riesgo en tiempo real, sino también poder responder activamente a los incidentes y terminar sesiones, señalizarlas para realizar un seguimiento minucioso o añadir supervisión adicional.

El aprendizaje automático permite a las empresas escudriñar millones de eventos y buscar esa aguja en el pajar de forma continua y constante, algo imposible de conseguir con el análisis forense manual. Una característica aún más valiosa es la ejecución en línea y en tiempo real del análisis basado en el aprendizaje automático, que permite aplicar controles preventivos realmente adaptables, no solo controles de detección de hechos consumados.

Detectar el uso indebido del acceso con privilegios casi en tiempo real

El Servicio de análisis de amenazas de accesos con privilegios de Centrify utiliza técnicas de análisis de comportamiento avanzadas, junto con las funciones de autenticación multifactorial (MFA) adaptable de Centrify Zero Trust Privilege, para añadir una capa adicional de seguridad y aplica la MFA adaptable cuando el comportamiento del usuario se sale de lo normal. La utilización del Servicio de análisis de amenazas para accesos con privilegios de Centrify puede marcar la diferencia entre sufrir una brecha de seguridad o seguirle la pista y detenerla.

AUTENTICACIÓN MULTIFACTORIAL ADAPTABLE

Añada una capa adicional de seguridad a fin de detener las brechas de seguridad mediante una MFA adaptable con reconocimiento del riesgo para los administradores de TI que acceden a sistemas Windows y Linux, elevan privilegios o utilizan credenciales con privilegios.

TÉCNICAS DE ANÁLISIS DEL COMPORTAMIENTO DE LOS USUARIOS

Utilice algoritmos de aprendizaje automático para analizar minuciosamente el comportamiento de un usuario con privilegios e identificar si es «anómalo» o está «fuera de lo normal» y, por consiguiente, es una actividad de riesgo. En caso afirmativo, puede generar una alerta o notificar ese comportamiento al departamento de seguridad. La detección de una actividad de riesgo también sirve para tomar decisiones de control de acceso en tiempo real, por ejemplo, en el contexto de la autenticación normal o de nivel superior. Además, las técnicas de análisis del comportamiento de los usuarios con privilegios se pueden utilizar para determinar qué privilegios se utilizan más y cuáles se utilizan menos, y sirven como función de control para sugerir cambios de roles y derechos.

«Cuando se tiene una imagen clara de la gran cantidad de prestaciones que ofrecen los servicios Zero Trust Privilege de Centrify, se empieza a entender cuántas comprobaciones de seguridad realiza. Todavía me sorprende el número de problemas que pude resolver utilizando únicamente esta solución».

— Matt Horn, director de operaciones de TI, GSI

www.centrify.com Tel. +1 (669) 444-5200

Reforzar el acceso seguro a los sistemas críticos

Añada una capa adicional de seguridad solo cuando sea necesario, y en función de la clasificación del riesgo, para reducir las amenazas relacionadas con la revelación de credenciales con privilegios. Configure el control de acceso según el comportamiento de los administradores de TI que acceden a servidores Windows y Linux, elevan privilegios o utilizan credenciales con privilegios.

- Identifique cualquier comportamiento anómalo mientras se está produciendo. Puede aplicar políticas con reconocimiento del riesgo a los usuarios que inician una sesión con privilegios, descargan una contraseña o elevan privilegios. Combinar las políticas con reconocimiento del riesgo y los controles de acceso según el rol, el contexto de usuario y la MFA permite tomar decisiones inteligentes y automatizadas en tiempo real sobre la conveniencia de conceder un acceso con privilegios concreto. Estas políticas de acceso, que se aplican dinámicamente, conceden acceso al usuario, solicitan un segundo factor de autenticación o bloquean el acceso por completo.
- Los servicios Zero Trust Privilege de Centrify son compatibles con una gran variedad de autenticadores a fin de ofrecerle la flexibilidad necesaria para que su personal de TI se autentique mediante el factor más conveniente y para que pueda utilizar los sistemas de MFA y los autenticadores que ya tenga. Los autenticadores compatibles con Centrify son:
  - Notificación de inserción en dispositivo móvil;
  - Preguntas de seguridad;
  - Llamada telefónica con verificación de PIN;
  - Tokens OATH;
  - Servidores de códigos de acceso de un solo uso;
  - Claves de seguridad FIDO U2F; y
  - Tarjetas inteligentes.
- Las funciones de MFA adaptable de Centrify se han diseñado de modo que se puedan utilizar con las inversiones existentes en RSA, tokens basados en OATH y tarjetas inteligentes como PIV/CAC. Todos estos medios pueden controlarse a través de la gestión centralizada de Centrify y aplicarse en toda la empresa.
- La aplicación móvil de Centrify para iOS y Android proporciona al usuario con privilegios una interfaz sencilla en la que puede recibir notificaciones de MFA o solicitudes de flujo de trabajo para su aprobación. La aplicación también proporciona una interfaz que permite al usuario gestionar *tokens* OATH cuya clave secreta es almacenada en la bóveda por el Servicio de acceso con privilegios de Centrify para dar soporte a la validación de usuario mediante códigos OTP, tal como requieren diversas aplicaciones y servicios con privilegios que utilizan su propia validación MFA compatible con OATH, como la consola de AWS®. Además, la aplicación móvil admite la carga y descarga de contraseñas en caso de emergencia.
- Centrify facilita asimismo los servicios de MFA para dispositivos de red, como routers, conmutadores o cortafuegos, en los que se requiere MFA para el acceso administrativo antes de que el usuario obtenga acceso con privilegios.

