법의학

Data Infrastructure Insights

NetApp
January 10, 2025

목차

법의학

법의학 - 모든 활동

모든 활동 페이지에서는 워크로드 보안 환경의 엔터티에 대해 수행되는 작업을 이해할 수 있습니다.

모든 활동 데이터 검토

Forensics > Activity Forensics * 를 클릭하고 * All Activity * 탭을 클릭하여 All Activity 페이지에 액세스합니다. 이 페이지에서는 테넌트의 활동에 대한 개요를 제공하고 다음 정보를 강조합니다.

- 활동 기록 _ 을(를) 보여주는 그래프(선택한 글로벌 시간 범위 기준)

  그래프에서 사각형을 드래그하여 그래프를 확대할 수 있습니다. 확대/축소된 시간 범위를 표시하기 위해 전체 페이지가 로드됩니다. 확대하면 사용자가 축소할 수 있는 버튼이 표시됩니다.

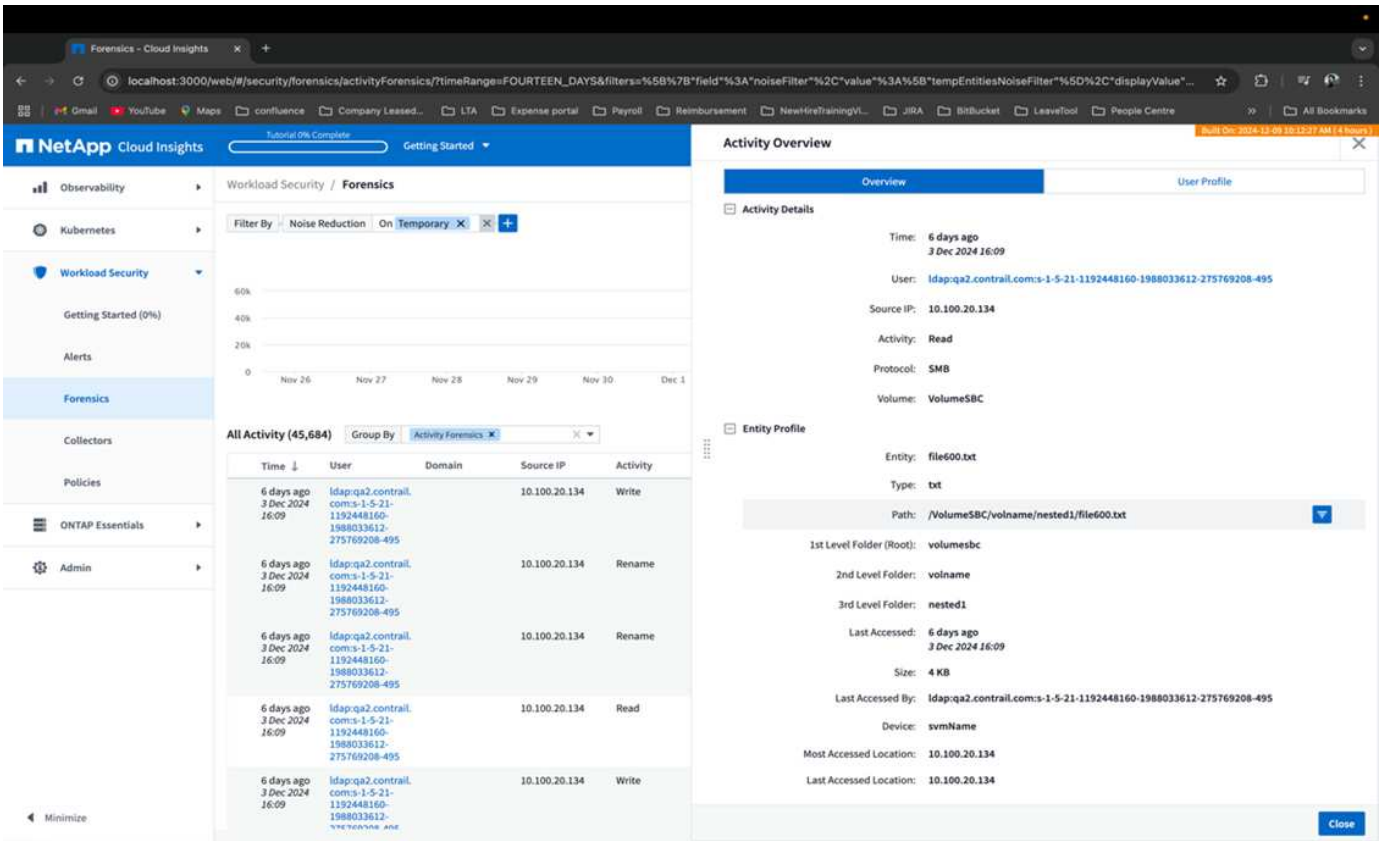
- 모든 활동 데이터 목록
- 그룹별 드롭다운은 사용자, 경로, 엔티티 유형 등을 기준으로 활동을 그룹화할 수 있는 옵션을 제공합니다
- 테이블 위에 있는 공통 경로 버튼을 클릭하면 엔터티 경로 세부 정보가 있는 슬라이드 아웃 패널을 볼 수 있습니다.

_ * All Activity * _ 표에는 다음 정보가 표시됩니다. 이러한 열 중 일부만 기본적으로 표시됩니다. "기어" 아이콘을 클릭하여 표시할 열을 선택할 수 있습니다.

