법의학

Data Infrastructure Insights

NetApp
January 13, 2026

목차

법의학

법의학 - 모든 활동

모든 활동 페이지는 워크로드 보안 환경에서 엔터티에 수행된 작업을 이해하는 데 도움이 됩니다.

모든 활동 데이터 검토

과학 수사 **>** 활동 과학 수사*를 클릭하고 *모든 활동 탭을 클릭하여 모든 활동 페이지에 액세스합니다. 이 페이지에서는 세입자의 활동에 대한 개요를 제공하며 다음 정보를 강조합니다.

- _활동 내역_을 보여주는 그래프(선택된 글로벌 시간 범위 기반)

  그래프에서 사각형을 끌어서 그래프를 확대/축소할 수 있습니다. 확대된 기간 범위를 표시하기 위해 전체 페이지가 로드됩니다. 확대하면 사용자가 확대 축소할 수 있는 버튼이 표시됩니다.

- 모든 활동 데이터 목록입니다.
- 드롭다운으로 그룹화하면 사용자, 폴더, 엔터티 유형 등으로 활동을 그룹화할 수 있는 옵션이 제공됩니다.
- 테이블 위에 있는 일반 경로 버튼을 클릭하면 엔터티 경로 세부 정보가 있는 슬라이드 아웃 패널을 볼 수 있습니다.

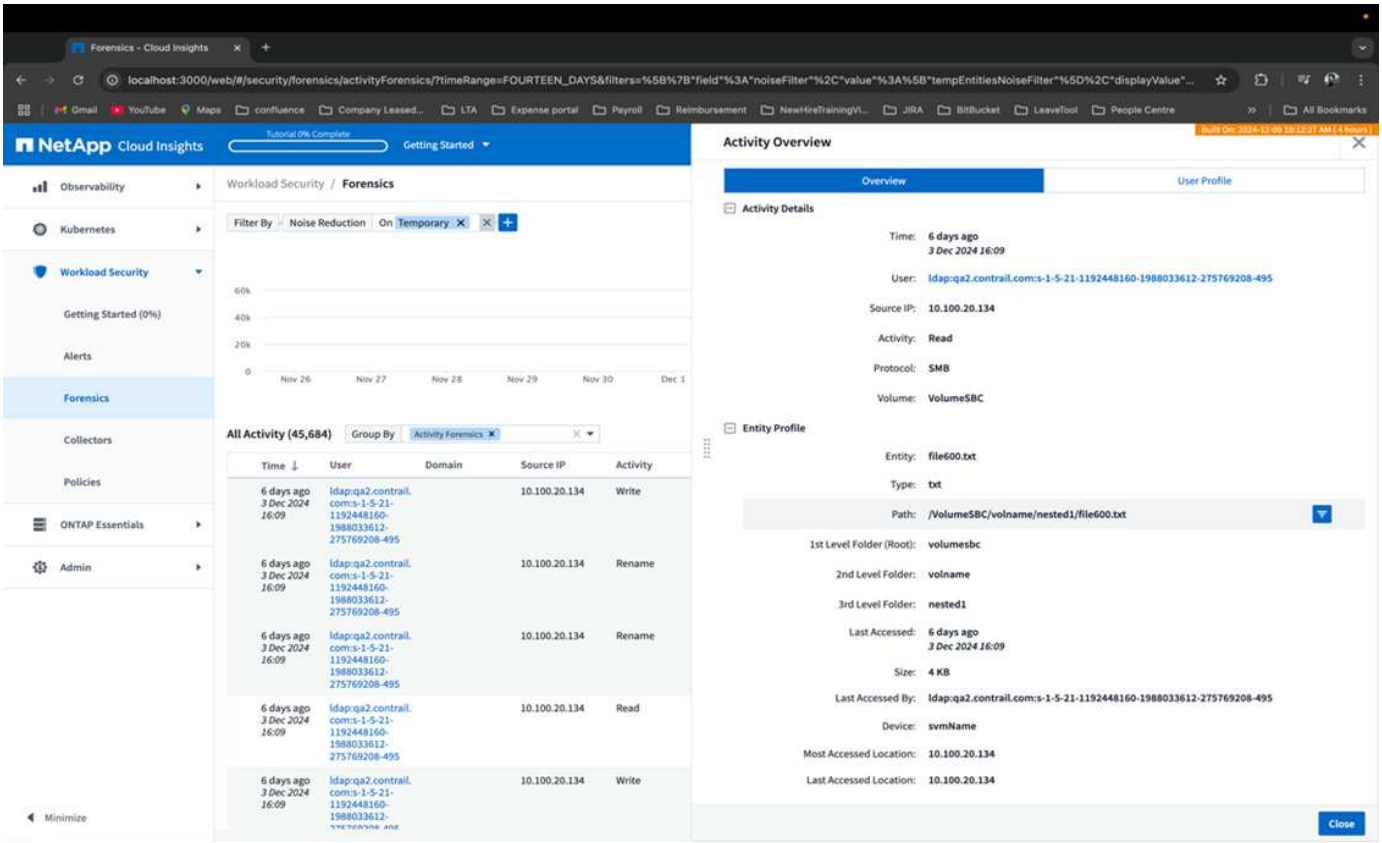
모든 활동 표에는 다음 정보가 표시됩니다. 이러한 열 중 일부가 기본적으로 표시되는 것은 아닙니다. "기어" 아이콘을 클릭하면 표시할 열을 선택할 수 있습니다.

