Cisco Secure Email Threat Defense 릴리스 노트

소개

이 문서에는 Cisco Secure Email Threat Defense의 제품 업데이트, 사용 주의 사항 및 알려진 문제에 대한 정보가 포함되어 있습니다.

2021년 7월 12일부터 2022년 9월 29일까지 보관된 Cisco Secure Email Cloud Mailbox의 릴리스 노트는 https://www.cisco.com/c/en/us/td/docs/security/cloud-mailbox/release-notes/cloud-mailbox-release-notes-archive.html 에서 확인할 수 있습니다.

제품 업데이트

2024년 5월 29일

해결된 문제

- 최근 업데이트로 인해 피싱 테스트 우회 규칙에서 발신자 정보가 처리되는 방식에 예기치 않은 문제가 발생했을 수 있습니다. 이러한 문제를 해결하기 위해 이러한 업데이트를 취소하고 3월 19일 이전의 방식으로 돌아가고 있습니다. 기존의 피싱 테스트 우회 규칙이 재생성되며 적용되는 데 며칠이 걸릴 수 있습니다. 우회 규칙 사용에 대한 자세한 지침은 우회 규칙에 관한 권고 요약, 13페이지를 참조하십시오.
- 사소한 버그 수정.

2024년 5월 14일

해결된 문제

- 사소한 버그 수정.

2024년 4월 30일

개선 사항

- 이제 사용자 어카운트가 Accounts(계정) 드롭다운 목록에 알파벳순으로 나열됩니다.
- 이제 공용 API 속도 제한이 북미 및 유럽 지역의 기업에 적용됩니다.
  - API 키는 **Administration(관리) > API Clients(API 클라이언트)**에서 생성할 수 있습니다.
  - 헤더 x-api-key의 요청에 API 키를 포함해야 합니다. 그렇지 않으면 요청이 실패합니다.

  - 테넌트당 현재 속도 제한은 5 요청/초이고, 버스트 제한은 10 요청/초이며, 일일 할당량은 요청 5,000 요청입니다. 한도가 소진된 경우 지원 팀에 연락하여 증가를 요청하십시오.

- W3C URL은 더 이상 이메일에서 추출되지 않으며 Secure Email Threat Defense UI에 표시되지 않습니다.

해결된 문제

- 사소한 버그 수정.

2024년 4월 16일

개선 사항

- Message Search API의 최신 업데이트를 통해 판정 지표, 작업 지표, 첨부 파일 및 링크, 마지막 작업을 기준으로 메시지를 필터링할 수 있습니다.
- 공용 API 속도 제한은 이제 인도 및 오스트레일리아 지역의 기업에 적용됩니다.
  - API 키는 **Administration(관리) > API Clients(API 클라이언트)**에서 생성할 수 있습니다.
  - 헤더 x-api-key의 요청에 API 키를 포함해야 합니다. 그렇지 않으면 요청이 실패합니다.
  - 테넌트당 현재 속도 제한은 5 요청/초이고, 버스트 제한은 10 요청/초이며, 일일 할당량은 요청 5,000 요청입니다. 한도가 소진된 경우 지원 팀에 연락하여 증가를 요청하십시오.

해결된 문제

- 사소한 버그 수정.

2024년 4월 3일

해결된 문제

- 사소한 버그 수정.

2024년 3월 19일

개선 사항

- 이번 릴리스에는 새로운 메시지 보고서 페이지가 도입되었습니다. 이 페이지는 확장된 메시지 보기와 타임라인 보기를 결합하고 추가 기능을 도입합니다. 다음과 같은 새로운 기능을 제공합니다.
  - 이메일 미리보기를 사용하면 최종 사용자에게 표시되는 메시지를 슈퍼 관리자 및 관리자 사용자가 확인할 수 있습니다.

