Cisco Secure Email Threat Defense
사용 설명서

목차

소개

Cisco Secure Email Threat Defense는 간편한 구축, 손쉬운 공격 복구, 탁월한 가시성에 중점을 둔 Microsoft 365용 통합 클라우드 네이티브 보안 솔루션입니다.

요구 사항

Cisco Secure Email Threat Defense를 성공적으로 설정하고 사용하려면 다음이 필요합니다.

- Secure Email Threat Defense를 구매하고 환영 이메일을 받았습니다.
- 다음 브라우저 중 하나의 최신 버전:
  - Google Chrome
  - Microsoft Edge
  - Mozilla Firefox
- 메시지 소스가 Microsoft 365이거나 가시성 및 교정 모드에서 Microsoft 365 인증을 사용하는 경우:
  - 전역 관리자 권한이 있는 Microsoft 365 어카운트.
  - 전달할 수 없는 저널 보고서를 수신할 수 있는 Microsoft 365 환경의 이메일 주소. 사용된 이메일 주소는 기록되지 않으므로 Secure Email Threat Defense가 분석하려는 주소는 사용하지 마십시오.

Secure Email Threat Defense 설정

Secure Email Threat Defense 설정은 다음 작업을 포함합니다.

1. 어카운트로 로그인, 11페이지
2. SEG(Secure Email Gateway)가 있는지 표시, 11페이지
3. 메시지 소스, 가시성 및 교정 선택, 11페이지
4. 메시지 소스 설정, 12페이지
5. 정책 설정 검토, 14페이지
6. Microsoft 이메일 도메인 가져오기, 14페이지

이 단계에서는 다음을 충족한다고 가정합니다**요구 사항, 9페이지**.

어카운트로 로그인

1. 시스코에서 보낸 환영 이메일의 안내에 따라 사용자 어카운트를 설정합니다.

   Secure Email Threat Defense Cisco Security Cloud Sign On을 사용하여 인증을 관리합니다. Security Cloud Sign On에 대한 자세한 정보는 https://cisco.com/go/securesignon를 참조하십시오. 기존 SecureX Threat Response, Cisco Secure Malware Analytics(이전 Threat Grid) 또는 Cisco Secure Endpoint(이전 AMP) 고객인 경우, 기존 자격 증명으로 로그인합니다. 기존 사용자가 아닌 경우 새 Security Cloud Sign On 어카운트를 생성하는 것이 필요합니다.

2. 로그인하면 이용 약관에 동의합니다.

3. 이제 **환영Cisco Secure Email Threat Defense** 페이지에 액세스할 수 있습니다. 다음 섹션에 설명된 대로 설정 마법사를 따릅니다.

SEG(Secure Email Gateway)가 있는지 표시

메시지 소스(다음 섹션에서 선택)에 관계없이 보안 SEG(Secure Email Gateway)가 존재하고 수신 저널에서 이를 식별하는 데 사용할 수 있는 헤더를 표시하여 Secure Email Threat Defense이 메시지의 실제 발신자를 확인할 수 있도록 하는 것이 중요합니다. 이 설정이 없으면 모든 메시지가 SEG에서 제공되는 것처럼 보일 수 있으며, 이로 인해 오탐이 발생할 수 있습니다.

1. 예 또는 아니요를 선택하여 SEG(Secure Email Gateway)가 있는지 표시한 후 **Next(다음)**을 클릭합니다.

2. 예라고 답한 경우 SEG 유형과 헤더를 입력합니다. **Next(다음)**를 클릭합니다.

메시지 소스, 가시성 및 교정 선택

1. 메시지 소스를 Microsoft O365 또는 게이트웨이로 선택합니다. 이전 단계에서 SEG 없음을 선택했다면 Microsoft O365가 메시지 소스로 간주됩니다.

2. 가시성 및 교정을 선택합니다.

   가시성 및 교정 모드에서는 적용할 수 있는 교정 정책의 유형을 정의합니다.

Microsoft 365 인증

- **읽기/쓰기 -** 가시성을 허용하고 온디맨드 또는 자동 교정(즉, 의심스러운 메시지 이동 또는 삭제)을 허용합니다. 읽기/쓰기 권한은 Microsoft 365에서 요청됩니다.
- **읽기 -** 가시성만 허용하며 교정은 허용하지 않습니다. 읽기 전용 권한은 Microsoft 365에서 요청됩니다.

  참고: 읽기/쓰기를 선택하는 경우, 설정이 완료되면 **정책 설정, 17페이지**에서 자동 교정 정책을 켜야 합니다. 모든 내부 이메일에 자동 교정 기능을 적용하려면 정책 페이지의 **도메인 목록에 없는 도메인에 자동 교정 기능 적용** 상자가 선택되어 있는지 확인합니다.

Microsoft 365 인증 모드의 경우, Secure Email Threat Defense는 Microsoft에서 액세스 권한을 요청합니다. 이러한 권한은 사용자가 읽기/쓰기 또는 읽기 모드를 선택하는지에 따라 달라집니다. 권한에 대한 자세한 내용은 연결된 Microsoft 설명서에서 확인할 수 있습니다.

두 가지 Microsoft 인증 모드 모두 **Organization.Read.All** 및 **User.Read를 요청 합니다.**

- https://learn.microsoft.com/en-us/graph/permissions-reference#organizationreadall
- https://learn.microsoft.com/en-us/graph/permissions-reference#userread

읽기/쓰기 모드 요청: **Mail.ReadWrite**

- https://learn.microsoft.com/en-us/graph/permissions-reference#mailreadwrite

읽기 모드 요청: **Mail.Read**

- https://learn.microsoft.com/en-us/graph/permissions-reference#mailread

인증 없음

이 옵션은 Cisco SEG를 메시지 소스로 사용하는 경우 사용할 수 있습니다. 가시성 만 제공합니다. 메시지를 교정할 수는 없습니다.

3. Microsoft 365 인증을 선택한 경우 Microsoft 365에 연결합니다.
   a. **Next(다음)**를 클릭하여 Microsoft 365에 연결합니다.
   b. 메시지가 표시되면 Microsoft 365 어카운트로 로그인합니다. 이 어카운트에는 전역 관리자 권한이 있어야 합니다. Secure Email Threat Defense은 어카운트를 저장하거나 사용하지 않습니다. 이러한 권한이 필요한 이유를 알아보려면 Cisco Secure Email Threat Defense FAQ: Secure Email Threat Defense 설정에 Microsoft 365 전역 관리자 권한이 필요한 이유는 무엇입니까?를 참조하십시오.
   c. **Accept(수락)**를 클릭하여 Secure Email Threat Defense 앱에 대한 권한을 수락합니다. Secure Email Threat Defense 설정 페이지로 리디렉션됩니다.
   d. **Next(다음)**를 클릭합니다.

메시지 소스 설정

선택한 메시지 소스에 대한 단계를 완료합니다.