- 엔터티에 접근한 *시간*에는 마지막 접근 시점의 연도, 월, 일, 시간이 포함됩니다.
- 링크를 통해 엔터티에 액세스한 *사용자*"사용자 정보" 슬라이드 아웃 패널로.
- 사용자가 수행한 활동 지원되는 유형은 다음과 같습니다.
  - 그룹 소유권 변경 - 파일이나 폴더의 그룹 소유권이 변경되었습니다. 그룹 소유권에 대한 자세한 내용은 다음을 참조하세요."이 링크."
  - 소유자 변경 - 파일이나 폴더의 소유권이 다른 사용자로 변경됩니다.
  - 권한 변경 - 파일이나 폴더의 권한이 변경되었습니다.
  - 만들기 - 파일이나 폴더를 만듭니다.
  - 삭제 - 파일이나 폴더를 삭제합니다. 폴더가 삭제되면 해당 폴더와 하위 폴더의 모든 파일에 대한 삭제 이벤트가 생성됩니다.
  - 읽기 - 파일을 읽었습니다.
  - 메타데이터 읽기 - 폴더 모니터링 옵션을 활성화한 경우에만 해당. Windows에서 폴더를 열거나 Linux에서 폴더 내에서 "ls"를 실행하면 생성됩니다.
  - 이름 바꾸기 - 파일이나 폴더의 이름을 바꿉니다.
  - 쓰기 - 데이터가 파일에 기록됩니다.
  - 메타데이터 쓰기 - 파일 메타데이터가 기록됩니다(예: 권한 변경).
  - 기타 변경 사항 - 위에 설명되지 않은 기타 이벤트. 매핑되지 않은 모든 이벤트는 "기타 변경" 활동 유형에 매핑됩니다. 파일과 폴더에 적용됩니다.
- 경로*는 엔터티 경로입니다. 이는 정확한 엔터티 경로(예: ***"/home/userX/nested1/nested2/abc.txt"***)이거나 재귀

검색을 위한 경로의 디렉토리 부분(예: "*/home/userX/nested1/nested2/*")이어야 합니다. 참고: 정규식 경로 패턴(예: *중첩)은 여기서 허용되지 않습니다. 또는 아래에 언급된 대로 개별 경로 폴더 수준 필터를 경로 필터링에 지정할 수도 있습니다.

- *1차 폴더(루트)*는 소문자로 된 엔티티 경로의 루트 디렉토리입니다.
- *2차 폴더*는 소문자로 된 엔티티 경로의 2차 디렉토리입니다.
- *3차 폴더*는 소문자로 된 엔티티 경로의 3차 디렉토리입니다.
- *4단계 폴더*는 소문자로 된 엔티티 경로의 4단계 디렉토리입니다.
- *엔터티 유형*에는 엔터티(즉, 파일) 확장자(.doc, .docx, .tmp 등)가 포함됩니다.
- 엔티티가 있는 *장치*입니다.
- 이벤트를 가져오는 데 사용되는 *프로토콜*입니다.
- 원본 파일의 이름이 변경되었을 때 이벤트 이름을 바꾸는 데 사용되는 *원래 경로*입니다. 이 열은 기본적으로 표에 표시되지 않습니다. 열 선택기를 사용하여 이 열을 표에 추가합니다.
- 엔티티가 있는 *볼륨*입니다. 이 열은 기본적으로 표에 표시되지 않습니다. 열 선택기를 사용하여 이 열을 표에 추가합니다.
- *엔터티 이름*은 엔터티 경로의 마지막 구성 요소입니다. 엔터티 유형이 파일인 경우 파일 이름입니다.

테이블 행을 선택하면 사용자 프로필이 있는 탭과 활동 및 엔터티 개요가 있는 다른 탭이 있는 슬라이드 아웃 패널이 열립니다.



기본 그룹화 방법은 활동 포렌식_입니다. 다른 _그룹화 방법(예: 엔터티 유형)을 선택하면 엔터티 그룹화 테이블이 표시됩니다. 선택하지 않으면 그룹화 *모두*가 표시됩니다.

- 활동 수는 하이퍼링크로 표시됩니다. 이를 선택하면 선택한 그룹이 필터로 추가됩니다. 해당 필터에 따라 활동 표가

업데이트됩니다.

