Cisco SA(Secure Access) 및 Cisco ETD(Email Threat Defense)에서 이메일 DLP 정책을 구성하는 방법

목차

소개

사전 요구 사항

- 요구 사항 및 사용된 구성 요소
- 이메일 DLP 정책 기능

네트워크 다이어그램

- Cisco Secure Email Threat Defense와 Cisco Secure Access의 통합을 보여 주는 네트워크 다이어그램과 트래픽 흐름도를 함께 아래에서 확인하십시오.

구성

- 1단계: Cisco Secure Access 로그인
- 2단계: 이메일 DLP 규칙 생성으로 이동합니다.

옵션 1: 사전 정의된 DLP 템플릿을 사용하여 이메일 DLP 규칙 생성

- 3단계: 기본 규칙 정보 구성
- 4단계: 데이터 분류 선택
- 5단계: 파일 제어 구성
- 6단계: 발신자 범위 정의
- 7단계: 수신자 범위 정의
- 8단계: 정책 작업 선택
- 9단계: 사용자 알림 구성
- 9단계: 사용자 알림 구성
- 10단계: 규칙 검토 및 저장

옵션 2: 사용자 지정 DLP 템플릿을 사용하여 이메일 DLP 규칙 생성

- 11단계: 사용자 지정 식별자 만들기
- 12단계: 데이터 분류 구성

문제 해결

- 규칙이 전자 메일과 일치하지 않습니다.
- 이메일은 차단되지 않음
- DLP 이벤트는 ETD에 표시되지 않음
- 첨부 파일 기반 일치가 검색되지 않음

모범 사례

요약

소개

이메일은 의도하지 않거나 허가되지 않은 데이터 노출에 가장 많이 사용되는 채널 중 하나입니다. Cisco는 조직이 이메일을 통해 공유되는 민감한 정보를 보호할 수 있도록 Cisco SA(Secure Access)와 Cisco ETD(Email Threat Defense)의 통합을 통해 이메일 DLP(Data Loss Prevention) 기능을 제공합니다.

이 아키텍처에서는 모든 이메일 DLP 정책 생성, 컨피그레이션 및 시행 작업이 Cisco Secure Access에서 수행됩니다. Cisco Email Threat Defense는 이메일 가시성 및 메시지 추적을 제공하는 한편, Cisco Secure Access는 DLP 규칙 및 적용 동작을 정의하는 정책 엔진 역할을 합니다.

이 문서에서는 사전 정의된 DLP 템플릿 또는 맞춤형 DLP 템플릿을 사용하여 Cisco Secure Access에서 이메일 DLP 정책을 생성하는 방법에 대해 설명합니다.

사전 요구 사항

컨피그레이션 프로세스를 시작하기 전에 다음 요구 사항이 충족되었는지 확인합니다.

- 관리 액세스: Cisco Email Threat Defense Inline 콘솔 및 Cisco Secure Access 콘솔에 대해 "전체 관리자" 권한이 있어야 합니다.
- 활성 서브스크립션: Email Threat Defense 및 Secure Access 테넌트가 모두 활성 상태이고 프로비저닝되었는지 확인합니다.
- 연결:Email Threat Defense와 Secure Access 간의 API 통합을 성공적으로 설정해야 합니다.
- 메일 흐름 구성: Email Threat Defense가 이메일 트래픽을 능동적으로 검사하려면 인라인 모드에서 올바르게 구축되어야 합니다.

중요: 이 솔루션은 Cisco Secure Access와 Cisco Email Threat Defense를 모두 사용하지만 이 문서에서 설명하는 모든 이메일 DLP 규칙 컨피그레이션 단계는 Cisco Secure Access에서만 수행됩니다.

요구 사항 및 사용된 구성 요소

이메일 DLP 정책을 성공적으로 구현하려면 다음 구성 요소가 사용됩니다.

- Cisco ETD(Email Threat Defense): 이메일 검사 지점의 역할을 합니다. 아웃바운드 이메일 트래픽을 캡처하고 DLP 엔진이 분석을 수행하는 데 필요한 통신 흐름을 원활하게 합니다.
- Cisco SA(Secure Access) - DLP 엔진: 모든 DLP 컨피그레이션이 상주하는 기본 구성 요소입니다. Secure Access 콘솔을 사용하여 다음을 정의합니다.
    - 데이터 식별자: 시스템에서 모니터링해야 하는 특정 패턴 또는 민감한 데이터 유형(예: PII, 신용카드 번호 또는 내부 프로젝트 코드).
    - DLP 정책: 민감한 데이터가 탐지될 때 시스템이 어떻게 반응해야 하는지를 지시하는 규칙(예: 차단, 암호화 또는 알림).

    - 정책 작업: DLP 엔진에 의해 트리거되는 자동화된 응답(예: 이메일 전송 방지 또는 필수 암호화 적용).
- 통합 프레임워크: 정책 평가 및 후속 시행을 위해 ETD가 이메일 메타데이터를 Secure Access DLP 엔진에 전달할 수 있도록 하는 백엔드 연결입니다.