- 마지막 액세스의 연도, 월, 일 및 시간을 포함하여 엔티티에 액세스한 * 시간.
- 슬라이드 아웃 패널로 에 대한 링크를 사용하여 엔티티에 액세스한 * 사용자 *"사용자 정보".
- 사용자가 수행한 * 작업 *. 지원되는 유형은 다음과 같습니다.
  - * 그룹 소유권 변경 * - 파일 또는 폴더의 그룹 소유권이 변경됩니다. 그룹 소유권에 대한 자세한 내용은 을 참조하십시오 "이 링크."
  - * 소유자 변경 * - 파일 또는 폴더의 소유권이 다른 사용자로 변경됩니다.
  - * 권한 변경 * - 파일 또는 폴더 권한이 변경됩니다.
  - * 생성 * - 파일 또는 폴더를 생성합니다.
  - * 삭제 * - 파일 또는 폴더를 삭제합니다. 폴더가 삭제되면 해당 폴더 및 하위 폴더에 있는 모든 파일에 대해 _DELETE_events가 획득됩니다.
  - * 읽기 * - 파일을 읽습니다.
  - * 메타데이터 읽기 * - 폴더 모니터링 활성화 옵션만 해당. Windows에서 폴더를 열거나 Linux의 폴더 내에서 "ls"를 실행하면 생성됩니다.
  - * 이름 바꾸기 * - 파일 또는 폴더의 이름을 바꿉니다.
  - * 쓰기 * - 데이터가 파일에 기록됩니다.
  - * 메타데이터 쓰기 * - 파일 메타데이터는 예를 들어 권한이 변경되었습니다.
  - * 기타 변경 * - 위에 설명되지 않은 기타 이벤트. 매핑되지 않은 모든 이벤트는 "기타 변경" 작업 유형에 매핑됩니다. 파일 및 폴더에 적용됩니다.

- Path * 는 _entity_path 입니다.
- 첫 번째 레벨 폴더(루트) * 는 소문자인 엔터티 경로의 루트 디렉토리입니다.
- 2nd Level Folder * 는 소문자인 엔터티 경로의 두 번째 레벨 디렉토리입니다.
- 세 번째 수준 폴더 * 는 소문자로 엔터티 경로의 세 번째 수준 디렉터리입니다.
- 4단계 폴더 * 는 소문자인 엔터티 경로의 상위 레벨 디렉토리입니다.
- 엔티티(예: 파일) 확장자를 포함한 * 엔티티 유형 *. doc, .docx, .tmp 등.
- 요소가 상주하는 * 장치 *.
- 이벤트를 가져오는 데 사용되는 * 프로토콜 * 입니다.
- 원본 파일의 이름을 바꿀 때 이름 바꾸기 이벤트에 사용되는 * Original Path * 입니다. 이 열은 기본적으로 표에 표시되지 않습니다. 열 선택기를 사용하여 이 열을 테이블에 추가합니다.
- 요소가 있는 * 볼륨 *. 이 열은 기본적으로 표에 표시되지 않습니다. 열 선택기를 사용하여 이 열을 테이블에 추가합니다.

테이블 행을 선택하면 한 탭에 사용자 프로필이 있고 다른 탭에 활동 및 엔터티 개요가 있는 슬라이드 아웃 패널이 열립니다.



default_Group by_method는 _ 활동 포렌식 _ 입니다. 예를 들어, 엔티티 유형 과 같은 다른_Group By_method 를 선택하면 entity_Group By_table 이 표시됩니다. 선택하지 않으면 *Group by* * All * 가 표시됩니다.

