

그룹 삭제를 위한 보안 엔드포인트의 업데이트 이벤트 이해

목차

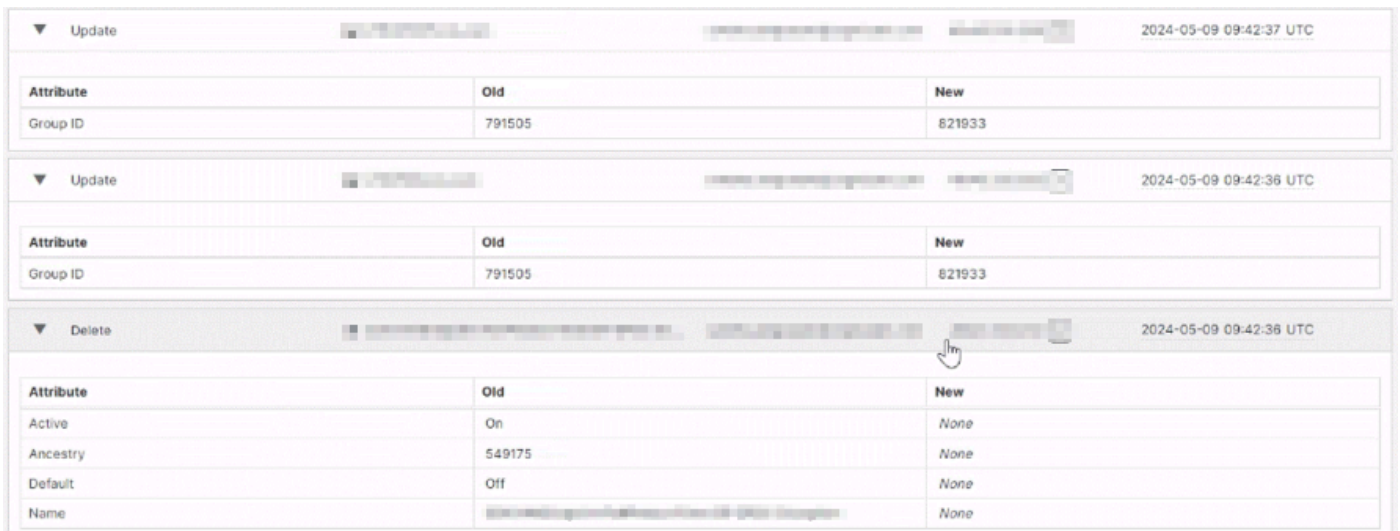
- [소개](#)
- [문제](#)
- [솔루션](#)

소개

이 문서에서는 빈 그룹이 삭제되었을 때 보안 엔드포인트 감사 로그가 업데이트 및 삭제 이벤트를 모두 기록하는 방법에 대해 설명합니다.

문제

이 이미지의 업데이트 이벤트는 시스템 또는 워크스테이션의 새 그룹 ID를 표시합니다. 이러한 워크스테이션은 AMP 콘솔 컴퓨터 페이지에 표시되지 않습니다. 이러한 업데이트 이벤트는 삭제를 수행하기 위해 로그인한 사람의 사용자 이메일과 연결되며, 이로 인해 발생한 사항에 대한 클라이언트 혼란이 발생할 수 있습니다. 경우에 따라 빈 그룹을 삭제한 후 30-40개의 업데이트 이벤트를 생성할 수 있습니다.



The image displays three screenshots of system logs. The first two show 'Update' events with a table of attributes. The third shows a 'Delete' event with a table of attributes.

Attribute	Old	New
Group ID	791505	821933

Attribute	Old	New
Group ID	791505	821933

Attribute	Old	New
Active	On	None
Ancestry	549175	None
Default	Off	None
Name	[REDACTED]	None

솔루션

이는 예상된 동작입니다. 빈 그룹을 삭제하는 동안 감사 로그 업데이트 이벤트에 표시되는 컴퓨터 또는 컴퓨터 호스트 이름은 해당 그룹의 일부였던 장치에 속하지만 지금은 비활성 상태입니다. 이러한 시스템은 90일 동안 활동이 없으면 콘솔에서 자동으로 제거되었지만 백엔드에서 그룹의 일부로 남았습니다.

그룹이 삭제되면 이러한 비활성 시스템이 기본 그룹으로 이동하며, 이는 업데이트 이벤트를 트리거합니다. 죄송합니다. 이러한 컴퓨터는 비활성 상태이므로 콘솔에 표시되지 않으므로 컴퓨터에서 검색할 때 찾을 수 없습니다.

그룹에 아직 할당된 비활성 시스템의 전체 목록을 얻으려면 TAC에 연결해야 합니다. 이 정보는 보안 엔드포인트 포털을 통해 검색할 수 없기 때문입니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.