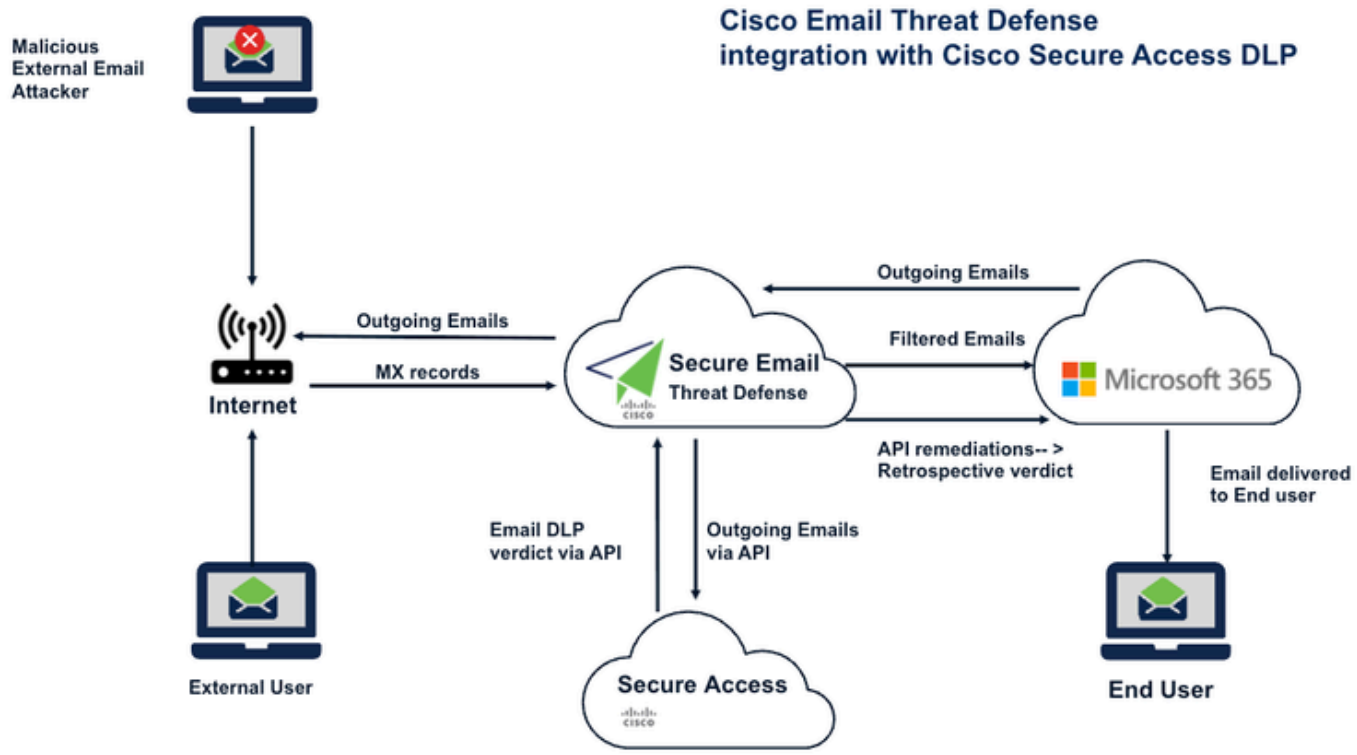
이메일 DLP 정책 기능

Cisco Secure Access에서 이메일 DLP 정책을 생성할 때 다음을 구성할 수 있습니다.

- 규칙 이름 및 설명
- 심각도 수준
- 데이터 분류
- 검사 범위:
    - 이메일 제목
    - 메시지 본문
    - 첨부 파일 이름
    - 첨부 파일 컨텐트
- 파일 제어:
    - MIP 레이블
    - Titus 레이블
- 발신인 조건
- 수신인 조건
- 정책 작업:
    - 모니터링
    - 차단
- 선택적 사용자 알림

네트워크 다이어그램

Cisco Secure Email Threat Defense와 Cisco Secure Access의 통합을 보여 주는 네트워크 다이어그램과 트래픽 흐름도를 함께 아래에서 확인하십시오.



참고: 위 그림에서 Exchange Server는 O365이지만, 이 DLP 컨피그레이션은 SMTP를 지원하는 모든 Exchange Server에서 수행할 수 있습니다.

참고: Cisco Email Threat Defense와 Cisco Secure Access를 API를 통해 통합하려면 "Cisco ETD(Email Threat Defense)를 Cisco Secure Access와 통합하는 단계:" 문서를 참조하십시오.

구성

Cisco Secure Access에서 이메일 DLP 정책 구성

1단계: Cisco Secure Access 로그인

필요한 권한이 있는 관리자 계정을 사용하여 Cisco SA(Secure Access) 콘솔에 로그인합니다.

2단계: 이메일 DLP 규칙 생성으로 이동합니다.

Secure Access 대시보드에서 다음으로 이동합니다.

