Cisco Secure Access로 실시간 DLP 문제 해결

목차

소개

- 사전 요구 사항 및 경고

개요

일반 문제 해결 체크리스트

오탐 문제 해결

- 분류자, 파일 및 문자열
- 파일 레이블
- 웹 사이트 및 대상

오탐 문제 해결

- 데스크톱 애플리케이션 지원
- DLP 분류자 Gotchas
- 정확한 데이터 일치(EDM)

소개

이 문서에서는 SWG(Secure Web Gateway) 환경에서 인라인 또는 실시간 DLP(Data Loss Prevention) 문제의 트러블슈팅 단계를 설명합니다.

사전 요구 사항 및 경고

- HTTPS 검사: HTTPS 검사가 활성화되었는지 확인합니다. DLP는 암호화된 트래픽을 검사할 수 없습니다. 웹 사이트가 Cisco Secure Access Root CA 또는 사용자 지정 CA로 암호 해독되고 있는지 확인합니다.
- QUIC 프로토콜: 모든 브라우저에서 QUIC 프로토콜을 비활성화합니다. QUIC는 SWG를 우회하고 DLP 검사를 방지하는 UDP를 사용합니다.
- IPv6: 트래픽이 SWG에 도달하지 않을 경우 듀얼 스택 기능으로 인해 우회해야 하므로 IPv6를 비활성화합니다.
- 보안 정책: 액세스 규칙에 "Allow - Override Security" 또는 "Isolation"이 활성화되어 있지 않은지 확인합니다.

개요

인라인 DLP는 SWG의 확장된 검사 기능입니다. SWG 프록시를 통해 업로드된 파일에서 중요, 기

밀 또는 개인 식별 가능한 데이터의 업로드를 모니터링하거나 차단합니다. 고객은 Cisco에서 정의한 식별자(예: 신용카드 또는 주민등록번호) 또는 맞춤형 키워드를 사용하여 데이터 분류를 생성합니다. 이러한 분류는 특정 ID 및 대상에 할당된 DLP 정책에 적용됩니다. DLP 엔진은 HTTP POST, PUT 및 PATCH 메서드만 검사합니다.

일반 문제 해결 체크리스트

DLP 탐지가 발생하지 않는 경우, 설명된 단계를 확인하십시오.

- 연결: 클라이언트가 http://policy.test.sse.cisco.com을 방문하여 SWG를 사용하고 있는지 확인합니다. 올바른 SWG 데이터 센터가 적용되었는지 확인하고 테스트 결과에 "Protected by Secure Access"가 표시되는지 확인합니다.
- 암호 해독: 보안 프로필에서 SSL 암호 해독이 활성화되었는지 확인합니다. 선택적 암호 해독 또는 "Do Not Decrypt" 목록 제외가 없는지 확인합니다.
- 트래픽 조정: 인터넷 설정에 외부 도메인 우회가 구성되어 있지 않은지 확인하십시오.
- 신원: DLP 정책이 Active Directory 그룹을 사용하는 경우 사용자가 올바른 그룹의 구성원인지 확인합니다.
- 응용 프로그램 설정: Microsoft 도메인이 DLP에 사용되는 경우 Office 365 Bypass 또는 M365 호환성 설정을 사용하지 않도록 설정해야 합니다.
- 활동 검색: Reporting(보고) > Activity Search(활동 검색)를 사용하여 전체 URL이 표시되고(해독됨) 예상 ID가 트래픽과 연결되었는지 확인합니다. Reporting(보고) > Data Loss Prevention(데이터 손실 방지)을 선택하여 모니터링 또는 차단 활동이 기록되었는지 확인합니다.
- 정책 구성: DLP 정책이 올바른 ID 및 대상 애플리케이션에 대해 구성되었는지 확인합니다.
- 테스트: Cisco 설명서에서 알려진 올바른 대상(예: pastebin.com 또는 dlptest.com) 및 알려진 올바른 샘플 테스트 문자열을 사용합니다.
- 지원 데이터: 사용자로부터 HAR 파일을 수집하여 트래픽이 SWG를 통해 라우팅되는지 확인하고 SWG 헤더를 확인합니다.

오탐 문제 해결

DLP가 활성 상태이지만 특정 분류자가 트리거되지 않는 경우 다음 영역을 조사합니다.