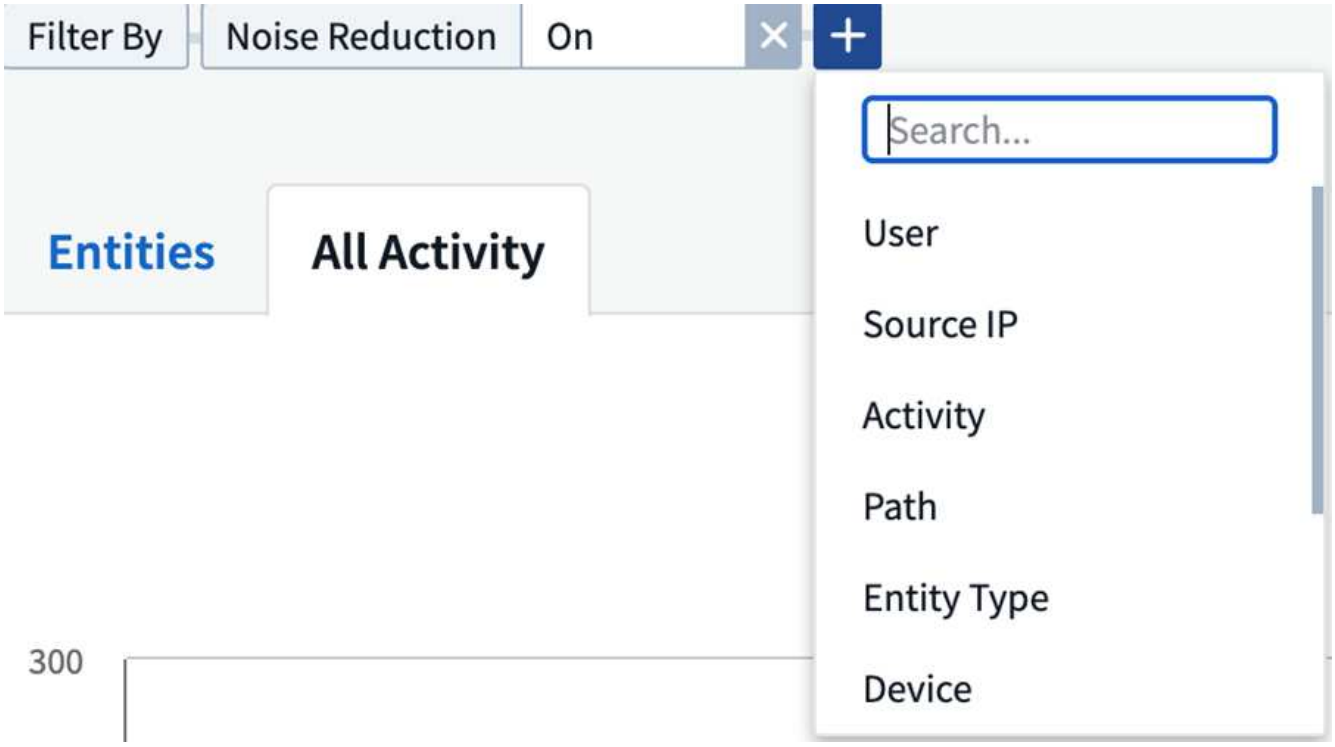
- 작업 수는 하이퍼링크로 표시됩니다. 이 항목을 선택하면 선택한 그룹이 필터로 추가됩니다. 활동 표는 해당 필터에 따라 업데이트됩니다.
- 필터를 변경하거나 시간 범위를 변경하거나 화면을 새로 고치면 필터를 다시 설정하지 않으면 필터링된 결과로 돌아갈 수 없습니다.

Forensic 활동 기록 데이터 필터링

데이터를 필터링하는 데 사용할 수 있는 두 가지 방법이 있습니다.

- 필터는 슬라이드 아웃 패널에서 추가할 수 있습니다. 이 값은 top_Filter by_list의 해당 필터에 추가됩니다.
- Filter by_필드에 입력하여 데이터를 필터링합니다.

  상단 '필터 기준' 위젯에서 * [+] * 버튼을 클릭하여 적절한 필터를 선택합니다.



  검색 텍스트를 입력합니다

  Enter 키를 누르거나 필터 상자 바깥쪽을 클릭하여 필터를 적용합니다.

다음 필드를 사용하여 Forensic Activity 데이터를 필터링할 수 있습니다.

- Activity * 유형.
- 엔터티에 액세스한 소스 IP * 입니다. 유효한 소스 IP 주소를 큰따옴표로 묶어야 합니다(예: “10.1.1.1.”). “10.1.1.**”, “10.1.**.*” 등과 같은 불완전한 IP는 작동하지 않습니다.
- 프로토콜 특정 작업을 가져오려면 * 프로토콜 * 을 선택합니다.
- * 작업을 수행하는 사용자의 사용자 이름 * 입니다. 필터링할 정확한 사용자 이름을 입력해야 합니다. 부분 사용자 이름 또는 접두사가 붙은 부분 사용자 이름 또는 ' * '로 접미사를 바꾼 검색은 작동하지 않습니다.
- * 노이즈 감소 * - 사용자가 최근 2시간 내에 생성한 파일을 필터링합니다. 사용자가 액세스하는 임시 파일(예: .tmp 파일)을 필터링하는 데에도 사용됩니다.
- 활동을 수행하는 사용자의 * 도메인 *. 필터링할 * 정확한 도메인 * 을 제공해야 합니다. 부분 도메인 또는 부분 도메인 앞에 와일드카드(' * ')가 있거나 접미사가 붙은 부분 도메인 검색은 작동하지 않습니다. _None_은(는) 누락된 도메인을 검색하기 위해 지정할 수 있습니다.

다음 필드에는 특수 필터링 규칙이 적용됩니다.

- **Entity Type**, entity(파일) 확장자를 사용하는 경우 - 따옴표 안에 정확한 엔터티 유형을 지정하는 것이 좋습니다. 예: _ "txt" _.
- *엔터티의 경로 * - 디렉터리 경로 필터(경로 문자열 / 로 끝나는)를 최대 4개까지 입력하여 더 빠른 결과를 얻을 수 있습니다. 예: *"/home/userX/nested1/nested2/"*. 자세한 내용은 아래 표를 참조하십시오.
- 1단계 폴더(루트) - 엔티티 경로의 루트 디렉토리입니다. 예를 들어, 엔터티 경로가 /home/userX/nested1/nested2/이면 home 또는 "home"을 사용할 수 있습니다.
- 두 번째 수준 폴더 - 엔터티 경로 필터의 두 번째 수준 디렉터리입니다. 예를 들어, 엔터티 경로가 /home/userX/nested1/nested2/이면 userX 또는 "userX"를 사용할 수 있습니다.
- 3rd 레벨 폴더 – 엔티티 경로 필터의 세 번째 레벨 디렉토리입니다.
- 예를 들어, 엔터티 경로가 /home/userX/nested1/nested2/이면 nested1 또는 "nested1"을 사용할 수 있습니다.
- 4th Level Folder - 엔티티 경로 필터의 디렉토리 4번째 수준 디렉토리입니다. 예를 들어, 엔터티 경로가 /home/userX/nested1/nested2/이면 nested2 또는 "nested2"를 사용할 수 있습니다.
- * 사용자 * 활동 수행 - 따옴표 안에 정확한 사용자를 지정하는 것이 좋습니다. 예: _ "관리자" _.
- 엔터티가 상주하는 * 장치 * (SVM
- * 볼륨 * 요소가 상주하는 곳입니다
- 원본 파일의 이름을 바꿀 때 이름 바꾸기 이벤트에 사용되는 * Original Path * 입니다.

