메시지

메시지 페이지에는 메시지 및 검색 결과가 표시되며, 가능한 보안 침해를 찾을 수 있습니다. 페이지당 최대 100개의 메시지를 표시할 수 있습니다.

메시지 페이지 아이콘

다음 표는 메시지 페이지에서 사용되는 아이콘과 그 의미를 보여줍니다.

표 1 메시지 페이지 아이콘

아이콘	이름	설명
	링크	메시지에 링크가 포함되어 있습니다.
	첨부 파일	메시지에 첨부 파일이 포함되어 있습니다.
	수동 조치 또는 수동 재분류	메시지가 수동으로 조치되었거나 재분류되었습니다. 메시지가 조치된 경우 작업 옆에 아이콘이 표시되고 메시지가 교정된 경우 판정 옆에 아이콘이 표시됩니다.
	회귀 판정	소급 판정이 적용되었습니다. 소급 판정은 Secure Email Threat Defense에서 메시지를 처음 검사한 후에 적용된 판정입니다.
	허용됨	메시지가 표시된 항목에 따라 허용되었습니다(허용 목록, MS 허용 목록 또는 안전한 발신자).
	판정 재정의	판정 재정의 메시지 규칙에 따라 판정이 재정의되었습니다.
	분석 우회	분석 우회 메시지 규칙으로 인해 메시지가 분석되지 않았습니다. 규칙의 유형(보안 사서함 또는 피싱 테스트)이 표시됩니다.
	BEC	메시지가 수동 또는 자동 조치를 통해 BEC(Business Email Compromise)로 표시되었습니다.
	스캠	메시지가 수동 또는 자동 조치를 통해 스캠으로 표시되었습니다.
	Phishing	메시지가 수동 또는 자동 조치를 통해 피싱으로 표시되었습니다.
	Malicious	메시지가 수동 또는 자동 조치를 통해 메시지가 악성으로 표시되었습니다.
	Spam	메시지가 수동으로 또는 자동 조치를 통해 스팸으로 표시되었습니다.

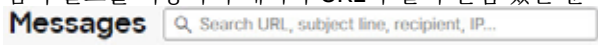
표 1 메시지 페이지 아이콘

아이콘	이름	설명
	그레이메일	메시지가 그레이메일로 표시되었습니다. 그레이메일은 마케팅, 소셜 또는 정크로 확인된 메일입니다.
	중립	메시지가 중립으로 표시되었습니다.
	수신	O365 테넌트 외부에서 수신한 메일입니다.
	내부	O365 테넌트 내에서 발송된 메일입니다.
	발신	O365 테넌트 외부의 수신자에게 발송된 메일

검색 및 필터

달력 컨트롤을 사용하여 정의된 기간(가장 최근 일, 주 또는 월)이나 지난 90일 내의 지정 기간의 데이터를 표시합니다.

검색 필드를 사용하여 해시나 URL과 같이 관심 있는 문자열 또는 지표를 검색합니다.

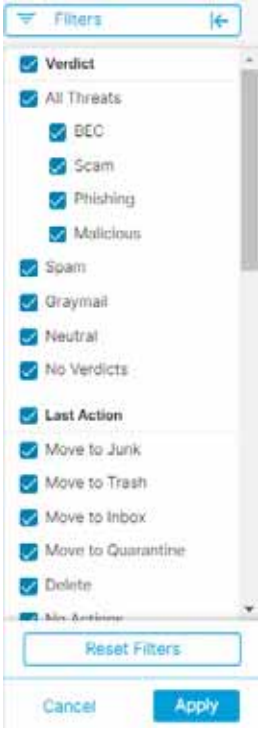


필터 패널

필터 패널을 사용하여 검색을 구체화합니다. 예를 들어, 특정 발신자로부터 전송된 모든 메일, 특정 판정이 있는 메일, 첨부 파일 또는 링크가 있는 메일, 재분류된 메일, 정크로 이동한 메일 등을 확인하고자 할 수 있습니다.

1. 화살표를 클릭하여 필터 패널을 확장합니다.

2. 원하는 항목을 선택한 다음 **Apply(적용)**를 클릭합니다. 참고로 판정에서 하나 이상의 항목을 선택해야 합니다.

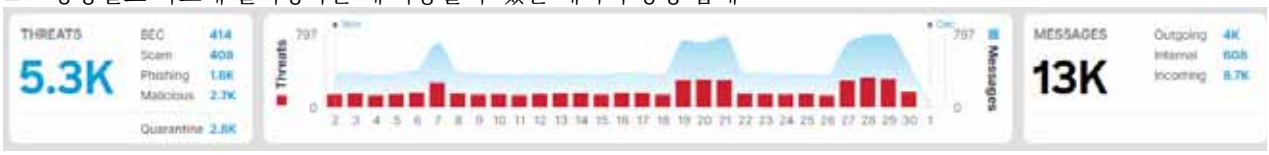


Reset Filters(필터 재설정) 버튼을 사용하여 필터를 기본값으로 재설정합니다.