분류자, 파일 및 문자열

- 파일 상태: 파일이 암호화되어 있지 않은지 또는 검사할 수 없는지 확인합니다. 간단한 텍스트 파일로 테스트합니다.
- 임계값: Policy(정책) > Data Classification(데이터 분류)에서 Threshold and Proximity(임계값

및 근접) 설정을 확인합니다. 분류자는 더 많은 적중 횟수 또는 맞춤 문자열에 근접성을 요구할 수 있다.
- Regex 패턴: 온라인 툴(예: regexr.com)을 사용하여 패턴을 시각화합니다. 패턴을 단순화하여 문자열의 작은 부분을 잡고 점진적으로 확장합니다.

파일 레이블

- 호환성: Confluence 또는 JIRA에서는 파일 레이블 탐지가 작동하지 않습니다.
- 메타데이터: Microsoft 응용 프로그램에서 문서 속성을 엽니다. 값은 Umbrella File 레이블과 정확히 일치해야 합니다. 대/소문자를 구분합니다.
- 암호화: 암호로 보호되거나 암호화된 파일에 대해서는 레이블 탐지가 작동하지 않습니다.

웹 사이트 및 대상

- 지원되는 앱: 지원되는 애플리케이션 목록을 검토합니다. 지원되지 않는 앱 또는 "모든 대상 "의 경우 특정 mime-type만 검사됩니다.
- 검색된 애플리케이션: 검사된 애플리케이션(예: dlptest.com)은 더 포괄적으로 검사됩니다. 임의의 웹사이트는 파일 위반에 대해서만 스캔될 수 있습니다.
- 파일 이름: 시스템은 파일 이름에서 특정 검사 응용 프로그램만 검색합니다.

오탐 문제 해결

DLP가 예기치 않게 내용과 일치하는 경우 Reporting(보고) > Data Loss Prevention(데이터 손실 방지)에서 분류자 이름 및 DLP 규칙을 확인합니다. 탐지가 합법적이지만 원치 않는 경우 Thresholds(임계값) 또는 Proximity(근접) 설정을 조정하여 정책을 세분화합니다.

데스크톱 애플리케이션 지원

데스크톱 기반 애플리케이션(예: Outlook, Teams 또는 Google Workspace)에 대한 지원은 최선의 방식으로 제공됩니다. 유효성은 파일 업로드 중에 사용되는 메시지 형식에 따라 다르며, 웹 기반 버전과 데스크톱 버전이 다를 수 있습니다. 검증되지 않은 애플리케이션의 경우 파일 업로드가 지원된다는 보장은 없습니다.

DLP 분류자 Gotchas

- 신용 카드 번호: Luhn 알고리즘이 유효성 검사에 사용됩니다. 유효한 신용 카드 번호로만 테스트합니다.
- 사용자 이름: 2-3개의 단어가 필요하며 각 단어는 대문자로 사용해야 합니다.
- 이름 조합: 이름과 기타 데이터 사이에는 구분 문자열이 필요합니다. 예를 들어 "Viagra - John Smith"는 일치하지만 "Viagra John Smith"는 일치하지 않습니다.
- 생년월일 "dob" 또는 "생년월일"과 같은 키워드 또는 헤더 근처에 있어야 합니다.
- 반대 의견 내용: 특정 예외 문자열은 텍스트가 책 또는 보고서와 비슷할 경우 이 분류자를 발생시키지 못하도록 합니다.
- 우편번호: 특정 위치 관련 키워드에 근접해야 합니다.

정확한 데이터 일치(EDM)

EDM을 조사하기 전에 일반적인 DLP 검사가 작동하는지 확인합니다. EDM 관련 문제의 경우 대시보드의 "Last Edit(마지막 수정)" 필드가 최신 상태인지 확인하고 인덱싱 툴 출력을 확인합니다.

명령 사용:

bloom 필터 파일(.blm)을 생성하려면 `-d` 옵션과 함께 색인 도구를 실행합니다. 이 명령은 EDM 인덱스의 유효성을 검사하고 레코드를 건너뛰어야 하는 이유를 트러블슈팅하는 데 사용됩니다. `-d` 플래그는 진단 블룸 필터 파일을 출력하도록 툴에 지시합니다. 이 파일은 샘플 파일 또는 HAR/웹 개발자 툴 데이터와 함께 지원 팀과 공유해야 합니다.

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.