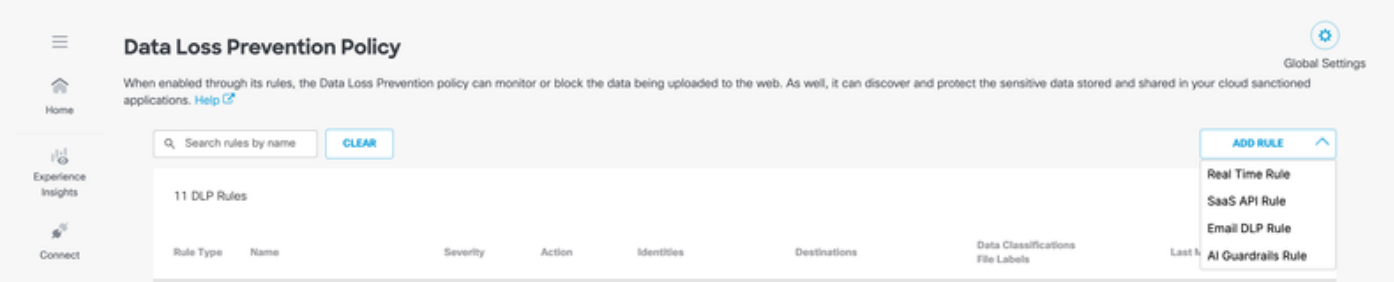
Secure(보안) > Policy(정책) > Data Loss Prevention Policy(데이터 손실 방지 정책) > Add Rule(규칙 추가) > Email DLP Rule(이메일 DLP 규칙)을 선택합니다.

그러면 Add New Email Rule(새 이메일 규칙 추가) 페이지가 열립니다.

Cisco Secure Access는 이메일 DLP 규칙을 생성하는 두 가지 방법을 제공합니다.

- 사전 정의된 DLP 템플릿을 사용하여 이메일 DLP 규칙 생성
- 사용자 지정 DLP 템플릿을 사용하여 이메일 DLP 규칙 생성

그림 1. 이메일 DLP 규칙 생성으로 이동합니다.



옵션 1: 사전 정의된 DLP 템플릿을 사용하여 이메일 DLP 규칙 생성

3단계: 기본 규칙 정보 구성

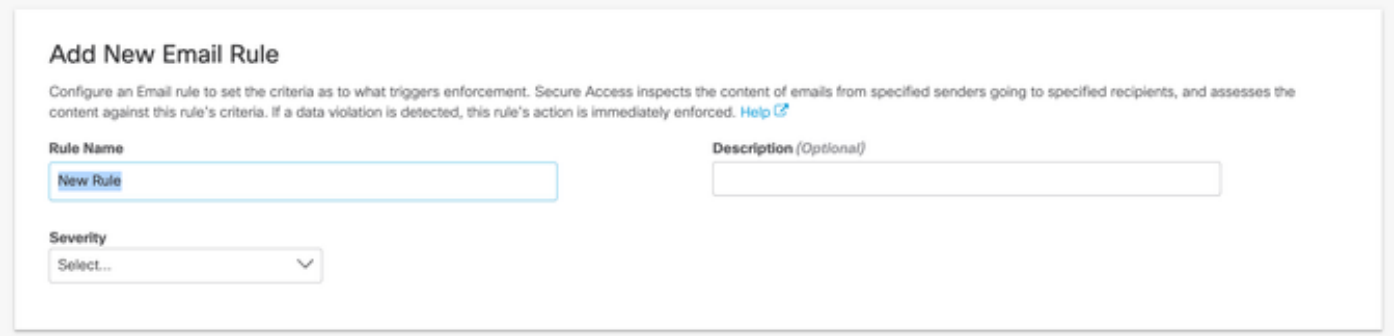
ADD RULE(규칙 추가) > Email DLP Rule(이메일 DLP 규칙) 창으로 이동합니다.

Add New Email Rule(새 이메일 규칙 추가) 창에 다음 세부사항을 입력합니다.

- 규칙 이름
  이메일 DLP 규칙에 대한 설명 이름을 입력합니다.
- 설명
  규칙의 목적에 대한 간단한 요약을 제공합니다.
- 심각도
  정책에 적합한 심각도 수준을 선택합니다.
    - 낮음

- 중간
- 높음
- Critical(심각)

이러한 필드는 관리, 보고 및 운영 가시성에 대한 규칙을 분류하는 데 도움이 됩니다.