Microsoft O365 메시지 소스

메시지 소스로 Microsoft O365를 선택한 경우, 저널을 Secure Email Threat Defense로 보내도록 Microsoft 365를 구성해야 합니다. 이렇게 하려면 저널 규칙을 추가합니다. 게이트웨이가 있는 경우 저널 규칙을 추가하기 전에 Microsoft 365에 커넥터를 추가합니다.

1. **SEG(Secure Email Gateway)를 사용하는 사용자의 경우:** Microsoft 365에서 커넥터를 추가합니다.

저널이 Secure Email Gateway를 통과하지 않고 Microsoft 365에서 Secure Email Threat Defense로 직접 전송되도록 하려면 Microsoft 365에 아웃바운드 커넥터를 추가하는 것이 좋습니다. 저널링을 설정하기 전에 커넥터를 추가해야 합니다.

Microsoft 365 Exchange 관리 센터의 **Add a connector(커넥터 추가)** 마법사에서 다음 설정을 사용하여 새 커넥터를 생성합니다.

- **Connection from(연결 출처):** Office 365.
- **Connection to(연결 대상):** 파트너 조직
- **Connector name(커넥터 이름):** Cisco Secure Email Threat Defense에 대한 아웃바운드(**Turn it on(켜기)** 확인란 선택).
- **Use of connector(커넥터 사용):** 이메일 메시지가 이러한 도메인으로 전송된 경우에만 (북미 환경의 경우 **mail.cmd.cisco.com**, 유럽 환경의 경우 **mail.eu.cmd.cisco.com**, 호주 환경의 경우 **mail.au.etd.cisco.com**을 추가하고, 인도 환경의 경우 **mail.in.etd.cisco.com**를 추가).
- **Routing(라우팅):** 파트너 도메인과 연결된 MX 레코드를 사용합니다.
- **Security restrictions(보안 제한):** 항상 신뢰할 수 있는 인증 기관(CA)에서 발급된 TLS(Transport Layer Security)를 사용합니다.
- **Validation email(검증 이메일):** Secure Email Threat Defense 설정 페이지에 있는 저널 주소.

  참고: O365 테넌트가 이미 기존 커넥터로 아웃바운드 메일을 라우팅하는 Exchange 전송 규칙을 사용하여 조건부 메일 라우팅을 구성한 경우 커넥터 유효성 검사에 실패할 수 있습니다. 저널 메시지는 시스템 권한이 있으며 전송 규칙의 영향을 받지 않는 반면, 커넥터 검증 테스트 이메일은 권한이 없으며 전송 규칙의 영향을 받습니다.

  이 검증 문제를 해결하려면 기존 전송 규칙을 찾아 Secure Email Threat Defense 저널 주소에 대한 예외를 추가합니다. 이 변경 사항이 적용될 때까지 기다렸다가 새 커넥터 유효성 검사를 다시 테스트합니다.

2. Secure Email Threat Defense로 저널을 보내도록 Microsoft 365를 구성합니다. 이를 위해 저널 규칙을 추가합니다.
   a. Secure Email Threat Defense 설정 페이지에서 저널 주소를 복사합니다. 나중에 이 과정을 반복해야 하는 경우, 관리 페이지에서 저널 주소를 찾을 수도 있습니다.
   b. Microsoft Purview 규정 준수 포털 https://compliance.microsoft.com/homepage로 이동합니다.
   c. **Solution(솔루션) > Data lifecycle management데이터 수명 주기 관리) > Exchange(legacy)(Exchange (레거시)) > Journal rules(저널 규칙)**로 이동합니다.
   d. 아직 하지 않았다면 **배달할 수 없는 저널 보고서를 다음 주소로 보내기** 필드에 Exchange 수신자를 추가한 다음 **Save(저장)**를 클릭합니다. 사용된 이메일 주소는 기록되지 않으므로 Secure Email Threat Defense분석하려는 주소는 사용하지 마십시오. 이 용도로 사용할 수신자가 없는 경우 수신자를 생성해야 합니다.
   e. **Journal rules(저널 규칙)** 페이지로 돌아갑니다. **+**버튼을 클릭하여 새 저널 규칙을 생성합니다.
   f. 설정 페이지의 Secure Email Threat Defense에 있는 저널 주소를 **저널 보고서 보내기** 필드에 붙여넣습니다.
   g. **Journal rule name(저널 규칙 이름)** 필드에 **CiscoSecure Email Threat Defense**를 입력합니다.
   h. **Journal messages sent or received from(주고받은 저널 메시지)**에서 **Everyone(모든 사람)**을 선택합니다.
   i. **Type of message to journal(저널에 기록할 메시지 유형)**에서 **All messages(모든 메시지)**를 선택합니다.
   j. **Next(다음)**를 클릭합니다.
   k. 선택한 사항을 검토한 다음 **Submit(제출)**을 클릭하여 규칙 생성을 완료합니다.
3. Secure Email Threat Defense 설정 페이지로 돌아갑니다. **Review Policy(정책 검토)**를 클릭합니다.

게이트웨이 메시지 소스

게이트웨이를 메시지 소스로 선택한 경우 Cisco Secure Email Cloud Gateway의 Threat Defense Connector를 활성화하여 Secure Email Threat Defense에 메시지를 전송합니다.

1. Secure Email Threat Defense 설정 페이지에서 메시지 수신 주소를 복사합니다. 나중에 이 과정을 반복해야 하는 경우 관리 페이지에서 메시지 수신 주소를 찾을 수 있습니다.
2. Secure Email Cloud Gateway UI에서 **Security Services(보안 서비스) > Threat Defense Connector(위협 방어 커넥터)**를 선택합니다.
3. **Enable Threat Defense Connector(위협 방어 커넥터 활성화)** 확인란을 선택합니다.
4. 1단계의 Secure Email Threat Defense에서 복사한 메시지 수신 주소를 입력합니다.
5. **Submit(제출)**을 클릭하여 변경 사항을 커밋합니다.
6. Secure Email Threat Defense 설정 페이지로 돌아갑니다. **Review Policy(정책 검토)**를 클릭합니다.

정책 설정 검토

정책 설정에 대한 자세한 내용은 **정책 설정, 17페이지**를 참조하십시오. **Microsoft O365 인증**을 선택한 경우: **읽기/쓰기** 모드를 선택한 경우 지금 **자동화된 교정** 설정을 확인해야 합니다. 모든 내부 이메일에 자동 교정을 적용하려면 **도메인 목록에 없는 도메인에 자동 교정 적용**이 선택되어 있는지 확인합니다. 도메인을 가져오면 **자동화된 교정 정책** 토글을 켤 수 있습니다.

Microsoft 이메일 도메인 가져오기

Secure Email Threat Defense Microsoft 365 테넌트에서 이메일 기능이 있는 도메인을 가져옵니다. 도메인을 가져오면 특정 도메인에 자동화된 교정을 적용할 수 있습니다. Secure Email Threat Defense는 **도메인 목록에 없는 도메인에 자동 교정 적용**을 선택하거나 선택 취소했는지에 따라 새로 가져온 도메인을 다르게 처리합니다.