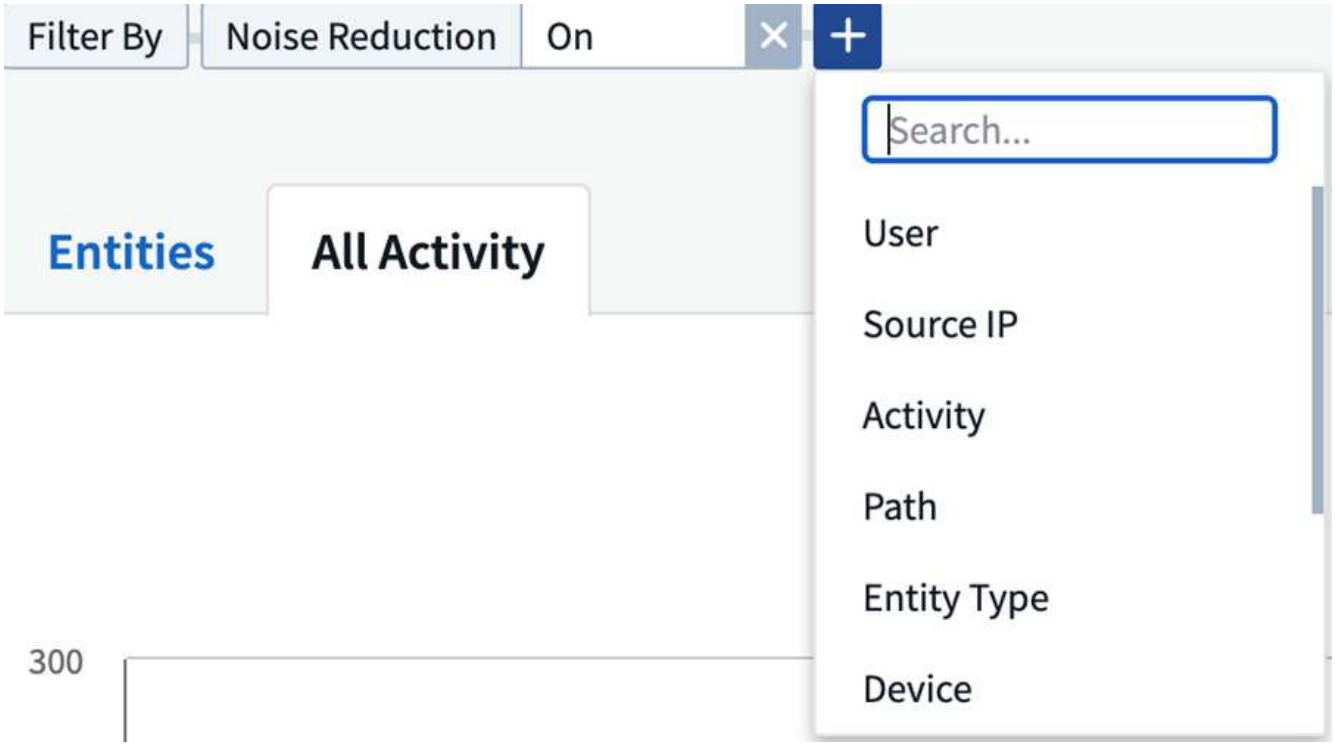
- 필터를 변경하거나, 시간 범위를 변경하거나, 화면을 새로 고침하는 경우 필터를 다시 설정하지 않으면 필터링된 결과로 돌아갈 수 없습니다.
- 엔티티 이름을 필터로 선택하면 그룹화 기준 드롭다운이 비활성화됩니다. 또한, 사용자가 이미 그룹화 기준 화면에 있는 경우 엔티티 이름을 필터로 사용하는 기능이 비활성화됩니다.

법의학 활동 내역 데이터 필터링

데이터를 필터링하는 데 사용할 수 있는 방법은 두 가지가 있습니다.

- 필터는 슬라이드 아웃 패널에서 추가할 수 있습니다. 해당 값은 상단의 필터 기준 목록에 있는 적절한 필터에 추가됩니다.
- 필터 기준 필드에 입력하여 데이터를 필터링합니다.

  [+] 버튼을 클릭하여 상단의 '필터 기준' 위젯에서 적절한 필터를 선택하세요.



  검색어를 입력하세요

  필터를 적용하려면 Enter 키를 누르거나 필터 상자 밖을 클릭하세요.

다음 필드를 기준으로 포렌식 활동 데이터를 필터링할 수 있습니다.

- 활동 유형.
- 프로토콜 프로토콜별 활동을 가져옵니다.
- 활동을 수행하는 사용자의 사용자 이름*입니다. 필터링하려면 정확한 사용자 이름을 제공해야 합니다. 사용자 이름의 일부 또는 일부 사용자 이름에 " 접두사나 접미사를 붙여 검색하면 작동하지 않습니다.
- *노이즈 감소*는 사용자가 지난 2시간 동안 만든 파일을 필터링하는 기능입니다. 또한 사용자가 액세스하는 임시

파일(예: .tmp 파일)을 필터링하는 데 사용됩니다.

