取证
Cloud Insights

NetApp
June 28, 2024

目录

取证

取证—所有活动

所有活动页面可帮助您了解对工作负载安全环境中的实体执行的操作。

检查所有活动数据

单击 * 取证 > 活动取证 * ，然后单击 * 所有活动 * 选项卡以访问所有活动页面。此页面概述了您环境中的活动，并重点介绍了以下信息：

- 显示 *Activity History* （根据选定全局时间范围，每分钟 / 每 5 分钟 / 每 10 分钟访问一次）的图形

  您可以通过在图形中拖动一个方框来缩放图形。此时将加载整个页面以显示缩放的时间范围。放大后，将显示一个按钮，用户可以通过该按钮进行缩小。

- 活动类型图表。要按活动类型获取活动历史记录数据，请单击相应的 x 轴标签链接。
- 实体类型 _ 上的活动图表。要按实体类型获取活动历史记录数据，请单击相应的 x 轴标签链接。
- 所有活动数据的列表

_* 所有活动 * _ 表显示了以下信息。请注意，默认情况下并不会显示所有这些列。您可以单击齿轮图标来选择要显示的列  。

- 访问实体的 * 时间 * ，包括上次访问的年份，月份，日期和时间。
- 通过指向的链接访问实体的 * 用户 * "用户信息"。
- 用户执行的 * 活动 * 。支持的类型包括：
  - * 更改组所有权 * - 文件或文件夹的组所有权已更改。有关组所有权的详细信息，请参见 "此链接。"
  - * 更改所有者 * —文件或文件夹的所有权已更改为其他用户。
  - * 更改权限 * - 文件或文件夹权限已更改。
  - * 创建 * - 创建文件或文件夹。
  - * 删除 * - 删除文件或文件夹。如果删除某个文件夹，则会为该文件夹和子文件夹中的所有文件获取 *delete* 事件。
  - * 读取 * - 文件已读取。
  - * 读取元数据 * - 仅在启用文件夹监控选项时才显示。将在 Windows 上打开文件夹或在 Linux 中的文件夹内运行 "ls" 时生成。
  - * 重命名 * - 重命名文件或文件夹。
  - * 写入 * - 将数据写入文件。
  - * 写入元数据 * - 写入文件元数据，例如，权限已更改。
  - * 其他更改 * —上述未提及的任何其他事件。所有未映射的事件都会映射到 " 其他更改 " 活动类型。适用于文件和文件夹。
- 指向实体的 * 路径 * ，并带有指向的链接 "实体详细信息数据"

