Ciencia forense

Cloud Insights

NetApp
July 26, 2024

Tabla de contenidos

Ciencia forense

Análisis forenses: Toda la actividad

La página All Activity permite comprender las acciones que se realizan en las entidades del entorno Workload Security.

Examen de todos los datos de actividad

Haga clic en **Forensics > Activity Forensics** y haga clic en la ficha **All Activity** para acceder a la página All Activity. En esta página se proporciona una descripción general de las actividades de su entorno, en la que se destaca la siguiente información:

- Un gráfico que muestra *Activity History* (al que se accede por minuto/cada 5 minutos/cada 10 minutos en función del intervalo de tiempo global seleccionado)

  Puede ampliar el gráfico arrastrando un rectángulo del gráfico. Se cargará toda la página para mostrar el intervalo de tiempo ampliado. Cuando se amplía, se muestra un botón que permite al usuario alejar el zoom.

- Un gráfico de *Activity Types*. Para obtener datos del historial de actividades por tipo de actividad, haga clic en el enlace de etiqueta del eje X correspondiente.
- Un gráfico de actividad en *Entity Types*. Para obtener datos del historial de actividades por tipo de entidad, haga clic en el enlace de etiqueta del eje X correspondiente.
- Una lista de los datos *All Activity*

La tabla **All Activity** muestra la siguiente información. Tenga en cuenta que no todas estas columnas se muestran de forma predeterminada. Puede seleccionar las columnas que desea mostrar haciendo clic en el icono "Gear" .

- El **tiempo** se accedió a una entidad incluyendo el año, mes, día y hora del último acceso.
- El **usuario** que accedió a la entidad con un enlace a la "Información del usuario".
- La **actividad** que realizó el usuario. Los tipos admitidos son:
  - **Cambiar propiedad de grupo**: La propiedad de grupo es de archivo o carpeta que se cambia. Para obtener más información sobre la propiedad del grupo, consulte "este enlace."
  - **Cambiar propietario**: La propiedad del archivo o carpeta se cambia a otro usuario.
  - **Permiso de cambio**: Se ha cambiado el permiso de archivo o carpeta.
  - **Crear -** Crear archivo o carpeta.
  - **Eliminar**: Permite eliminar archivos o carpetas. Si se elimina una carpeta, se obtienen eventos *delete* para todos los archivos de esa carpeta y subcarpetas.
  - **Leer**: Se lee el archivo.
  - **Leer metadatos**: Sólo para activar la opción de supervisión de carpetas. Se generará al abrir una carpeta en Windows o al ejecutar “ls” dentro de una carpeta en Linux.
  - **Renombrar**: Permite cambiar el nombre del archivo o carpeta.
  - **Escribir**: Los datos se escriben en un archivo.

- **Escribir metadatos** - los metadatos del archivo se escriben, por ejemplo, el permiso cambiado.
- **Otro Cambio** - cualquier otro evento que no se describe anteriormente. Todos los eventos no asignados se asignan al tipo de actividad “otros cambios”. Aplicable a archivos y carpetas.