필터링 시 위의 필드는 다음 항목의 대상이 됩니다.

- 정확한 값은 따옴표 안에 있어야 합니다. 예: "searchText"
- 와일드카드 문자열은 따옴표를 포함하지 않아야 합니다. 예: searchText, * searchText*, 는 'earchtext'가 포함된 문자열을 필터링합니다.
- 접두사가 있는 문자열(예: searchText*)은 'earchtext'로 시작하는 문자열을 검색합니다.

활동 포렌식 필터 예:

사용자가 필터 식을 적용했습니다	예상 결과	성능 평가	설명
경로="/home/userX/nested1/nested2/"	지정된 디렉토리 아래의 모든 파일과 폴더의 반복적인 조회	빠릅니다	디렉터리 검색은 최대 4개의 디렉터리가 빠릅니다.
경로="/home/userX/nested1/"	지정된 디렉토리 아래의 모든 파일과 폴더의 반복적인 조회	빠릅니다	디렉터리 검색은 최대 4개의 디렉터리가 빠릅니다.
경로 = "/home/userX/nested1/test"	지정된 경로 regex 아래의 모든 파일과 폴더의 반복적인 조회(테스트 * 는 파일 또는 디렉토리 또는 둘 다를 의미할 수 있음)	느린 속도	디렉터리+파일 정규식 검색은 디렉터리 검색보다 검색 속도가 느립니다.
경로="/home/userX/nested1/nested2/nested3/"	지정된 디렉토리 아래의 모든 파일과 폴더의 반복적인 조회	느린 속도	4개 이상의 디렉터리 검색은 검색 속도가 느립니다.

사용자가 필터 식을 적용했습니다	예상 결과	성능 평가	설명
기타 모든 비 경로 기반 필터. 사용자 및 엔터티 유형 필터는 따옴표로 묶는 것이 좋습니다. 예: User="Administrator" Entity Type="txt"		빠릅니다	

참고:

1. 선택한 시간 범위가 3일 이상인 경우 모든 활동 아이콘 옆에 표시된 활동 수는 30분으로 반올림됩니다. 예: _9월 1일 오전 10시 15분부터 9월 7일 오전 10시 15분까지의 시간 범위에는 9월 1일 오전 10시부터 9월 7일 오전 10시 30분까지 활동 카운트가 표시됩니다.
2. 마찬가지로 선택한 시간 범위가 3일 이상이면 활동 기록 그래프에 표시된 카운트 메트릭은 30분으로 반올림됩니다.

법의학적 활동 기록 데이터 정렬

활동 기록 데이터를 시간, 사용자, 소스 *IP*, 활동, _, _*Entity Type*, 1단계 폴더(루트), 2단계 폴더, 3단계 폴더 및 4단계 폴더별로 정렬할 수 있습니다. 기본적으로 테이블은 Descending_time_order를 기준으로 정렬됩니다. 즉, 최신 데이터가 먼저 표시됩니다. Device_and_Protocol_fields에 대해 정렬이 사용되지 않습니다.

비동기 내보내기에 대한 사용자 안내서

개요

스토리지 워크로드 보안의 비동기식 내보내기 기능은 대규모 데이터 내보내기를 처리하도록 설계되었습니다.