- **도메인 목록에 없는 도메인에 자동 교정 적용**을 선택하면 가져오는 모든 새 도메인에 자동 교정이 적용됩니다.
- **도메인 목록에 없는 도메인에 자동 교정 적용을 선택 취소**하면 가져온 새 도메인에 자동 교정이 적용되지 않습니다.

기본적으로 **도메인 목록에 없는 도메인에 자동 교정 적용**은 선택 취소되어 있습니다.

수동 가져오기

Microsoft 365 이메일 도메인을 수동으로 가져오려면 다음을 수행합니다(처음 Secure Email Threat Defense을 설정할 때 권장).

1. **Policy(정책)** 페이지로 이동합니다.
2. Secure Email Threat Defense로 도메인을 가져오려면 **Update Imported Domains(가져온 도메인 업데이트)** 버튼을 클릭합니다.
3. 각 도메인 옆의 확인란을 사용하여 해당 도메인의 자동화된 교정 설정을 조정합니다.
4. 또한 **도메인 목록에 없는 도메인에 자동 교정 적용**을 선택하여 모든 내부 이메일과 나중에 자동으로 가져오는 모든 도메인에 자동 교정이 적용되도록 하는 것이 좋습니다.
5. **Save and Apply(저장 및 적용)**를 클릭합니다.

자동 가져오기

도메인은 24시간마다 자동으로 가져오기 때문에 목록이 최신 상태로 유지됩니다.

정책 설정

Policy(정책) 페이지의 설정은 Cisco Secure Email Cloud Mailbox가 메일을 처리하는 방법을 결정합니다. **Secure Email Threat Defense 설정, 11페이지**의 경우 기본 설정이 적용됩니다. 설정을 변경하려면 변경한 다음 **Save and Apply(저장 및 적용)** 버튼을 클릭합니다.

표 1 정책 설정

설정	설명	옵션	기본
메시지 소스	메시지의 소스를 정의합니다.	■ **Microsoft 365** ■ **게이트웨이**(수신 메시지 전용)	Secure Email Threat Defense를 설정할 때 수동으로 선택합니다.
가시성 및 교정	적용할 수 있는 교정 정책의 유형을 정의합니다.	■ **Microsoft 365 인증** – **읽기/쓰기** - 가시성을 허용하고 온디맨드 또는 자동 교정(즉, 의심스러운 메시지 이동 또는 삭제)을 허용합니다. 읽기/쓰기 권한은 Microsoft 365에서 요청됩니다. – **읽기** - 가시성만 허용하며 교정은 허용하지 않습니다. 읽기 전용 권한은 Microsoft 365에서 요청됩니다. **읽기**를 선택하는 경우, **첨부 파일 분석** 및 **메시지 분석** 방향만 설정하면 됩니다. 교정 정책이 적용되지 않습니다. ■ **인증 없음** 가시성만 허용합니다.	Secure Email Threat Defense를 설정할 때 수동으로 선택합니다. Microsoft 365 인증 설정을 변경하는 경우, Microsoft 365 권한을 재설정하도록 리디렉션됩니다. 저널링 설정으로 이동할 수도 있습니다. 이미 저널링을 설정한 경우 이 단계를 건너뛸 수 있습니다. **참고: Microsoft 365 Authentication: Read/Write(Microsoft 365 인증: 읽기/쓰기)**를 선택할 경우 **자동화된 교정 정책** 설정도 확인해야 합니다.
SEG(Secure Email Gateway)	SEG(Secure Email Gateway)의 유무는 Secure Email Threat Defense가 발신자 IP를 식별하는 방식에 영향을 미칩니다.	■ 선택 항목이 없음(SEG 없음) ■ **SEG가 있음** – **Cisco SEG 헤더 (X- IronPort-RemoteIP) 사용** – **맞춤형 SEG 헤더 사용** 사용하려는 헤더를 추가해야 합니다.	Secure Email Threat Defense를 설정할 때 수동으로 선택합니다. 자세한 내용은 게이트웨이를 사용하는 정책 설정, 19페이지를 참고하십시오.

표 1 정책 설정

설정	설명	옵션	기본
메시지 분석	동적으로 분석할 메시지로서 다음을 포함합니다. ■ 메시지 방향 ■ Cisco Secure Malware Analytics에서 분석할 메일 첨부 파일의 방향 ■ 스팸 및 그레이메일 분석	■ **메시지 방향** – **수신** – **발신** – **내부** ■ **첨부 파일 방향** – **수신** – **발신** – **내부** ■ **스팸 및 그레이메일** – **On(켜기)** 또는 **Off(끄기)**	■ **메시지 방향** – Microsoft O365 메시지 소스의 경우 **모두** – 게이트웨이 메시지 소스에 대한 **수신** ■ **첨부 파일 방향** – **수신** ■ **스팸 및 그레이메일** – 2023년 5월 9일 이후에 생성된 모든 어카운트에 대해 **끄기**
자동화된 교정 정책	확인된 메시지에 대한 교정 작업은 다음과 같습니다. ■ **위협** (BEC, 스캠, 피싱 또는 악성) ■ **스팸** ■ **그레이메일**	■ **작업 없음** ■ **격리로 이동** ■ **휴지통으로 이동** ■ **정크로 이동** **참고:** 발신자 주소가 Exchange의 발신자 허용 목록에 속하거나 메시지가 Microsoft 365에서 이미 교정된 경우, 교정 작업이 적용되지 않습니다.	■ **자동화된 교정 정책** 토글 - **끄기** ■ 위협 - **격리로 이동** ■ 스팸 - **정크로 이동** ■ 그레이메일 - **작업 없음**
안전한 발신자: Microsoft 안전한 발신자 메시지를 스팸 또는 그레이메일 판정으로 교정하지 않습니다.	Microsoft가 저널 헤더에서 안전한 발신자로 태그를 지정하고 스팸 또는 그레이메일에 대한 Secure Email Threat Defense 판정이 있는 메시지는 이 확인란을 선택하는 경우, 교정되지 않습니다.	**선택** 또는 **선택 취소**	**선택 취소됨**
가져온 도메인 - 메시지 방향을 결정하는 데 도움이 되도록 도메인을 가져옵니다. 도메인을 자동화된 교정 정책에서 제외할 수 있습니다.			
자동 교정 적용	특정 도메인에 자동 교정을 적용합니다.	**선택** 또는 **선택 취소**	**선택 취소됨. 읽기/쓰기** 교정 모드를 켤 때 이 확인란을 선택하여 특정 도메인에 자동 교정을 적용합니다.
위의 도메인 목록에 없는 도메인에 자동 교정 적용	도메인이 명시적으로 나열되지 않은 경우 적용됩니다. 예를 들어 새 도메인이 Microsoft 365 어카운트에 추가되었지만 Secure Email Threat Defense로 가져오지 않은 경우 입니다.	**선택** 또는 **선택 취소**	**선택 취소됨. 읽기/쓰기** 모드를 켤 때 이 확인란을 선택하여 모든 내부 이메일에 자동 교정이 적용합니다.