    참고: 사용자가 이메일을 미리 볼 때 감사 로그 레코드가 생성됩니다. 감사 로그는 **Administration(관리) > Business(비즈니스) > Preferences(환경 설정)**에서 다운로드할 수 있습니다.
  - 지난 30일간 전송한 총 메시지 수와 메시지 발신자가 보낸 총 위협 메시지를 보여주는 Sender Messages(발신자 메시지) 그래프.
  - 메시지를 수신한 최종 사용자 사서함 목록을 표시하는 Mailbox List(사서함 목록). 목록에는 마지막 교정 작업 전에 메시지를 읽었는지와 메시지에 대한 교정 오류가 표시됩니다.

자세한 내용은 Cisco Secure Email Threat Defense 사용 설명서를 참조하십시오.

- 피싱 테스트 우회 메시지 규칙은 이제 발신자 이메일 주소 또는 도메인 기준을 Envelope From(봉투 발신자)와만 매치합니다.
- 공개 보고 API의 최신 업데이트는 다음과 같습니다.
  - 상위 10개 위협 발신자 보고서 및 회귀적 판정 수 보고서.
  - 최대 90일로 증가한 날짜 범위.
- 대용량 파일에서 간헐적으로 충돌하는 문제로 인해 .doc 파일에 대한 QR 코드 탐지를 제거했습니다. 가능한 한 빨리 이 기능을 다시 제공하도록 하겠습니다.

해결된 문제

- 사소한 버그 수정.

2024년 3월 4일

개선 사항

- 교정 개선 사항: 발신 및 내부 메시지의 경우, Move to Inbox(받은 편지함으로 이동) 작업을 수행하면 메시지가 받은 편지함 대신 메시지를 최초 발신자 Sent(발신) 폴더로 이동합니다.

해결된 문제

- 사소한 버그 수정.

2024년 2월 21일

개선 사항

- 더 많은 파일 유형에서 QR 코드 탐지를 사용할 수 있습니다. 이전에 발표된 그래픽 파일 외에도 pdf, word, xls, ppt 파일에 있는 QR 코드에서 URL이 추출되어 분석을 위해 엔진으로 전송됩니다.

해결된 문제

사소한 버그 수정.

2024년 2월 06일

개선 사항

- 혼합 방향은 UI 및 API에서 제거되었습니다. 이 값은 Microsoft에서 더 이상 입력하지 않습니다.
- 공용 API의 최신 업데이트는 다음과 같습니다.
  - 새로운 보고 API: 방향별로 스캔한 총 메시지, 판정별 총 트래픽, 위협 메시지를 수신한 상위 10개 대상.
  - 메시지 검색 API 업데이트: 이제 기술별로 메시지를 필터링할 수 있습니다.

해결된 문제

- 사소한 버그 수정.

2024년 2월 1일

개선 사항

- QR 코드 탐지
  - 메시지 본문과 .jpg, .jpeg, .png 첨부 파일에 있는 QR 코드에서 URL이 추출됩니다. 이러한 URL은 메시지에 포함된 다른 URL과 함께 분석됩니다.
  - QR 코드 URL이 링크 섹션의 확장된 메시지 보기에 표시됩니다.
  - URL이 악의적인 것으로 간주되면 악성 URL 기술을 보여줍니다.
  - QR 코드가 포함된 일부 메시지의 경우QR 코드 탐지 기술이 표시됩니다. 이 기술은 향후 릴리스의 모든 QR 코드에 사용할 수 있습니다.

2024년 1월 30일

개선 사항

- Secure Email Threat Defense UI 전체에서 스타일 변경 사항을 적용하여 Cisco Security 제품 전반에 걸쳐 일관성을 향상합니다. 변경 사항은 다음과 같습니다.
  - 다운로드, 도움말, 알림 및 사용자 설정은 페이지 헤더에서 액세스할 수 있습니다.
  - 이전에는 화면 상단에 있었던 메뉴 항목은 왼쪽 메뉴에서 액세스할 수 있습니다.

해결된 문제

- 사소한 버그 수정.

2024년 1월 18일

해결된 문제

- 사소한 버그 수정.