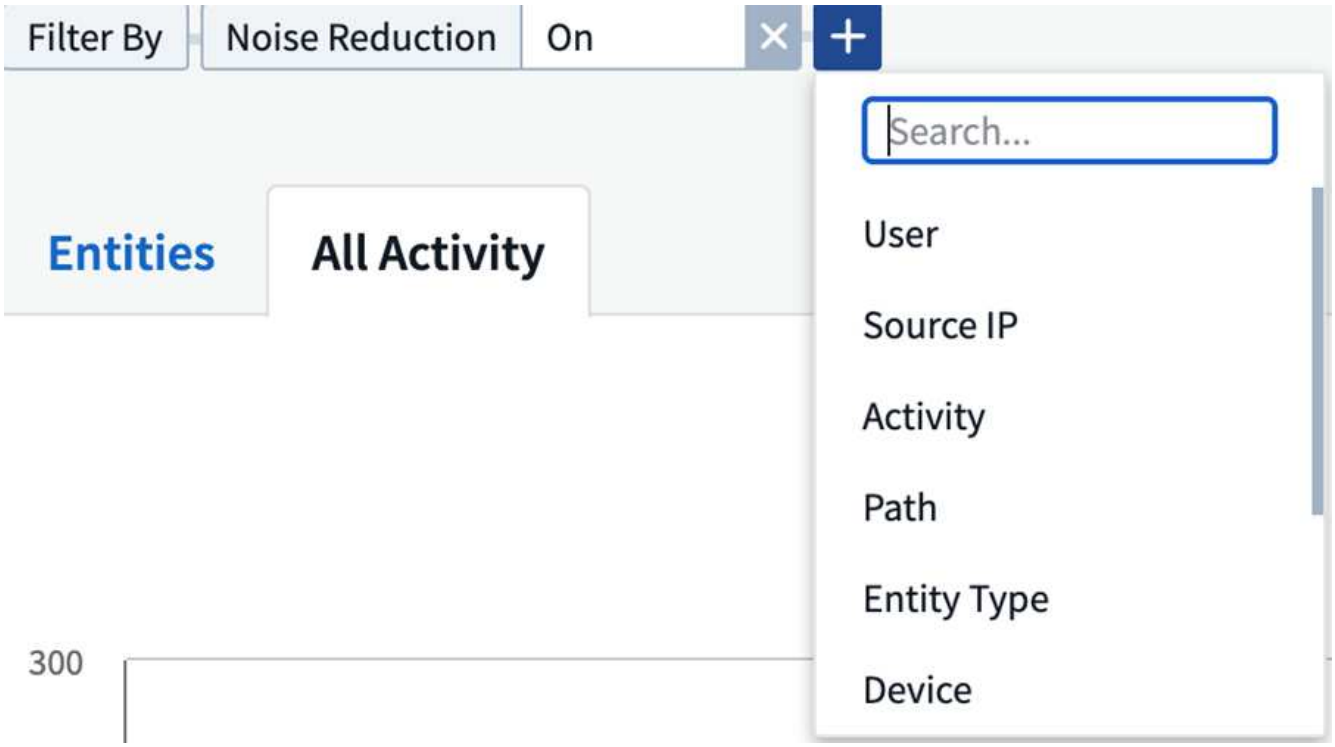
- El **camino** a la entidad con un enlace al "Datos de detalle de entidad"
- El **Tipo de entidad**, incluida la extensión de entidad (por ejemplo, archivo) (.doc, .docx, .tmp, etc.)
- El **dispositivo** donde residen las entidades
- El **Protocolo** utilizado para obtener eventos.
- La **Ruta original** se utiliza para cambiar el nombre de los eventos cuando se cambió el nombre del archivo original. Esta columna no está visible de forma predeterminada en la tabla. Utilice el selector de columna para agregar esta columna a la tabla.
- El **volumen** donde residen las entidades. Esta columna no está visible de forma predeterminada en la tabla. Utilice el selector de columna para agregar esta columna a la tabla.

Filtrado de datos del historial de actividades forenses

Existen dos métodos que se pueden utilizar para filtrar datos.

1. Pase el ratón sobre el campo de la tabla y haga clic en el icono de filtro que aparece. El valor se agrega a los filtros apropiados en la lista Top *Filter by*.
2. Filtre los datos escribiendo en el campo *Filter by*:

   Seleccione el filtro adecuado en el widget "Filtrar por" superior haciendo clic en el botón **[+]**:



   Introduzca el texto de búsqueda

   Pulse Intro o haga clic fuera del cuadro de filtro para aplicar el filtro.

Puede filtrar los datos de la actividad forense por los siguientes campos:

- El tipo **actividad**.
- **IP de origen** desde la que se accedió a la entidad. Debe proporcionar una dirección IP de origen válida entre comillas dobles, por ejemplo “10.1.1.1”. Los IP incompletos, como “10.1.1.**”, “10.1.**.*”, etc., no funcionarán.
- **Protocolo** para obtener actividades específicas del protocolo.
- **Nombre de usuario** del usuario que realiza la actividad. Debe proporcionar el nombre de usuario exacto para filtrar. La búsqueda con nombre de usuario parcial o nombre de usuario parcial con prefijo o sufijo ‘*’ no funcionará.
- **Reducción de ruido** para filtrar los archivos que el usuario crea en las últimas 2 horas. También se utiliza para filtrar archivos temporales (por ejemplo, archivos .tmp) a los que accede el usuario.