메시지 그래프 및 빠른 필터

메시지 페이지 상단에는 메시지 그래프와 빠른 필터가 제공되며, 메시지 트래픽을 그래픽으로 보여줍니다. 이 그래프를 사용하여 메시지를 빠르게 필터링합니다. 그래프에는 다음이 포함됩니다.

- 합계를 확인하고 위협을 쉽게 필터링하기 위한 위협 및 범주 분류
- 격리된 항목을 필터링하는 데 사용할 수 있는 격리 합계
- 방향별로 빠르게 필터링하는 데 사용할 수 있는 메시지 방향 합계



판정

Secure Email Threat Defense는 다음 위협 판정을 메시지에 적용합니다.

- **BEC:** BEC(Business Email Compromise)는 사회 공학 및 침입 기술을 사용하여 조직에 재정적 피해를 주는 정교한 스캠입니다.
- **스캠:** 스캠은 복권이나 갈취 사기와 같은 수법을 사용하여 개인에게 재정적 피해를 주는 것에 중점을 둡니다.

- **피싱:** 이러한 메시지는 사용자 이름, 비밀번호, 신용카드 번호 등과 같은 민감한 정보를 얻기 위해 합법적인 서비스를 부정하게 복사하거나 모방한 혐의로 유죄 판정을 받은 적이 있습니다.
- **Malicious(악성) :** 이러한 메시지는 악의적인 소프트웨어의 전달 또는 전파를 포함하거나, 이러한 메시지를 전달하거나, 이를 지원한 경우입니다.

소급 판정

소급 판정은 Secure Email Threat Defense에서 메시지를 처음 검사한 후 메시지에 언젠가 적용된 판정입니다.

Secure Email Threat Defense의 소급 판정은 다른 시스코 보안 제품의 판정과 약간 다릅니다. Secure Email Threat Defense는 인라인 메일 프로세서는 아니지만 메시지의 초기 분석을 완료하기까지 고정 시간 범위가 있습니다. Talos의 심층 URL 분석 등 분석 시간이 더 긴 최신 콘텐츠 엔진은 소급 판정으로 처리됩니다. 판정이 지연되면 조치도 지연됩니다. 따라서 Secure Email Threat Defense는 이러한 판정에 태그를 명확하게 지정합니다.

소급 판정은 판정 옆에 있는 메시지 페이지에서 파란색 아이콘으로 표시됩니다. 아이콘 위에 커서를 놓으면 소급 판정이 적용된 시간과 메시지가 수신된 시간과 판정이 적용된 시간의 차이를 확인할 수 있습니다.

소급 판정 이메일 알림

소급 판정에 대한 이메일 알림 켜기 또는 끄기:

1. **Administration(관리)** > **Business(비즈니스)**를 선택합니다.
2. **Preferences(환경설정)**에서 **Send Notifications for Retrospective Verdicts(소급 판정에 대한 알림 전송)**을 선택하거나 선택 취소합니다.

확인란을 선택하는 경우 소급 판정 이메일 알림이 지정된 알림 이메일 주소로 전송됩니다. 이 알림은 기본적으로 켜져되어 있습니다.