게이트웨이를 사용하는 정책 설정

Cisco Email Security 어플라이언스 또는 유사한 게이트웨이가 있는 경우 다음 정책 설정 사용을 고려하십시오.

표 2 게이트웨이를 사용하는 제안된 정책 설정

설정 이름	권장 선택
SEG(Secure Email Gateway)	**SEG가 있으며**, 헤더를 표시함
메시지 분석	**스팸 및 그레이메일** 끄기
Remediation Actions(교정 작업)	**위협 - 격리로 이동**

Secure Email Threat Defense이 메시지의 실제 발신자를 확인할 수 있도록 수신 저널에서 SEG(Secure Email Gateway)가 존재하고 이를 식별하는 데 사용할 수 있는 헤더를 표시하는 것이 중요합니다. 이 설정이 없으면 모든 메시지가 SEG에서 제공되는 것처럼 보일 수 있으며, 이로 인해 오탐이 발생할 수 있습니다.

Cisco Secure Email Cloud Gateway (이전 CES) 또는 Cisco Secure Email Gateway (이전 ESA)의 헤더를 확인 또는 구성하는 방법에 대한 자세한 내용은 https://docs.ces.cisco.com/docs/configuring-asyncos-message-filter-to-add-sender-ip-header-for-cloud-mailbox 를 참조하십시오.

Microsoft 365를 메시지 소스로 사용하는 경우, 저널이 Microsoft 365에서 Secure Email Threat Defense로 직접 전송되도록 어플라이언스를 건너뛰는 것이 좋습니다. 이 작업은 Secure Email Threat Defense 설정, 11페이지에 설명된 대로 Microsoft 365에서 커넥터를 추가하면 됩니다.

메시지 소스 전환

메시지 소스를 변경하려면 **Policy(정책)** 페이지로 이동합니다.

1. 새 메시지 소스의 라디오 버튼을 선택합니다.
2. 메시지 소스를 전환한다는 알림이 표시됩니다. **Continue(계속)**를 클릭합니다.
3. 메시지 소스 전환 대화 상자가 나타납니다. Secure Email Threat Defense에 메시지 전송을 중지하도록 이전 메시지 소스를 구성해야 합니다. 이를 수행하는 방법에 대한 자세한 내용은 Secure Email Threat Defense저널 규칙 삭제, 67페이지 또는 메시지 전송을 중지하도록 게이트웨이 구성, 68페이지를 참조하십시오.
4. 이전 소스에서 저널 또는 메시지 전송을 중지했음을 나타내는 확인란을 선택하고 **Next(다음)**를 클릭합니다.
5. 대화 상자에 표시되는 메시지 수신 주소 또는 저널 주소를 사용하여 새 메시지 소스를 구성합니다. 각 유형의 메시지 소스를 설정하는 단계는 메시지 소스 설정, 12페이지에 자세히 설명되어 있습니다.

메시지 소스 전환

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.

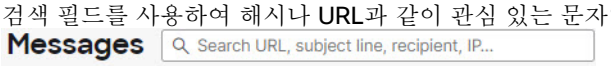
표 1 메시지 페이지 아이콘

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.

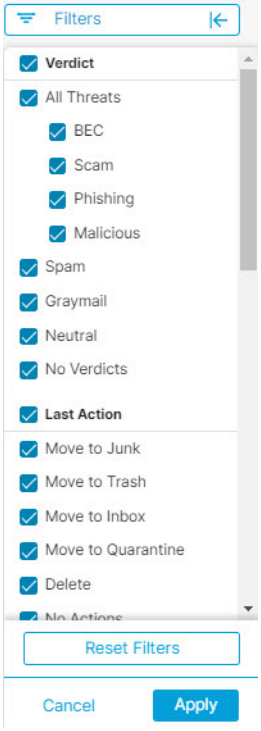


필터 패널

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.

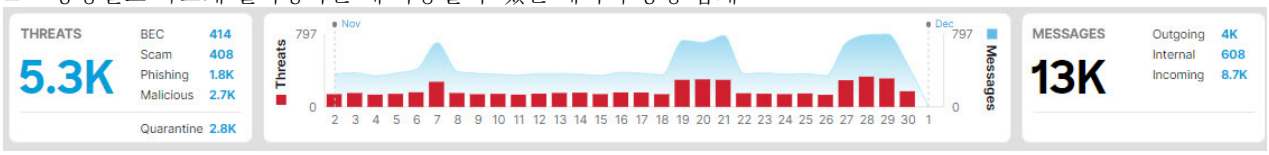


Reset Filters(필터 재설정) 버튼을 사용하여 필터를 기본값으로 재설정합니다.

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.

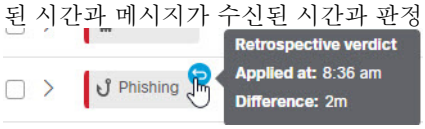
- **피싱:** 이러한 메시지는 사용자 이름, 비밀번호, 신용카드 번호 등과 같은 민감한 정보를 얻기 위해 합법적인 서비스를 부정하게 복사하거나 모방한 혐의로 유죄 판정을 받은 적이 있습니다.
- **Malicious(악성) :** 이러한 메시지는 악의적인 소프트웨어의 전달 또는 전파를 포함하거나, 이러한 메시지를 전달하거나, 이를 지원한 경우입니다.

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.

