LOS 3 PRINCIPALES REGISTROS DE ESTACIONES DE TRABAJO QUE SUPERVISAR

Mejore la seguridad de puntos finales supervisando los registros de seguridad, Sysmon y PowerShell

Escrito por Brian Hymer, arquitecto de soluciones de Quest

Quest

Introducción

¿POR QUÉ CENTRARSE EN LA SEGURIDAD DE LAS ESTACIONES DE TRABAJO?

La mayoría de los ataques de hoy en día empiezan en las estaciones de trabajo de los usuarios. ¿Por qué? Bueno, en parte se debe a que las estaciones de trabajo, a diferencia de los servidores, normalmente son el reino de los usuarios no técnicos, que son una presa más fácil para los atacantes. Por ejemplo, el informe de investigaciones de infracción de datos (DBIR) del 2017 de Verizon descubrió que 1 de cada 14 usuarios cayó en la trampa de hacer clic en un enlace malicioso o abrir un adjunto infectado, y al 25 % de ellos se les engañó más de una vez. Asimismo, los usuarios de las estaciones de trabajo son víctimas de descargas involuntarias (drive-by downloads) de sitios web que piensan que son fiables, introducen unidades USB que contienen ransomware u otro malware sin ser conscientes de ello y cometen otros errores críticos que permiten que los atacantes se infiltren en la red corporativa.

Es fácil echar toda la culpa a los usuarios, pero los ataques se vuelven cada vez más sofisticados. En concreto, los hackers recopilan datos de los medios sociales que pueden usar para hacer que sus mensajes de correo electrónico de phishing sean cada vez más convincentes y ocultan malware en los archivos descargables que parece tener el mismo aspecto que los activos originales que los usuarios están buscando. Incluso los propios profesionales de TI a veces caen en estas trampas más sofisticadas.

Quest

La otra cara de la moneda es que las estaciones de trabajo de los usuarios también son especialmente vulnerables por varias razones. En primer lugar, muchas vulnerabilidades de seguridad modernas dependen de acciones interactivas del usuario local, que son la práctica más habitual en las estaciones de trabajo. En segundo lugar, la mayoría de los ataques aprovecha los archivos maliciosos y el contenido web, y las estaciones de trabajo entran en contacto con muchos más archivos de Internet que los servidores. Por último, muchas vulnerabilidades implican aplicaciones dirigidas por una GUI de terceros que se usan en las estaciones de trabajo, como las extensiones de los navegadores de Internet. Mantener esas aplicaciones bien revisadas sigue siendo un punto débil de muchas organizaciones.

La mayoría de los ataques empiezan en las estaciones de trabajo de los usuarios. Aprenda a contraatacarlos.

¿CÓMO PUEDE ACCEDER A LA INFORMACIÓN QUE NECESITA?

Esta combinación de usuarios no técnicos y estaciones de trabajo vulnerables es irresistible para los hackers, por lo que tiene que convertir la seguridad de puntos finales en una prioridad. La clave para detectar los ataques lo antes posible y detenerlos antes de que se cause un daño real es supervisar correctamente sus estaciones de trabajo. ¿Pero cuál es la mejor forma de hacerlo? Este libro electrónico revela los tres registros más importantes para lograr una seguridad en las estaciones de trabajo de Windows más alta (los registros de seguridad, Sysmon y PowerShell) y detalla exactamente qué eventos recopilar para cada uno y por qué.

Por supuesto, con el gran número de estaciones de trabajo y la enorme cantidad de datos de registros de la mayoría de las organizaciones, hay algunos retos reales a la hora de recopilar y archivar los registros de las estaciones de trabajo, por no hablar de supervisarlos, analizarlos y realizar búsquedas en ellos. Por eso, le mostraremos también brevemente cómo InTrust® de Quest® y IT Security Search de Quest® pueden ayudarle a reforzar aún más la seguridad de puntos finales sin dejar muerto a su equipo de TI ni liquidar su presupuesto de almacenamiento.

Quest

Registro de seguridad de Windows

Una supervisión de los registros de las estaciones de trabajo eficaz empieza por el registro de seguridad de Windows. Es el primer registro de la actividad relacionada con la seguridad en las estaciones de trabajo y muchos eventos de seguridad importantes solos se registran ahí.

QUÉ EVENTOS RECOPILAR

El registro de seguridad de Windows es el único lugar para acceder a los siguientes eventos:

- **Enumeración del usuario y grupo locales (eventos 4798 y 4799):** el código malicioso a menudo enumera las cuentas del usuario local y los grupos locales de la estación de trabajo para encontrar credenciales útiles. Hay algunas razones legítimas para enumerar usuarios y grupos, por lo que habrá algunos falsos positivos. Sin embargo, si aísla esos casos, supervisar los eventos 4798 y 4799 puede ayudarte a detectar el código malicioso antes de que pueda realizar movimientos laterales a otros sistemas y usar las credenciales que ha recopilado.
- **Creación de cuentas locales y cambios de grupos locales (eventos 4720, 4722-4726, 4738, 4740, 4767, 4780, 4781, 4794, 5376 y 5377):** a menudo los atacantes también crean o modifican las cuentas locales y los grupos locales (especialmente el grupo de administradores locales), por lo que debe controlar esos eventos.
- **Intentos de inicio de sesión con las cuentas locales (evento 4624):** normalmente los usuarios inician sesión en sus estaciones de trabajo con

Muchos eventos de seguridad importantes solo se registran en el registro de seguridad de Windows.

una cuenta de dominio, por lo que los intentos exitosos y fallidos de iniciar sesión con una cuenta local pueden ser un gran indicador de ataques. El evento 4624 registra todos los tipos de intento de inicio de sesión, incluidos los inicios de sesión de dominios, pero es fácil filtrar para excluirlos porque en esos casos el nombre de dominio es el nombre del equipo.