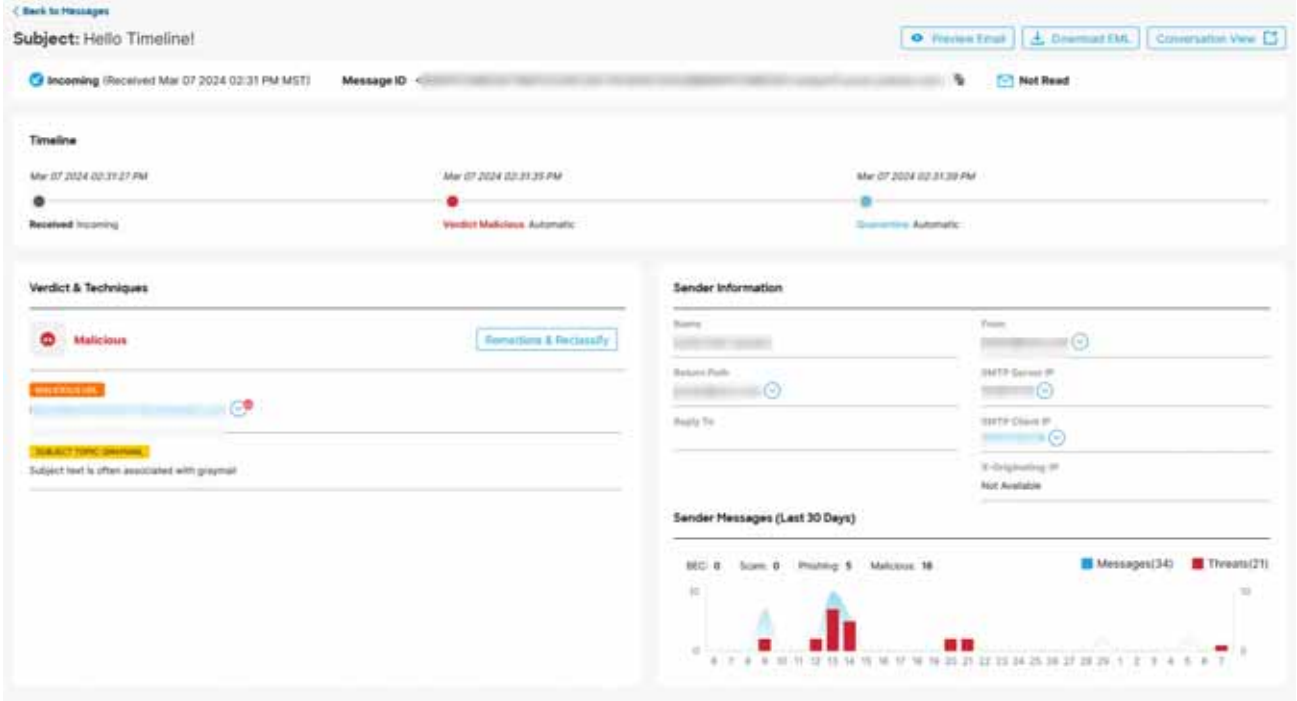
메시지 보고서

메시지 보고서에서는 메시지에 대한 세부 정보를 조사할 수 있습니다.세부 보고서에 액세스하려면 **>** 아이콘을 선택하거나 메시지 행의 아무 곳이나 클릭합니다.

메시지 보고서에는 메시지에 대한 다음과 같은 세부 정보가 표시됩니다.

- 메시지 방향, Microsoft 메시지 ID 및 조치 시점에 메시지를 읽었는지 여부
- 타임라인
- 판정 및 기술
- 발신자 정보
- 발신자 메시지
- 수신자, 봉투 수신자, 사서함을 포함한 수신자 정보
- 링크
- 첨부 파일
- 이메일 미리 보기

메시지 보고서에서는 대화 보기 및 EML 다운로드에 대한 액세스도 제공됩니다.



타임라인

메시지의 타임라인은 메시지 보고서에 표시됩니다.

타임라인에 다음이 표시됩니다.

- **Received(수신됨):** 메시지가 수신된 시간 및 메시지 방향에 대한 세부 정보
- **Rule(규칙):** 적용된 메시지 규칙에 대한 정보
- **Verdict(판정):** 렌더링 또는 적용된 판정과 작업을 수행한 사용자에 대한 정보
- **Action(작업):** 메시지에 대해 수행된 작업과 작업을 수행한 사용자에 대한 정보입니다. 여기에는 다음 항목이 포함됩니다.
  - 메시지가 이동된 위치 및 방법
  - 메시지의 교정 오류와 오류가 발생한 사서함에 대한 정보

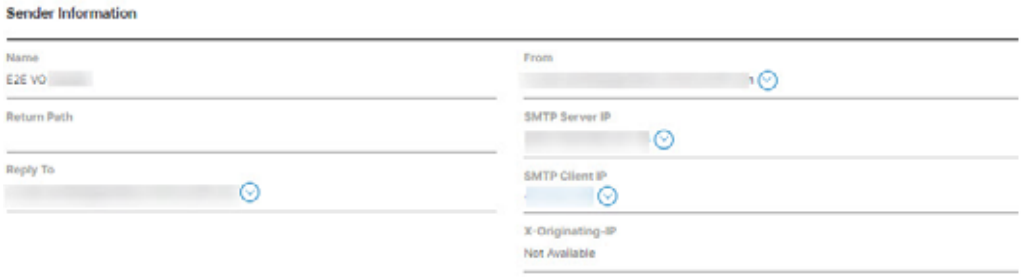
판정 및 기술

판정 및 기술 패널에서는 메시지에 적용된 판정과 판정에 영향을 미쳤을 수 있는 탐지된 기술을 시각적으로 표시합니다. 기술은 심각도를 나타내기 위해 색상으로 구분됩니다. 악성 파일 이름/SHA256 및 URL은 사용 가능한 경우 동적으로 표시됩니다. 유동 텍스트가 불가능한 경우 정적 설명이 표시됩니다.

이 패널에서 직접 메시지를 조치 및/또는 재분류할 수 있습니다. 조치 및 재분류) 버튼을 클릭한 다음 메시지 이동 및 재분류, 29페이지에 제공된 지침을 따릅니다.