Los siguientes campos están sujetos a reglas de filtrado especiales:

- **Tipo de entidad**, utilizando la extensión de entidad (archivo)
- **Ruta** de la entidad
- **Usuario** realizando la actividad
- **Dispositivo** (SVM) donde residen las entidades
- **Volumen** donde residen las entidades
- La **Ruta original** se utiliza para cambiar el nombre de los eventos cuando se cambió el nombre del archivo original.

Los campos anteriores están sujetos a lo siguiente al filtrar:

- El valor exacto debe estar entre comillas: Ejemplo: "searchtext"
- Las cadenas con caracteres comodín no deben contener comillas: Ejemplo: searchtext, *searchtext*, filtrará las cadenas que contengan ‘reconfigurar texto’.
- Cadena con un prefijo, ejemplo: searchtext* , buscará cualquier cadena que comience por ‘reconfigurar texto’.

Ordenar datos del historial de actividades forenses

Puede ordenar los datos del historial de actividades por *Time, User, Source IP, Activity, Path* y *Entity Type*. De forma predeterminada, la tabla se ordena por orden *time* descendente, lo que significa que los datos más recientes se mostrarán primero. La ordenación está desactivada para los campos *Device* y *Protocol*.

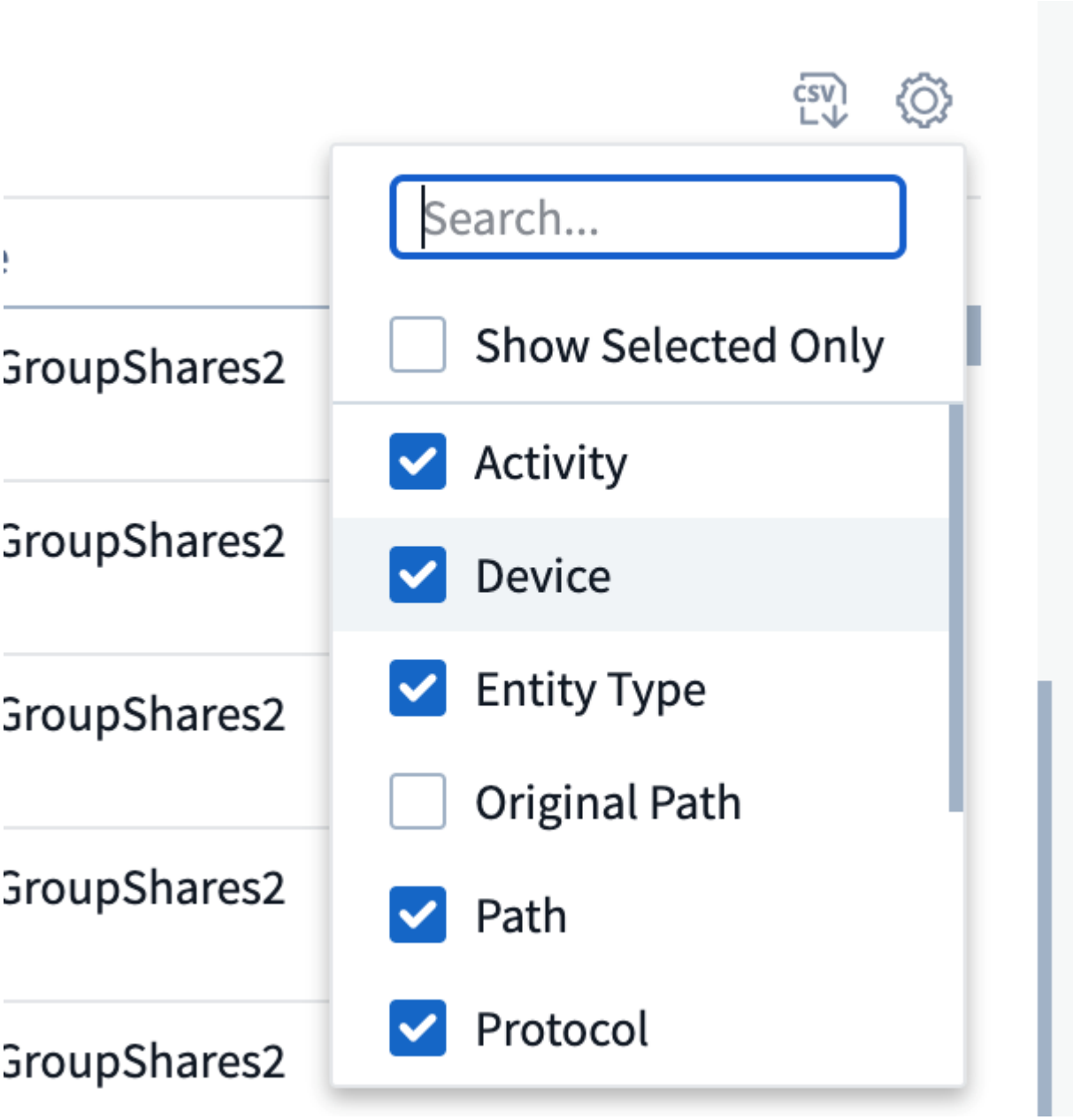
Exportando toda la actividad

Puede exportar el historial de actividades a un archivo .CSV haciendo clic en el botón *Export* situado encima de la tabla Historial de actividades. Tenga en cuenta que sólo se exportan los 100.000 registros principales. Dependiendo de la cantidad de datos, la exportación puede tardar desde unos segundos hasta varios minutos.

En */opt/netapp/cloudsecure/agent/export-script/* encontrará un script de ejemplo para extraer datos forenses a través de la API. Consulte el archivo Léame en esta ubicación para obtener más información sobre el script.

Selección de columna para toda la actividad

La tabla *All Activity* muestra las columnas SELECT de forma predeterminada. Para agregar, eliminar o cambiar las columnas, haga clic en el icono de engranaje situado a la derecha de la tabla y seleccione una de las columnas disponibles.