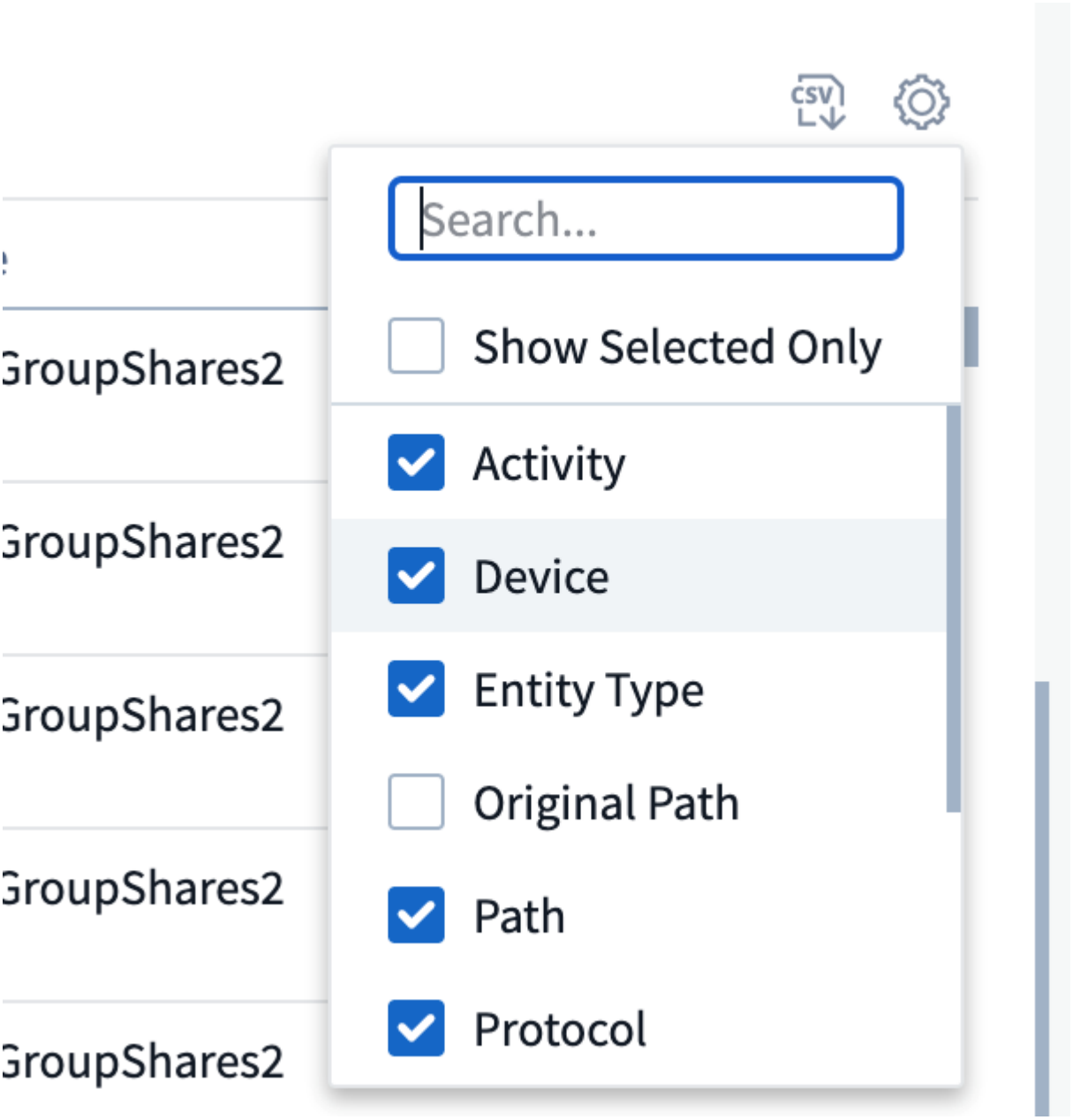
단계별 가이드**:** 비동기 내보내기를 사용하여 데이터 내보내기

1. * 내보내기 시작 * : 내보내기에 대해 원하는 시간 기간과 필터를 선택하고 내보내기 버튼을 클릭합니다.
2. * 내보내기가 완료될 때까지 대기 *: 처리 시간은 몇 분에서 몇 시간까지 소요될 수 있습니다. 포렌식 페이지를 몇 번 새로 고쳐야 할 수 있습니다. 내보내기 작업이 완료되면 "마지막 내보내기 CSV 파일 다운로드" 버튼이 활성화됩니다.
3. * 다운로드 *: "마지막 생성 내보내기 파일 다운로드" 버튼을 클릭하여 .zip 형식으로 내보낸 데이터를 가져옵니다. 이 데이터는 사용자가 다른 비동기 내보내기를 시작하거나 3일이 경과할 때까지 다운로드할 수 있습니다. 이 버튼은 다른 비동기 내보내기가 시작될 때까지 활성화된 상태로 유지됩니다.
4. * 제한 사항 *:
    - 비동기 다운로드 수는 현재 사용자당 1개, 테넌트당 3개로 제한됩니다.
    - 내보낸 데이터는 최대 100만 개의 레코드로 제한됩니다.

API를 통해 포렌식 데이터를 추출하는 샘플 스크립트는 에이전트의 _/opt/NetApp/cloudsecure/agent/export-script/_에 있습니다. 스크립트에 대한 자세한 내용은 이 위치에 있는 Readme 파일을 참조하십시오.

모든 활동에 대한 열 선택

ALL ACTIVITY_TABLE에는 기본적으로 선택 열이 표시됩니다. 열을 추가, 제거 또는 변경하려면 테이블 오른쪽에 있는 기어 아이콘을 클릭하고 사용 가능한 열 목록에서 선택합니다.



활동 기록 보존

활성 워크로드 보안 환경에서는 활동 기록이 13개월 동안 유지됩니다.