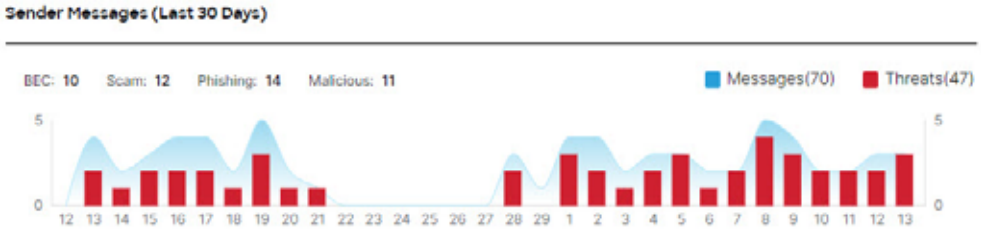
발신자 정보

발신자 정) 패널에는 이름, 이메일 주소, 반환 경로, 회신 대상, SMTP 서버와 클라이언트 IP, X-원본 IP를 포함하여 메시지 발신자에 대한 알려진 정보가 표시됩니다.



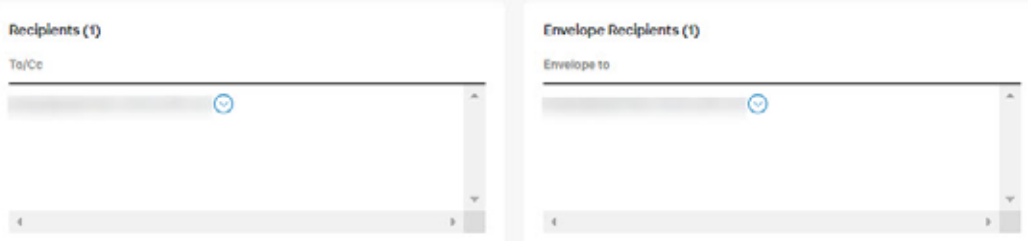
발신자 메시지

발신자 메시지 그래프에는 지난 30일간 전송한 총 메시지 수와 메시지 발신자가 보낸 총 위협 메시지가 표시됩니다. 이렇게 하면 사용자로부터의 위협 메시지 패턴이 있는지를 신속하게 확인할 수 있습니다.



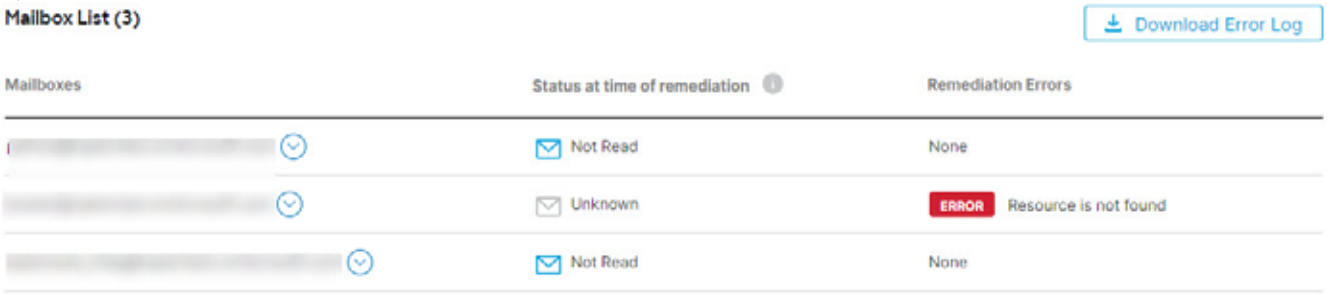
수신자 정보

수신자 및 봉투 수신자 패널에는 메시지를 보낸 사람에 대한 정보가 표시됩니다.



사서함 목록

사서함 목록에는 수신 및 내부 메시지를 받은 최종 사용자 사서함의 목록이 표시됩니다. 목록에는 마지막 조치 작업 전에 메시지를 읽었는지와 메시지에 대한 교정 오류도 표시됩니다. 시스템이 메시지 조치를 시도하기 전에 사용자가 메시지를 삭제하거나 이동했다면 조치 오류가 발생할 수 있습니다.