2023년 12월 13일

개선 사항

- 이제 메시지 규칙을 삭제할 수 있습니다. 이전에는 규칙 비활성화만 할 수 있었습니다.
- 이제 영향력이 큰 직원 목록을 일반적으로 사용할 수 있습니다. 이 목록을 사용하여 사용자 가장 공격으로부터 조직을 보호합니다.
  - 조직 내 중요한 사람 100명의 목록을 작성합니다. 목록은 표시 이름 및 발신자 이메일 주소에 대한 정밀 검사를 위해 엔진으로 전송됩니다.
  - 구성된 정보에서 벗어나는 경우 확정된 메시지의 판정 세부 정보 패널에서 사용자 사칭으로 식별됩니다.

- 공용 API의 최신 업데이트는 다음과 같습니다.
  - 메시지 검색 API의 요청 본문에 있는 **"isRetroVerdict": true**를 추가하여 회귀 판정을 기반으로 메시지를 필터링하는 기능.
  - 공용 API에 속도 제한이 구현되었습니다. API 키는 **Settings(설정) > Administration(관리) > API Clients(API 클라이언트)**에서 생성할 수 있습니다.

    참고: 속도 제한은 2024년 2월부터 적용됩니다. 헤더 x-api-key의 요청에 API 키를 포함해야 합니다. 그렇지 않으면 요청이 실패합니다.
- 메시지 다운로드 보고서에서 Auto Remediated(자동 교정) 열이 Remediation Method(교정 방법)으로 이름이 변경되고 메시지가 자동으로 수정되었는지, 수동으로 수정되었는지 또는 API로 수정되었는지가 표시됩니다.

해결된 문제

- 사소한 버그 수정.

2023년 12월 4일

해결된 문제

- 사소한 버그 수정.

2023년 11월 16일

개선 사항

- 공용 API에 추가하면 메시지를 프로그래밍 방식으로 교정 및 재분류할 수 있습니다. 자세한 내용은 API 가이드를 참고하십시오. 이 가이드는 Secure Email Threat Defense 도움말 메뉴 또는 https://developer.cisco.com/docs/message-search-api 에서 액세스할 수 있습니다.

해결된 문제

- 사소한 버그 수정.

2023년 10월 31일

개선 사항

- Email Threat Defense는 이제 첨부 파일을 검사하고 엔진 분석을 위해 URL을 추출합니다.
  - 250개가 넘는 파일 유형을 지원하며 엔진으로 전송합니다.
  - 파일 분석은 5가지 레벨의 아카이브 파일(예: .zip 파일)을 지원합니다.
- 허용 목록 및 판정 재정의 메시지 규칙을 사용하면 스팸 및 그레이메일 외에 위협 판정을 선택할 수 있습니다.

해결된 문제

- 사소한 버그 수정.

2023년 10월 18일

해결된 문제

- 사소한 버그 수정.

2023년 10월 3일

개선 사항

- 이제 홈페이지 및 영향 보고서의 위협 및 원치 않는 메시지 아이콘을 클릭할 수 있습니다.

해결된 문제

- 사소한 버그 수정.

2023년 9월 20일

개선 사항

- 타임라인 보기에 다음이 표시됩니다.
  - 교정 시점에 메시지를 읽은 사서함 목록.
  - 메시지의 교정 오류와 오류가 발생한 사서함에 대한 정보. 타임라인에서 오류 로그를 다운로드할 수도 있습니다.

해결된 문제

- 사소한 버그 수정.

2023년 9월 8일

해결된 문제

- 사소한 버그 수정.

2023년 8월 28일

개선 사항

- 이제 작은 EML 파일이 즉시 다운로드됩니다. 용량이 큰 파일은 다운로드 페이지에서 계속 액세스할 수 있습니다.
- 이제 수신자 검색 필드에 Envelope To(봉투 수신자) 및 Delivered To(전달받은 주소) 필드가 포함됩니다.

사용 중단 알림

- 사용자 인터페이스의 Organizational-Bcc 및 공개 메시지 검색 API 응답의 bccAddresses는 더 이상 사용되지 않으며 향후 릴리스에서 제거될 예정입니다. 이제 BCC 주소가 To/Cc 필드에 캡처됩니다.