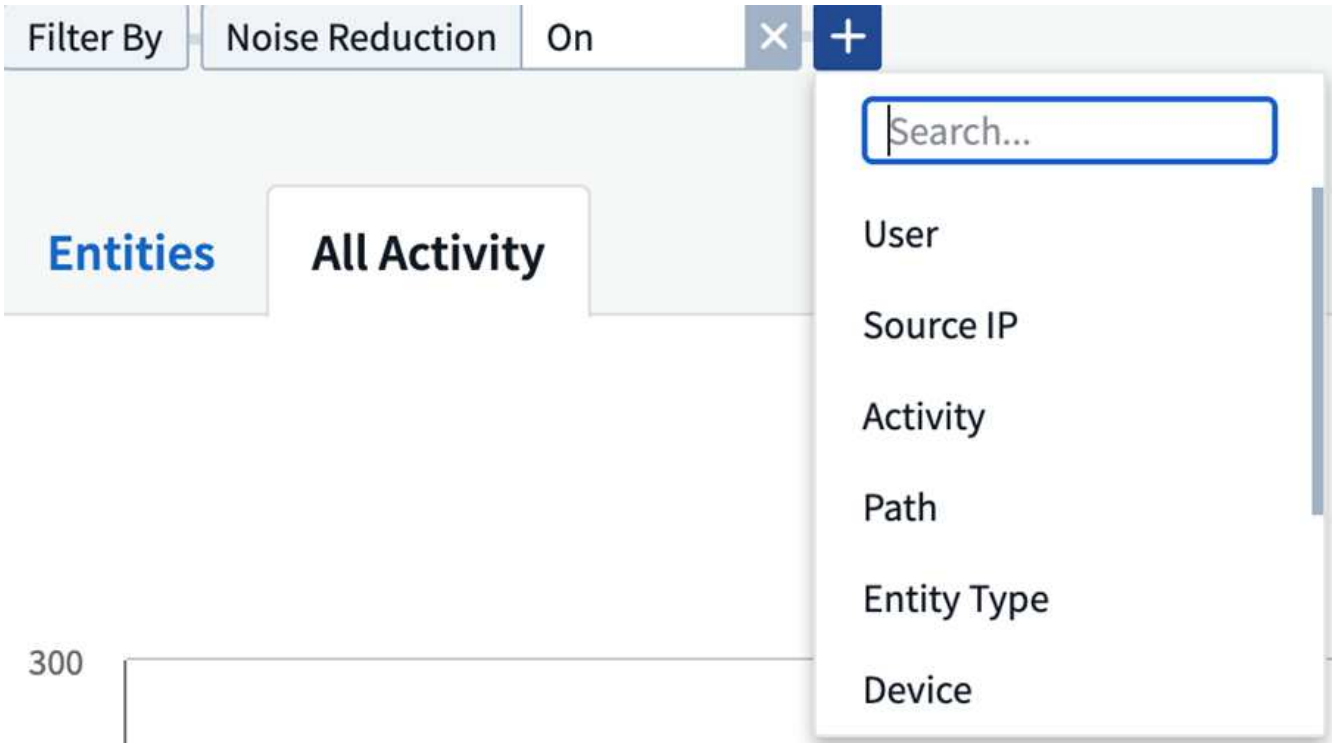
- 实体类型 * ，包括实体（即文件）扩展名（ .doc ， .docx ， .tmp 等）
- 实体所在的 * 设备 *
- 用于提取事件的 * 协议 * 。
- 重命名原始文件时用于重命名事件的 * 原始路径 * 。默认情况下，此列在表中不可见。使用列选择器将此列添加到表中。
- 实体所在的 * 卷 * 。默认情况下，此列在表中不可见。使用列选择器将此列添加到表中。

筛选取证活动历史记录数据

您可以使用两种方法筛选数据。

1. 将鼠标悬停在表中的字段上，然后单击显示的筛选器图标。该值将添加到 Top _Filter by" 列表中的相应筛选器中。
2. 通过在 _Filter by" 字段中键入来筛选数据：

   通过单击 * '+]* 按钮从顶部的 Filter by ' 小工具中选择相应的筛选器：



   输入搜索文本

   按 Enter 或单击筛选器框外侧以应用筛选器。

您可以按以下字段筛选取证活动数据：

- * 活动 * 类型。
- 访问实体的 * 源 IP* 。您必须使用双引号提供有效的源 IP 地址，例如 "10.1.1.1." 。诸如 "10.1.* " ， "10.1.* 。 * " 等不完整的 IP 将不起作用。

- 提取协议专用活动的 * 协议 * 。
- 执行活动的用户的 * 用户名 * 。您需要提供确切的用户名以进行筛选。使用部分用户名或部分用户名预先设置或后缀为‘ * ' 的搜索将不起作用。
- * 降噪 * 用于筛选用户在过去 2 小时内创建的文件。它还用于筛选用户访问的临时文件（例如 .tmp 文件）。

以下字段受特殊筛选规则的约束：

- * 实体类型 * ，使用实体（文件）扩展名
- 实体的 * 路径 *
- * 用户 * 正在执行活动
- 实体所在的 * 设备 * （ SVM ）
- 实体所在的 * 卷 *
- 重命名原始文件时用于重命名事件的 * 原始路径 * 。

筛选时，上述字段受以下限制：

- 确切值应在引号内：示例： "searchText"
- 通配符字符串不能包含任何引号：例如： searchText ， * searchText* 将筛选包含 ‘searchtext ' 的任何字符串。
- 带有前缀的字符串示例： searchText* 将搜索以 ‘searchtext ' 开头的任何字符串。

对取证活动历史记录数据进行排序

您可以按 *time* ，用户，源 *IP* ，活动，路径 _ 和 *_Entity Type* 对活动历史记录数据进行排序。默认情况下，此表按降序 *time* 顺序排序，这意味着将首先显示最新数据。已对 *Device* 和 *Protocol* 字段禁用排序。