- **Inicio de sesión con credenciales explícitas (evento 4648):** este evento se genera cuando un proceso intenta iniciar sesión especificando explícitamente las credenciales de otra cuenta. Esto ocurre de forma legítima con las tareas programadas o cuando se usa el comando "RUNAS", por ejemplo. Sin embargo, como la mayoría de las tareas programadas no se ejecutan en las estaciones de trabajo, este evento también puede indicar un proceso malicioso que intenta iniciar otro proceso con credenciales específicas o un atacante que asigna una unidad a otro equipo usando las credenciales que ha recopilado.
- **Cuándo estuvo el usuario presente y activo físicamente (eventos 4800-4803):** recuerde que los usuarios a veces se mantienen con la sesión iniciada durante varias semanas seguidas, por lo que, además de mirar los eventos de inicio de sesión y de cierre de sesión, tiene que fijarse en cuándo estaba bloqueada y desbloqueada la consola de la estación de trabajo. Toda actividad en una estación de trabajo mientras está bloqueada debe investigarse a fondo.
- **Cambio en la configuración del firewall (eventos 4944-4958):** en función de cómo esté configurado el sistema, las aplicaciones pueden añadir automáticamente excepciones al firewall de Windows mientras se instalan, especialmente cuando el usuario tiene autoridad de administrador local. Esas excepciones no tienen por qué ser deliberadamente maliciosas para crear brechas de seguridad graves. Si confía en el firewall de Windows como un importante control de seguridad, tiene que estar informado de cualquier cambio en su configuración.
- **Conexiones de dispositivos plug-and-play (evento 6416, solo Windows 10):** a menudo el malware se introduce en una estación de trabajo a través de unidades USB u otros dispositivos plug-and-play. Es importante auditar las conexiones de todos esos dispositivos; por ejemplo, se han producido ataques a través de teclados, así como a través de unidades USB que se identifican como teclados.

Hay otros eventos importantes que puede obtener del registro de seguridad, pero le recomiendo que los obtenga de Sysmon en su lugar porque la calidad de los datos es mejor. Estos eventos incluyen:

- Creación del proceso
- Conexiones a la red
- Cambios en el registro
- Creación de archivos

Estos eventos se explicarán en detalle en la sección "Sysmon" más abajo.

> Consejo del experto: cree trampas (carpetas o bibliotecas de documentos de SharePoint con nombres tentadores) y vigile los intentos de acceder a ellos.

CÓMO RECOPILAR EVENTOS EN EL REGISTRO DE SEGURIDAD

La política de auditoría de una estación de trabajo determina qué tipo de información sobre el sistema encontrará en el registro de seguridad. Windows usa nueve categorías de política de auditoría y 50 subcategorías de política de auditoría para ofrecerle un control detallado sobre qué información se registra. Puede elegir si quiere registrar eventos exitosos, eventos fallidos o ambos.

Le recomiendo que active la auditoría para las siguientes subcategorías de auditoría. Elija tanto "éxito" como "fallo" para los eventos de inicio de sesión y "éxito" solo para los demás.

Inicio de sesión/Cierre de sesión

- Inicio de sesión
- Cierre de sesión
- Bloqueo de cuenta
- Otros eventos de inicio de sesión/ cierre de sesión

Administración de cuentas

- Administración de cuentas de usuario
- Administración de grupos de seguridad

Cambio de directivas

- Auditar el cambio de directivas
- Cambio en la directiva de autenticación
- Cambio en la directiva de autorización

Esta lista representa la auditoría mínima que recomiendo, pero puede que quiera activar subcategorías adicionales. Recuerde que no tiene que recopilar y archivar todos los eventos que se registran. Personalmente, yo me inclino por una mayor auditoría, porque no ralentiza el sistema (excepto en muy pocos casos, como cuando se auditan todos los accesos a todos los archivos). Simplemente asegúrese de aumentar el tamaño de los registros; recomiendo entre 200 MB y 1 GB.

Inclínese por una mayor auditoría, porque casi nunca ralentiza el sistema. Asegúrese de incrementar el tamaño de los registros.

Sysmon

Sysmon es un servicio gratuito de Microsoft que supervisa la actividad del sistema y la registra en un registro de eventos de Windows, que también se llama "Sysmon".

QUÉ EVENTOS RECOPILAR

Como se ha comentado anteriormente, el registro de Sysmon y el registro de seguridad se solapan en algunos aspectos. Recomiendo usar Sysmon para los siguientes eventos porque la calidad de los datos es mejor:

- **Creación de procesos (ID de evento 1):** el registro de seguridad de Windows le dirá cuando se inicia un proceso EXE y le proporcionará su nombre y ruta. Sin embargo, los atacantes pueden crear fácilmente un programa malicioso con el mismo nombre que una herramienta legítima, como c:\windows\notepad.exe, o modificar un programa existente para que realice acciones ilícitas. Para detectar esos casos, necesita un hash del contenido del archivo, que el registro de seguridad no proporciona, pero Sysmon sí. Un hash es un resumen matemático único de la

El registro de Sysmon y el registro de seguridad se solapan en algunos aspectos, pero Sysmon proporciona datos de mejor calidad para algunos eventos.

secuencia de bits del archivo, por lo que sustituir o modificar el archivo da como resultado un hash diferente. Si utiliza aplicaciones web gratuitas para analizar el hash, puede determinar fácilmente si se ha cambiado o sustituido un archivo con código malicioso conocido, como un troyano.