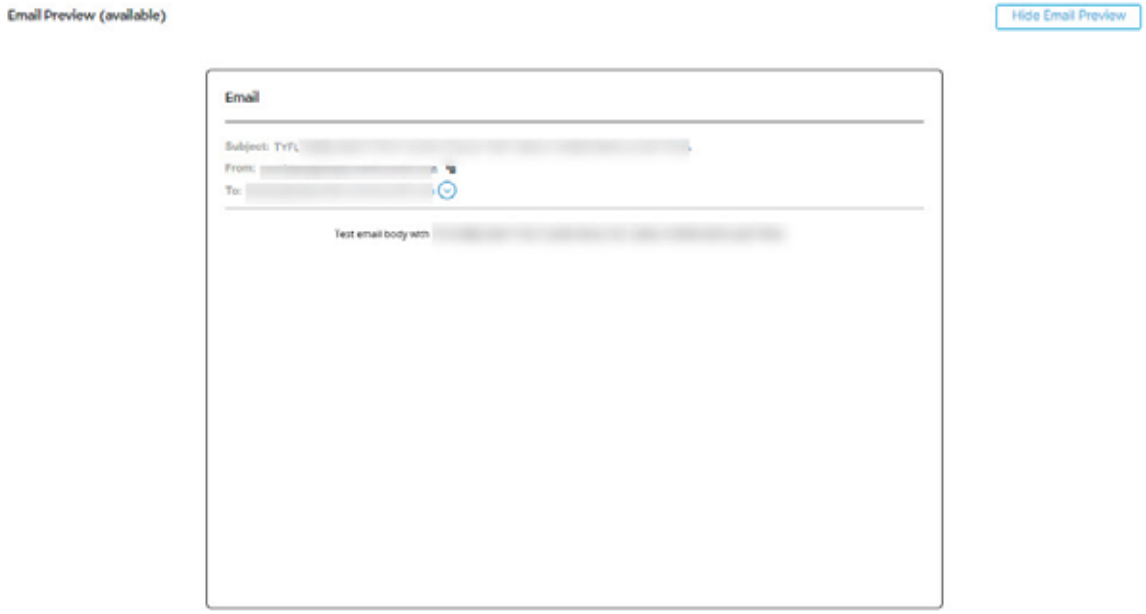


링크 및 첨부 파일

링크 및 첨부 파일 패널에는 메시지에서 발견된 링크 및 첨부 파일에 대한 정보가 표시됩니다.

이메일 미리 보기

이메일 미리보기를 사용하면 슈퍼 관리자 및 관리자 사용자가 EML 파일을 다운로드할 필요 없이 최종 사용자에게 표시되는 메시지를 요청하고 확인할 수 있습니다. 메시지가 이미지로 표시됩니다. 미리보기를 보려면 **Open Email Preview(이메일 미리보기 열기)** 버튼을 클릭합니다.



사용자가 메시지를 미리 볼 때 감사 로그 레코드가 생성됩니다. 감사 로그는 **Administration(관리)** > **Business(비즈니스)** > **Preferences(환경설정)**에서 다운로드할 수 있습니다.

대화 보기

대화 보기에서는 대화를 전체적으로 볼 수 있습니다. 대화 보기를 사용하여 대화의 메시지를 추적하고 메일 플로우를 완벽하게 파악합니다. 이는 위협이 시작된 위치와 조직 내에서 어떻게 전파되는지를 파악하는 데 유용할 수 있습니다.

메시지 보고서에서 페이지 오른쪽 상단에 있는 **Conversation(대화) View(보기)** 버튼을 클릭하면 특정 이메일과 연결된 메시지를 볼 수 있습니다.

대화에서 이전 또는 이후에 온 메시지를 볼 수 있도록 대화의 노드를 확장하려면 **+** 아이콘을 클릭합니다. 확장된 노드는 노드 아래의 메시지 그리드에 추가됩니다. 노드와 메시지는 방향을 나타내기 위해 수신, 발신 또는 내부와 같이 색상으로 구분됩니다.

노드 원 내의 숫자는 메시지가 전송된 주소의 수를 나타냅니다. 노드 내의 아이콘은 위협이 탐지되었거나 판정이 적용되었음을 나타냅니다. 노드를 선택하면 그리드에서 해당 메시지가 강조 표시됩니다.

XDR 피벗 메뉴

Secure Email Threat Defense 비즈니스가 Cisco XDR과 통합된 경우, 메시지 보고서 내에서 XDR 피벗 메뉴에 액세스 할 수 있습니다. XDR과의 통합에 대한 자세한 내용은 XDR, 61페이지를 참조하십시오.

메시지 이동 및 재분류

메시지가 잘못 분류되었다고 생각하는 경우 메시지 페이지를 사용하여 메시지를 이동하거나 재분류할 수 있습니다. 페이지당 표시되는 메시지 수를 변경하여 한 번에 최대 100개의 메시지를 이동하거나 재분류할 수 있습니다. 또한 메시지 보고서 페이지의 판정 및 기술 패널에서 직접 메시지를 이동하고 재분류할 수도 있습니다.

또한 조치 및 재분류 API를 사용하여 메시지를 이동하고 재분류할 수도 있습니다. 자세한 내용은 API 가이드 https://developer.cisco.com/docs/message-search-api/를 참조하십시오.