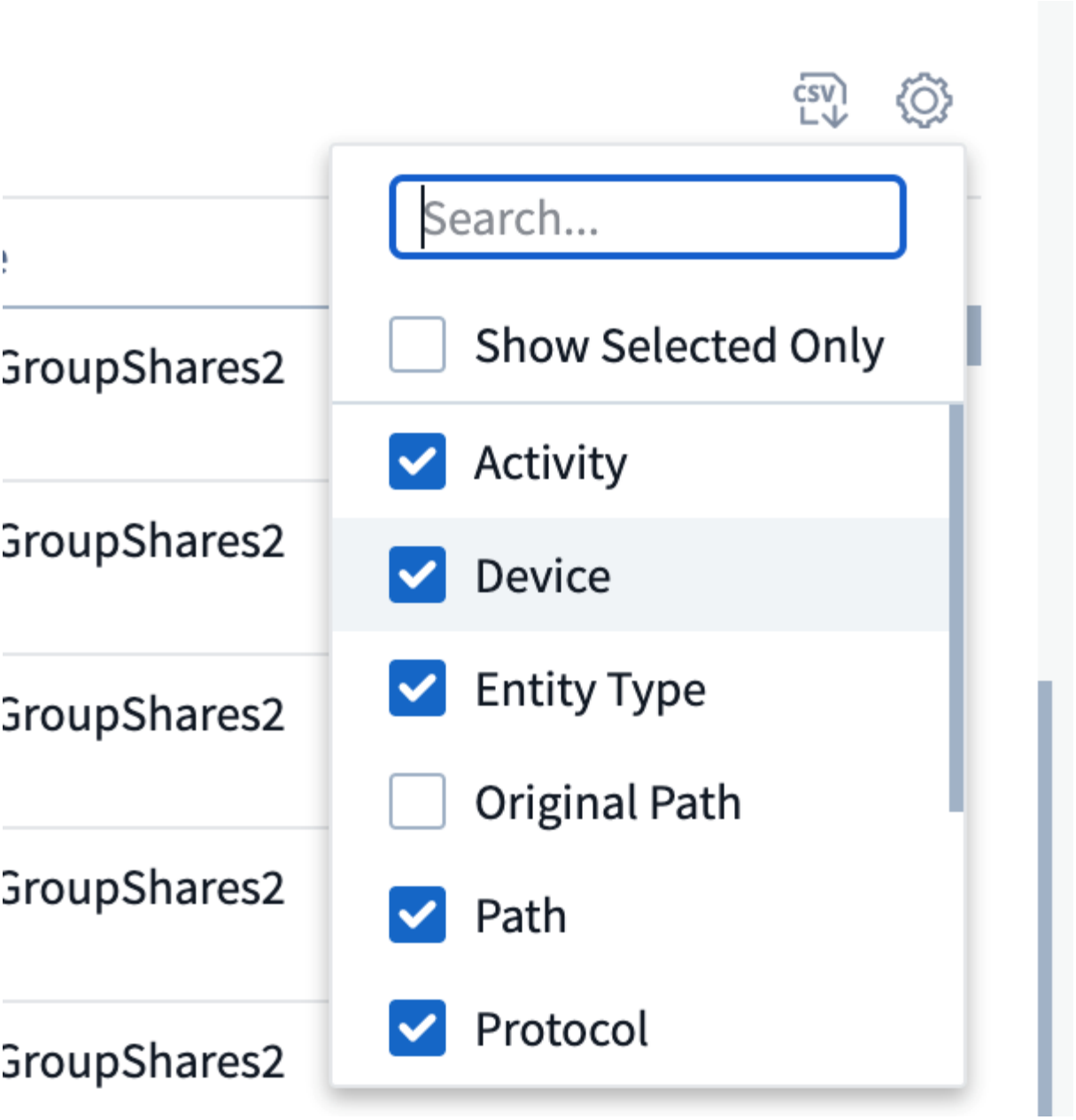
导出所有活动

您可以单击 "Activity History" 表上方的 *Export* 按钮将活动历史记录导出到 .CSV 文件。请注意、仅导出排名前10万位的记录。根据数据量的不同、导出可能需要几秒钟到几分钟才能完成。

用于通过API提取取证数据的示例脚本位于：/opt/NetApp/云 安全/agent/extr导 出脚本/_。有关该脚本的更多详细信息、请参见此位置的自述文件。

