Umbrella의 활동 검색 보고서에서 누락된 Active Directory 사용자 문제 해결

목차

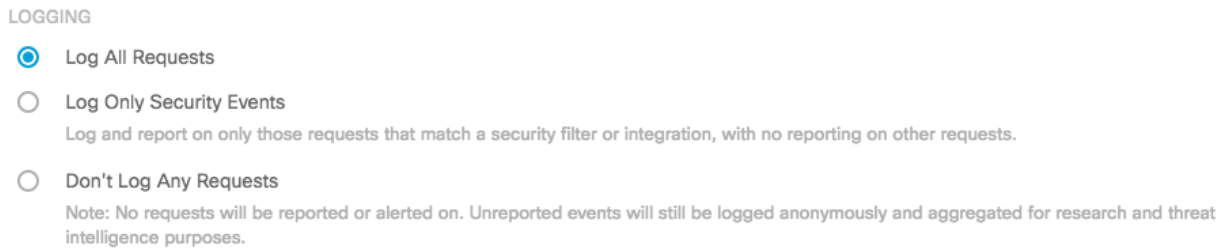
소개

이 문서에서는 Cisco Umbrella의 활동 검색 보고서에 대해 설명합니다. Activity Search Report(활동 검색 보고서)는 사용자가 생성하는 모든 DNS 쿼리에 대한 거의 실시간으로 표시되는 보고서입니다. Cisco Umbrella Active Directory(AD) 통합을 설정한 경우, AD 사용자가 활동 검색에서 ID 열을 채우는 것을 볼 수 있습니다. 그러나 사용자가 ID 열에서 누락되는 경우가 있습니다.

해결

Activity Search(활동 검색)의 Identity(ID) 열에 AD 사용자가 직접 표시되어야 하지만 표시되지 않거나, 일부는 표시되지만 기대한 수만큼 표시되지는 않는다고 생각되는 경우 몇 가지 사항을 확인할 수 있습니다.

1. 사이트 및 Active Directory
    - 모든 AD 구성 요소를 검사하여 보고된 오류나 문제가 없는지 확인합니다. 구성 요소에 회색, 주황색 또는 빨간색 상태 표시등이 나타나면 이러한 세부 정보를 확인하고 지원 티켓(umbrella-support@cisco.com)을 여십시오.
        - 영향을 받는 사용자(활동 검색에 표시되지 않는 사용자)의 진단 테스트
        - 확장된 오류 메시지와 함께 VA(Virtual Appliance) 콘솔의 스크린샷
        - AD 커넥터 감사 로그
2. 로깅 설정
    - 모든 정책의 Advanced Settings(고급 설정)에서 하단에 로깅할 양에 대한 섹션이 있습니다. 다음으로 설정할 수 있습니다.
        - 모든 요청 기록
        - 보안 이벤트만 기록
        - 요청을 기록하지 않음
    - 정책이 현재 "Log Only Security Events(보안 이벤트만 로깅)"로 설정된 경우, 이는 예상한 만큼의 쿼리가 표시되지 않거나 일부 사용자의 결과가 전혀 표시되지 않는 이유를 설명할 수 있습니다.



3. 올바른 정책 우선 순위
    - 정책 목록에서 AD 사용자 정책보다 높은 네트워크 ID에 적용되는 정책이 있는 경우 네트워크 ID 정책이 적용될 가능성이 높습니다. 이는 다시 활동 검색에서 네트워크가 보고된 ID로 표시됨을 의미합니다. 모범 사례 및 정책 우선 순위에 대한 Cisco Umbrella 설명서도 확인하십시오.

원인

활동 검색에서 "ID"를 가져오는 위치

DNS 쿼리가 Umbrella로 오면 AD 통합이 예상대로 작동한다고 가정하면 이 정보는 쿼리에서 전달됩니다.

- 내부 IP 주소
- AD ID 해시(사용자, 호스트 또는 둘 다)
- 이그레스 IP
- 쿼리하는 도메인

AD ID 해시는 가상 어플라이언스에 의해 쿼리에 추가되며, 가상 어플라이언스는 이 정보를 전달받고, AD 커넥터에서 로그온 이벤트에 해당하는 내부 IP 주소를 전달받습니다.

그런 다음 Cisco Umbrella는 이 정보를 사용하여 조직을 찾고 적용할 정책을 결정합니다. AD 사용자에게 특별히 적용되는 정책이 없지만 네트워크 또는 사이트에 대한 정책이 있는 경우 Cisco Umbrella는 해당 ID를 사용하여 정책을 적용합니다. 즉, 질의, ID 및 응답이 활동 검색에서 보고될 때 보고되는 정책을 트리거한 ID입니다. 다른 정보는 요청에서 계속 태그가 지정되므로 AD 사용자를 검색하고 네트워크를 ID로 보고하는 활동을 가져올 수 있습니다. 또한 활동 검색 데이터를 CSV 파일로 내보낼 경우 쿼리와 연결된 모든 ID 정보가 표시됩니다.

추가 정보

아직 AD 사용자가 보이지 않는 경우 지원(umbrella-support@cisco.com)에 문의하여 진단 테스트 결과와 관련된 AD 커넥터 감사 로그를 확인하십시오.

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.