참고: 재분류는 선택한 메시지의 판정에만 영향을 미칩니다. 선택한 발신자가 보낸 향후 메시지에 대한 조치의 변경 사항이나 메시지 내용을 기반으로 한 변경 사항은 표시되지 않습니다. 메시지가 Cisco Talos의 검토를 위해 대기열에 추가됩니다. Talos는 피드백을 사용하여 향후 분류에 영향을 줄 수 있습니다. 오탐 메시지의 경우, 판정 재정의 규칙, 57페이지을 추가하는 것이 좋습니다.

하이브리드 Exchange 어카운트 정보

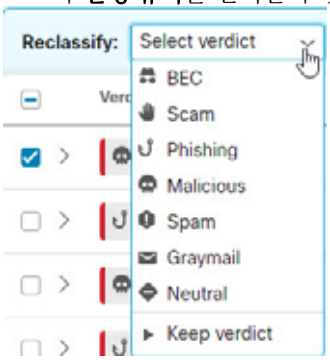
Secure Email Threat Defense Exchange Online(O365)에 있는 사서함에서만 작동할 수 있습니다. 사서함을 온프레미스 Exchange에서 Exchange Online(O365)으로 마이그레이션하는 과정에서 조치(이동 또는 삭제)는 Exchange Online(O365)에 있는 사서함에서만 작동합니다. 온프레미스 Exchange 사서함에 대한 조치가 실패했다는 알림은 표시되지 않습니다.

읽기 교정 모드

읽기 모드에 있는 경우 메시지를 재분류(다른 판정 적용)할 수 있습니다.

1. 재분류할 메시지를 선택합니다.

2. 드롭다운 메뉴에서 판정을 선택합니다. 메시지를 **BEC**, **스캠**, **피싱**, **악성**, **스팸**, **그레이메일** 또는 **중립**으로 재분류하거나 **판정 유지**를 선택할 수 있습니다.



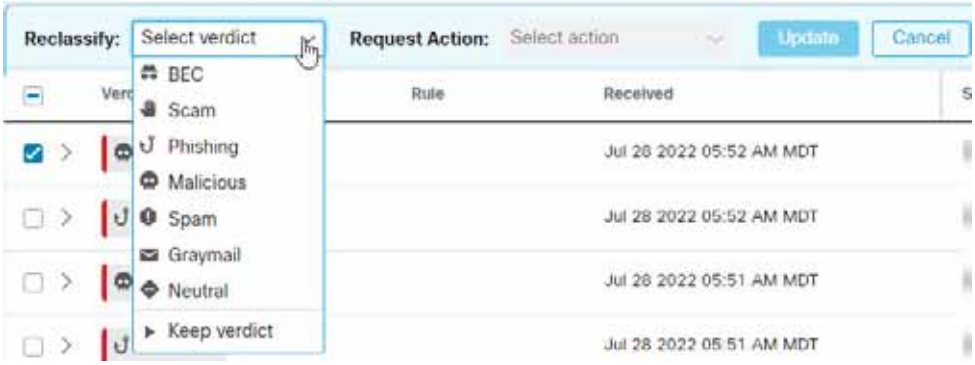
3. 새 분류를 적용하려면 **Update(업데이트)**를 클릭합니다.

읽기/쓰기 교정 모드

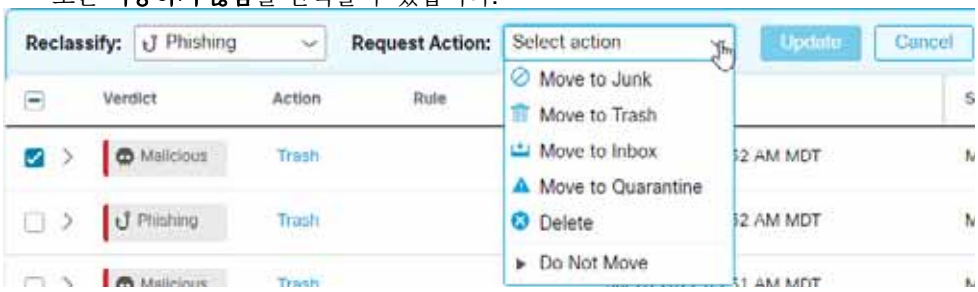
읽기/쓰기 교정 모드에 있는 경우 의심스러운 메시지를 사용자 수신함에서 정크 또는 휴지통으로 옮기거나 사용자가 액세스할 수 없는 격리 폴더로 옮길 수 있습니다. 마찬가지로 정크, 휴지통 또는 격리로 이동한 메시지가 의심스럽지 않음으로 확인되면 해당 메시지를 다시 사용자 수신함으로 이동시킬 수 있습니다. 또한 메시지를 완전히 삭제할 수도 있습니다. 이 프로세스를 통해 메시지를 재분류(다른 판정 적용)할 수도 있습니다.

1. 이동하거나 재분류할 메시지를 선택합니다.