Retención del historial de actividades

El historial de actividad se conserva durante 13 meses para entornos de seguridad de carga de trabajo activa.

Aplicabilidad de los filtros en la página Forensics

Filtro	Qué hace	Ejemplo	¿En qué filtros es aplicable?	No aplicable para qué filtros	Resultado
* (Asterisk)	le permite buscar todo	Auto*03172022	Usuario, RUTA, Tipo de entidad, Tipo de dispositivo, volumen, Ruta original		Devuelve todos los recursos que empiezan por “Auto” y terminan por “03172022”

? (signo de interrogación)	le permite buscar un número específico de caracteres	AutoSabotageUser1_03172022?	Usuario, Tipo de entidad, dispositivo, volumen		Devuelve AutoSabotageUser1_03172022A, AutoSabotageUser1_03172022AB, AutoSabotageUser1_031720225, etc.
O.	permite especificar varias entidades	AutoSabotageUser1_03172022 o AutoRansomUser4_03162022	Usuario, dominio, nombre de usuario, RUTA, tipo de entidad, Dispositivo, ruta original		Devuelve cualquiera de los valores de AutoSabotageUser1_03172022 O AutoRansomUser4_03162022
NO	permite excluir el texto de los resultados de la búsqueda	NO es AutoRansomero4_03162022	Usuario, dominio, nombre de usuario, RUTA, tipo de entidad, RUTA original, volumen	Dispositivo	Devuelve todo lo que no empieza con"AutoRansomUser4_03162022"
Ninguno	Busca valores NULL en todos los campos	Ninguno	Dominio		devuelve los resultados en los que el campo de destino está vacío

Ruta / Búsqueda de ruta original

Los resultados de búsqueda con y sin / serán diferentes

/AutoDir1/AutoFile	Funciona
AutoDir1/AutoArchivo	No funciona
/AutoDir1/Autoarchivo (Dir1)	La subcadena parcial dir1 no funciona
"/AutoDir1/Autofile03242022"	La búsqueda exacta funciona
Auto*03242022	No funciona
AutoSabotageUser1_03172022?	No funciona
/AutoDir1/AutoFile03242022 O /AutoDir1/AutoFile03242022	Funciona
NO /AutoDir1/AutoFile03242022	Funciona
NO /AutoDir1	Funciona
NO /Autofile03242022	No funciona
*	Muestra todas las entradas