为所有活动选择列

默认情况下， *all activity* 表会显示 SELECT 列。要添加，删除或更改列，请单击表右侧的齿轮图标，然后从可用列列表中进行选择。



活动历史记录保留

对于活动工作负载安全环境、活动历史记录保留13个月。

取证页面中的筛选器适用性

筛选器	功能	示例	适用于哪些筛选器?	不适用于哪些筛选器	结果
* （星号）	用于搜索所有内容	Auto* 03172022	用户、路径、实体类型、设备类型、卷、 原始路径		返回以"Auto"开头、以"03172022 "结尾的所有资源

？（问号）	用于搜索特定数量的字符	AutoSabotageUser1_03172022?	用户、实体类型、设备、卷		返回AutoSabotageUser1_03172022A、AutoSabotageUser1_03172022AB、AutoSabotageUser1_03172 0225等
或	用于指定多个实体	AutoSabotageUser1_03172022 或AutoRansomUser4_03162022	用户、域、用户名、路径、实体类型、 设备、原始路径		返回任意AutoSabotageUser1_03172022 或AutoRansomUser4_03162022
不是	用于从搜索结果中排除文本	非AutoRansomUser4_03162022	用户、域、用户名、路径、实体类型、 原始路径、卷	设备	返回不以"AutoRansomUser4_03162022"开头的所有内容
无	在所有字段中搜索空值	无	domain		返回目标字段为空的结果

路径/原始路径搜索

使用和不使用/的搜索结果将有所不同

/AutoDir1/AutoFile	工作正常
AutoDir1/AutoFile	不起作用
/AutoDir1/AutoFile (Dir1)	dir1部分子字符串不起作用
"/AutoDir1/AutoFile03242022"	精确搜索有效
Auto* 03242022	不起作用
AutoSabotageUser1_03172022?	不起作用
/AutoDir1/AutoFile03242022 或/AutoDir1/AutoFile03242022	工作正常
非/AutoDir1/AutoFile03242022	工作正常
非/AutoDir1	工作正常
非/AutoFile03242022	不起作用
*	显示所有条目

故障排除

问题	请尝试此操作

在 "All actives" 表的 ‘User ' 列下，用户名显示为："ldap： HQ.COMPANYNAME.COM:S-1-5-21-3577637-1906459482-1437260136-1831817” 或 "ldap： default： 80038003"	可能的原因包括： 1.尚未配置任何用户目录收集器。要添加一个，请转到*工作负载安全性>收集器>用户目录收集器*，然后单击*+用户目录收集器*。选择 *Active Directory* 或 *LDAP Directory Server* 。 2. 已配置用户目录收集器，但它已停止或处于错误状态。请进入*收集器>用户目录收集器*并检查状态。请参见 "用户目录收集器故障排除" 文档中有关故障排除提示的章节。 正确配置后，此名称将在 24 小时内自动解析。 如果仍无法解决此问题，请检查您是否添加了正确的用户数据收集器。确保用户确实属于添加的 Active Directory/LDAP 目录服务器。
UI 中未显示某些 NFS 事件。	检查以下内容： 1.运行设置了 POSIX 属性的 AD 服务器的用户目录收集器时，应通过 UI 启用 unixid 属性。2. 在 UI 3 的用户页面中搜索时，应看到执行 NFS 访问的任何用户。NFS 4 不支持原始事件（尚未发现用户的事件）。不会监控对 NFS 导出的匿名访问。5. 确保使用的 NFS 版本低于 NFS4.1 。
在Forsics_All Activity_或_indices_页面的筛选器中键入包含通配符(如星号(*))的某些字母后、页面加载速度非常慢。	搜索字符串中的星号(*)将搜索所有内容。但是，诸如_*<searchTerm>_或_*<searchTerm>*之类的前导通配符字符串会导致查询速度较慢。 要获得更好的性能，请改用前缀字符串，格式为<searchTerm>*_(换言之，请附加星号_(*)_after_搜索词)_。 示例：使用字符串_*testvolume**，而不是_*testvolume_或_*test*volume_。 使用基于前缀的搜索以递归方式查看给定文件夹下的所有活动(分层搜索)。例如、*/path1/path2/path3_*或"/path1/path2/path3"将以递归方式列出/path1/path2/path3_下的所有活动。 或者、使用所有活动选项卡下的"Add to Filter"(添加到筛选器)选项。
使用路径筛选器时遇到"Request failed with status code 500/503"错误。	请尝试使用较小的日期范围来筛选记录。
使用_path_筛选器时、取证UI加载数据的速度较慢。	如果路径为_/AAA/BBB/CCC/DDD_、则不要搜索： AAA/BBB/CCC* 或 AAA/BBB/C/* 尝试搜索： AAA/BBB/CCC/* 通过此搜索、可以更快地加载数据。

