Veriato

Veriato Recon®

ROBO DE PROPIEDAD INTELECTUAL, FUGAS Y INFRACCIONES DE DATOS

SOLUCIÓN ADVANZADA DE AMENZAS INTERNAS

Para las empresas que tienen propiedad intelectual sensible, que en caso de robo o expuestos por un usuario interno representa un riesgo para la empresa, y quieren proteger la información crítica sin restringir el acceso o bloquear los sistemas tan fuerte que la productividad se ve obstaculizada. Veriato Recon es un software para el análisis del comportamiento de los usuarios que proporciona una alerta temprana de comportamientos sospechosos supervisando pasivamente el comportamiento del usuario y alertando cuando las acciones contradicen las políticas o varían de patrones bien definidos.

En lugar de centrarse en la protección de sus bienes, Veriato Recon supervisa el comportamiento del usuario para los indicadores de riesgo, grabando y alertando cuando hay un riesgo elevado, permitiendo la interdicción rápida, reduciendo los falsos positivos, y asegurando informes procesables.

VENTAJAS PRINCIPALES

DETECCIÓN Y ALERTA TEMPRANA

El análisis del comportamiento de usuarios de Veriato Recon proporciona una visión crítica en los cambios de patrones establecidos que están directamente relacionados con el comportamiento de las amenazas internas. La detección temprana es clave para mitigar el riesgo, daño y amenazas que los usuarios internos presentan. Al centrarse directamente en el comportamiento de los usuarios internos, Veriato Recon puede aislar las anomalías y alertar sobre ellas inmediatamente.

SISTEMA DE REGISTRO

No hay que acumular información de fuentes distintas en un esfuerzo para reconstruir lo que ocurrió. Ahorre tiempo y dinero con un sistema de registro que no requiere conocimientos especializados para descifrar. Veriato Recon apoya las mejores prácticas de la revisión de la actividad en línea de los empleados que se van de la empresa por un plazo de 30 días antes de renunciar o ser despedido.

INTEGRACIONES DE TERCEROS

Las mejores prácticas dictan agregar datos de la actividad del usuario a otras fuentes de información para reducir el riesgo de una amenaza interna. Integraciones con los principales proveedores de SIEM, junto con la capacidad de exportar datos a través de syslog, proporciona un flujo de inteligencia de la actividad del usuario a las soluciones que a invertido en - haciéndolos más efectivos.

ANÁLISIS ÚTIL DEL COMPORTAMIENTO DE USUARIO

Veriato Recon guarda los datos subyacentes de la actividad del usuario en las máquinas locales, y solamente transmite alertas e información transaccional a través de la red. No requiere hardware dedicado, y una vez implementado requiere muy poca interacción con TI. A diferencia de muchas soluciones de análisis de comportamiento del usuario, está diseñado para ser fácilmente ajustado para su entorno.

PROBLEMA

Las amenazas internas son más prevalentes que nunca antes. Debido a que se le ha concedido acceso al empleado (o está suplantando a alguien que ha sido), las defensas del perímetro y los controles de acceso se vuelven ineficaces. Como los usuarios internos tienen acceso autorizado, y frecuentemente son de confianza, los ataques internos son más difíciles de detectar que las amenazas externas. La probabilidad que un empleado le cause daño a su compañía aumenta porque saben cuáles son los activos de información que necesitan y exactamente dónde encontrarlos.

SOLUCIÓN

El análisis del comportamiento del usuario de Veriato Recon detecta riesgos internos y amenazas internas tempranas y de forma fiable. Al aprender el comportamiento normal de sus usuarios, Veriato Recon puede detectar cambios en los patrones de comportamiento directamente relacionados con las amenazas y avisarle si el problema se manifiesta plenamente. Análisis del comportamiento de usuario, User Behavior Analysis (“UBA), ofrece una perspectiva muy necesaria y diferente porque esta enfocado en las acciones de los empleados. El enfoque de Veriato Recon a UBA combina una interfaz de usuario intuitiva con capacidades analíticas potentes. Esta combinación poderosa mejora la efectividad del programa de amenazas internas, aumenta sus otras inversiones de seguridad (como SIEM), y reduce el riesgo de ataques internos.

NUEVO EN LA VERSIÓN 8.4

Aunque hay muchas formas de amenazas internas, estas son las más comunes, más publicitadas, y por lo general las más dañinas. Veriato Recon v8.4 introduce Análisis de Comportamiento del usuario que se enfoca en la detección, disuasión y protección contra la extracción de datos.

splunk> | HP ArcSight Action Certified | CITRIX ready

CARACTERÍSTICAS PRINCIPALES

BASES DE REFERENCIA DEL COMPORTAMIENTO

Recon siempre está activo, supervisando los patrones de comportamiento de los usuarios y buscando signos de una amenaza interna. El software aprende lo que parece normal, y se adapta a cambios en la rutina sin problemas. El agente corre silenciosamente, en segundo plano, y Veriato Recon no interfiere con los procesos de negocio o la productividad.