Resolución de problemas

Problema	Pruebe esto
En la tabla "todas las actividades", bajo la columna "Usuario", el nombre de usuario se muestra como: "ldap:HQ.COMPANYNAME.COM:S-1-5-21-3577637-1906459482-1437260136-1831817” o "ldap:default:80038003"	Las posibles razones pueden ser: 1. Aún no se ha configurado ningún recopilador de directorios de usuario. Para agregar uno, vaya a **Workload Security > Collectors > User Directory Collectors** y haga clic en **+User Directory Collector**. Seleccione *Active Directory* o *LDAP Directory Server*. 2. Se ha configurado un recopilador de directorios de usuarios, sin embargo se ha detenido o está en estado de error. Vaya a **Colectores > Colectores de directorios de usuarios** y compruebe el estado. Consulte la "Solución de problemas del recopilador de directorios de usuarios" de la documentación para obtener consejos sobre la solución de problemas. Una vez configurada correctamente, el nombre se resolverá automáticamente en 24 horas. Si todavía no se resuelve, compruebe si ha agregado el recopilador de datos de usuario correcto. Asegúrese de que el usuario forma parte del servidor de directorio de Active Directory/LDAP agregado.
Algunos eventos de NFS no se ven en la interfaz de usuario de.	Compruebe lo siguiente: 1. Se debe ejecutar un recopilador de directorios de usuarios para el servidor AD con el conjunto de atributos POSIX con el atributo unixid habilitado desde la interfaz de usuario. 2. Cualquier usuario que haga acceso a NFS debe verse cuando se busca en la página de usuario desde UI 3. Los eventos sin formato (los eventos para los que aún no se ha detectado el usuario) no son compatibles con NFS 4. El acceso anónimo a la exportación de NFS no se supervisará. 5. Asegúrese de que la versión NFS se utiliza en menor valor que NFS4.1.
Después de escribir algunas letras que contienen un carácter comodín como asterisco (*) en los filtros de las páginas Forensics *All Activity* o *entities*, las páginas se cargan muy lentamente.	Un asterisco (*) en la cadena de búsqueda busca todo. Sin embargo, las cadenas comodín iniciales como **<searchTerm>* o **<searchTerm>** resultarán en una consulta lenta. Para obtener un mejor rendimiento, utilice cadenas de prefijo en su lugar, en el formato *<searchTerm>** (en otras palabras, agregue el asterisco (*) *after* un término de búsqueda). Ejemplo: Utilice la cadena *testvolume**, en lugar de **testvolume* o **test*volume*. Utilice una búsqueda basada en prefijo para ver todas las actividades debajo de una carpeta determinada de forma recursiva (búsqueda jerárquica). por ejemplo, */path1/path2/path3* o *“/path1/path2/path3”* enumerará todas las actividades de forma recursiva bajo */path1/path2/path3*. También puede utilizar la opción “Agregar a filtro” en la pestaña Todas las actividades.

Encuentro un error de solicitud fallida con el código de estado 500/503 al utilizar un filtro de ruta.	Intente utilizar un rango de fechas más pequeño para filtrar registros.
La interfaz de usuario forense carga los datos lentamente cuando se utiliza el filtro *PATH*.	Si la ruta es */AAA/BBB/CCC/DDD*, entonces en lugar de buscar: AAA/BBB/CCC* O. AAA/BBB/C* Intente buscar: AAA/BBB/CCC/* Esta búsqueda debería permitir que los datos se carguen más rápido.