2. 재분류 드롭다운 메뉴에서 판정을선택합니다. 메시지를 **BEC**, **스캠**, **피싱**, **악성**, **스팸, 그레이메일** 또는 **중립**으로 재분류하거나 **판정 유지**를 선택할 수 있습니다.



3. 요청 작업 드롭다운 메뉴에서 작업을 선택합니다. **정크로 이동**, **휴지통으로 이동**,**수신함으로 이동**, **격리로 이동**, **삭제** 또는 **이동하지 않음**을 선택할 수 있습니다.



4. **Update(업데이트)**를 클릭하여 새 분류를 적용하고 메시지에 대해 작업을 수행합니다.

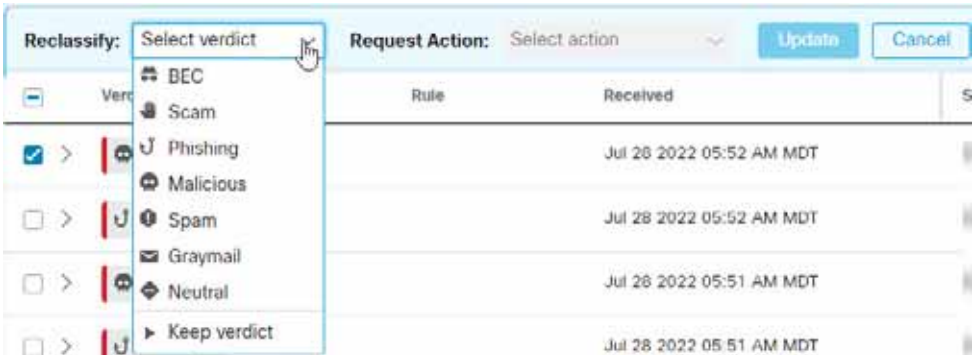
이동된 메시지는 **Last Action(마지막 작업)** 열에 표시됩니다.

참고: 발신 및 내부 메시지의 경우, 수신함으로 이동 작업을 수행하면 메시지가 수신함 대신 메시지를 최초 발신자의 발신 폴더로 이동합니다.

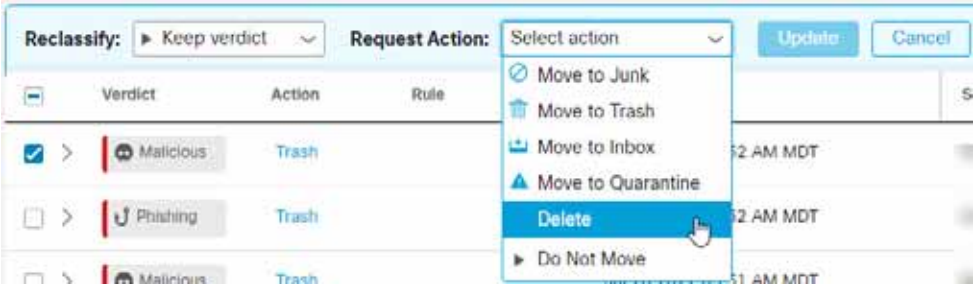
메시지 삭제

슈퍼 관리자 및 관리 사용자는 재분류/교정 워크플로우의 삭제 작업을 사용하여 사서함에서 메시지를 영구적으로 삭제할 수 있습니다. 삭제된 메시지는 **restoreableitemspurge** 폴더로 이동합니다. 이 폴더는 사용자가 액세스할 수 없으며 Secure Email Threat Defense은 삭제된 메시지를 수신함으로 복구할 수 없습니다.

1. 삭제할 메시지를 선택합니다.
2. 재분류 드롭다운 메뉴에서 판정을 선택합니다. 메시지를 **BEC**, **스캠**, **피싱**, **악성**, **스팸**, **그레이메일** 또는 **중립**으로 재분류하거나 **판정 유지**를 선택할 수 있습니다.



3. 요청 작업 드롭다운 메뉴에서 **Delete(삭제)**를 선택합니다.



4. 메시지를 삭제하려면 **Update(업데이트)**를 클릭합니다.
5. 삭제 확인 대화 상자는 메시지를 복구할 수 없음을 알리고 계속할 것임을 확인합니다. **Delete(삭제)**를 클릭하여 계속합니다.

삭제가 **Last Action(마지막 작업)** 열에 표시됩니다.