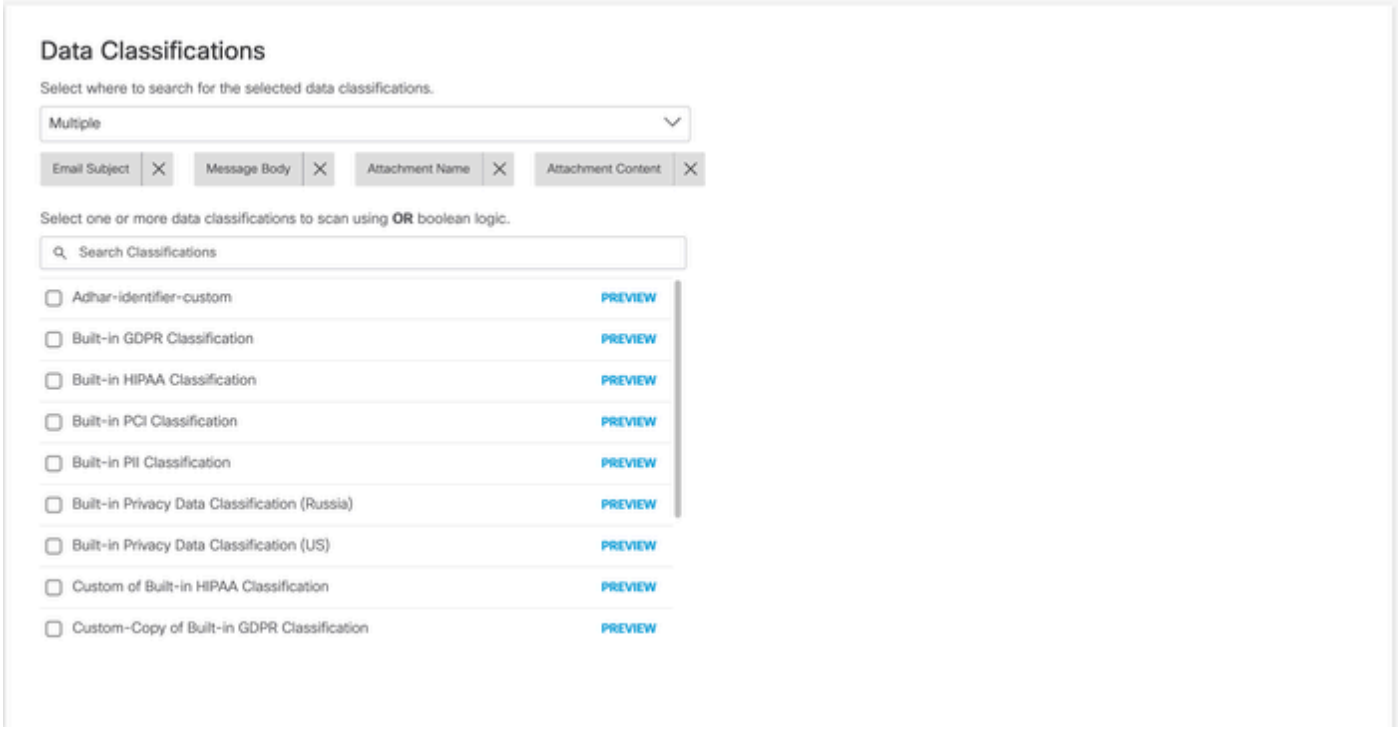
4단계: 데이터 분류 선택

Data Classifications(데이터 분류)에서 잠재적인 DLP 위반이 있는지 이메일 콘텐츠를 검사하는 데 사용할 사전 정의된 DLP 템플릿을 선택합니다.

다음으로, 선택한 분류와 일치해야 하는 위치를 선택합니다. 지원되는 검사 위치는 다음과 같습니다.

- 이메일 제목
- 메시지 본문
- 첨부 파일 이름
- 첨부 파일 컨텐트

이렇게 하면 정책에서 민감한 정보에 대한 메시지 내용과 첨부 파일을 모두 검사할 수 있습니다.



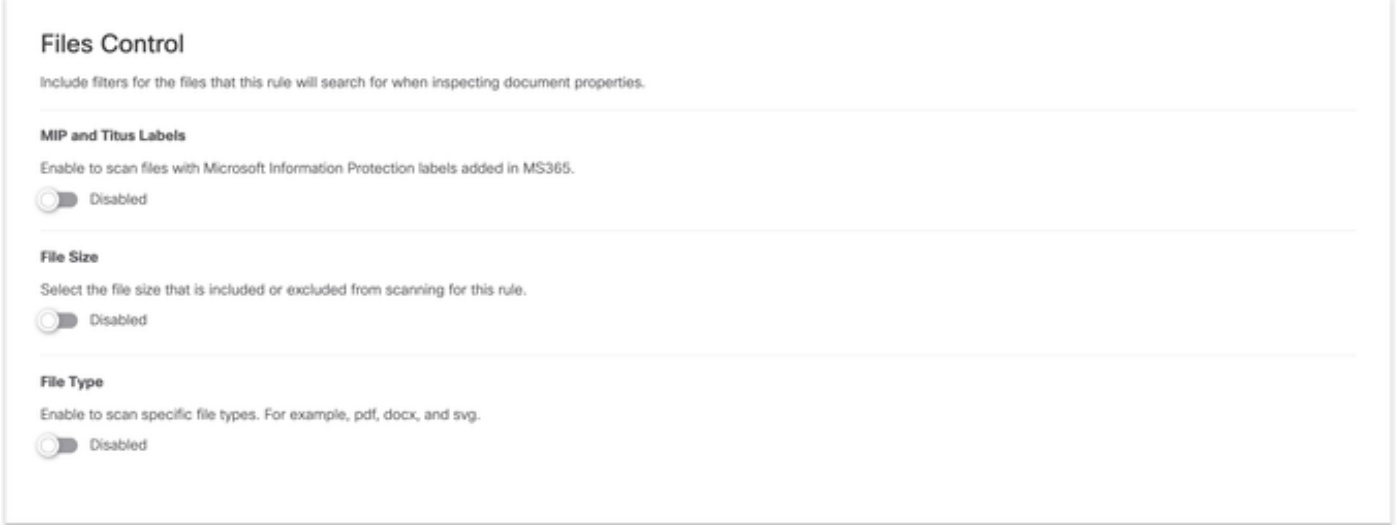
5단계: 파일 제어 구성

Files Control(파일 제어)에서 규칙에 대한 파일 기반 검사 기준을 구성합니다.