- 활동을 수행하는 사용자의 도메인*입니다**.** 필터링하려면 *정확한 도메인*을 제공해야 합니다**.** 부분 도메인이나 와일드카드**()**로 접두사나 접미사가 붙은 부분 도메인을 검색하는 것은 작동하지 않습니다. _None_을 지정하면 누락된 도메인을 검색할 수 있습니다.

다음 필드에는 특별 필터링 규칙이 적용됩니다.

- 엔터티 유형, 엔터티(파일) 확장자를 사용합니다. 따옴표 안에 정확한 엔터티 유형을 지정하는 것이 좋습니다. 예를 들어 *"txt"*.
- 엔티티의 경로 - 이는 정확한 엔티티 경로(예: "*/home/userX/nested1/nested2/abc.txt*")이거나 재귀 검색을 위한 경로의 디렉토리 부분(예: "*/home/userX/nested1/nested2/*")이어야 합니다. 참고: 정규식 경로 패턴(예: *중첩*)은 여기서 허용되지 않습니다. 더 빠른 결과를 얻으려면 최대 4개 디렉토리까지 디렉토리 경로 필터(경로 문자열이 /로 끝남)를 사용하는 것이 좋습니다. 예를 들어, "*/home/userX/nested1/nested2/*". 자세한 내용은 아래 표를 참조하세요.
- 1단계 폴더(루트) - 필터로서의 엔티티 경로의 루트 디렉토리. 예를 들어, 엔티티 경로가 /home/userX/nested1/nested2/인 경우 home 또는 "home"을 사용할 수 있습니다.
- 2차 폴더 - 엔터티 경로 필터의 2차 디렉토리입니다. 예를 들어, 엔티티 경로가 /home/userX/nested1/nested2/인 경우 userX 또는 "userX"를 사용할 수 있습니다.
- 3차 폴더 – 엔터티 경로 필터의 3차 디렉토리입니다.
- 예를 들어, 엔티티 경로가 /home/userX/nested1/nested2/인 경우 nested1 또는 "nested1"을 사용할 수 있습니다.
- 4단계 폴더 - 디렉토리 엔터티 경로 필터의 4단계 디렉토리입니다. 예를 들어, 엔티티 경로가 /home/userX/nested1/nested2/인 경우 nested2 또는 "nested2"를 사용할 수 있습니다.
- 활동을 수행하는 사용자 - 따옴표로 정확한 사용자를 지정하는 것이 좋습니다. 예를 들어, ″관리자″.
- 장치 (SVM) 엔티티가 상주하는 곳
- 볼륨 엔터티가 있는 곳
- 원본 파일의 이름이 변경되었을 때 이벤트 이름을 바꾸는 데 사용되는 *원래 경로*입니다.
- *엔터티에 접근한 소스 IP*입니다.
  - 와일드카드 * 및 ?를 사용할 수 있습니다. 예: 10.0.0.**, 10.0?.0.10, 10.10**
  - 정확한 일치가 필요한 경우 유효한 소스 IP 주소를 큰따옴표로 묶어 제공해야 합니다(예: "10.1.1.1."). "10.1.1.", "10.1..*" 등과 같이 큰따옴표가 포함된 불완전한 IP는 작동하지 않습니다.
- 엔터티 이름 - 필터로서의 엔터티 경로의 파일 이름입니다. 예를 들어, 엔티티 경로가 /home/userX/nested1/testfile.txt이면 엔티티 이름은 testfile.txt입니다. 정확한 파일 이름을 따옴표로 묶어 지정하는 것이 좋습니다. 와일드카드 검색은 피하세요. 예를 들어, "testfile.txt". 또한, 이 엔터티 이름 필터는 짧은 시간 범위(최대 3일)에 권장됩니다.

필터링 시 이전 필드는 다음 사항에 따라 달라집니다.

- 정확한 값은 따옴표 안에 있어야 합니다. 예: "searchtext"
- 와일드카드 문자열에는 따옴표가 포함될 수 없습니다. 예: searchtext, *searchtext*는 'searchtext'를 포함하는 모든 문자열을 필터링합니다.
- 접두사가 있는 문자열(예: searchtext*)은 'searchtext'로 시작하는 모든 문자열을 검색합니다.

모든 필터 필드는 대소문자를 구분하여 검색합니다. 예를 들어, 적용된 필터가 'searchtext' 값을 갖는 엔터티 유형인 경우 엔터티 유형이 'searchtext', 'SearchText', 'SEARCHTEXT'인 결과가 반환됩니다.