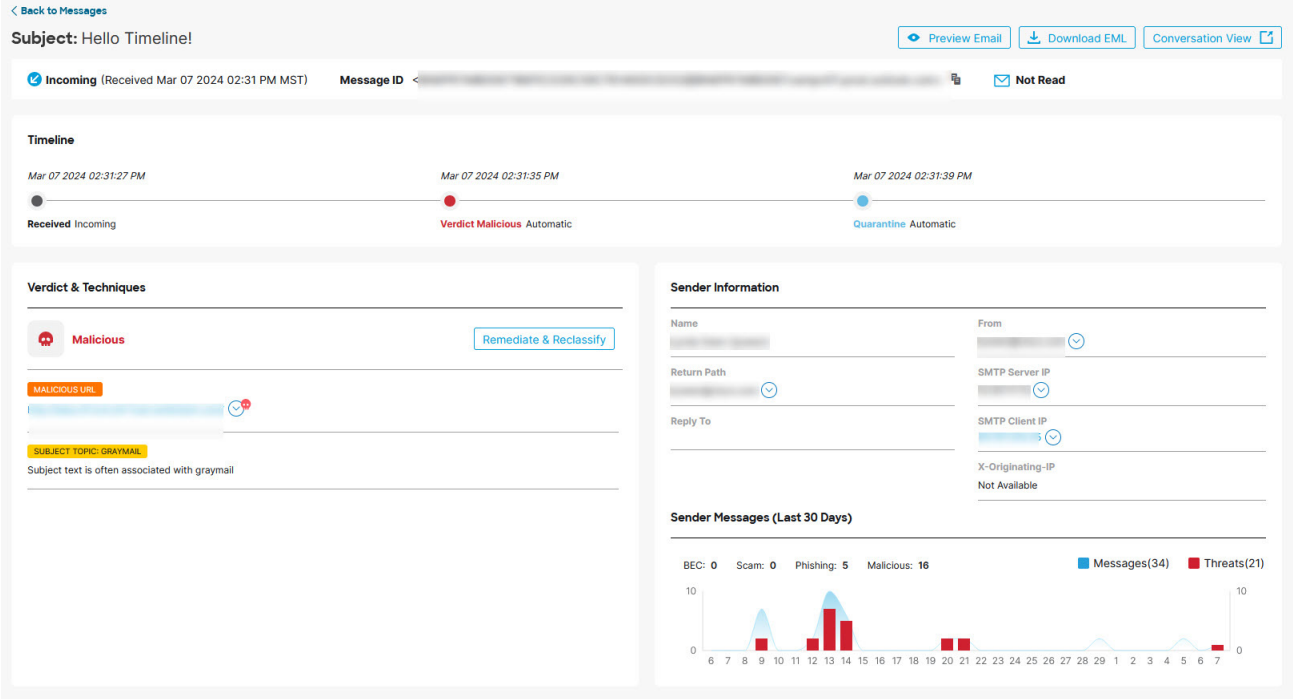
메시지 보고서

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.

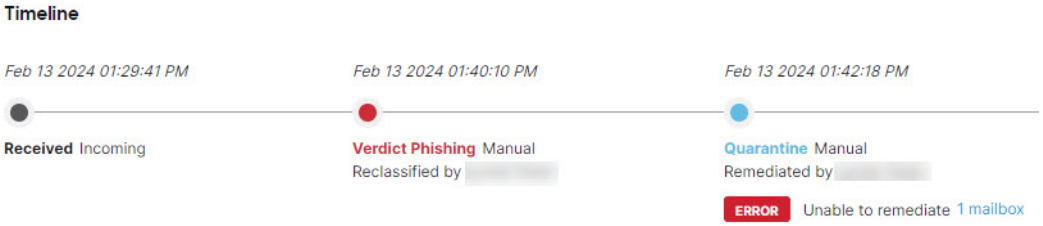
- 메시지 방향, Microsoft 메시지 ID 및 조치 시점에 메시지를 읽었는지 여부
- 타임라인
- 판정 및 기술
- 발신자 정보
- 발신자 메시지
- 수신자, 봉투 수신자, 사서함을 포함한 수신자 정보
- 링크
- 첨부 파일
- 이메일 미리 보기

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

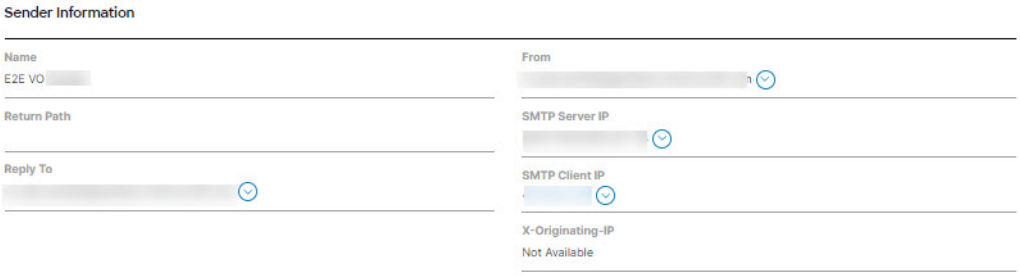
판정 및 기술

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.

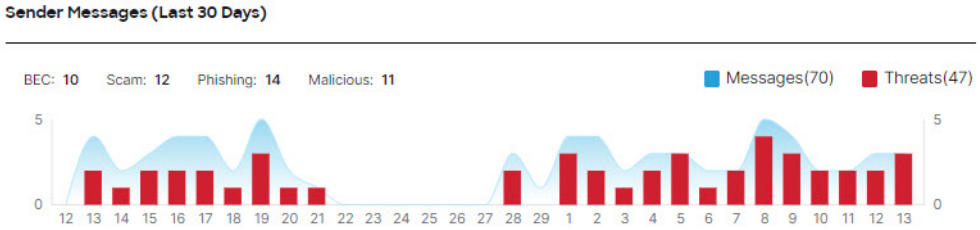
발신자 정보

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



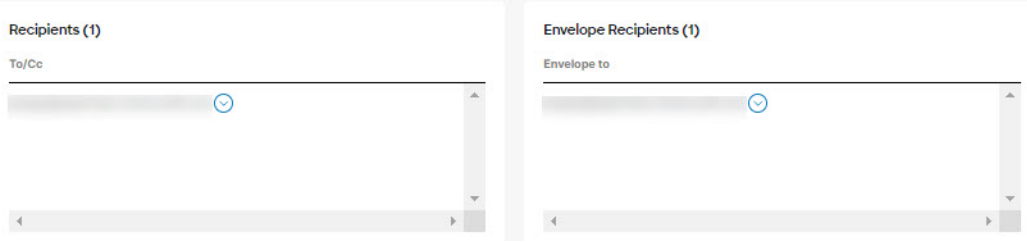
발신자 메시지

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.



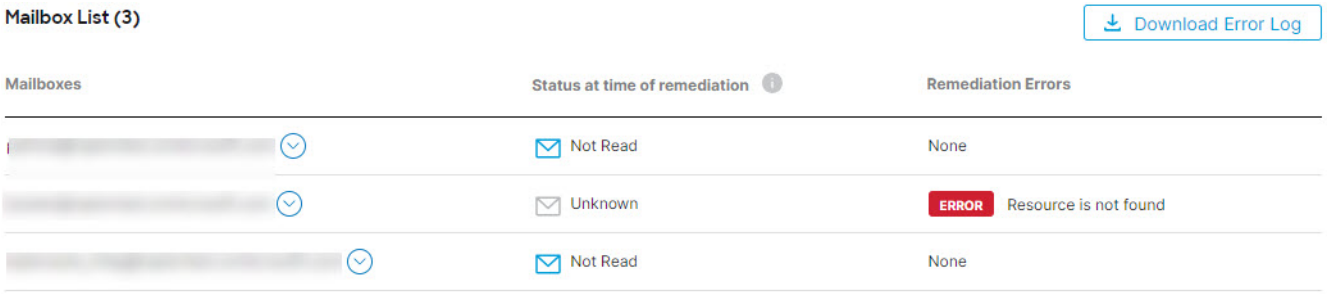
수신자 정보

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.