- **Conexiones a la red (ID de evento 3):** supervisar las conexiones a la red también puede ayudarle a detectar a los atacantes. Por supuesto, el volumen de los datos será muy alto, por lo que tendrá que establecer bases de referencia de actividad normal para detectar conexiones sospechosas. Tanto el registro de seguridad como Sysmon le permiten recopilar eventos de conexión a la red, pero Sysmon enlaza cada conexión a un proceso mediante los campos ProcessID y ProcessGUID, y también proporciona las direcciones IP, los números de puerto y el estado IPv6 de los nombres de host de origen y destino.
- **Cambios de registro (ID de evento 12-14):** una vez que los atacantes introducen su código malicioso en una estación de trabajo mediante un mensaje de correo electrónico de phishing, una descarga involuntaria (drive-by download) o por cualquier otro medio, quieren que ese código se ejecute incluso después de que se reinicie la estación de trabajo. La manera más común de lograr esa permanencia es modificar el registro, por ejemplo, añadiendo una clave de ejecución. Puede monitorizarlo con el registro de seguridad de Windows, pero Sysmon proporciona mucho más contexto, incluida información esencial como quién hizo el cambio, qué equipo utilizó, cuándo pasó, el ID del proceso y el nuevo nombre de cualquier tecla o valor a los que se les cambió el nombre.
- **Creación de archivos (ID de evento 11):** el registro de seguridad de Windows le dirá que se ha creado (o sobrescrito) un nuevo archivo en una determinada carpeta, pero no le proporciona el nombre de ese nuevo archivo. Sysmon sí que lo hace, lo que facilita identificar e investigar los eventos de creación de archivos sospechosos para que pueda bloquear los ataques más pronto. Especialmente, debe supervisar las ubicaciones de inicio automático como la carpeta Inicio, así como los directorios temporales y de descarga, donde a menudo aparece el malware durante la infección inicial.

Además, recomiendo usar Sysmon para supervisar los siguientes eventos que no están incluidos en el registro de seguridad:

- **Cargas de imágenes y controladores (ID de evento 6 y 7):** además de proporcionar el hash para los inicios de procesos EXE tal y como se ha explicado anteriormente, Sysmon también monitoriza las cargas de controladores de dispositivos y DLL, que los atacantes usan también. Informa incluso de si el archivo está firmado, quién lo firmó y si la firma es válida.
- **Creación remota de subprocesos (ID de evento 8):** las herramientas de hackeo sofisticadas pueden inyectar un DLL en un proceso en ejecución y después ponerlo en marcha en otro subproceso. Aunque esta función tiene usos legítimos, como la depuración, tiene que saber cuándo se produce en un sistema de producción.
- **Lecturas de acceso sin procesar (ID de evento 9):** el evento RawAccessRead detecta cuándo un proceso realiza operaciones de lectura en la unidad usando la denotación. Esta técnica la usa a menudo el malware para la filtración de datos de archivos que están bloqueados para la lectura, así como para evitar las herramientas de auditoría de acceso de archivos. El evento indica el proceso de origen y el dispositivo de destino.
- **Conexión y creación de canalizaciones con nombre (ID de evento 17 y 18):** algún software malicioso se comunica con diferentes componentes mediante un canal de comunicaciones en Windows que se llama canalizaciones con nombre.
- **Actividad de eventos WMI (ID de evento 19):** el malware puede ejecutarse registrando un filtro de evento Instrumental de administración de Windows (WMI). Este evento registra el espacio de nombres de WMI, el nombre del filtro y la expresión de filtro.

- **Creación de flujo de archivos con nombre (ID de evento 15):** este evento le ayuda a detectar variantes de malware que introducen sus ejecutables o ajustes de configuración mediante descargas del navegador.
- **Cambio en la hora de creación de los archivos (ID de evento 2):** para evadir algunos tipos de supervisión de la integridad de los archivos, los atacantes pueden modificar las horas de creación de los archivos. Por ejemplo, crearán un archivo, pero cambiarán inmediatamente su hora de creación para que no aparezca en una lista de archivos creados recientemente. Sysmon lo detectará.

CÓMO HABILITAR EL REGISTRO

Para instalar Sysmon, solo tiene que descargar el ejecutable de Microsoft y ejecutar el siguiente comando:

```
Sysmon -i
```

Para controlar qué ID de evento se registran, especifique la configuración adecuada en un archivo de configuración XML y después ejecute este comando.

```
Sysmon -c config.xml
```

Muchos de los eventos que he enumerado anteriormente generarán algunos falsos positivos, así que, por ejemplo, podría especificar una lista de archivos EXE que Sysmon debe excluir de la supervisión. Para obtener una plantilla de archivo de configuración que es un buen punto de inicio para la supervisión de cambios en el sistema, visite https://github.com/SwiftOnSecurity/sysmon-config.

El archivo de configuración de Sysmon controla los eventos que se registran.

PROTECCIÓN DE SYSMON DE LAS ALTERACIONES

Es más fácil alterar Sysmon que el registro de seguridad de Windows. Afortunadamente, hay unas pocas técnicas que pueden mitigar este riesgo. En primer lugar, puede ocultar Sysmon cambiando el nombre del controlador (utilice la etiqueta DriverName en el archivo de configuración) y cambiando el nombre del servicio (renombre el ejecutable antes de instalarlo).