해결된 문제

- 사소한 버그 수정.

2023년 8월 10일

개선 사항

- 관리자는 이제 **Settings(설정)** > **Administration(관리)** > **User(사용자)** 페이지에서 사용자의 역할을 변경할 수 있습니다.
- 확장된 메시지 보기에는 저널 헤더에서 추출된 추가 수신자 데이터가 표시됩니다. 스크롤 가능한 섹션은 To/Cc, Envelope To(봉투 수신자), Delivered To(전달받은 주소) 3개까지 가능합니다.
- 메시지 규칙 상태 열 필터는 마지막으로 선택한 설정이 기본값으로 브라우저에 저장됩니다.

해결된 문제

- 사소한 버그 수정.

2023년 7월 31일

해결된 문제

- 사소한 버그 수정.

2023년 7월 18일

개선 사항

- 영향력이 큰 직원 페이지에는 지난 30일 동안 사용자가 사칭당한 횟수가 표시됩니다.
- 공용 메시지 검색 API의 최신 업데이트는 다음과 같습니다.
  - 확장된 검색 기능: 수신자 이메일 주소, 발신자 이메일 주소, 인터넷 메시지 ID.
  - 이제 API 응답에서 메시지가 수동으로 재분류되었는지를 나타낼 수 있습니다.
  - 공용 API 가이드로 연결되는 링크는 Secure Email Threat Defense 도움말 메뉴에서 액세스할 수 있습니다. 이 가이드는 https://developer.cisco.com/docs/message-search-api/ 에 있습니다.

해결된 문제

- 사소한 버그 수정.

2023년 6월 29일

해결된 문제

- 사소한 버그 수정.

2023년 6월 19일

개선 사항

- 상태를 기준으로 메시지 규칙을 필터링하여 활성화 또는 비활성화된 규칙을 표시하거나 숨길 수 있습니다.

해결된 문제

- 사소한 버그 수정.

2023년 6월 9일

개선 사항

- 메시지 그래프 및 빠른 필터 업데이트:
  - 이제 주별 보기에서 각 요일의 시작이 명확하게 강조 표시되어 특정 요일을 자세히 살펴볼 수 있습니다.
  - 위협 및 방향 메트릭은 파란색으로 표시되어 메시지를 필터링하는 데 사용할 수 있는 링크임을 나타냅니다.

해결된 문제

- 사소한 버그 수정.

2023년 5월 19일

개선 사항

- Cisco Secure Email Threat Defense 공용 API가 이 릴리스에 도입되었습니다. API를 사용하면 안전하고 확장 가능한 방식으로 프로그래밍 방식으로 액세스하고 데이터를 사용할 수 있습니다. API 설명서는 https://doc.api.etd.cisco.com/ 을 참조하십시오.

해결된 문제

- 사소한 버그 수정.

2023년 5월 11일

개선 사항

- 2023년 5월 11일 이후에 생성된 비즈니스의 경우 스팸 및 그레이메일 분석은 기본적으로 꺼짐으로 설정됩니다. 이 설정은 정책 페이지에서 조정할 수 있습니다.
- 메시지 그래프 및 빠른 필터

  - 위협 및 메시지는 메시지 페이지 상단에 그래픽으로 표시됩니다.
  - 위협 및 범주 분류를 사용하면 합계를 확인하고 위협을 쉽게 필터링할 수 있습니다.
  - 격리 합계가 표시되며 필터링할 수 있습니다.
  - 메시지 방향 합계가 표시되고 필터링할 수 있습니다.
- 이제 홈페이지 메시지 스캔 그래프가 메시지 페이지로 피벗되어 1시간(일별 보기), 3시간(주간 그래프 지점) 및 일(주간 X 축 레이블)에 대한 맞춤형 시간 프레임이 표시됩니다.

해결된 문제

- 사소한 버그 수정.