활동 포렌식 필터 예:

사용자가 적용한 필터 표현식	예상 결과	성과 평가	논평
경로 = "/home/userX/nested1/nested2/"	지정된 디렉토리 아래의 모든 파일 및 폴더에 대한 재귀적 조회	빠른	최대 4개의 디렉토리를 검색하면 빠르게 검색됩니다.
경로 = "/home/userX/nested1/"	지정된 디렉토리 아래의 모든 파일 및 폴더에 대한 재귀적 조회	빠른	최대 4개의 디렉토리를 검색하면 빠르게 검색됩니다.
경로 = "/home/userX/nested1/test"	경로 값이 /home/userX/nested1/test와 일치하는 정확한 일치	더 느리게	정확한 검색은 디렉토리 검색에 비해 검색 속도가 느립니다.
경로 = "/home/userX/nested1/nested2/nested3/"	지정된 디렉토리 아래의 모든 파일 및 폴더에 대한 재귀적 조회	더 느리게	4개 이상의 디렉토리에서 검색하면 검색 속도가 느려집니다.
기타 경로 기반이 아닌 필터. 사용자 및 엔터티 유형 필터는 따옴표로 묶는 것이 좋습니다(예: User="Administrator" 엔터티 유형="txt").		빠른	
엔티티 이름 = "test.log"	파일 이름이 test.log인 정확한 일치	빠른	정확히 일치하므로
엔티티 이름 = *test.log	test.log로 끝나는 파일 이름	느린	와일드 카드로 인해 느릴 수 있습니다.
엔티티 이름 = test*.log	test로 시작하고 .log로 끝나는 파일 이름	느린	와일드 카드로 인해 느릴 수 있습니다.
엔티티 이름 = test.lo	test.lo로 시작하는 파일 이름 예: test.log, test.log.1, test.log1과 일치합니다.	더 느리게	끝에 와일드카드가 있어서 느릴 수 있습니다.
엔티티 이름 = 테스트	test로 시작하는 파일 이름	가장 느림	끝에 와일드카드가 있고 보다 일반적인 값이 사용되기 때문에 가장 느릴 수 있습니다.

메모:

1. 모든 활동 아이콘 옆에 표시되는 활동 수는 선택한 시간 범위가 3일을 초과하는 경우 30분으로 반올림됩니다. 예를 들어, _9월 1일 오전 10시 15분 ~ 9월 7일 오전 10시 15분_의 시간 범위는 9월 1일 오전 10시부터 9월 7일 오전 10시 30분까지의 활동 수를 표시합니다.
2. 마찬가지로, 선택한 시간 범위가 3일을 넘을 경우 활동 내역 그래프에 표시되는 카운트 지표는 30분으로 반올림됩니다.

법의학 활동 내역 데이터 정렬

활동 내역 데이터를 시간, 사용자, 소스 *IP*, 활동, 엔터티 유형, 1차 폴더(루트), 2차 폴더, 3차 폴더, 4차 폴더별로 정렬할 수 있습니다. 기본적으로 표는 시간 순으로 내림차순으로 정렬됩니다. 즉, 최신 데이터가 먼저 표시됩니다. *Device* 및 *Protocol* 필드에 대한 정렬이 비활성화되었습니다.

비동기 내보내기 사용자 가이드

개요

Storage Workload Security의 비동기 내보내기 기능은 대용량 데이터 내보내기를 처리하도록 설계되었습니다.