Sin embargo, sigue habiendo métodos que los hackers pueden usar para encontrar Sysmon, por lo que tiene que supervisar ataques contra este. Por suerte, Sysmon monitoriza los cambios en él mismo usando los siguientes eventos:

- **ID de evento 4:** informa de un cambio de estado de servicio de Sysmon (iniciar o detener)
- **ID de evento 16:** informa de un cambio de estado de configuración de Sysmon, incluido el hash del archivo de configuración

Asimismo, puede definir una tarea programada a través de la directiva de grupo que se active periódicamente y ejecute el siguiente comando para aplicar la configuración correcta (sustituya "server\share" con la ruta correcta de su entorno):

```
\\server\share\sysmon -i -accepteula -c \\server\
share\sysmon.xml

if errorlevel 1 \\server\share\sysmon -c \\server\
share\sysmon.xml
```

Hay también herramientas de terceros que pueden restablecer automáticamente su configuración de Sysmon tras cambios indebidos.

Registros de PowerShell

QUÉ EVENTOS RECOPILAR

A los hackers les encanta utilizar PowerShell porque es muy potente. Por lo tanto, es esencial vigilar de cerca la actividad de PowerShell. Hay dos registros de PowerShell: el registro Microsoft-Windows-PowerShell/Operational recibe casi toda la atención, pero también está el registro Windows PowerShell. Recomiendo supervisar algunos eventos de ambos:

Registro Windows PowerShell

- **Proveedores cargados (ID de evento 600):** los proveedores de PowerShell son programas que hacen que los datos de un determinado almacén de datos estén disponibles en PowerShell para que pueda verlos y gestionarlos. Por ejemplo, los proveedores integrados incluyen Entorno (para gestionar variables del entorno Windows) y Registro (para gestionar el registro de Windows). Puede crear sus propios proveedores e instalar proveedores que desarrollen otros. Incluya en listas blancas los proveedores que normalmente usa en su entorno para minimizar los falsos positivos y vigile las nuevas áreas de PowerShell que se están usando, que podrían indicar una actividad maliciosa. En particular, si ve que se ha cargado el proveedor WSMan, sabrá que se ha iniciado una sesión PowerShell remota.

Microsoft-Windows-PowerShell/Operational (que en PowerShell 6 se llama "Microsoft-Windows-PowerShellCore/Operational")

- **Registro de módulos (ID de evento 4103):** el registro de módulos ofrece una auditoría más detallada que incluye todos los comandos ejecutados y todos sus parámetros (pero no el resultado del comando).
- **Registro de bloque de script (ID de evento 4104):** el registro de bloque de script muestra todos los bloques de código de PowerShell que se ejecutó, lo que proporciona mucho más contexto que ver cada comando individual. Incluso si un hacker intenta ocultar u ofuscar un comando, este evento mostrará el comando de PowerShell real que se ejecutó, por lo que es mucho más potente que capturar comandos ejecutados en el sistema. Asimismo, este registro puede capturar algunas de las llamadas API de bajo nivel que se están ejecutando, lo que proporciona incluso más detalles sobre lo que están haciendo los hackers. Este evento normalmente se registra como detallado, pero, si Microsoft detecta que se está usando un comando sospechoso o una técnica de scripting en un bloque de código, se registrará como advertencia en su lugar.

CÓMO HABILITAR EL REGISTRO

El registro Windows PowerShell captura los eventos de forma predeterminada, por lo que no tiene que habilitar el registro para ver qué proveedores se han cargado (ID de evento 600).

Puede activar o desactivar el registro de módulos y el registro de bloque de script usando la configuración de la directiva de grupo correspondiente en Plantillas administrativas | Componentes de Windows | Windows PowerShell.

A los hackers les encanta utilizar PowerShell porque es muy potente.

Quest

Inconvenientes de usar estos registros nativos

De forma conjunta, el registro de seguridad de Windows, Sysmon y los registros de PowerShell le pueden dar algo de visibilidad de las estaciones de trabajo de sus usuarios que puede ayudarle a detectar e impedir los ataques. Sin embargo, hay varias razones para no confiar solo en estos registros y en las herramientas nativas para garantizar la seguridad de las estaciones de trabajo.

Es difícil y lento

El primer reto es el de obtener los registros de todas sus estaciones de trabajo a tiempo y de un modo eficaz, especialmente si muchas de ellas son dispositivos portátiles. Después, tiene que tener flujos de trabajo para analizarlos de forma rápida y eficiente, para que pueda detectar e investigar la actividad sospechosa a tiempo para evitar daños serios.