2023년 4월 20일

개선 사항

- Secure Malware Analytics 탐지는 판정 상세 정보 패널에 악성 행동 지표 기술로 표시됩니다.
- Secure Endpoint 탐지는 판정 상세 정보 패널에 낮은 파일 평판 기술로 표시됩니다.
- 메시지 수신자는 영향력이 큰 직원이 먼저 표시되도록 정렬됩니다.

해결된 문제

- 사소한 버그 수정.

2023년 4월 13일

개선 사항

- Secure Email Threat Defense가 SecureX와 추가로 통합됩니다. 이제 통합 제품의 SecureX 피벗 메뉴에서 직접 특정 관찰 가능 개체를 포함하는 메시지를 격리할 수 있습니다. 또한 피벗을 사용하여 Secure Email Threat Defense에서 검색을 시작할 수 있습니다. 피벗할 수 있는 관찰 가능 개체는 다음과 같습니다.
  - 이메일 주소
  - 이메일 메시지 ID
  - 이메일 제목
  - 파일 이름
  - 발신자 IP
  - SHA 256
  - URL

2023년 3월 22일

개선 사항

- Cisco Secure Email Cloud Gateway를 메시지 소스로 사용하는 기업을 위한 새로운 인증 없음 모드가 도입되었습니다. 이 가시성 전용 모드에서는 Microsoft에 인증하지 않고도 Secure Email Threat Defense로 트래픽을 전송할 수 있습니다. 이 모드에서는 메시지를 교정할 수 없습니다. 신규 비즈니스에 대한 초기 설정 흐름 및 정책 페이지 설정이 이 구성을 지원하도록 업데이트됩니다.

해결된 문제

- 2023년 3월 12일 Daylight Saving Time(서머 타임) 조정과 함께 도입되었던 그래프 표시 방식 관련 문제가 이제 해결되었습니다.

2023년 3월 15일

개선 사항

- 사용자 프로파일 메뉴에서 Secure Email Threat Defense 시스템 상태 페이지에 대한 링크를 사용할 수 있습니다.

해결된 문제

- 사소한 버그 수정.

2023년 2월 27일

개선 사항

- 정책 페이지에 스팸 및 그레이메일 분석 및 교정 기능을 켜거나 끌 수 있는 새로운 옵션이 있습니다. 끄기를 선택하면 스팸 및 그레이메일 및 원치 않는 메일 패널과 옵션이 제거됩니다.
  - 기존 어카운트는 기본적으로 스팸 및 그레이메일 분석이 켜짐으로 설정되어 있습니다.
  - 향후 Cisco SEG 구성을 사용하는 어카운트는 기본적으로 스팸 및 그레이메일 분석이 꺼짐으로 설정됩니다. SEG에서 스팸 및 그레이메일 분석을 이미 수행하고 있습니다.
- 영향력이 큰 직원 목록에 있는 개인에 대해 설정된 정보의 편차는 확정된 메시지의 판정 세부 사항 패널에서 기술로 식별됩니다.

해결된 문제

- 일부 고객은 Secure Email Threat Defense에 도달하기 전에 HTTP 헤더가 제거되는 로그인 문제를 경험했습니다. 문제가 해결 되었습니다.

2023년 2월 8일

해결된 문제

- 사소한 버그 수정.

2023년 1월 31일

개선 사항

- 홈페이지에는 하루 또는 일주일 동안의 데이터 표시를 전환할 수 있는 옵션이 있습니다.
- 정책 페이지의 가져온 도메인 섹션에는 가져온 도메인의 총 수와 자동 교정을 위해 표시된 도메인 수가 표시됩니다. 목록에는 부분 일치 검색으로 목록을 필터링할 수 있는 검색 기능이 있습니다.
- 이제 영향 보고서의 시작 날짜를 편집할 수 있습니다. 이렇게 하면 30일 범위 또는 달력 월별 보기의 경우 매월 1일을 선택할 수 있습니다.
- 메시지 페이지 필터에는 필터가 적용된 시간이 표시됩니다. 새로운 Reset All(모두 재설정) 링크가 페이지 맨 위에 추가되어 필터를 기본값으로 다시 설정하는 작업을 간소화합니다. Reset Filters(필터 재설정) 버튼은 사용하기 쉽도록 필터 패널 하단에 있습니다.
- 이제 타임라인 보기에 수신, 교정, 재분류 등의 이벤트의 시간(초)가 표시됩니다.
- 이제 재분류된 마우스 포인터 텍스트에 날짜 및 시간이 표시됩니다.
- 새로운 초기 필드 평가판 기능: 영향력이 큰 직원 목록
  - 관리자는 표시 이름과 발신자 이메일 주소에 대한 심층 조사를 위해 최대 100명의 목록을 생성하여 Talos로 전송할 수 있습니다.
  - **참고:** 지금 목록을 작성하면 향후 릴리스의 판정 세부 사항에서 사용자 사칭 기술을 확인할 수 있습니다.

