

Secure Access Activity Search(보안 액세스 활동 검색)에 알 수 없는 규칙 이름 표시

목차

문제

Umbrella에서 SSE로 마이그레이션하는 동안 Secure Access Activity Search 이벤트는 명명된 정책 규칙을 표시하는 대신 Rule Name을 Unknown으로 표시합니다. 이 동작은 chatgpt.com에 대한 요청과 같은 허용된 트래픽을 비롯한 다양한 트래픽 유형에 대해 관찰되었습니다. 문제는 이러한 UNKNOWN 규칙 이름 항목이 정책 구성 문제 또는 교정이 필요한 마이그레이션 문제를 나타내는 지 여부였습니다.

환경

- Cisco SSE(Secure Access)
- Umbrella에서 SSE로 마이그레이션하는 조직
- 보안 액세스 활동 검색 보고
- 새로 확인된 도메인으로 분류된 트래픽

해결

고객이 생성/명명된 규칙이 아닌 Secure Access 시스템 논리에 의해 처리되는 이벤트에는 Rule Name UNKNOWN 동작이 예상되고 정상입니다. 이는 일반적으로 Newly Seen Domains(새로 확인된 도메인)로 분류된 트래픽에 대해 발생합니다. 여기서 도메인은 쿼리 시간에 새로 확인되었으며 Activity Search(활동 검색) 또는 Security Activity(보안 활동) 보고서에서 그렇게 보고됩니다.

알 수 없는 규칙 이름으로 활동 검색 이벤트 해석

Rule Name UNKNOWN의 이벤트가 발생하면 다음 이벤트 필드를 검토하여 시행 이유를 확인하고 적절한 정책 적용을 확인합니다.

- Action - 트래픽이 허용되었는지 차단되었는지 표시합니다.
- Event Block Reason/Block Reason - 구체적인 시행 세부 정보 제공
- Categories(카테고리) - 콘텐츠 카테고리(예: 새로 확인된 도메인)를 표시합니다.
- 대상 도메인/IP - 요청의 대상
- 사용자/소스 ID - 트래픽의 소스
- 타임스탬프 - 이벤트가 발생한 시간

Categories(카테고리) 필드에 New Seen Domains(새로 확인된 도메인)가 표시되면 rule-name(규칙 이름) 필드의 UNKNOWN(알 수 없음)은 정상적인 동작이며 실패한 마이그레이션 또는 정책 손상을 나타내지 않습니다.

예기치 않은 동작에 대한 검증 단계

트래픽이 특정 명명된 규칙과 일치해야 하지만 UNKNOWN(알 수 없음)으로 표시된 경우, 정책 경로 검증을 위해 이 정보를 수집합니다.

- 2-3 샘플 이벤트 타임스탬프
- 각 이벤트의 대상 도메인/IP
- 각 이벤트의 사용자/소스 ID

이 정보를 사용하여 예상 정책 경로를 실제 이벤트 동작과 비교하고 추가 조사가 필요한지 여부를 확인할 수 있습니다.

원인

UNKNOWN 규칙 이름은 Secure Access 시스템 논리가 고객이 생성한/명명된 정책 규칙을 적용하지 않고 트래픽을 처리할 때 나타납니다. 이는 특정 트래픽 범주, 특히 Newly Seen Domains(새로 확인된 도메인)에 대해 문서화된 동작으로, 내장된 범주화 및 처리 메커니즘이 초기 도메인 평가 시 명명된 규칙보다 우선합니다.

관련 콘텐츠

- [새로 본 도메인 보안 활성화](#)
- [Cisco 기술 지원 및 다운로드](#)

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.