모든 대상에 대한 실시간 DLP 양식 데이터 차단 문제 해결

목차

소개

이 문서에서는 모든 양식 데이터를 차단하기 위한 실시간 DLP(데이터 손실 보호) 규칙 구성과 관련된 문제를 해결하는 방법에 대해 설명합니다.

배경 정보

모든 양식 데이터를 차단하기 위해 실시간 DLP 규칙을 구성할 때, 진정한 긍정 및 잘못된 긍정 모두 클라우드 애플리케이션의 의도하지 않은 결과로 이어질 위험이 있습니다. 이러한 결과는 사용자가 로그인 페이지를 사용할 수 없는 가능성을 포함하여 클라우드 애플리케이션의 성공적인 운영에 영향을 미칠 수 있습니다. 이 문서에서는 이러한 위험을 강조하고 발생할 수 있는 문제를 해결하기 위한 트러블슈팅 단계를 제공합니다.

문제 해결

실시간 DLP 규칙에서 모든 양식 데이터를 차단하는 과정에서 문제가 발생하는 경우 다음 단계를 통해 문제를 해결하고 해결할 수 있습니다.

1. Refine Data Identifiers(데이터 식별자 세분화) - 이 단계는 중요한 데이터를 효과적으로 차단하고 합법적인 양식 데이터를 중단 없이 통과시키는 것 사이의 균형을 유지하는 데 도움이 됩니다.

    - DLP 규칙을 트리거하는 특정 데이터 식별자를 식별하려면 Data Loss Prevention 보고서(Reporting > Additional Reports > Data Loss Prevention)를 통해 차단된 DLP 이벤트 세부 정보를 검토합니다.

    - 허용치 레벨을 조정하거나 근접성 조건을 추가하여 오탐을 줄이고 필요에 따라 매칭할 수 있는 능력을 유지하여 데이터 식별자를 세분화하는 것이 좋습니다.

2. Exclude Blocked URLs(차단된 URL 제외) - URL을 제외함으로써 로그인 페이지 및 애플리케이션의 다른 필수 구성 요소가 차단 DLP 규칙의 영향을 받지 않도록 할 수 있습니다.

    - 활동 검색(Reporting > Core Reports > Activity Search) 및 DLP 이벤트 세부사항을 통해

활동 로그를 분석하여 차단되는 URL을 식별합니다.

- "Select Destination Lists and Applications for Exclusion(제외할 대상 목록 및 애플리케이션 선택)"에 구성된 대상 목록에 이러한 URL을 추가합니다.

3. DLP 규칙 동작 수정 - 문제가 지속되고 의도하지 않은 결과가 모든 양식 데이터 차단의 이점을 초과하는 경우 양식 데이터 검사를 중지하도록 DLP의 동작을 수정해야 합니다. '파일 업로드 및 검증된 애플리케이션의 양식 데이터만'을 선택하기만 하면 행동 변경이 가능하다.

결론

모든 양식 데이터를 차단하도록 실시간 DLP 규칙을 구성할 때 의도하지 않은 결과와 관련된 위험을 인식하는 것이 중요합니다. 이러한 위험은 로그인 페이지 사용 기능을 포함하여 클라우드 애플리케이션의 원활한 운영에 영향을 미칠 수 있습니다. 이 가이드에 설명된 트러블슈팅 단계를 사용하여 이러한 위험을 완화하고 클라우드 애플리케이션의 성공적인 작동을 보장하면서 데이터 보호를 유지하십시오.

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.