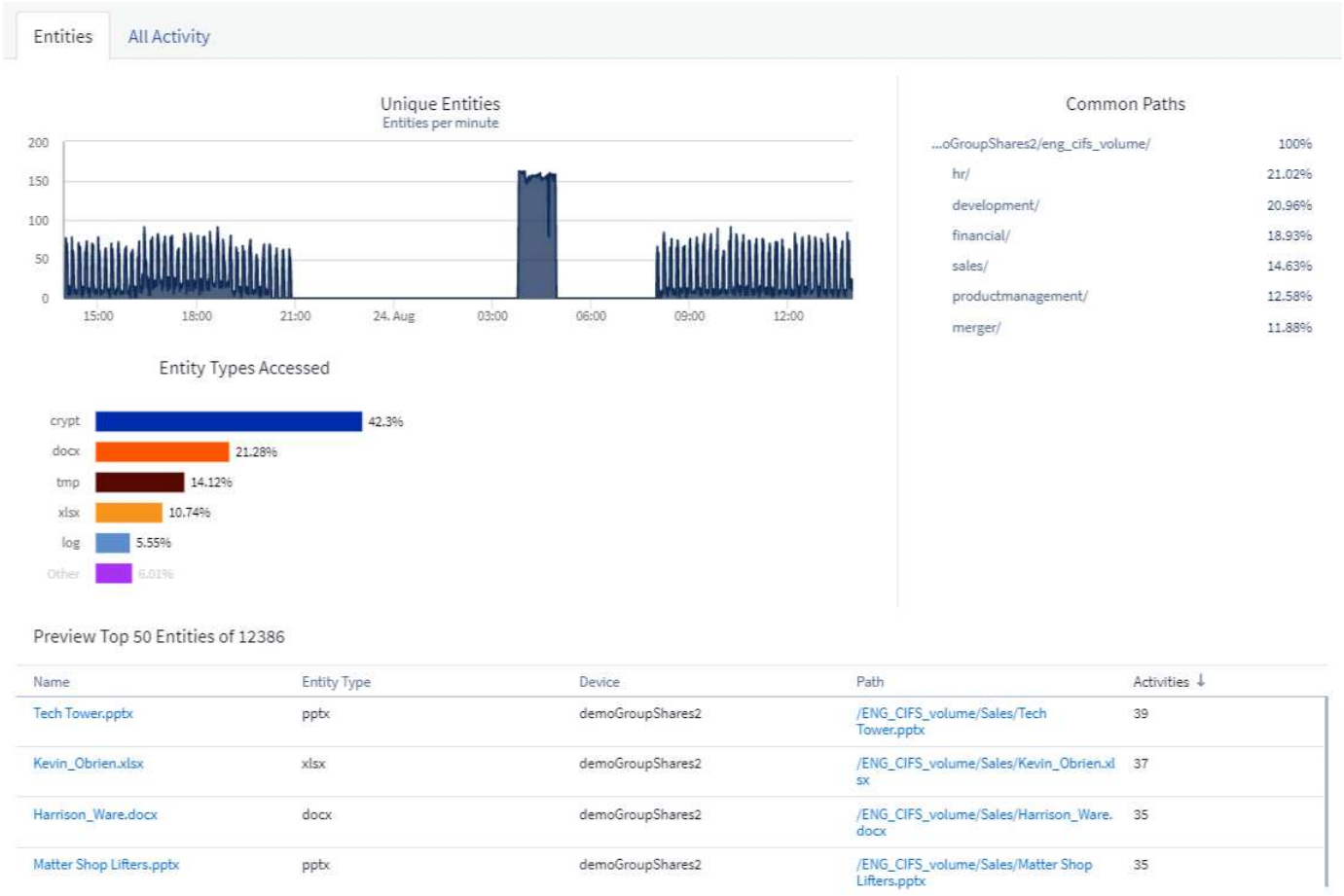
取证实体页面

" 取证实体 " 页面提供了有关环境中实体活动的详细信息。

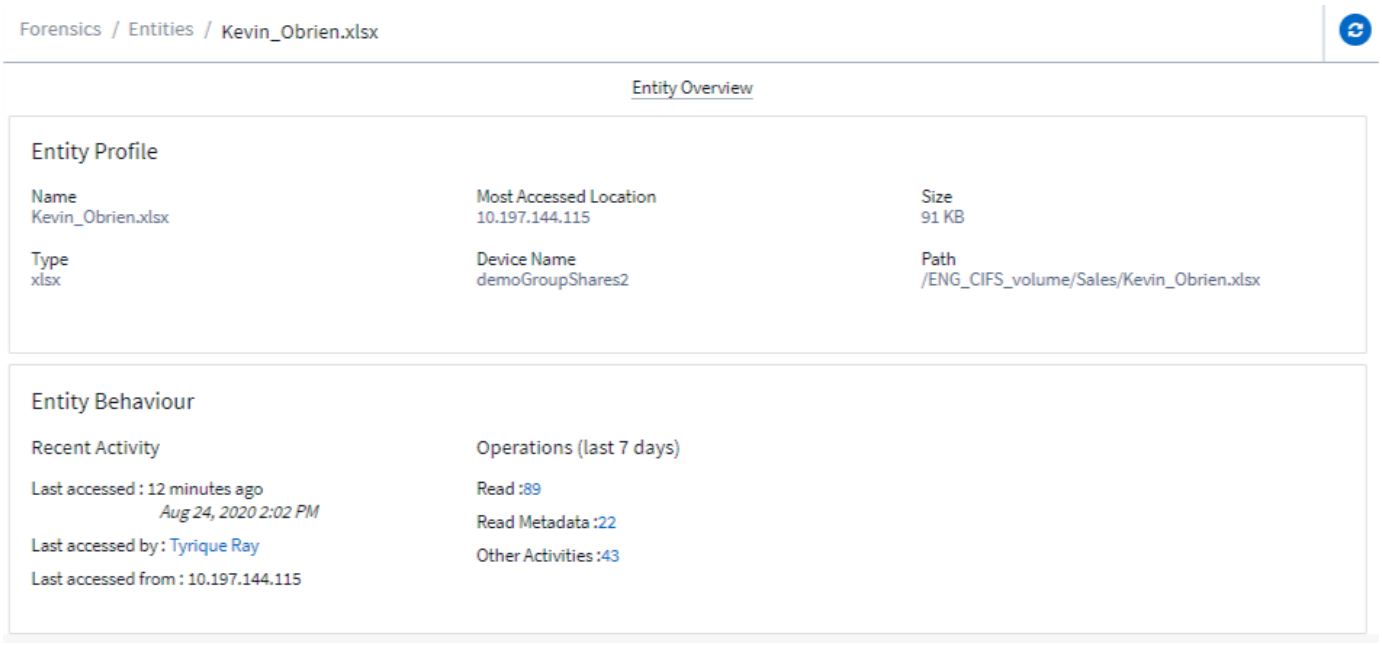
检查实体信息

单击 * 取证 > 活动取证 * ，然后单击 *entities* 选项卡以访问实体页面。

此页面简要介绍了环境中的实体活动，并重点介绍了以下信息： * 显示每分钟访问的 *unique entities* 的图形 * 已访问的 _Entity types 的图表 * _ 通用路径 _ 的细分 * 在实体总数中排名前 50 位的实体 _ 的列表



单击列表中的某个实体将打开该实体的概述页面，其中显示了该实体的配置文件，其中包含名称，类型，设备名称，最常访问的位置 IP 和路径等详细信息，以及用户， IP ， 和上次访问实体的时间。



取证用户概述

用户概述中提供了每个用户的信息。使用这些视图可以了解用户特征，关联实体和近期活动。

用户配置文件

用户配置文件信息包括用户的联系信息和位置。配置文件提供以下信息：

- 用户的名称
- 用户的电子邮件地址
- 用户的经理
- 用户的电话联系人
- 用户的位置

用户行为

用户行为信息用于标识用户最近执行的活动和操作。这些信息包括：

- 近期活动
  - 上次访问位置
  - 活动图
  - 警报
- 过去七天的操作
  - 操作数

刷新间隔

用户列表每 12 小时刷新一次。

保留策略

如果未再次刷新，则用户列表将保留 13 个月。13 个月后，数据将被删除。如果删除了工作负载安全环境、则会删除与该环境关联的所有数据。