데이터 분류가 없는 보안 액세스 DLP 파일 크기 규칙 텍스트 파일에 대한 모니터 이벤트를 생성하지 않음

목차

문제

파일 크기 기준으로만 구성된 Cisco Secure Access Web DLP 정책(데이터 분류 없음)은 .txt 파일 업로드에 대한 DLP 모니터 이벤트를 생성하지 않는 반면, 동일한 정책이 .xlsx, .png, .pdf 파일과 같은 다른 파일 유형에 대한 모니터 이벤트를 올바르게 트리거합니다. 영향을 받는 정책 상위 관리 정책 - 웹은 다음으로 구성됩니다.

- 사용자 지정 파일 크기가 1KB~49MB인 파일 제어
- 데이터 분류 기준 없음
- 모니터링으로 설정된 작업

테스트 결과 다음과 같은 결과가 나타났습니다.

- TXT 파일 업로드는 Action = Monitor일 때 DLP 이벤트에 나타나지 않습니다.
- Action = Block(작업 = 차단)일 때 동일한 TXT 파일이 DLP 이벤트를 올바르게 생성합니다.
- 작업 로그는 TXT 파일을 비롯한 모든 파일 업로드를 표시합니다.
- 기타 파일 형식(PNG, PDF, XLSX)은 Monitor 작업과 함께 예상대로 DLP 이벤트를 생성합니다.

또한 DLP 규칙에 데이터 분류가 구성되지 않은 경우, 로깅된 DLP 이벤트는 구성된 규칙 심각도 설정에 관계없이 항상 Medium 심각도를 표시합니다.

환경

- Cisco Secure Access(이전의 Cisco Umbrella)
- DLP(Data Loss Prevention) 웹 정책
- HTTPS 암호 해독이 활성화된 인터넷 액세스 정책
- 웹 애플리케이션을 통해 수행된 파일 업로드 테스트

해결

이러한 동작은 문서화되지 않았지만 설계에 따라 다릅니다. 로그 오버로드를 방지하기 위해 Monitor 작업과 함께 파일 크기 전용 기준을 사용할 경우 text/plain과 같은 MIME 유형은 DLP 모니터링에서 우회됩니다. 개발진은 이를 외부적으로 문서화되지 않은 의도적인 행동이라고 확인했다.

해결 방법 옵션

옵션 1(권장): 데이터 분류 추가

Action = Monitor(작업 = 모니터링)를 유지하면서 DLP 규칙에 광범위한 데이터 분류 기준을 추가합니다.

이렇게 하면 다음과 같은 작업이 복원됩니다.

- TXT 파일 DLP 이벤트 생성
- 규칙 컨피그레이션을 기반으로 올바른 심각도 처리

옵션 2: 작업을 차단으로 변경

규칙 작업을 Monitor(모니터링)에서 Block(차단)으로 변경합니다. 이렇게 하면 TXT 파일에 대한 DLP 이벤트가 생성되지만, 모니터링 전용 활용 사례에서는 원하지 않는 차단도 시행됩니다.

랩 테스트 결과

포괄적인 실험실 테스트를 통해 행동 패턴이 확인되었습니다.

테스트 시나리오 1: 데이터 분류 및 파일 크기가 포함된 DLP 규칙(1KB-49MB), 작업 = 차단

- PII가 있는 TXT 파일: 차단 및 기록됨
- PDF 파일: 차단 및 기록됨
- PII가 없는 TXT 파일: 허용됨(예상)
- PNG 및 PII: 허용됨(분류에 따라 예상됨)

테스트 시나리오 2: 파일 크기만 있는 DLP 규칙(데이터 분류 없음), 작업 = 차단

- 모든 파일 형식(TXT, PDF, PNG): 차단 및 기록됨
- 규칙이 Low(낮음)로 구성되었음에도 불구하고 심각도가 Medium(중간)으로 표시됨

테스트 시나리오 3: 파일 크기만 있는 DLP 규칙(데이터 분류 없음), 작업 = 모니터링

- TXT 파일: DLP 이벤트에 허용되지만 로그인되지 않음
- PDF 및 PNG 파일: DLP 이벤트 허용 및 로그인
- 작업 로그는 TXT 파일을 포함한 모든 업로드를 표시합니다.

원인

이는 Cisco Secure Access DLP에서 의도적이지만 문서화되지 않은 동작입니다. 시스템은 과도한 로그 생성을 방지하기 위해 Monitor 작업과 함께 파일 크기 전용 규칙을 사용할 경우 텍스트/일반

MIME 유형에 대한 DLP 이벤트 로깅을 우회합니다. 동작은 action-dependent 및 MIME-type에 따라 다릅니다.

- 파일 크기만 기준으로 작업을 모니터링합니다. 로깅에서 우회된 TXT 파일
- 파일 크기 전용 조건으로 작업 차단: TXT 파일이 정상적으로 로깅됨
- 데이터 분류가 있는 모든 작업: TXT 파일이 정상적으로 로깅됨

심각도 문제는 DLP 이벤트가 콘텐츠 인식 모드에서 작동할 때 규칙 설정이 아닌 데이터 분류 메타데이터에서 심각도를 파생하기 때문에 발생합니다. Data Classification이 없으면 시스템은 구성된 규칙 심각도와 상관없이 기본적으로 "Medium" 심각도로 설정됩니다.

관련 콘텐츠

- Cisco Secure Access DLP 파일 크기 컨피그레이션

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.