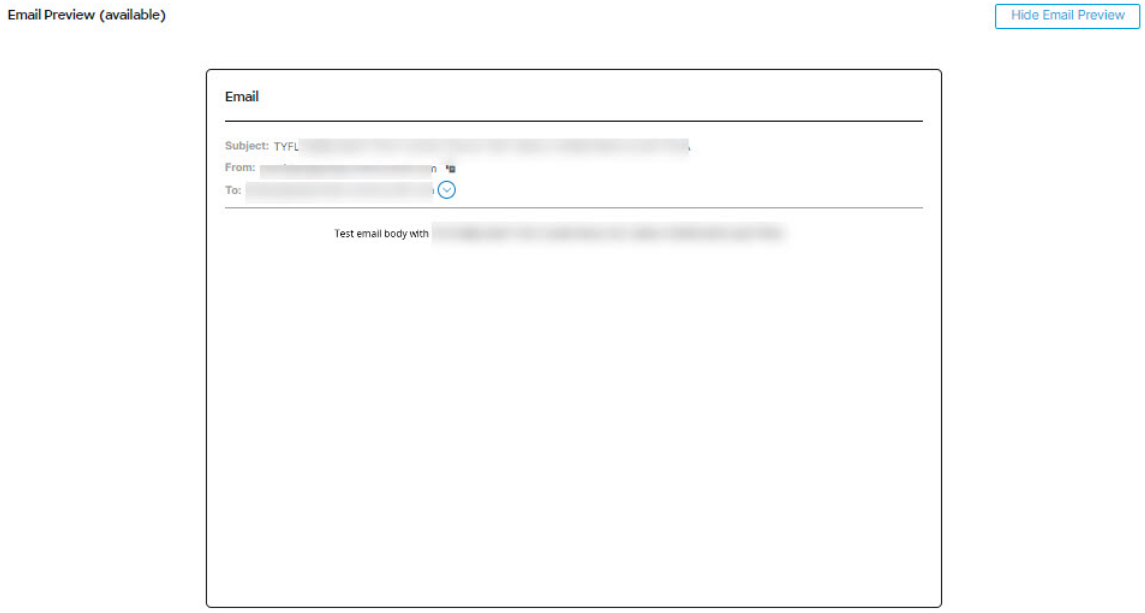


링크 및 첨부 파일

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.

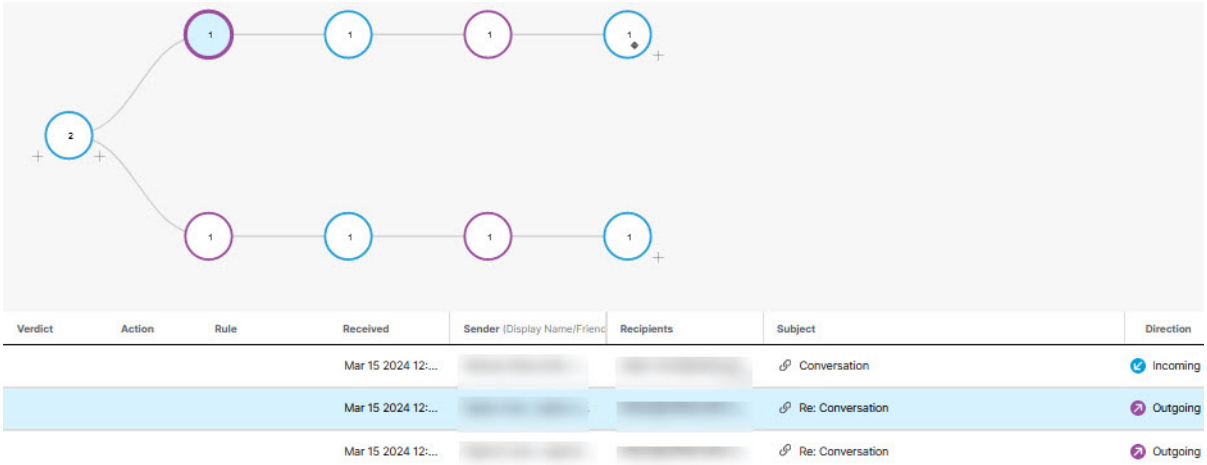
대화 보기

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

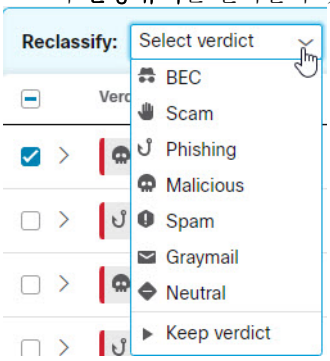
Secure Email Threat Defense Exchange Online(O365)에 있는 사서함에서만 작동할 수 있습니다. 사서함을 온프레미스 Exchange에서 Exchange Online(O365)으로 마이그레이션하는 과정에서 조치(이동 또는 삭제)는 Exchange Online(O365)에 있는 사서함에서만 작동합니다. 온프레미스 Exchange 사서함에 대한 조치가 실패했다는 알림은 표시되지 않습니다.

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.



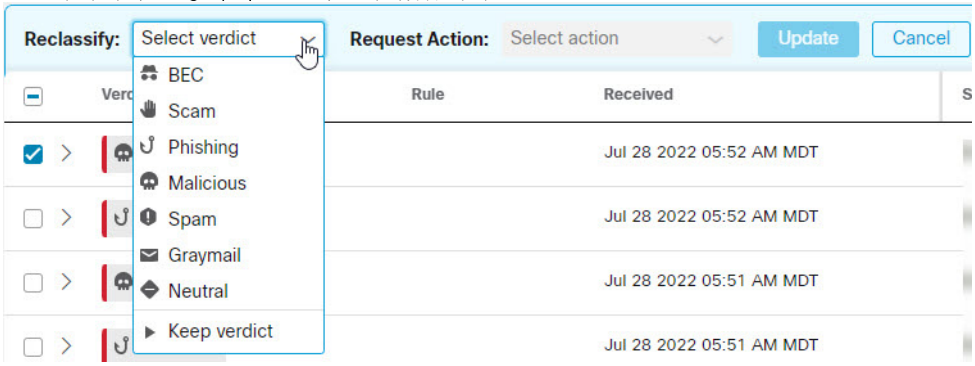
3. 새 분류를 적용하려면 **Update(업데이트)**를 클릭합니다.

읽기/쓰기 교정 모드

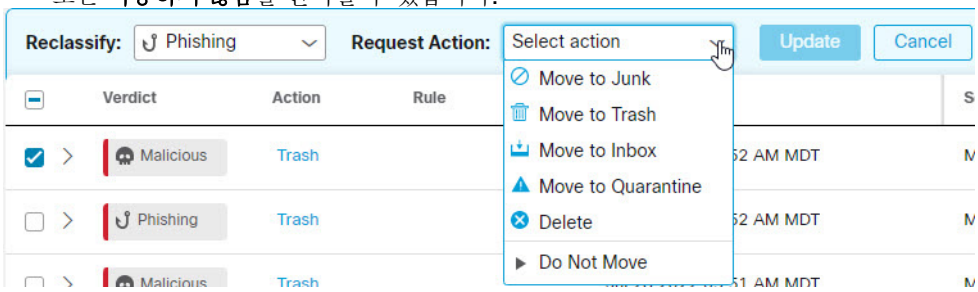
읽기/쓰기 교정 모드에 있는 경우 의심스러운 메시지를 사용자 수신함에서 정크 또는 휴지통으로 옮기거나 사용자가 액세스할 수 없는 격리 폴더로 옮길 수 있습니다. 마찬가지로 정크, 휴지통 또는 격리로 이동한 메시지가 의심스럽지 않음으로 확인되면 해당 메시지를 다시 사용자 수신함으로 이동시킬 수 있습니다. 또한 메시지를 완전히 삭제할 수도 있습니다. 이 프로세스를 통해 메시지를 재분류(다른 판정 적용)할 수도 있습니다.