포렌식 페이지의 필터 적용 가능성

필터	기능	예	이 필터에 적용 가능합니다	이러한 필터에는 적용되지 않습니다	결과
* (별표)	모든 것을 검색할 수 있습니다	Auto * 03172022 검색 텍스트에 하이픈 또는 밑줄이 포함된 경우 대괄호로 표현식을 지정합니다. 예: svm-123 검색에는 (svm *)	사용자, 엔터티 유형, 장치, 볼륨, 원래 경로, 1stLevel 폴더, 2ndLevel 폴더, 3rdLevel 폴더, 4thLevel 폴더		"Auto"로 시작하여 "03172022"로 끝나는 모든 리소스를 반환합니다.
? (물음표)	특정 수의 문자를 검색할 수 있습니다	AutoSabotageUser1_03172022?	사용자, 엔티티 유형, 디바이스, 볼륨, 1stLevel 폴더, 2ndLevel 폴더, 3rdLevel 폴더, 4thLevel 폴더		AutoSabotageUser1_03172022A, AutoSabotageUser1_03172022B, AutoSabotageUser1_031720225 등을 반환합니다
또는	여러 요소를 지정할 수 있습니다	AutoSabotageUser1_03172022 또는 AutoRansomUser4_03162022	사용자, 도메인, 엔터티 유형, 원래 경로		AutoSabotageUser1_03172022 또는 AutoRansomUser4_03162022 중 하나를 반환합니다
아닙니다	검색 결과에서 텍스트를 제외할 수 있습니다	AutoRansomUser4_03162022가 아닙니다	사용자, 도메인, 엔터티 유형, 원래 경로, 1stLevel 폴더, 2ndLevel 폴더, 3rdLevel 폴더, 4thLevel 폴더	장치	"AutoRansomUser4_03162022"로 시작하지 않는 모든 항목을 반환합니다.
없음	모든 필드에서 NULL 값을 검색합니다	없음	도메인		대상 필드가 비어 있는 결과를 반환합니다

경로/원래 경로 검색

/ 을(를) 사용하거나 사용하지 않고 검색 결과는 다릅니다

"/AutoDir1/AutoFile03242022"	정확한 검색만 작동합니다. 정확한 경로가 /AutoDir1/AutoFile03242022 인 모든 활동을 반환합니다(대/소문자 구분 없음).
"/AutoDir1/"	Works; AutoDir1과 일치하는 1단계 디렉터리의 모든 작업을 반환합니다(대/소문자 구분 없음).
"/AutoDir1/AutoFile03242022/"	Works; AutoDir1 및 AutoFile03242022와 일치하는 2단계 디렉터리와 일치하는 1단계 디렉터리의 모든 작업을 반환합니다(대소문자 구분 없음).
/AutoDir1/AutoFile03242022 또는 /AutoDir1/AutoFile03242022	작동하지 않습니다

NOT/AutoDir1/AutoFile03242022	작동하지 않습니다
NOT/AutoDir1	작동하지 않습니다
NOT/AutoFile03242022	작동하지 않습니다
*	작동하지 않습니다

로컬 루트 **SVM** 사용자 활동 변경

로컬 루트 SVM 사용자가 작업을 수행하는 경우 NFS 공유가 마운트된 클라이언트의 IP가 사용자 이름에 고려되며, 이 IP는 포렌식 작업 및 사용자 활동 페이지 모두에서 root@<ip-address-of-the-client>로 표시됩니다.

예를 들면 다음과 같습니다.

- SVM-1이 워크로드 보안에 의해 모니터링되고 해당 SVM의 루트 사용자가 IP 주소가 10.197.12.40인 클라이언트에 공유를 마운트하는 경우, 포렌식 활동 페이지에 표시되는 사용자 이름은 *root@10.197.12.40* 입니다.
- 동일한 SVM-1이 IP 주소가 10.197.12.41인 다른 클라이언트에 마운트되는 경우 법의학 활동 페이지에 표시되는 사용자 이름은 *root@10.197.12.41* 입니다.
- • IP 주소별로 NFS 루트 사용자 활동을 분리하는 데 사용됩니다. 이전에는 모든 활동이 IP 구분 없이 _root_user 만 수행하는 것으로 간주되었습니다.

문제 해결

문제	시도해 보십시오
“All Activities(모든 활동)” 테이블의 ‘User(사용자)’ 열 아래에 사용자 이름이 “LDAP:HQ.COMPANYNAME.COM:S-1-5-21-3577637-1906459482-1437260136-1831817” 또는 “LDAP:default:80038003”으로 표시됩니다.	가능한 원인은 다음과 같습니다. 1. 아직 구성된 사용자 디렉토리 Collector가 없습니다. 하나를 추가하려면 * Workload Security > Collector > User Directory Collector * 로 이동하고 * + User Directory Collector * 를 클릭합니다. Active Directory_or_LDAP Directory Server_를 선택합니다. 2. 사용자 디렉터리 수집기가 구성되었지만 중지되었거나 오류 상태입니다. Collectors > User Directory Collectors * 로 이동하여 상태를 확인하십시오. "사용자 디렉토리 수집기 문제 해결"문제 해결 팁은 설명서의 섹션을 참조하십시오. 올바르게 구성하면 24시간 내에 자동으로 이름이 확인됩니다. 그래도 해결되지 않으면 올바른 사용자 데이터 수집기를 추가했는지 확인합니다. 사용자가 실제로 추가된 Active Directory/LDAP Directory Server에 속하는지 확인합니다.
일부 NFS 이벤트는 UI에서 표시되지 않습니다.	다음을 확인하십시오. 1. POSIX 속성이 설정된 AD 서버의 사용자 디렉토리 수집기는 UI에서 활성화된 unixid 속성으로 실행해야 합니다. 2. UI 3의 사용자 페이지에서 NFS 액세스를 수행하는 모든 사용자를 검색할 때 표시됩니다. 원시 이벤트(사용자가 아직 검색되지 않은 이벤트)는 NFS 4에서 지원되지 않습니다. NFS 내보내기에 대한 익명 액세스는 모니터링되지 않습니다. 5. NFS 버전이 NFS4.1 미만에서 사용되는지 확인합니다.