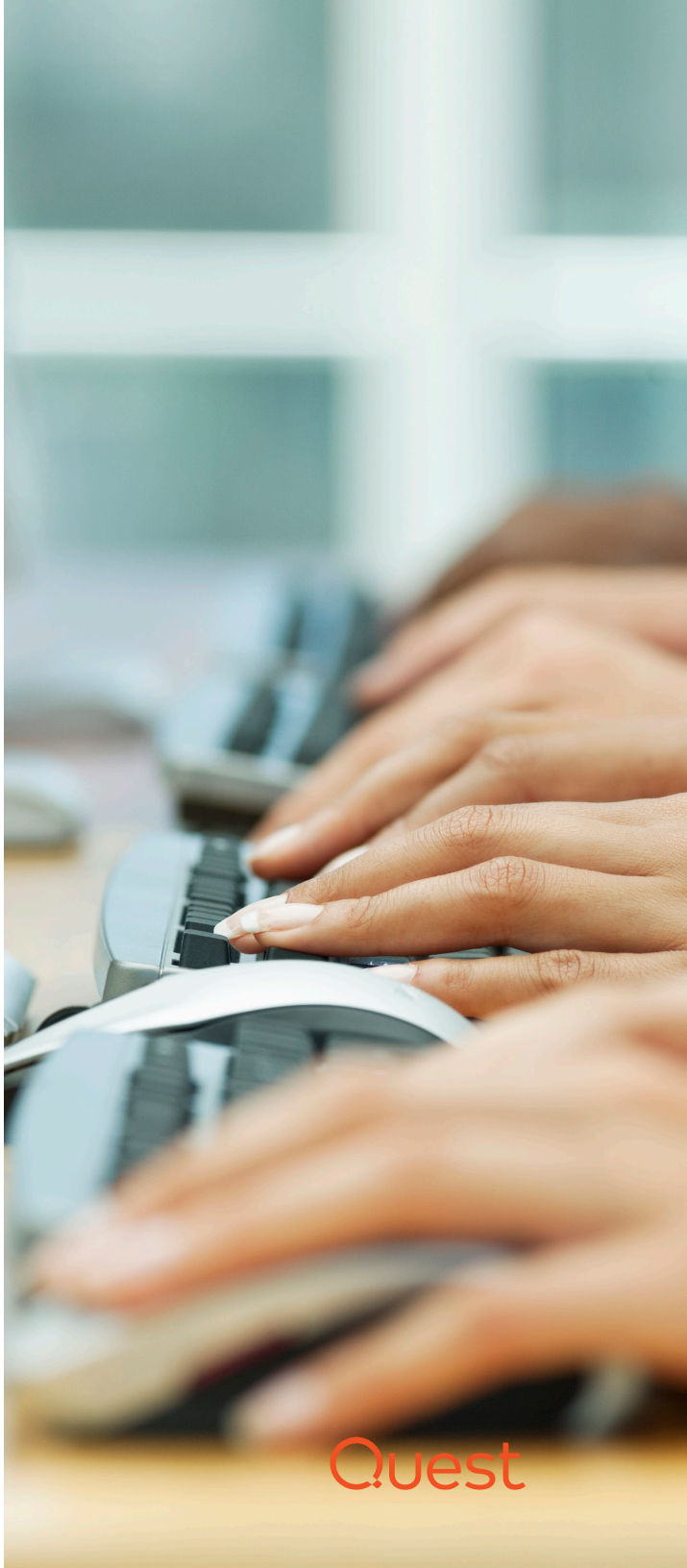
Eso no es sencillo, en parte porque los registros nativos son muy crípticos. Por ejemplo, anteriormente en este libro electrónico he recomendado habilitar la subcategoría Cambio en la directiva de autorización en el registro de seguridad de Windows. Si lo hace, podrá ver cuándo se cambian los permisos en los archivos y las carpetas; pero, a menos que sea un gurú de los registros de Windows, no sabrá mucho más, porque los datos del registro no se proporcionan en nada que se asemeje a un formato que puedan leer los humanos. En vez de eso, cada vez que se produzca un cambio de permisos, tendrá que ejecutar manualmente un comando de PowerShell como este:

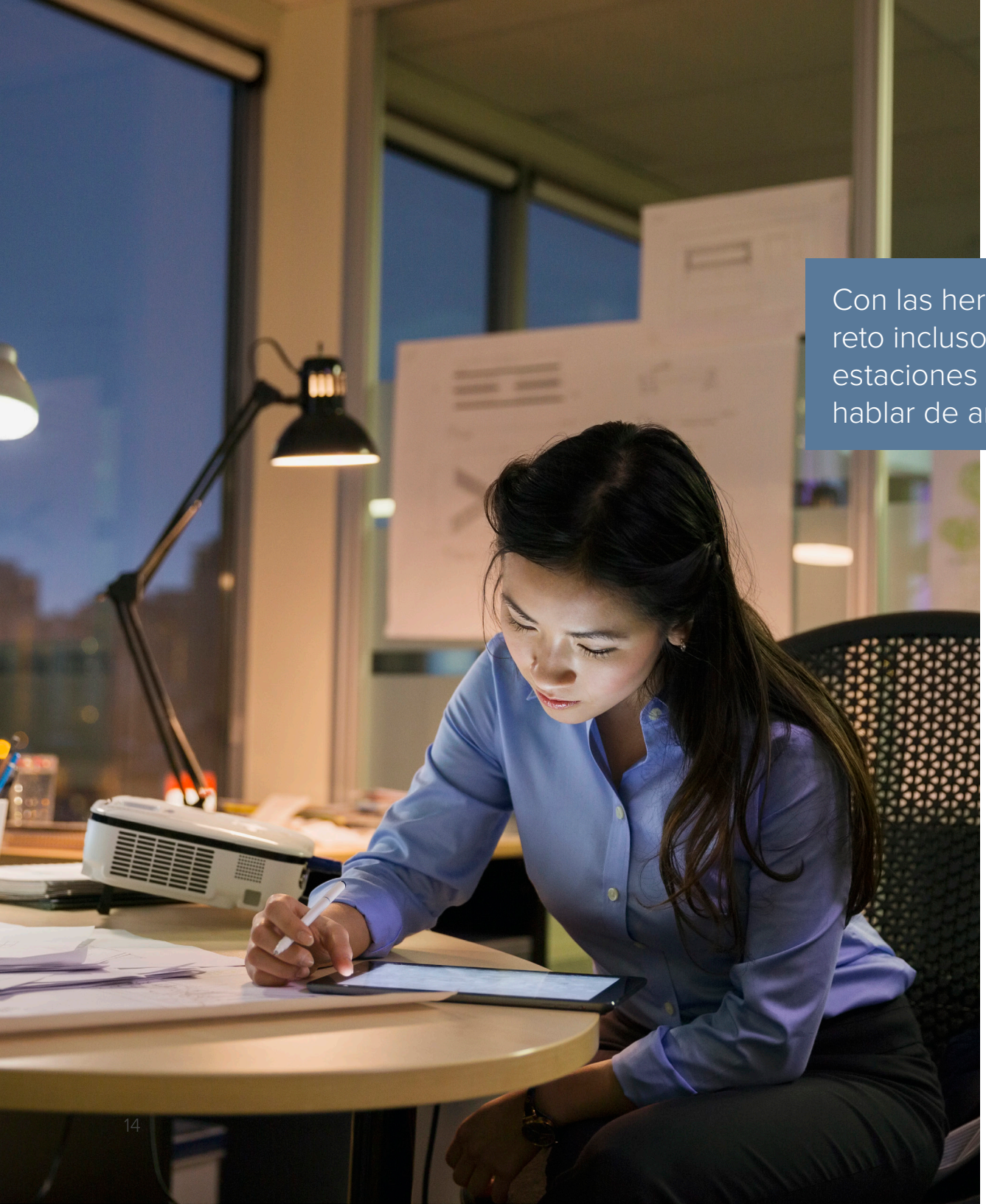
```
(get-acl <folder name>).access | ft
IdentityReference,FileSystemRights,AccessControlType,IsInherited,
InheritanceFlags -auto
```