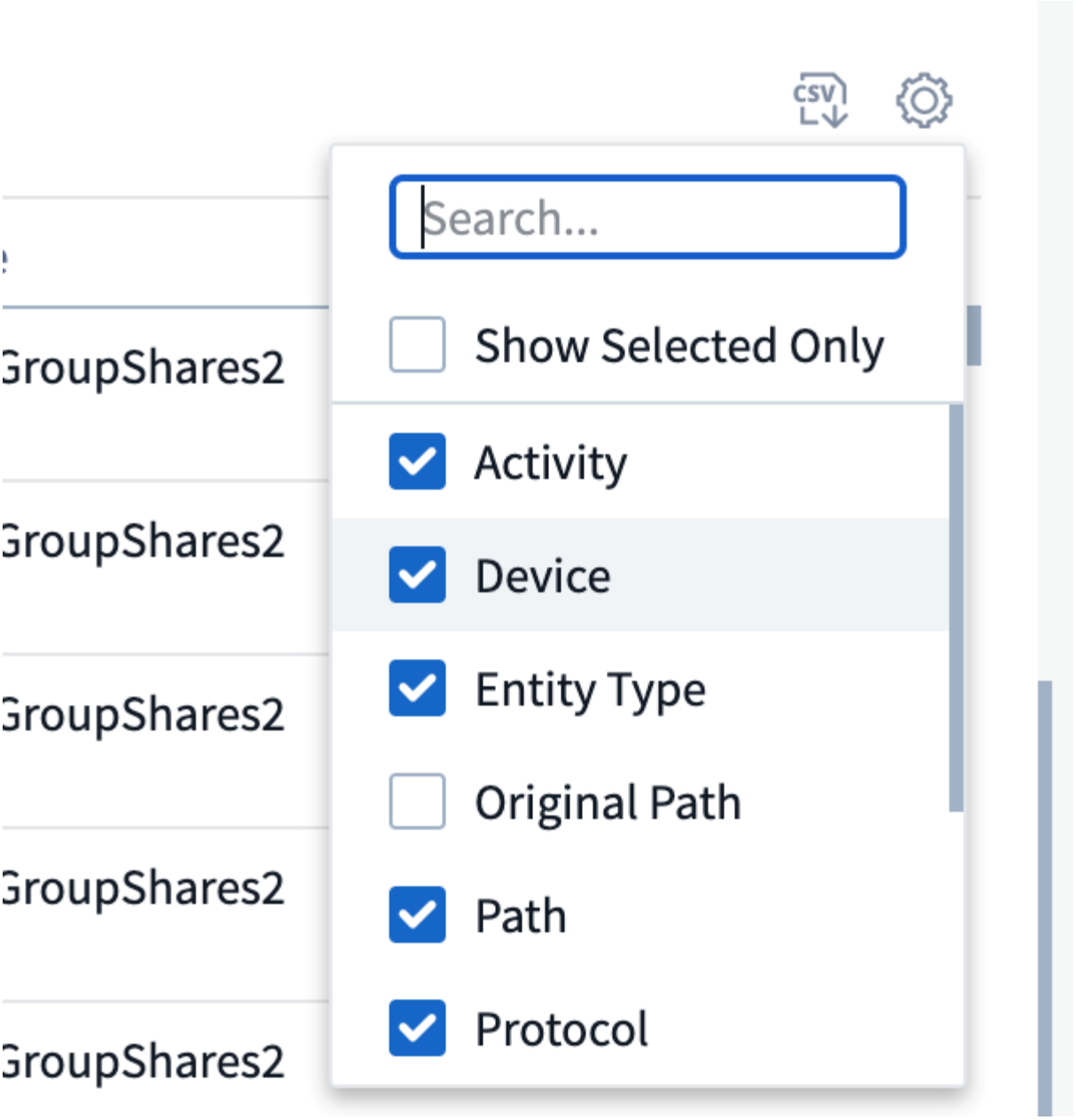
단계별 가이드**:** 비동기 내보내기를 통한 데이터 내보내기

1. 내보내기 시작: 내보내기에 필요한 기간과 필터를 선택하고 내보내기 버튼을 클릭합니다.
2. 내보내기가 완료될 때까지 기다리세요: 처리 시간은 몇 분에서 몇 시간까지 걸릴 수 있습니다. 법의학 페이지를 여러 번 새로 고쳐야 할 수도 있습니다. 내보내기 작업이 완료되면 "마지막으로 내보낸 CSV 파일 다운로드" 버튼이 활성화됩니다.
3. 다운로드: "마지막으로 생성된 내보내기 파일 다운로드" 버튼을 클릭하면 내보낸 데이터를 .zip 형식으로 받을 수 있습니다. 이 데이터는 사용자가 다른 비동기 내보내기를 시작하거나 3일이 경과할 때까지 다운로드할 수 있습니다. 어느 쪽이 먼저 발생하는지에 따라 달라집니다. 다른 비동기 내보내기가 시작될 때까지 버튼은 활성화된 상태로 유지됩니다.
4. 제한 사항:
    - 비동기 다운로드 수는 현재 각 활동 및 활동 분석 테이블의 경우 사용자당 1개, 테넌트당 3개로 제한되어 있습니다.
    - 활동 표의 경우 내보낼 수 있는 데이터는 최대 100만 개의 레코드로 제한되고, 그룹화 기준의 경우 레코드 수는 50만 개로 제한됩니다.

API를 통해 포렌식 데이터를 추출하는 샘플 스크립트는 에이전트의 _/opt/netapp/cloudsecure/agent/export-script/_에 있습니다. 스크립트에 대한 자세한 내용은 이 위치의 readme를 참조하세요.

모든 활동에 대한 열 선택

모든 활동 표에는 기본적으로 선택된 열이 표시됩니다. 열을 추가, 제거 또는 변경하려면 표 오른쪽에 있는 기어 아이콘을 클릭하고 사용 가능한 열 목록에서 선택하세요.



활동 내역 보존

활성 워크로드 보안 환경의 활동 내역은 13개월 동안 보관됩니다.