Forensics_All Activity_or_Entities_pages의 필터에 별표(*)와 같은 와일드카드 문자가 포함된 일부 문자를 입력하면 페이지가 매우 느리게 로드됩니다.	검색 문자열의 별표(\ )는 모든 항목을 검색합니다. 그러나 _ * <searchTerm>_또는 _ * <searchTerm> * _ 과(와) 같은 선행 와일드카드 문자열은 쿼리 속도를 느리게 만듭니다. 보다 나은 성능을 얻으려면 접두사 문자열을 대신 ***<searchTerm>**** 형식으로 사용합니다(즉, 별표( )*after_a* 검색 용어를 추가합니다*).* 예*:* _ * *testvolume_or* * test * volume_ 대신 *testvolume* * 문자열을 사용하십시오. 디렉토리 검색을 사용하여 지정된 폴더 아래의 모든 활동을 재귀적으로 봅니다(계층 검색). 예: "/path1/path2/path3/"는 /path1/path2/path3 아래에 재귀적으로 모든 활동을 나열합니다. 또는 All Activity(모든 활동) 탭 아래의 "Add to Filter(필터에 추가)" 옵션을 사용합니다.
경로 필터를 사용할 때 "상태 코드 500/503으로 요청 실패" 오류가 발생합니다.	레코드를 필터링하려면 더 작은 날짜 범위를 사용하십시오.
Forensic UI에서 _PATH_FILTER를 사용할 때 데이터가 느리게 로드되고 있습니다.	더 빠른 결과를 얻으려면 디렉터리 경로 필터(경로 문자열 / 로 끝나는)를 최대 4개까지 사용하는 것이 좋습니다. 예를 들어 디렉터리 경로가 /aa/bbb/ccc/dd인 경우 "/aa/bb/ccc/dd/"를 검색하여 데이터를 더 빨리 로드하십시오.

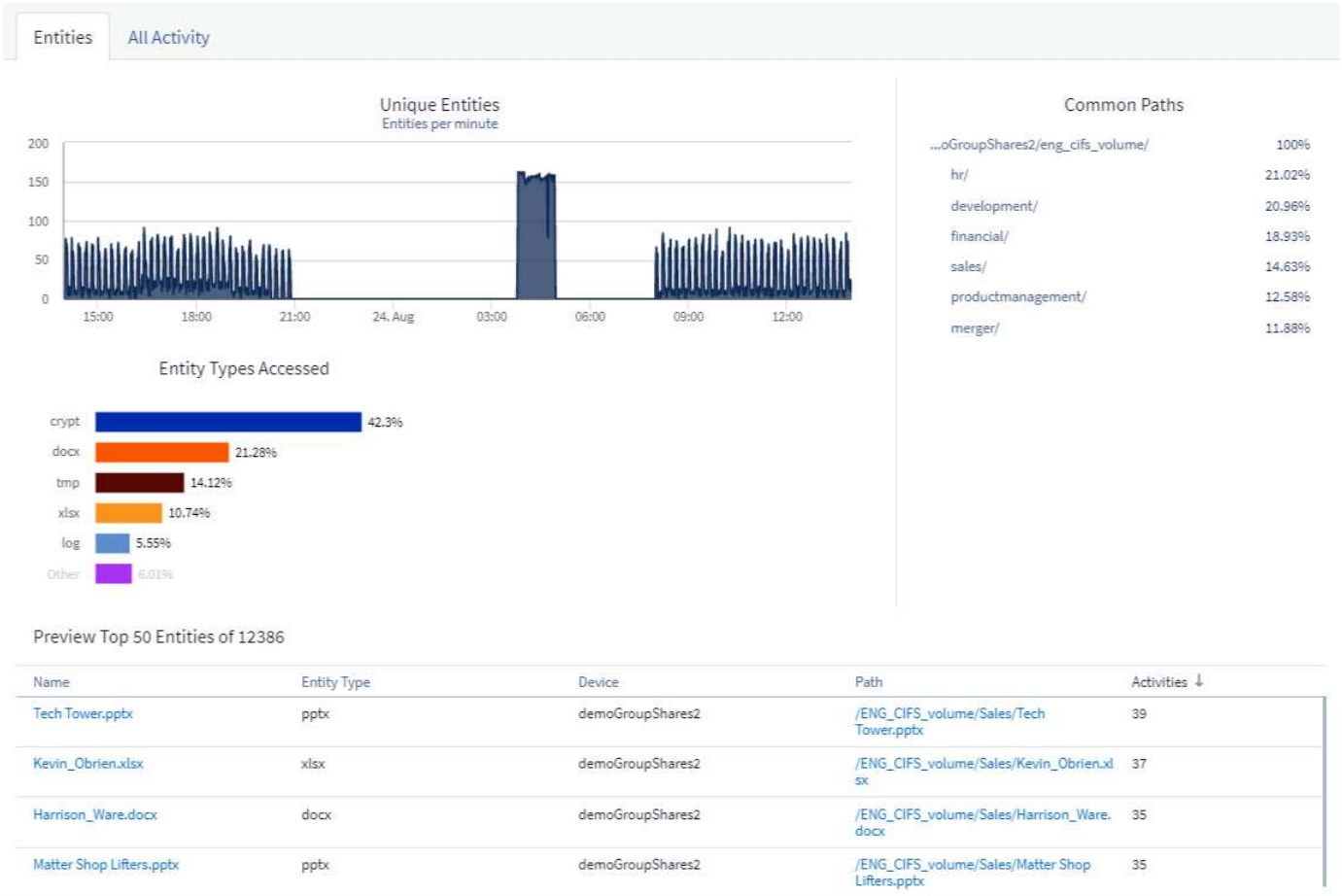
포렌식 엔터티 페이지

포렌식 엔터티 페이지에서는 테넌트의 엔터티 활동에 대한 자세한 정보를 제공합니다.