En el tiempo que le lleve detectar el cambio en los permisos y ejecutar este comando, un atacante puede infiltrarse fácilmente en su red.

Es caro de varias formas

Hay que tener en cuenta los gastos. Lleva tiempo realizar todas estas tareas de análisis y administración de datos de los registros, lo que incrementa los costes de personal. Si utiliza una solución SIEM (security information and event management) o una herramienta de gestión de registros que le cobre por el procesamiento en función de los eventos por segundo o los megabytes al día, el gran volumen de eventos que genera el registro nativo puede suponerle una cantidad importante. Además, puede que





se esté gastando un dineral en almacenamiento también, especialmente si almacena los datos sin compresión.

> Con las herramientas nativas, es todo un reto incluso recopilar registros de todas sus estaciones de trabajo y portátiles, por no hablar de analizarlos de manera eficaz.

Sencillamente no puede obtener la visibilidad que necesita

Por último, existen grandes brechas. Para empezar, las tareas manuales por su propia naturaleza son propensas a despistes y errores humanos, lo que significa que podría pasar por alto perfectamente eventos críticos que sucedan en sus estaciones de trabajo. Además, los propios datos del registro están incompletos y fragmentados. Por ejemplo, he explicado cómo puede usar Sysmon para supervisar los eventos de creación de archivos, pero evidentemente la creación de archivos solo es una pequeña parte de la amplia tarea de auditar el sistema de archivos. Por desgracia, no hay realmente ninguna manera de realizar una auditoría del sistema de archivos de calidad (o muchas otras tareas críticas) con herramientas nativas.

Quest

Mejora de la seguridad de las estaciones de trabajo con InTrust y IT Security Search de Quest

Con las herramientas de terceros adecuadas, todo el mundo gana. Le permiten mejorar drásticamente la seguridad de las estaciones de trabajo al tiempo que reduce los costes de personal y almacenamiento. De forma conjunta, InTrust® y IT Security Search de Quest® le dan la visibilidad que necesita de la actividad de las estaciones de trabajo en una solución integrada y fácil de usar.

INTRUST

InTrust de Quest es una solución de gestión de registros de eventos que le permite recopilar, almacenar, buscar y analizar grandes cantidades de datos de TI de varias fuentes de datos, sistemas y dispositivos, de forma segura y eficiente. El repositorio de datos se ha indexado para unas búsquedas rápidas y probablemente ofrece la mejor compresión en el mercado: 20-1 con indexación y 40-1 sin ella.

Mejor aún, no tiene que ser un experto en registros de Windows para obtener información que se puede llevar a la práctica de InTrust,