여기에는 다음이 포함됩니다.

- MIP 레이블
- Titus 레이블

이러한 설정은 DLP 시행에서 첨부 파일과 연결된 민감도 레이블 또는 메타데이터를 고려해야 하는 경우에 유용합니다.



6단계: 발신자 범위 정의

Senders(발신자) 섹션에서 정책이 적용되는 발신자를 지정합니다.

사용 가능한 옵션은 다음과 같습니다.

- 모든 발송인
- 특정 발신자
- 특정 보낸 사람 제외

이렇게 하면 규칙을 광범위하게 적용하거나 선택한 사용자 또는 그룹으로 제한할 수 있습니다.

7단계: 수신자 범위 정의

Recipients(수신자) 섹션에서 정책 평가에 포함하거나 제외해야 하는 사용자 또는 그룹을 선택합니다.

사용 가능한 옵션은 다음과 같습니다.

- 모든 사용자 포함
- 특정 사용자 포함
- 특정 사용자 제외

이를 통해 원하는 수신자를 기준으로 정책 적용을 맞춤화할 수 있습니다.

8단계: 정책 작업 선택

Action(작업) 섹션에서 Cisco Secure Access가 DLP 규칙을 위반하는 것으로 확인된 이메일을 처리하는 방법을 선택합니다.

사용 가능한 작업은 다음과 같습니다.

- 모니터링
  이메일이 허용되며, 가시성 및 보고를 위해 이벤트가 로깅됩니다.
- 차단
  민감한 데이터의 전송을 방지하기 위해 이메일이 삭제됩니다.

참고: 현재 양성으로 식별된 이메일은 Monitor(모니터링) 작업을 통해 허용되거나 Block(차단) 작업을 통해 삭제될 수 있습니다.

중요: 이메일 DLP 작업은 Cisco Secure Access에서만 구성됩니다. Secure Access에 의해 이메일이 차단된 경우, Cisco ETD 메시지 추적에도 이벤트가 표시됩니다.

9단계: 사용자 알림 구성

알림 옵션은 수신자에게만 제공됩니다.

User Notifications(사용자 알림)에서 이메일이 DLP 정책과 일치할 때 사용자에게 알림을 보낼지 여부를 구성합니다.
"Actor's Manager" 또는 "Custom Recipient"에게 알릴 수 있는 옵션이 있습니다. "Custom Recipient(맞춤형 수신자)"는 누구라도 될 수 있습니다.

필요에 따라 이메일 메시지 템플릿을 Default(기본값)에서 Custom(맞춤형) 알림으로 구성합니다.

활성화된 경우 알림은 사용자 인식을 개선하고 반복되는 정책 위반을 줄이는 데 도움이 됩니다. 조직의 운영 및 규정 준수 요구 사항에 따라 이 설정을 구성합니다.

9단계: 사용자 알림 구성

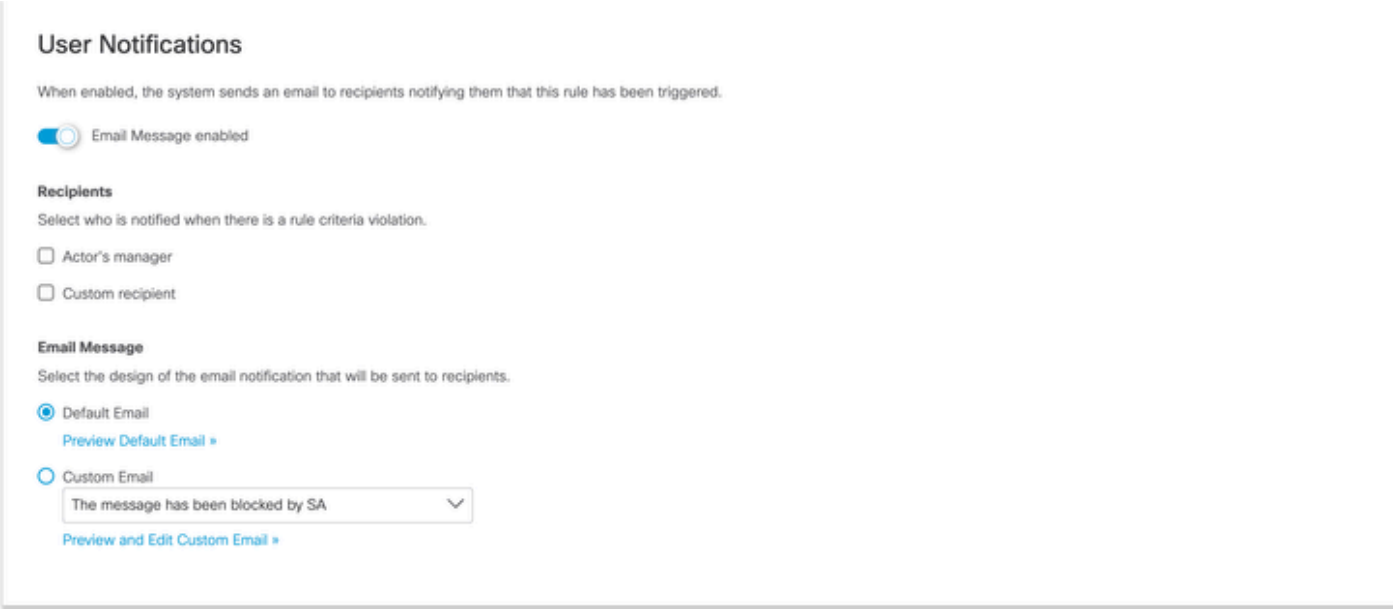
사용자 알림은 보안 인식을 높이고 규정 준수를 보장하는 강력한 툴입니다. 이메일이 DLP 정책을 트리거하면 사용자 또는 관리자에게 알림으로써 위반에 대한 즉각적인 피드백과 컨텍스트를 제공할 수 있습니다.