해결된 문제

- 사소한 버그 수정.

2022년 12월 15일

개선 사항

- 이제 메시지 페이지 필터를 사용하여 발신자 IP 주소로 검색할 수 있습니다.
- 알림에 대해 Clear All(모두 지우기) 버튼이 추가되었습니다.
- **Settings(설정) > Download(다운로드) > Download EML(EML 다운로드)** 페이지에서 메시지 제목을 클릭하면 해당 메시지로 쉽게 돌아갈 수 있습니다.

해결된 문제

- 사소한 버그 수정.

2022년 11월 17일

개선 사항

- 메시지 페이지의 발신자 열이 발신자(표시 이름/아는 발신자)로 변경되었습니다.

해결된 문제

- 사소한 버그 수정.

2022년 11월 9일

개선 사항

- 이제 Cisco Secure Email Cloud Gateway를 메시지 소스로 사용하는 기능을 사용할 수 있습니다. 이 초기 릴리스에서는 Microsoft O365 사서함으로 지원이 제한됩니다. 신규 비즈니스에 대한 초기 설정 흐름 및 정책 페이지 설정이 이 구성을 지원하도록 업데이트됩니다.
- 이제 브랜드 사칭 탐지를 지원합니다. 구성을 변경할 필요가 없습니다. 현재 1,500개의 브랜드가 색인화되어 있으며, 향후 더 많은 브랜드가 추가될 예정입니다.
- 홈페이지 대시보드에는 지난 24시간 동안의 비즈니스 상태를 빠르게 보여주는 새로운 위젯과 그래프가 포함되어 있으며, 필터링된 메시지 목록으로 빠르게 전환할 수 있습니다. 다음 항목이 포함됩니다.
  - 위협: BEC, 사기, 피싱 및 악성 탐지 횟수를 표시합니다.
  - 원치 않는 메일: 스팸 및 그레이메일 탐지의 스파크라인 그래프를 보여줍니다.
  - 검사된 메시지: 메시지 트래픽의 그래프를 보여줍니다.
  - 잠재적으로 침해된 어카운트: 조직 내에서 위협 메시지를 전송하는 것이 확인된 내부 주소를 나열합니다.
  - 빠른 메시지 필터: 회귀 판정, 격리된 메시지, 메시지 규칙이 적용된 메시지에 대한 빠른 링크를 표시합니다.
- https://ciscosecureemailthreatdefense.statuspage.io 에서 새로운 Secure Email Threat Defense 상태 페이지를 사용할 수 있습니다. 구독 상태가 변경될 때 업데이트를 받습니다.

해결된 문제

- 사소한 버그 수정.

2022년 10월 25일

개선 사항

- Cisco Secure Email Cloud Mailbox가 Cisco Secure Email Threat Defense로 이름이 변경되었습니다. 향후 인터페이스, 설명서 및 마케팅 자료에서 이름이 변경되는 것을 확인할 수 있습니다.

해결된 문제

- 사소한 버그 수정.

사용 주의 사항

우회 규칙에 관한 권고 요약

우회 규칙을 생성하고 사용할 때는 다음과 같은 중요 주의 사항에 유의하십시오.