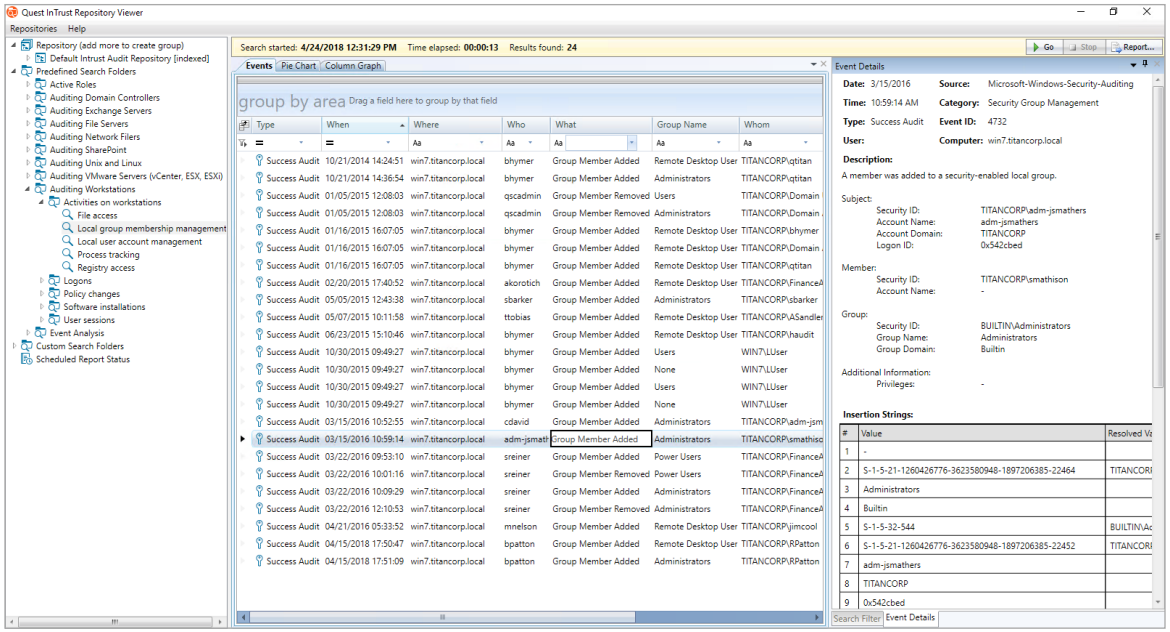


Figura 1. InTrust simplifica la gestión de registros de eventos para habilitar una mejor seguridad de las estaciones de trabajo al tiempo que se reducen los costes.

No tiene que ser un experto en registros de Windows para obtener información que se puede llevar a la práctica de InTrust.

Quest

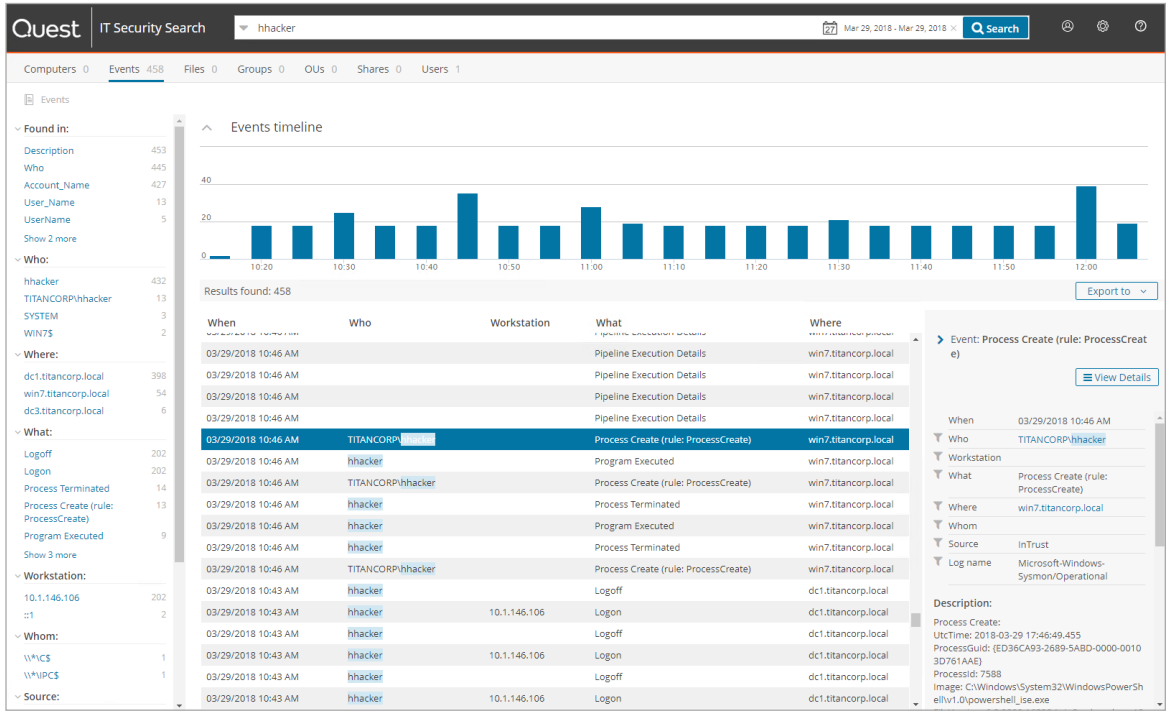


Figura 2. Revisión de datos de registro de una estación de trabajo Windows en IT Security Search

IT Security Search permite una respuesta a los incidentes de seguridad y un análisis forense rápidos entre varios sistemas en una vista unificada.

porque normaliza los datos críticos de quién, cuándo, qué, dónde y de quién a un formato fácil de leer por las personas, tal y como se ilustra en el informe integrado que se muestra en la figura 1.

Además de todo eso, InTrust ofrece tanto una implementación fácil como una capacidad de ampliación masiva: puede implementar agentes de InTrust en 5000 estaciones de trabajo en tan solo 20 minutos. InTrust puede ingerir unos 60 000 eventos por segundo y un servidor de InTrust puede supervisar más de 10 000 puntos finales. Si tiene más puntos finales, lo único que tiene que hacer es añadir otro servidor de InTrust y dividir la carga.

IT SECURITY SEARCH

IT Security Search de Quest es una solución gratuita incluida en InTrust, así como en otras soluciones de auditoría de Quest, entre las que se incluyen Enterprise Reporter, Change Auditor, Recovery Manager for AD y Active Roles. Extrae datos de diversos sistemas de TI y dispositivos en una vista unificada y ofrece un motor de búsqueda interactivo basado en la web y similar a Google para una respuesta a los incidentes de seguridad y un análisis forense rápidos, sin necesidad de formación o experiencia en registros.