포렌식 페이지에서 필터 적용 가능성

필터	그것이 하는 일	예	다음 필터에 적용 가능	이 필터에는 적용되지 않습니다.	결과
* (별표)	모든 것을 검색할 수 있습니다	Auto*03172022 검색 텍스트에 하이픈이나 밑줄이 포함된 경우 괄호 안에 표현식을 입력합니다. 예: svm-123을 검색하는 경우 (svm*)	사용자, 엔터티 유형, 장치, 볼륨, 원래 경로, 1차 폴더, 2차 폴더, 3차 폴더, 4차 폴더, 엔터티 이름, 소스 IP		"Auto"로 시작하고 "03172022"로 끝나는 모든 리소스를 반환합니다.
? (물음표)	특정 수의 문자를 검색할 수 있습니다	AutoSabotageUser1_03172022?	사용자, 엔터티 유형, 장치, 볼륨, 1차 폴더, 2차 폴더, 3차 폴더, 4차 폴더, 엔터티 이름, 소스 IP		AutoSabotageUser1_03172022A, AutoSabotageUser1_03172022B, AutoSabotageUser1_031720225 등을 반환합니다.
또는	여러 엔터티를 지정할 수 있습니다.	AutoSabotageUser1_03172022 또는 AutoRansomUser4_03162022	사용자, 도메인, 엔터티 유형, 원래 경로, 엔터티 이름, 소스 IP		AutoSabotageUser1_03172022 또는 AutoRansomUser4_03162022 중 하나를 반환합니다.
아니다	검색 결과에서 텍스트를 제외할 수 있습니다.	NOT AutoRansomUser4_03162022	사용자, 도메인, 엔터티 유형, 원래 경로, 1차 폴더, 2차 폴더, 3차 폴더, 4차 폴더, 엔터티 이름, 소스 IP	장치	"AutoRansomUser4_03162022"로 시작하지 않는 모든 항목을 반환합니다.
None	모든 필드에서 NULL 값을 검색합니다.	None	도메인		대상 필드가 비어 있는 결과를 반환합니다.

경로 검색

/가 있는 경우와 없는 경우의 검색 결과가 다릅니다.

"/자동 디렉토리1/자동 파일03242022"	정확한 검색만 작동합니다. /AutoDir1/AutoFile03242022(대소문자 구분 없이)와 같은 정확한 경로를 가진 모든 활동을 반환합니다.
"/자동 디렉토리1/ "	작동합니다. AutoDir1과 일치하는 1차 디렉토리가 있는 모든 활동을 반환합니다(대소문자 구분 없음).
"/자동 디렉토리1/자동 파일03242022/"	작동합니다. 1차 디렉토리가 AutoDir1과 일치하고 2차 디렉토리가 AutoFile03242022와 일치하는 모든 활동을 반환합니다(대소문자 구분 없음).

/AutoDir1/AutoFile03242022 또는 /AutoDir1/AutoFile03242022	작동하지 않습니다
/AutoDir1/AutoFile03242022가 아닙니다	작동하지 않습니다
/AutoDir1이 아닙니다	작동하지 않습니다
아니요 /AutoFile03242022	작동하지 않습니다
*	작동하지 않습니다

로컬 루트 **SVM** 사용자 활동 변경

로컬 루트 SVM 사용자가 어떤 활동을 수행하는 경우, NFS 공유가 마운트된 클라이언트의 IP가 이제 사용자 이름에 고려되며, 이는 포렌식 활동 및 사용자 활동 페이지 모두에서 root@<클라이언트의 IP 주소>로 표시됩니다.

예를 들어:

- SVM-1이 Workload Security에서 모니터링되고 해당 SVM의 루트 사용자가 IP 주소 10.197.12.40의 클라이언트에 공유를 마운트하는 경우, 포렌식 활동 페이지에 표시되는 사용자 이름은 _root@10.197.12.40_입니다.
- 동일한 SVM-1이 IP 주소 10.197.12.41의 다른 클라이언트에 마운트되면 포렌식 활동 페이지에 표시되는 사용자 이름은 _root@10.197.12.41_이 됩니다.

*• 이는 IP 주소별로 NFS 루트 사용자 활동을 분리하기 위해 수행됩니다. 이전에는 모든 활동이 IP 구분 없이 *root* 사용자에 의해서만 수행되는 것으로 간주되었습니다.

문제 해결

문제	이것을 시도해보세요
"모든 활동" 테이블의 "사용자" 열에서 사용자 이름은 "ldap:HQ.COMPANYNAME.COM:S-1-5-21-3577637-1906459482-1437260136-1831817" 또는 "ldap:default:80038003"으로 표시됩니다.	가능한 이유는 다음과 같습니다. 1. 아직 사용자 디렉토리 수집기가 구성되지 않았습니다. 하나를 추가하려면 *워크로드 보안 > 수집기 > 사용자 디렉터리 수집기*로 이동하여 *+사용자 디렉터리 수집기*를 클릭합니다. *Active Directory* 또는 _LDAP 디렉터리 서버_를 선택하세요. 2. 사용자 디렉토리 수집기가 구성되었지만 중지되었거나 오류 상태입니다. *수집기 > 사용자 디렉토리 수집기*로 가서 상태를 확인하세요. 를 참조하세요"사용자 디렉토리 수집기 문제 해결" 문제 해결 팁에 대한 설명서 섹션입니다. 올바르게 구성하면 이름은 24시간 이내에 자동으로 확인됩니다. 그래도 문제가 해결되지 않으면 올바른 사용자 데이터 수집기를 추가했는지 확인하세요. 사용자가 실제로 추가된 Active Directory/LDAP 디렉터리 서버에 속해 있는지 확인하세요.