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.

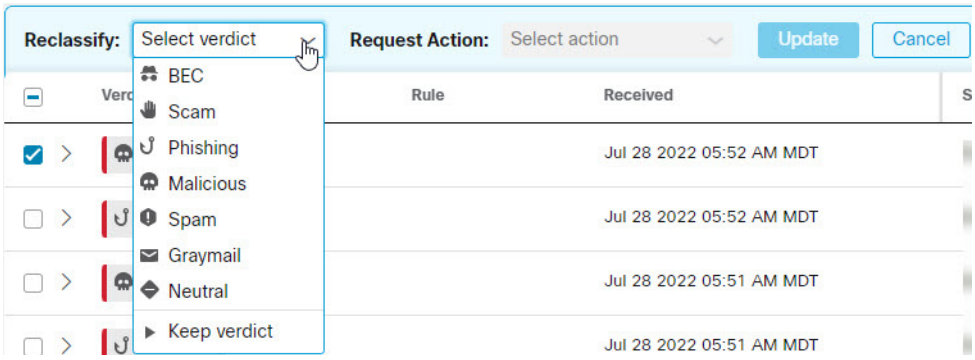
이동된 메시지는 **Last Action(마지막 작업)** 열에 표시됩니다.

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

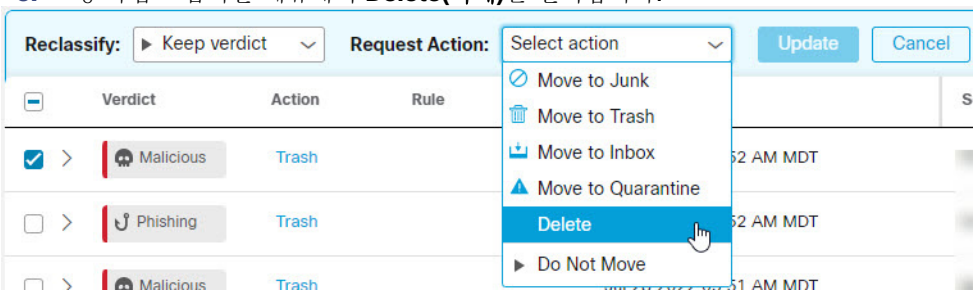
메시지 삭제

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.

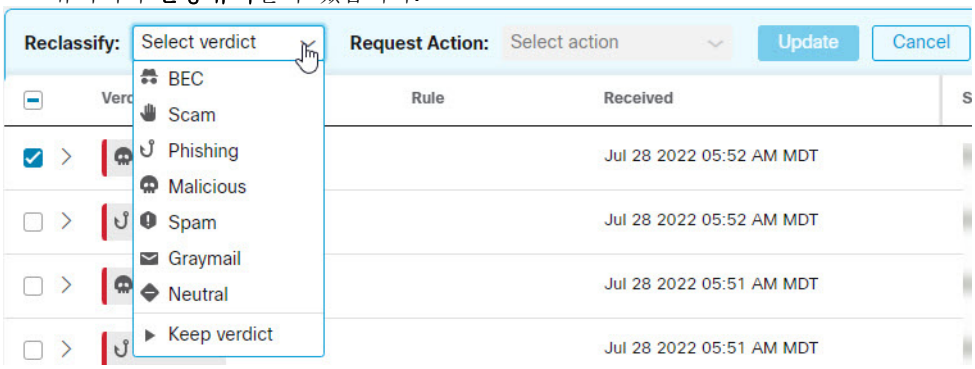
메시지 격리

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.

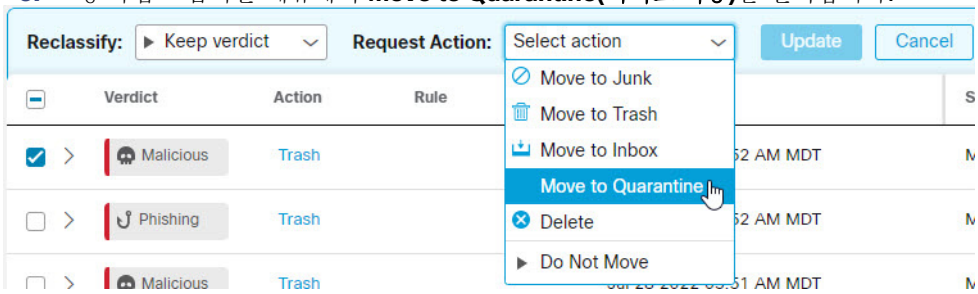
메시지를 수동으로 격리로 옮기려면 다음을 수행합니다.

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.



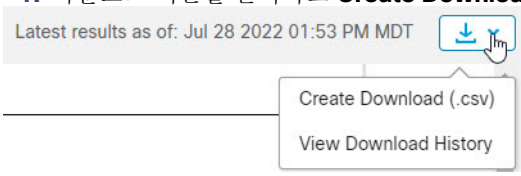
4. **Update(업데이트)**를 클릭하여 메시지를 격리합니다.

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

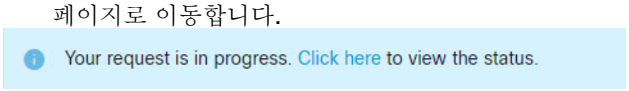
검색 결과 다운로드

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.



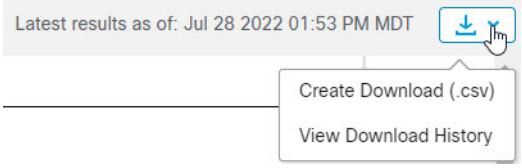
2. 요청이 진행 중임을 나타내는 배너가 나타납니다. 텍스트를 클릭하면 **Downloads: Messages(다운로드: 메시지)** 페이지로 이동합니다.



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

다운로드

화면의 오른쪽 상단 모서리의 **Downloads(다운로드)** 메뉴에서 액세스할 수 있는 페이지에서 다음을 생성하고 관리할 수 있습니다.

- 검색 결과 메시지 데이터 CSV
- 교정 오류 로그 CSV
- EML 다운로드 요청

메시지

보안, 컴플라이언스, 분석 또는 관리 목적으로 이메일 데이터를 활용해야 하는 경우 검색 결과 메시지 데이터를 CSV 형식으로 다운로드 할 수 있습니다. CSV는 다음 특성에 따라 데이터를 구성합니다.