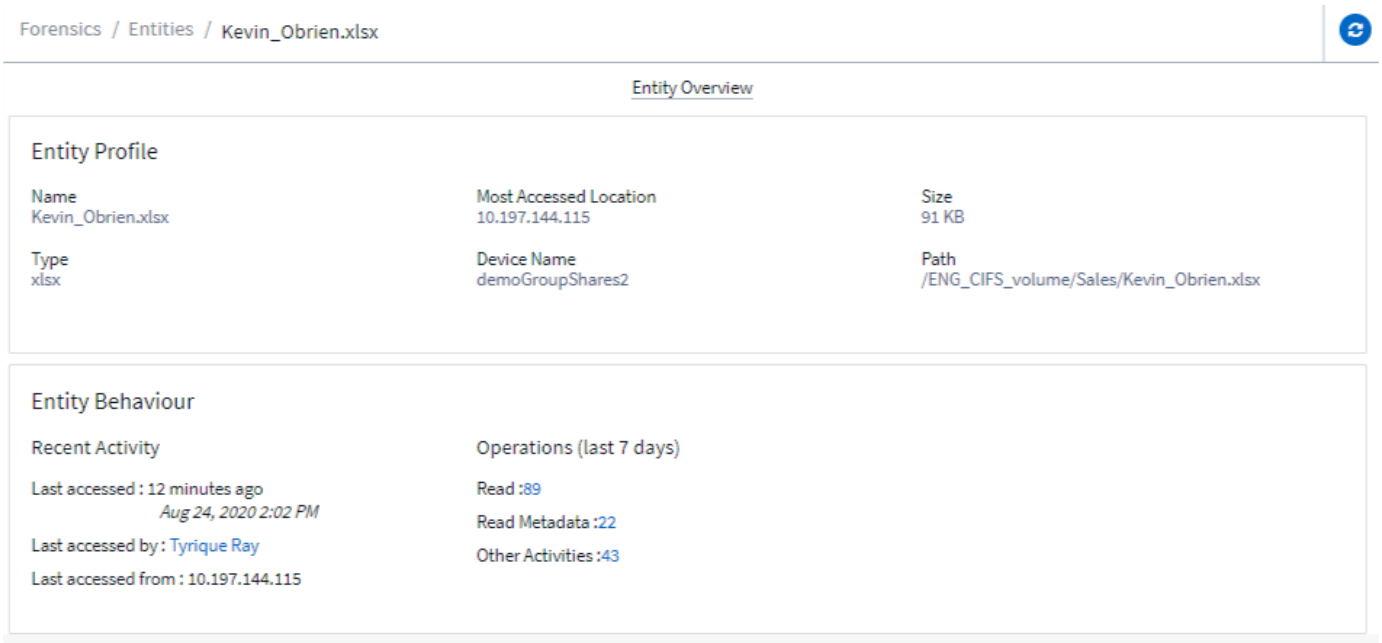
엔터티 정보 검사

Forensics > Activity Forensics * 를 클릭하고 _Entities_탭을 클릭하여 Entities 페이지에 액세스합니다.

이 페이지에서는 테넌트의 엔터티 활동에 대한 개요를 제공하고 다음 정보를 강조합니다. * 분당 *UNIQUE_ACCESS_ACCESS_ACCESS_*를 보여 주는 그래프 * *_Entity Types ACCESS* * 전체 엔터티 수 중 *Common Paths* * 에 대한 분석 결과



목록에서 엔티티를 클릭하면 엔티티의 개요 페이지가 열리고 이름, 유형, 장치 이름, 가장 많이 액세스되는 위치 IP 및 경로 등의 세부 정보와 사용자, IP, 경로 등의 엔터티 동작이 표시됩니다. 엔티티에 마지막으로 액세스한 시간입니다.



Forensic 사용자 개요

각 사용자에 대한 정보는 사용자 개요 에 나와 있습니다. 이러한 뷰를 사용하여 사용자 특성, 관련 엔터티 및 최근 활동을 파악할 수 있습니다.

사용자 프로필

사용자 프로필 정보에는 사용자의 연락처 정보 및 위치가 포함됩니다. 프로필은 다음 정보를 제공합니다.

- 사용자의 이름입니다
- 사용자의 이메일 주소입니다
- 사용자 관리자
- 사용자의 전화 연락처입니다
- 사용자의 위치입니다

사용자 행동

사용자 동작 정보는 사용자가 수행한 최근 작업 및 작업을 식별합니다. 이 정보에는 다음이 포함됩니다.

- 최근 활동
  - 마지막 액세스 위치입니다
  - 활동 그래프
  - 경고
- 최근 7일 동안의 작업
  - 작업 수

새로 고침 간격

사용자 목록은 12시간마다 새로 고쳐집니다.

보존 정책

다시 새로 고치지 않으면 사용자 목록이 13개월 동안 유지됩니다. 13개월 후 데이터가 삭제됩니다. 워크로드 보안 환경이 삭제된 경우 환경과 관련된 모든 데이터가 삭제됩니다.