참고: 알림 설정은 주로 이메일 수신자와 지정된 이해관계자를 대상으로 합니다.

알림을 구성하려면

1. 알림 수신자 정의: User Notifications(사용자 알림) 섹션에서 알림을 수신할 사용자를 지정합니다. 두 가지 기본 옵션이 있습니다.
   - 배우의 매니저: 정책 위반을 트리거한 사용자의 관리자에게 직접 알림을 보냅니다.
   - 사용자 지정 받는 사람: 모든 이메일 주소(예: 보안 운영 센터 또는 특정 부서 책임자)를 지정할 수 있습니다.
2. 메시지 템플릿 선택: Defaultnotification 템플릿 또는 Customnotification 중에서 선택할 수 있습니다.
   - 권장 사항: 조직에 특정 규정 준수 메시지 또는 내부 브랜딩 요구 사항이 있는 경우 사용자 지정을 사용하여 이메일 본문을 맞춤화하여 수신자에게 명확하고 실행 가능한 지침을 제공합니다.
3. 검토 및 저장: 구성이 완료되면 설정이 조직의 운영 및 규정 준수 정책에 맞게 조정되어야 합니다.

모범 사례: 이러한 알림을 활성화하면 민감한 데이터 처리 절차에 대해 실시간으로 사용자를 교육하여 반복되는 정책 위반을 줄일 수 있는 효과적인 방법입니다.



참고: 알림 옵션은 테넌트 컨피그레이션 및 정책 설정에 따라 달라질 수 있습니다.

10단계: 규칙 검토 및 저장

규칙 컨피그레이션을 완료한 후

1. 구성된 모든 설정을 검토합니다.
2. 선택한 데이터 분류, 검사 범위, 발신자 및 수신자 조건, 작업이 원하는 정책 동작과 일치하는지 확인합니다.
3. Save(저장)를 클릭하여 이메일 DLP 규칙을 생성합니다.

이제 Cisco Secure Access에서 이메일 DLP 정책이 활성화됩니다.

옵션 2: 사용자 지정 DLP 템플릿을 사용하여 이메일 DLP 규칙 생성

맞춤형 DLP 템플릿 생성에는 두 가지 기본 단계가 포함됩니다. 사용자 지정 식별자 정의 및 데이터 분류 구성.