- 우회 규칙은 규칙 조건과 일치하는 메시지에 대한 모든 검사 및 보호를 우회합니다. 고객 직원 보안 인식 교육(피싱 테스트) 이외의 사용 사례 또는 조직의 보안 사서함에 대한 최종 사서함 사용자 보고 이외의 사용 사례에는 우회 규칙을 사용하지 마십시오. 이러한 시나리오는 우회 규칙만 지원됩니다. 기타 모든 시나리오의 경우에는 판정 재정의 또는 허용 규칙만 지원됩니다.
- 피싱 테스트 공급업체에서 제공하는 전용 발신자 IP 주소/CIDR 블록만 우회 규칙의 기반으로 사용할 것을 강력히 권장합니다.
- 피싱 테스트 공급업체가 전용 발신자 IP 주소/CIDR 차단을 제공할 수 없는 경우, 우회 규칙에 발신자 도메인 또는 이메일 주소를 사용하면 스푸핑 가능성이 있는 메시지를 우회할 수 있으므로 주의하세요.
- 바이패스 규칙에서 발신자 도메인 또는 이메일 주소를 사용하려면 발신자 이메일 인증이 공급업체의 SPF 레코드에 의해 엄격하게 범위가 지정되고 조직의 업스트림 엣지 이메일 제어가 강력하게 시행되며 지정된 발신자 도메인 또는 발신자 이메일 주소가 우회 규칙과 일치하려는 모든 메시지의 최종 반환 경로 헤더와 정확히 일치하는 것을 별도로 검증해야 합니다.
- 지원 케이스를 열어 위의 지침을 따르는 기존 우회 규칙을 검증하도록 지원을 요청하십시오.

Microsoft Excel 셀 크기 제한

Microsoft Excel에서는 셀당 32,767자로 제한됩니다. 데이터를 CSV로 내보낸 다음 Excel에서 열 경우, 문자 제한을 초과하는 데이터는 다음 행으로 이동합니다.

Microsoft 어카운트에 성이 없으면 Microsoft를 사용하여 Security Cloud Sign On에 로그인할 수 없습니다.

Microsoft 365에서는 어카운트에 이름과 성이 정의되어 있지 않아도 됩니다. 성이 없는 Microsoft 어카운트로 인증을 시도할 때 Security Cloud 로그온에서 다음 오류가 반환됩니다.

400 잘못된 요청. 사용자를 만들 수 없습니다. 필수 속성이 누락되었습니다.

이 문제를 해결하려면 Microsoft 365 어카운트에 이름과 성이 모두 정의되어 있는지 확인하십시오.

메시지가 수동으로 재분류될 때 Trends(추세) 지연

메시지를 수동으로 재분류할 경우 변경 사항이 추세 페이지에 반영되기까지 최대 1시간이 지연될 수 있습니다.

알려진 문제

Microsoft 허용 목록 및 안전한 발신자

Microsoft의 MSAllowList 플래그에 대한 최근 변경 사항으로 인해, 조직에서 개별 사용자가 사서함에서 허용 목록을 구성하도록 허용하고 메시지가 사용자의 허용 목록에 포함되는 경우 Secure Email Threat Defense에서 Microsoft 허용 목록이 항상 적용되는 것은 아닙니다.

Secure Email Threat Defense에서 이러한 설정을 준수하도록 하려면 Policy(정책) 페이지에서 **Do not remediate Microsoft Safe Sender messages with Spam or Graymail verdicts(Microsoft 수신 허용 - 발신자 메시지를 스팸 또는 그레이메일 판정으로 치료하지 않음)** 확인란을 선택합니다. 수신 허용 - 발신자 플래그는 스팸 및 그레이메일 판정에는 적용되지만 악성 및 피싱 판정에는 적용되지 않습니다. 즉, 스팸 또는 그레이메일 판정이 있는 수신 허용 - 발신자 메시지는 치료되지 않습니다.

대화 보기

대화 보기를 사용할 때 다음 문제가 발생할 수 있습니다.

- + 기호는 추가 메시지가 없더라도 + 기호를 클릭할 때까지 사라지지 않습니다.
- 수평 노드는 9개로 제한됩니다.