일부 NFS 이벤트는 UI에서 볼 수 없습니다.	다음 사항을 확인하세요. 1. POSIX 속성이 설정된 AD 서버용 사용자 디렉터리 수집기는 UI에서 unixid 속성을 활성화하여 실행해야 합니다. 2. UI 3의 사용자 페이지에서 검색하면 NFS 액세스를 수행하는 모든 사용자가 표시되어야 합니다. 원시 이벤트(사용자가 아직 검색되지 않은 이벤트)는 NFS 4에서 지원되지 않습니다. NFS 내보내기에 대한 익명 액세스는 모니터링되지 않습니다. 5. 사용하는 NFS 버전이 4.1 이하인지 확인하세요. (NFS 4.1은 ONTAP 9.15 이상에서 지원됩니다.)
포렌식 모든 활동 또는 엔터티 페이지의 필터에 별표(*)와 같은 와일드카드 문자가 포함된 몇 글자를 입력한 후 페이지가 매우 느리게 로드됩니다.	검색 문자열에 별표(*)를 넣으면 모든 것을 검색합니다. 하지만 *<*searchTerm*> 또는 *<*searchTerm*>*_와 같은 와일드카드 문자열을 앞에 붙이면 쿼리 속도가 느려집니다. 더 나은 성능을 얻으려면 대신 접두사 문자열을 사용하세요. 형식은 _<*searchTerm*>*_입니다. (즉, 검색어 _뒤에 별표(*)를 추가하세요.) 예: *testvolume* 또는 *test*volume* 대신 *testvolume** 문자열을 사용하세요. 디렉토리 검색을 사용하여 지정된 폴더 아래에 있는 모든 활동을 재귀적으로 확인합니다(계층적 검색). 예를 들어, "/path1/path2/path3/"은 /path1/path2/path3 아래에 있는 모든 활동을 재귀적으로 나열합니다. 또는 모든 활동 탭 아래의 "필터에 추가" 옵션을 사용하세요.
경로 필터를 사용할 때 "요청이 상태 코드 500/503으로 실패했습니다" 오류가 발생합니다.	레코드 필터링에 더 작은 날짜 범위를 사용해 보세요.
path 필터를 사용하면 포렌식 UI에서 데이터 로드 속도가 느려집니다.	더 빠른 결과를 얻으려면 최대 4개 디렉토리까지 디렉토리 경로 필터(경로 문자열이 /로 끝남)를 사용하는 것이 좋습니다. 예를 들어 디렉토리 경로가 /Aaa/Bbb/Ccc/Ddd인 경우 "/Aaa/Bbb/Ccc/Ddd/"를 검색하여 데이터를 더 빨리 로드해 보세요.
포렌식 UI가 데이터를 느리게 로드하고 엔터티 이름 필터를 사용할 때 오류가 발생합니다.	더 작은 시간 범위와 큰따옴표로 묶인 정확한 값으로 검색을 시도해 보세요. 예를 들어, entityPath가 "/home/userX/nested1/nested2/nested3/testfile.txt"인 경우 엔티티 이름 필터로 "testfile.txt"를 사용해 보세요.

포렌식 사용자 개요

각 사용자에 대한 정보는 사용자 개요에서 제공됩니다. 이러한 보기를 사용하면 사용자 특성, 관련 엔터티, 최근 활동을 파악할 수 있습니다.

사용자 프로필

사용자 프로필 정보에는 사용자의 연락처 정보와 위치가 포함됩니다. 프로필에는 다음과 같은 정보가 제공됩니다.

- 사용자 이름
- 사용자의 이메일 주소
- 사용자 관리자
- 사용자를 위한 전화 연락처
- 사용자의 위치

사용자 행동

사용자 행동 정보는 사용자가 최근에 수행한 활동과 작업을 식별합니다. 이 정보에는 다음이 포함됩니다.

- 최근 활동
  - 마지막 접속 위치
  - 활동 그래프
  - 알림
- 지난 7일간의 작업
  - 작업 수

새로 고침 간격

사용자 목록은 12시간마다 새로 고쳐집니다.

보존 정책

새로고침하지 않으면 사용자 목록은 13개월 동안 보관됩니다. 13개월 후에 데이터가 삭제됩니다. 워크로드 보안 환경이 삭제되면 해당 환경과 관련된 모든 데이터가 삭제됩니다.