En particular, puede revisar fácilmente los registros de la estación de trabajo de Windows críticos que hemos tratado. Puede filtrar los datos para eliminar ruido y dinamizar la investigación a medida que surja otra información, tal y como se ilustra en la figura 2.

Conclusión

Los atacantes no paran de mejorar sus tácticas y a menudo las estaciones de trabajo son su objetivo. Un uso sensato de los registros de seguridad, Sysmon y PowerShell puede ayudarle a detectar y bloquear los ataques, incluido el ransomware y otro malware, a tiempo para prevenir daños serios. InTrust y IT Security Search de Quest simplificarán el proceso de recopilar y analizar esos datos de registro, además de muchos otros datos de su entorno para reducir el tiempo de respuesta, la carga de trabajo de TI y los costes de almacenamiento.

Para obtener más información, consulte estos recursos:

- **In Trust:** quest.com/products/intrust
- **IT Security Search:** quest.com/products/it-security-search
- **Casos de los clientes:** techvalidate.com/portals/why-intrust

ACERCA DEL AUTOR

Brian Hymer es arquitecto de soluciones en Quest y un experto en el archivo de seguridad de Windows y la recuperación de bosques de Active Directory. Sus 30 años de experiencia en el sector de TI abarcan varios sectores, que incluyen el energético, el de ventas minoristas, la sanidad, el de los seguros y el financiero. Durante sus 18 años en Quest, se ha centrado en ayudar a los clientes de todo el mundo a implementar y usar los productos de Quest en un amplio abanico de entornos. Asimismo, ha presentado numerosos webinars en todo el mundo.

InTrust y IT Security Search de Quest le ayudan a reducir el tiempo de respuesta, la carga de trabajo de TI y los costes de almacenamiento.

ACERCA DE QUEST

En Quest, nos hemos propuesto resolver los problemas complejos con soluciones simples. Para ello, hemos adoptado una filosofía centrada en ofrecer un servicio y productos excepcionales, y en simplificar los negocios que se hagan con nosotros. Nuestro objetivo pasa por entregar tecnología que evite tener que elegir entre eficiencia y eficacia, lo que significa que tanto usted como su organización pueden dedicar menos tiempo a la administración de tecnología informática y más a innovar en la empresa.

Si tiene alguna duda sobre el uso que puede hacer de este material, póngase en contacto con nosotros:
www.quest.com

Ebook-Top3WorkstationLogs-InTrust-US-GM-ES-WL-33820

© 2018 Quest Software Inc. Todos los derechos reservados.

Esta guía contiene información registrada protegida por derechos de autor. El software descrito en esta guía se suministra bajo una licencia de software o un acuerdo de confidencialidad. Este software puede utilizarse o copiarse solo de conformidad con los términos del acuerdo aplicable. Ninguna parte de esta guía puede reproducirse ni transmitirse de ninguna forma ni por ningún medio, electrónico o mecánico, incluidas las fotocopias y las grabaciones, para ningún fin que no sea el uso personal del comprador, sin el permiso por escrito de Quest Software Inc.

La información incluida en este documento se facilita en relación con los productos de Quest Software. No se otorga ningún tipo de licencia, expresa o implícita, por la doctrina de los actos propios ni de ningún otro modo, sobre ningún tipo de derecho de propiedad intelectual por medio de este documento o en relación con la venta de productos Quest Software. CON LAS SALVEDADES ESTABLECIDAS EN LAS CONDICIONES QUE SE ESPECIFICAN EN EL ACUERDO DE LICENCIA PARA ESTE PRODUCTO, QUEST SOFTWARE NO ASUME NINGÚN TIPO DE RESPONSABILIDAD Y RECHAZA TODO TIPO DE GARANTÍA EXPRESA, IMPLÍCITA O LEGAL RELACIONADA CON SUS PRODUCTOS, INCLUIDAS, ENTRE OTRAS, LAS GARANTÍAS IMPLÍCITAS DE COMERCIABILIDAD, IDONEIDAD PARA UN PROPÓSITO EN PARTICULAR O DE NO VULNERACIÓN. EN NINGÚN CASO QUEST SOFTWARE SERÁ RESPONSABLE POR NINGÚN DAÑO DIRECTO, INDIRECTO, CONSECUENTE, PUNITIVO, ESPECIAL O INCIDENTAL (INCLUIDOS, SIN LIMITACIONES, LOS DAÑOS POR LUCRO CESANTE, INTERRUPCIÓN DE ACTIVIDADES COMERCIALES O PÉRDIDA DE INFORMACIÓN) QUE SURJA DEL USO O LA INCAPACIDAD DE USO DE ESTE DOCUMENTO, INCLUSO SI SE HA NOTIFICADO A QUEST SOFTWARE LA POSIBILIDAD DE DICHOS DAÑOS. Quest Software no formula ningún tipo de manifestación ni garantía con respecto a la exactitud o integridad del contenido de este documento y se reserva el derecho de realizar cambios a las especificaciones y descripciones de los productos en cualquier momento y sin previo aviso. Quest Software no se compromete a actualizar la información contenida en este documento.

Patentes

Quest Software se enorgullece de utilizar tecnología avanzada. Este producto puede estar sujeto a patentes o solicitudes de patentes en trámite. Para obtener la información más actualizada sobre las patentes aplicables a este producto, visite nuestro sitio web en www.quest.com/legal.

Marcas

Quest, InTrust y el logotipo de Quest son marcas y marcas registradas de Quest Software Inc. Para consultar la lista completa de las marcas de Quest, visite www.quest.com/legal/trademark-information.aspx. El resto de las marcas son propiedad de sus respectivos titulares.

Quest