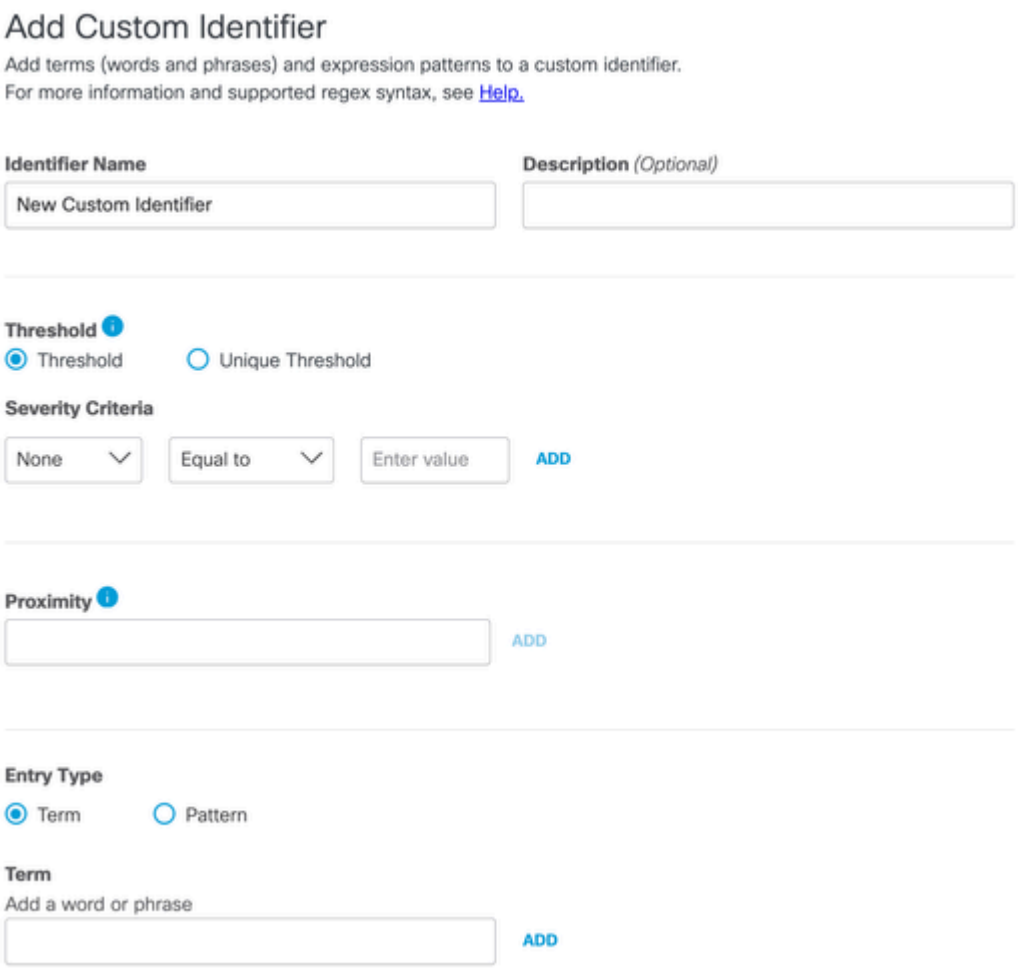
참고: 데이터 분류 엔진은 유연성이 뛰어나 단일 사용자 지정 식별자 또는 AND/OR 부울 연산자로 연결된 사용자 지정 식별자와 사전 정의 식별자의 조합을 사용하여 정책을 구축할 수 있습니다.

11단계: 사용자 지정 식별자 만들기

탐지를 위한 새 데이터 패턴을 정의하려면 다음 단계를 수행합니다.

1. Secure Access Dashboard에 로그인합니다.
2. Secure(보안) > Data Classification(데이터 분류)으로 이동합니다.
3. 사용자 지정 식별자 추가를 클릭합니다.
4. Add Custom Identifier(사용자 지정 식별자 추가) 창에서 다음 매개변수를 구성합니다.

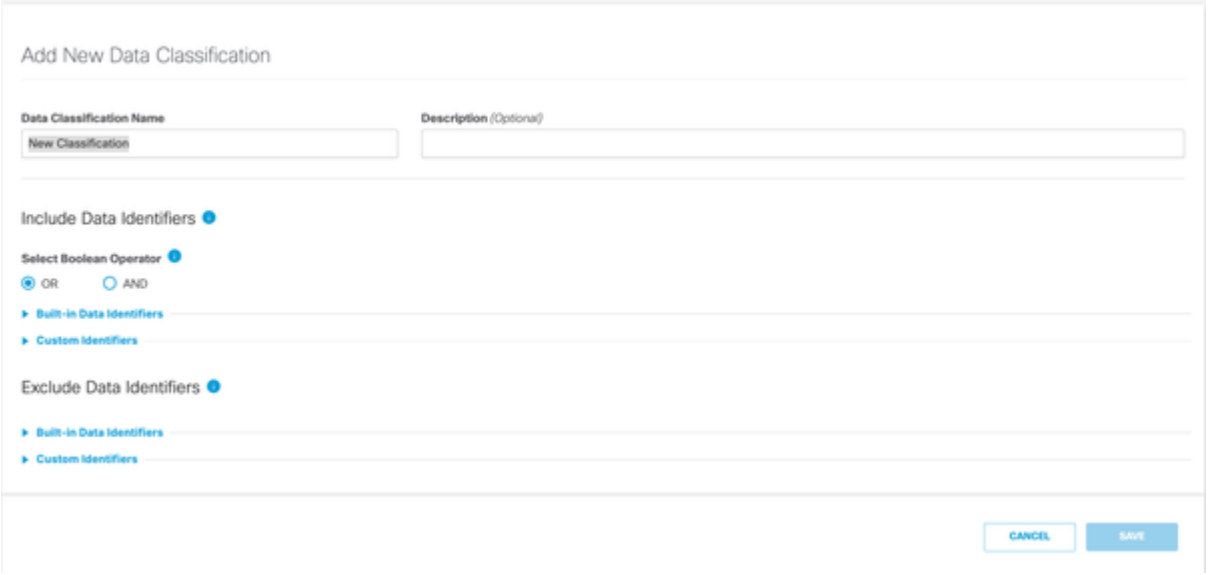
- 이름 및 설명: 탐지할 데이터 유형에 대한 고유한 이름과 간단한 설명을 제공합니다.
- 임계값:
    - 임계값: 탐지된 데이터의 총 빈도를 모니터링합니다.
    - 고유 임계값: 중복된 데이터를 무시하고 데이터의 발생 빈도만 모니터링합니다.
- 심각도 기준: 탐지 빈도에 따라 심각도 수준(Very Low, Low, Medium, High)을 할당합니다. 같음, 보다 큼, 보다 작음 또는 범위와 같은 비교 연산자를 사용하여 이러한 연산자를 정의할 수 있습니다.
- 근접성: 근접 임계값을 설정합니다. 이는 이 식별자 내에 정의된 모든 용어 및 패턴에 개별 용어가 아니라 전체적으로 적용됩니다.
- 항목 유형: 시스템이 데이터를 식별하는 방법을 정의합니다.
    - 용어: 특정 단어나 구.
    - 패턴: 특정 데이터 형식(예: 신용 카드 번호 또는 내부 프로젝트 코드)을 탐지하는 데 사용되는 정규식(regex)입니다.