Utilizar técnicas de análisis del comportamiento para minimizar la exposición a riesgos

El panorama de amenazas actual requiere que los controles de seguridad puedan adaptarse al contexto de riesgo y utilizar el aprendizaje automático para analizar minuciosamente el comportamiento de los usuarios con privilegios. Adaptar el control no solo significa notificar una actividad de riesgo en tiempo real, sino también poder responder activamente a los incidentes y terminar sesiones, señalizarlas para realizar un seguimiento minucioso o añadir supervisión adicional.

- Utilice una serie de paneles personalizables y widgets interactivos para comprender mejor los riesgos de TI y los patrones de acceso a su infraestructura. Al adaptar la política de seguridad al comportamiento de cada usuario y señalizar automáticamente los comportamientos de riesgo, puede tener visibilidad inmediata del riesgo de la cuenta, sin el sobrecoste derivado de examinar millones de archivos de registro y cantidades ingentes de datos históricos.
- Comprenda mejor los patrones de acceso y los eventos al obtener detalles sobre eventos, sistemas, ubicación, tiempo, comandos con privilegios, etc. Los usuarios de TI pueden examinar en detalle los eventos individuales para comprender los posibles riesgos de un evento específico. El riesgo de cada evento se calcula en tiempo real y se expresa como alto, medio o bajo si se detecta cualquier actividad anómala.
- Obtenga información simplificada sobre las actividades anómalas mediante una vista de escala de tiempo detallada. Identifique los factores específicos que contribuyen a una anomalía para comprender todos los aspectos de una amenaza potencial, todo desde una única consola. Los equipos de seguridad pueden ver la detección de anomalías de acceso al sistema en alta resolución mediante herramientas de análisis como paneles, vistas de navegador y herramientas de investigación.
- Los datos de acceso con privilegios se capturan y almacenan para facilitar las consultas potentes mediante herramientas de gestión de registros y mediante la integración con herramientas externas de generación de informes. Las integraciones simplificadas con herramientas SIEM como Micro Focus® ArcSight™, IBM® QRadar™ y Splunk® identifican rápidamente los riesgos o las actividades sospechosas.
- Utilice cualquier aplicación habilitada para Webhook (por ejemplo, Slack® o cualquier sistema existente de respuesta a incidentes de incorporación como PagerDuty®) para activar el envío de alertas en tiempo real, eliminar la necesidad de notificar las alertas a varios puntos de contacto y mejorar el tiempo de respuesta. Cuando se produce una alerta, el Servicio de análisis de amenazas para accesos con privilegios de Centrify permite al usuario enviar fácilmente las alertas a aplicaciones de terceros a través de Webhook. Esta función permite al usuario responder a una alerta de amenaza y reducir sus repercusiones.
- Consiga información específica y detallada acerca de cualquier actividad con privilegios sospechosa. Los administradores de TI pueden tomar medidas correctoras de inmediato para proteger la infraestructura contra un riesgo potencial o una amenaza que esté en curso. Pueden hacerlo directamente desde la pantalla de alerta o terminar una sesión de forma manual o automática en función del riesgo.
- Los eventos analizados desde el Servicio de análisis de amenazas para accesos con privilegios de Centrify se utilizan para crear perfiles del patrón de comportamiento normal de un usuario en cualquier inicio de sesión o en cualquier actividad con privilegios que incluya la ejecución de comandos. De este modo, es posible identificar las anomalías en tiempo real para habilitar así el control de acceso en función del riesgo. Los eventos de alto riesgo se señalizan de inmediato, generan una alerta y se notifican al departamento de TI a fin de agilizar el análisis y minimizar significativamente el esfuerzo necesario para evaluar el riesgo en los entornos híbridos actuales de TI.

Nuestra misión es impedir la principal causa de las brechas de seguridad: el uso indebido del acceso con privilegios. Centrify facilita a sus clientes un método Cloud Ready Zero Trust Privilege para proteger el acceso a la infraestructura, a DevOps, a la nube, a los contenedores, al Big Data y a otras superficies de la empresa actual expuestas a ataques. Para obtener más información, visite www.centrify.com.

Sede central en EE. UU. +1 (669) 444 5200
EMEA +44 (0) 1344 317950
Asia-Pacífico +61 1300 795 789
Brasil +55 11 3958 4876
Latinoamérica +1 305 900 5354
sales@centrify.com

www.centrify.com