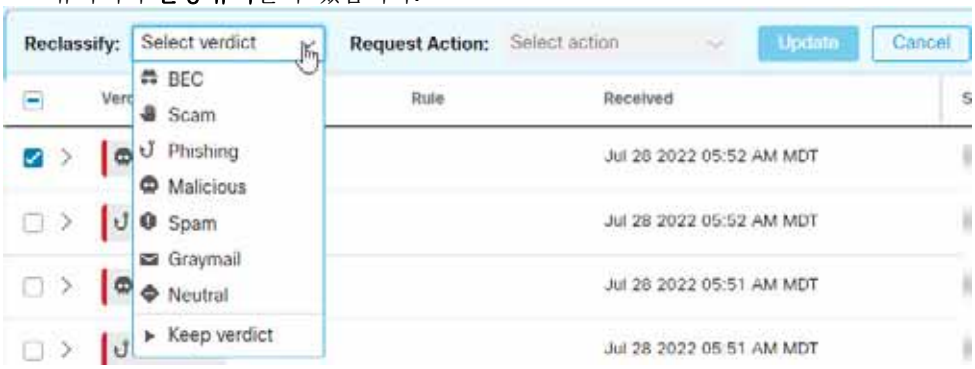
메시지 격리

격리 폴더는 각 사서함에 대해 자동으로 생성되며 Outlook 사용자에게는 표시되지 않습니다. 비밀 폴더 이름은 **Administration(관리)** > **Business(비즈니스)** 페이지에서 슈퍼 관리자 및 관리자 사용자에게 표시됩니다. Outlook에서 격리 폴더의 메시지는 삭제 사서함 비우기 설정에 따라 자동으로 제거됩니다. Secure Email Threat Defense 격리 폴더에서 삭제된 메시지를 사용자 수신함으로 다시 복구할 수 없습니다.

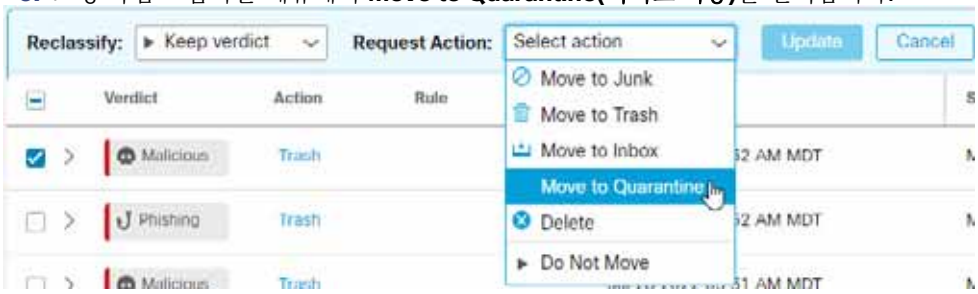
메시지를 수동으로 격리로 옮기려면 다음을 수행합니다.

1. 격리로 이동할 메시지를 선택합니다.

2. 재분류 드롭다운 메뉴에서 판정을 선택합니다. 메시지를 **BEC**, **스캠**, **피싱**, **악성**, **스팸**, **그레이메일** 또는 **중립**으로 재분류하거나 **판정 유지**할 수 있습니다.



3. 요청 작업 드롭다운 메뉴에서 **Move to Quarantine(격리로 이동)**을 선택합니다.



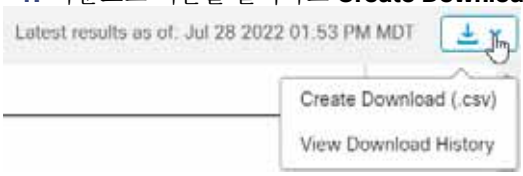
4. **Update(업데이트)**를 클릭하여 메시지를 격리합니다.

격리로 이동이 **Last Action(마지막 작업)** 열에 표시됩니다.

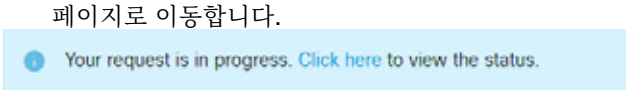
검색 결과 다운로드

검색 결과에서 메시지 데이터의 CSV 파일을 다운로드할 수 있습니다. 다운로드할 수 있는 메시지는 10,000개로 제한됩니다. 데이터를 다운로드하려면 다음 단계를 완료하십시오.

1. 다운로드 버튼을 클릭하고 **Create Download (.csv)(다운로드 생성(.csv))**를 선택합니다.



2. 요청이 진행 중임을 나타내는 배너가 나타납니다. 텍스트를 클릭하면 **Downloads: Messages(다운로드: 메시지)** 페이지로 이동합니다.



3. 다운로드가 준비되면 작업 열 아래의 다운로드 아이콘을 클릭하여 파일을 다운로드 합니다.

다운로드 기록

다운로드 기록은 90일 동안 유지됩니다. 다운로드 버튼을 클릭하고 **View Download History(다운로드 기록 보기)**를 선택하여 **Downloads: Messages(다운로드: 메시지)** 페이지로 이동합니다.

이 페이지에는 다운로드를 요청한 날짜 범위, 다운로드를 시작한 날짜 및 상태가 표시됩니다. 작업 열 아래의 다운로드 아이콘을 선택하여 파일을 다운로드합니다.

검색 결과 다운로드