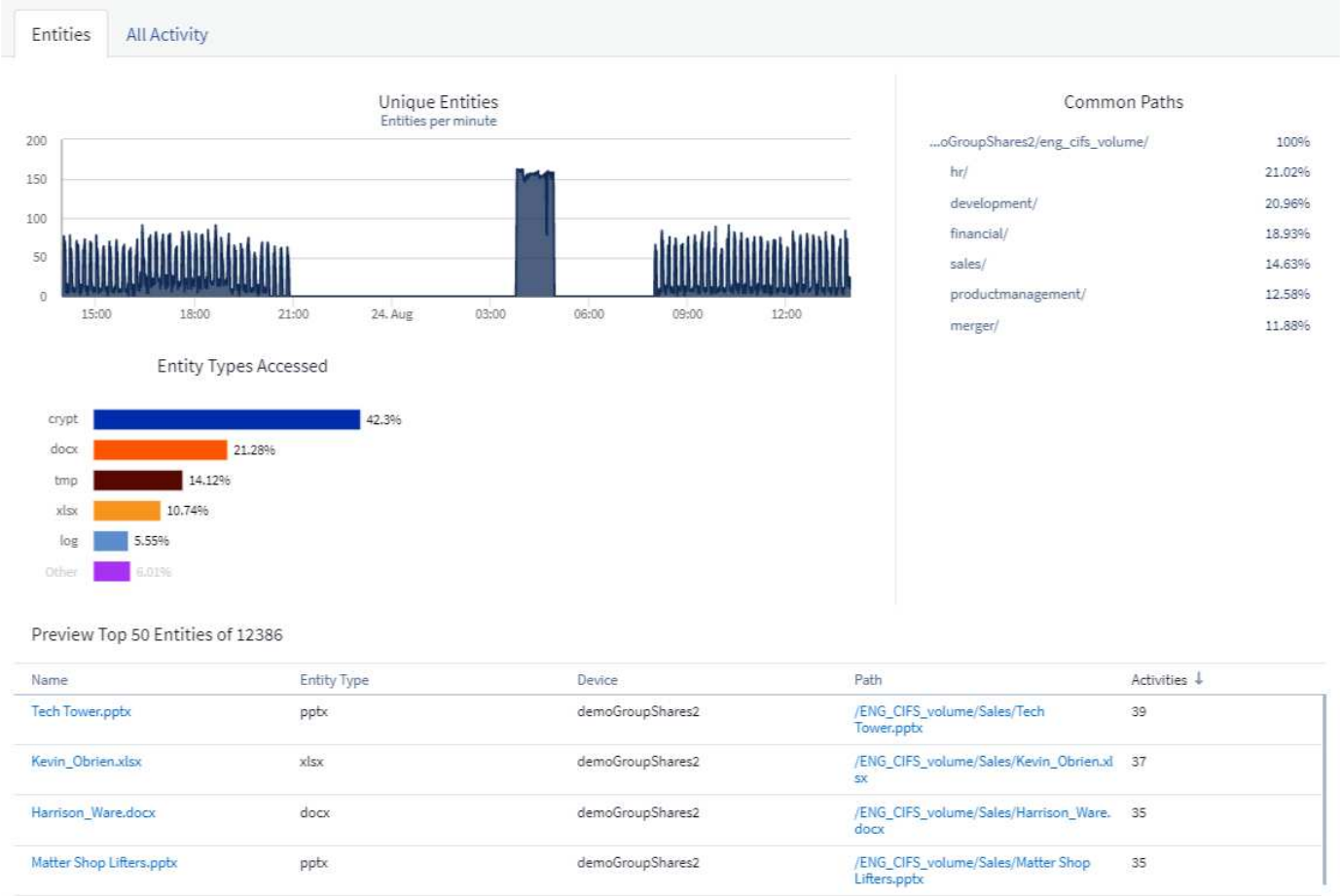
Página de entidades forenses

La página entidades Forensics proporciona información detallada sobre la actividad de la entidad en su entorno.