DETECCIÓN Y ALERTA DE ANOMALÍDADES

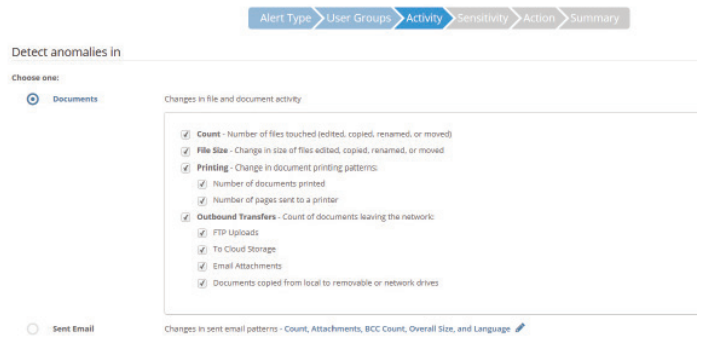
Veriato Recon aplica algoritmos y análisis estadístico para detectar anomalías en el comportamiento del usuario que indican un riesgo o amenaza interna elevado. Una vez detectado, las alertas son enviadas por correo electrónico y, a su discreción, a su solución SIEM. Veriato Recon también incluye palabras claves y frases que son indicadores probados de la actividad de amenazas internas.

REGISTRO DE ACTIVIDAD DEL USUARIO

Los registros de las actividades del empleado son creados y almacenados localmente en la maquina donde la actividad está ocurriendo por un máximo de 30 días. Para asegurar que los registros están seguros y disponibles, los registros de las actividades del empleado están cifrado y ofuscado. Los registros de las actividades del empleado proporcionan un registro completo de todo lo que el empleado hizo antes, durante y después de una alerta.

FÁCIL INTEGRACIÓN CON VERIATO 360

Construido sobre la base probada de Veriato 360, Veriato Recon es implementado y gestionado de la misma consola. Las empresas que desean colocar una combinación de análisis del comportamiento del usuario y supervisión de las actividades del usuario lo encontraran excepcionalmente fácil de implementar y gestionar, permitiendo cubertura total de riesgos internos altos y bajos.



Vaya a www.veriato.com para una prueba gratuita
o correo electronico: sales@veriato.com

ACERCA DE VERIATO

Veriato es un innovador en análisis del comportamiento del usuario y el líder mundial en la supervisión de la actividad del usuario. Mas de 36,000 empresas, escualas, organizaciones gubernamentales y agencias de aplicación de la ley mundial se han confiado en las soluciones de Veriato para ver la actividad de los usuarios en su red, y disfrutar del aumento de la seguridad y la productividad que vienen con él. La misión de Veriato es ofrecer software y soprte de clase mundial que permite a nuestros clientes proteger sus archivos más valiosos, reducir el riesgo, y obtener una visibilidad incomparable en sus operaciones. Las soluciones galardonadas de Veriato incluyen Veriato Recon (análisis de comportamiento basado en la detección de amenazas internas), Veriato 360 (monitoreo de la actividad de los usuarios a nivel empresial), Veriato Investigator (herramienta para la investigación de empleados), Veriato Log Manager (gestión de registro de eventos y seguridad) and Veriato Server Manager (solución para la administración de servidores).

CARACTERÍSTICAS ADICIONALES

COBERTURA COMPLETA

El análisis del comportamiento del usuario de Veriato Recon asegura que no existan fallos en su plan de detección de amenazas internas, permitiendo una cobertura completa de todos los usuarios, incluyendo los de mayor riesgo y los empleados de menor riesgo.

ALINEADOS A SUS NIVELES DE RIESGO

Utilizando el análisis de comportamiento del usuario junto con la supervisión de la actividad del usuario para los puestos de trabajo y empleados de mayor riesgo le permite alinear adecuadamente su escrutinio con el riesgo.

AUMENTE LAS IMPLEMENTACIONES DE SIEM

Los expertos recomiendan la utilización de los datos de actividad del usuario dentro de su SIEM para proporcionar monitoreo y detección de amenazas internas más efectivos.

ABORDA LAS INQUIETUDES SOBRE LA PRIVACIDAD

A diferencia de monitoreo de la actividad del usuario, el análisis del comportamiento del usuario de Veriato Recon no expone el contenido subyacente - sólo información sobre y análisis de datos transaccionales y metadatos.

REQUISITOS DEL SISTEMA

Grabadora (para computadoras y computadoras portátiles siendo supervisadas)

- Windows® 8, Windows® 7, Windows Vista®, Windows XP, Windows Server 2012, Windows Server® 2008
- Mac OS® X 10.6 o superior corriendo en un 64-bit Procesador Intel
- Acceso a la red (En red en un dominio de Windows, grupo de trabajo o Red Novell®)
- Permiso de nivel de administrador a la computadora para la instalación remota del Centro de control

Centro de Control

- Windows 8, Windows 7, Windows Vista, Windows XP, Windows Server 2012, Windows Server 2008
- Acceso a Windows o acceso privilegiado a el base de datos

Tableros de Mandos

- Windows 8, Windows 7, Windows Vista, Windows XP, Windows Server 2012, Windows Server 2008
- Acceso a la red a la instancia de SQL Veriato 360
- Acceso a Windows o acceso privilegiado al base de datos

Componentes de Servidores

- Sistema operativo Windows, x32 o x64:
- Windows Server 2012
- Windows Server 2008
- Windows Server 2003
- Windows 8
- Windows 7
- Windows Vista
- Servidor de clase empresarial (Pentium® III / Intel® Xeon®, 8 GB RAM) se recomienda para uso continuo, pero cualquier sistema de Windows más reciente es apropiado para la evaluación
  - ° SQL Server Host Server—Sistema Operativo en Inglés
  - ° SQL Server Host Server—Sistema de archivos NTFS (no FAT32)
  - ° Se recomienda dirección IP estática
  - ° 40 GB de espacio libre en disco