12단계: 데이터 분류 구성

사용자 지정 식별자가 저장되면 이를 데이터 분류 개체로 통합할 수 있습니다.

1. Secure(보안) > Data Classification(데이터 분류) > Add(추가)로 이동합니다(오른쪽 상단 모서리에 있는 버튼 사용).
2. 사용 가능한 목록에서 새로 만든 사용자 지정 식별자를 선택합니다.
3. (선택 사항) 사용자 지정 식별자를 AND/ORlogic을 사용하여 미리 정의된 식별자와 결합하여 탐지 범위를 세분화합니다.
4. 이메일 DLP 정책에서 사용할 수 있도록 컨피그레이션을 저장합니다.
5. 자세한 내용은 아래 스크린샷을 참조하십시오.
6. 이제 4단계부터 10단계까지 동일한 단계를 수행하여 맞춤형 데이터 분류를 사용하여 정책을 생성합니다.



이러한 구성을 통해 조직은 내부 데이터 구조 및 규정 준수 요구 사항에 특별히 맞춤화된 민감한 정보를 탐지할 수 있습니다.

문제 해결

이메일 DLP 규칙이 예상대로 작동하지 않을 경우 다음을 검토합니다.

규칙이 전자 메일과 일치하지 않습니다.

- 올바른 데이터 분류 템플릿이 선택되었는지 확인합니다.
- 관련 검사 위치가 활성화되었는지 확인합니다.
  - 이메일 제목
  - 메시지 본문
  - 첨부 파일 이름
  - 첨부 파일 컨텐트
- 발신자 및 수신자 필터가 테스트 이메일을 실수로 제외하지 않도록 합니다.

이메일은 차단되지 않음

- 규칙 작업이 Blockand notMonitor로 설정되어 있는지 확인합니다.
- 규칙이 저장되고 활성화되었는지 확인합니다.
- 이메일 콘텐츠가 구성된 DLP 기준과 긍정적으로 일치하는지 확인합니다.

DLP 이벤트는 ETD에 표시되지 않음

- Cisco ETD 및 Cisco Secure Access가 올바르게 통합되었는지 확인합니다.
- ETD에서 관련 이메일 트래픽을 능동적으로 처리하고 있는지 확인합니다.
- Cisco Secure Access에 정책 이벤트가 먼저 있는지 확인합니다.

첨부 파일 기반 일치가 검색되지 않음

- 검사 범위에서 첨부 파일 이름 및/또는 첨부 파일 내용이 선택되었는지 확인합니다.
- MIPorTitusus와 같은 레이블이 규칙 논리의 일부인 경우 파일 제어 설정을 확인합니다.

모범 사례

이메일 DLP 정책을 구축할 때 다음 모범 사례를 고려하십시오.

- Monitormode로 시작하여 Block을 적용하기 전에 정책 동작을 검증합니다.
- 더 쉽게 관리할 수 있도록 명확하고 설명적인 규칙 이름을 사용합니다.
- 의도하지 않은 일치를 줄이기 위해 발신자 및 수신자 조건의 범위를 신중하게 지정합니다.
- 광범위한 구축 전에 대표 데이터로 테스트합니다.
- ETD 메시지 추적을 정기적으로 검토하여 차단되거나 모니터링되는 이메일 활동을 검증합니다.
- 비즈니스별 데이터 식별자가 필요한 경우 사용자 지정 템플릿을 사용하십시오.

요약

Cisco Secure Access는 통합된 Cisco Secure Access 및 Cisco Email Threat Defense 구축에서 이메일 DLP 정책을 구성하기 위한 중앙 플랫폼입니다. ETD는 가시성 및 메시지 추적을 제공하지만 모든 DLP 규칙 생성, 분류 선택, 적용 작업 및 알림이 Secure Access에서 구성됩니다.

관리자는 사전 정의된 DLP 템플릿이나 사용자 지정 DLP 템플릿을 사용하여 이메일 내용과 첨부 파일을 검사하고 발신자와 수신자 범위를 정의하며 모니터링 또는 차단 작업을 적용하여 이메일을 통한 민감한 데이터 손실을 방지할 수 있습니다.

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.