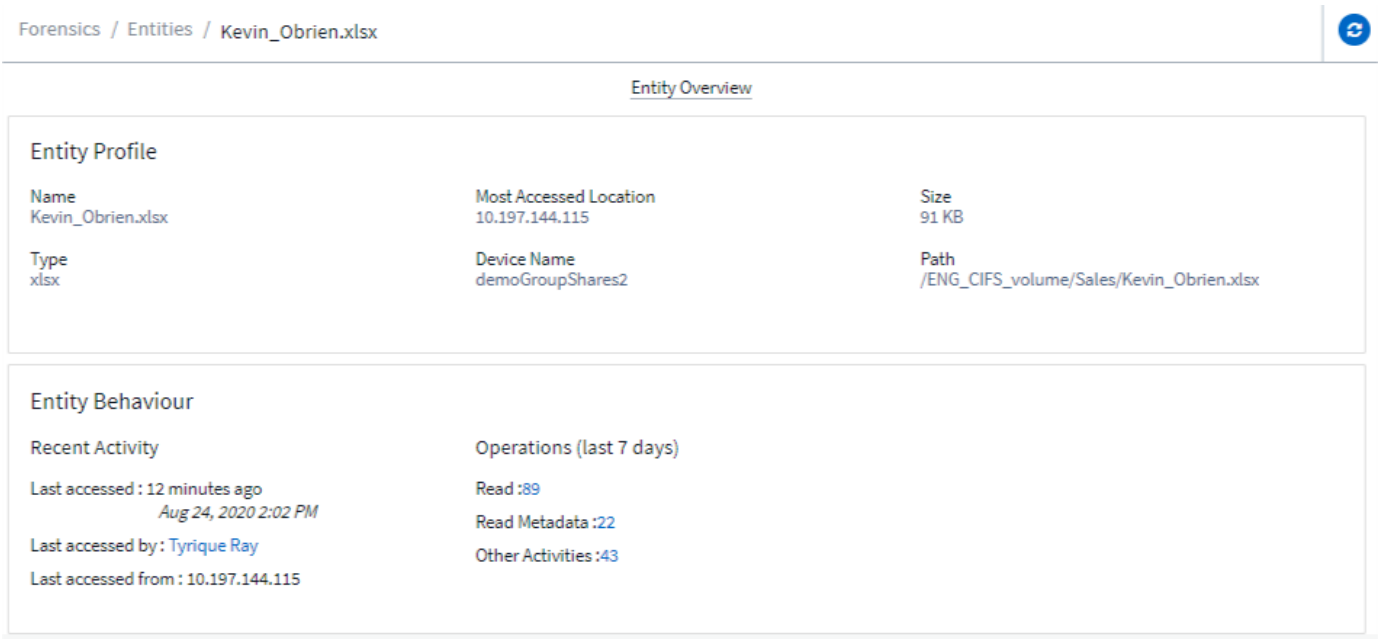
Examen de la Información de entidad

Haga clic en **Forensics > Activity Forensics** y haga clic en la ficha *Entities* para acceder a la página de entidades.

En esta página se proporciona información general sobre la actividad de las entidades del entorno, en la que se destaca la siguiente información: * Un gráfico que muestra *Unique Entities* al que se accede por minuto * un gráfico de *Entity Types accedidos* * un desglose de *Common paths* * una lista de las *Top 50 entidades* del número total de entidades



Al hacer clic en una entidad de la lista se abre una página de resumen de la entidad, mostrando un perfil de la entidad con detalles como nombre, tipo, nombre del dispositivo, dirección IP de la ubicación y ruta de acceso a los que se accede más, así como el comportamiento de la entidad, como el usuario, la dirección IP, y hora a la que se accedió por última vez a la entidad.



Descripción general del usuario forense

La información de cada usuario se proporciona en la sección Información general del usuario. Utilice estas vistas para comprender las características del usuario, las entidades asociadas y las actividades recientes.

Perfil de usuario

La información del perfil de usuario incluye la información de contacto y la ubicación del usuario. El perfil proporciona la siguiente información:

- Nombre del usuario
- Dirección de correo electrónico del usuario
- Administrador del usuario
- Contacto telefónico para el usuario
- Ubicación del usuario

Comportamiento del usuario

La información sobre el comportamiento del usuario identifica las actividades y operaciones recientes realizadas por el usuario. Esta información incluye:

- Actividad reciente
  - Última ubicación de acceso
  - Gráfico de actividades
  - Alertas
- Operaciones de los últimos siete días
  - Cantidad de operaciones

Actualizar intervalo

La lista de usuarios se actualiza cada 12 horas.

Política de retención

Si no se vuelve a actualizar, la lista de usuarios se conserva durante 13 meses. Después de 13 meses, los datos se eliminarán. Si se elimina el entorno Workload Security, se eliminan todos los datos asociados con el entorno.