- 메시지 ID
- 판정(BEC, 스캠, 피싱, 악성, 스팸, 그레이메일, 중립 또는 판정 없음)
- 마지막 작업(격리, 정크메일, 휴지통 또는 받은 편지함)
- 교정 방법(자동, 수동, 또는 API)
- 회귀 판정(참 또는 거짓)
- 수신(날짜 및 시각)
- 표시 이름
- 발신자
- 회신 대상
- 반환 경로:
- Envelope From
- 송신 IP
- 수신 IP
- X-원래 IP
- 수신자
- 제목
- 첨부 파일
- URL
- 방향 (수신, 발신, 또는 내부)

- 규칙 이름
- 규칙 유형
- 소스
- 전달 대상
- 봉투 대상

두 가지 방법으로 메시지 데이터를 다운로드 할 수 있습니다.

- 검색 결과 다운로드, 32페이지에 설명된 대로 메시지 페이지에서 필터링된 특정 데이터 또는 더 긴 기간에 대한 데이터를 다운로드하려면 이 옵션을 사용합니다. 현재 검색 및 필터 결과에서 메시지에 대한 데이터의 CSV 파일이 생성됩니다.
- 아래 설명된 대로 **Downloads(다운로드) > Messages(CSV)(메세지(CSV))**탭을 클릭합니다. 이 기능은 지난 24시간, 지난 7일, 특정 날짜나 주 등 특정 기간의 모든 메시지 데이터를 다운로드하려는 경우에 유용합니다.

다운로드 페이지에서 메시지 데이터의 CSV를 생성하여 다운로드하려면 다음을 수행합니다.

1. **Downloads(다운로드) > Messages(CSV)(메세지(CSV))**를 선택합니다.
2. **Create CSV(CSV 생성)**를 클릭합니다.
3. 표시되는 대화 상자에서 다운로드 대상 날짜 범위를 선택한 다음 **Create CSV(CSV 생성)**를 클릭합니다.
4. 다운로드 준비가 완료되면 작업 열 아래의 다운로드 아이콘 을 클릭하여 파일을 다운로드 합니다.

EML 다운로드

슈퍼 관리자 및 관리자는 확장된 메시지 보기에서 EML 다운로드를 요청할 수 있습니다. 작은 다운로드는 즉시 이루어집니다. 대용량 다운로드는 다운로드될 때까지 또는 7일 동안(둘 중 더 빠른 시점) 다운로드 페이지에서 사용할 수 있습니다. 파일은 다운로드 페이지에서 한 번만 다운로드할 수 있습니다. **Downloads(다운로드) > Download EML(EML 다운로드)**에서 직접 다운로드 페이지로 이동할 수 있습니다.

EML 파일을 요청하고 다운로드하려면 다음을 수행합니다.

1. 메시지 보고서에서 **Request EML Download(EML 다운로드 요청)** 버튼을 클릭합니다. 더 작은 메세지는 즉시 다운로드됩니다.
2. 느린 다운로드의 경우, 요청이 진행 중임을 나타내는 배너가 나타납니다. 텍스트를 클릭하면 **Downloads: Download EML(다운로드: EML 다운로드)** 페이지로 이동합니다.
3. 다운로드가 준비되면 작업 열 아래의 다운로드 아이콘을 클릭하여 파일을 다운로드 합니다.

교정 오류 로그

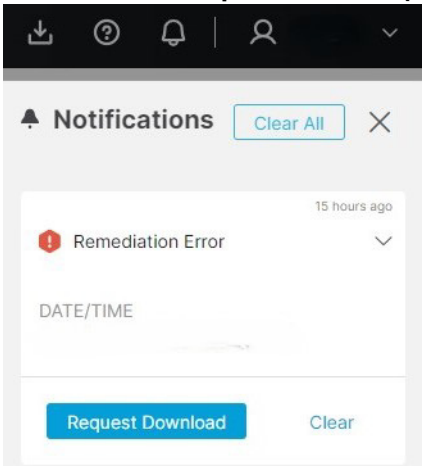
교정 오류가 발생하면 알림(종 아이콘) 메뉴 아래에 알림이 표시됩니다. 교정 오류 로그를 통해 개별 사서함에 대한 교정 실패를 조사할 수 있습니다. 예를 들어 사서함 소유자가 메시지를 이미 삭제한 경우 휴지통으로 이동 요청이 실패할 수 있습니다. 교정 오류 로그에는 *Resource is not found(리소스를 찾을 수 없습니다)*로 표시됩니다.

교정 오류 로그는 다음 속성을 기준으로 데이터를 구성하는 CSV 파일입니다.

- Request ID(요청 ID)
- 타임스탬프
- 사용자 이메일 ID
- 폴더 요청

- Mailbox
- Action Type(조치 유형)
- 이유

알림을 확장하고 **Request Download(다운로드 요청)**를 클릭하여 알림에서 직접 오류 로그 다운로드를 요청할 수 있습니다.



또는 다음 단계를 완료하여 교정 오류 로그를 생성하고 다운로드합니다.

1. **Downloads(다운로드) > Remediation Error Log(교정 오류 로그)**를 선택합니다.
2. **Create CSV(CSV 생성)**를 클릭합니다.
3. 표시되는 대화 상자에서 다운로드 대상 날짜 범위를 선택한 다음 **Create CSV(CSV 생성)**를 클릭합니다.
4. 다운로드 준비가 완료되면 작업 열 아래의 다운로드 아이콘을 클릭하여 파일을 다운로드 합니다.

교정 오류 로그

인사이트

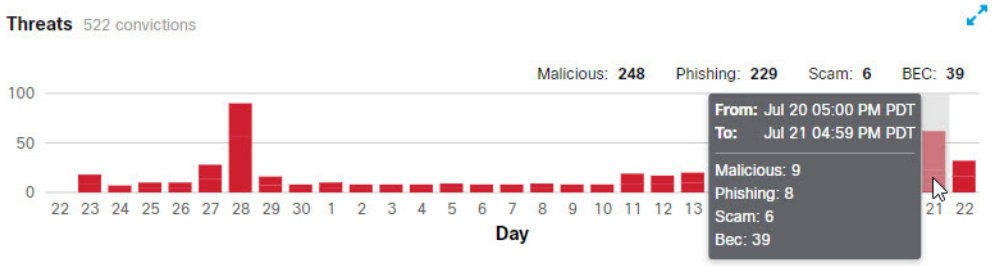
추세

Trends(추세) 페이지에는 이메일 데이터에 대한 그래픽 정보가 표시됩니다. **Insights(인사이트) > Trends(추세)**를 선택하여 추세를 봅니다.

- 달력 컨트롤을 사용하여 특정 일, 주 또는 월의 데이터를 표시합니다.
- 그래프에서 관심 있는 데이터를 클릭하면 메시지 페이지의 데이터 세부 정보로 이동합니다
- 범례 항목을 클릭하면 메시지 페이지의 관련 데이터로 이동합니다. 예를 들어 모든 Incoming(수신)을 클릭하면 현재 차트에 표시되어 있는 모든 수신 메시지를 확인할 수 있습니다.
- 다운로드 버튼을 클릭하여 추세 데이터를 다운로드합니다. 결과는 다음이 포함된 CSV 파일로 내보내집니다.
  - 지난 24시간 또는 특정 날짜를 보는 경우 지난 90일 동안의 데이터를 시간별 롤업
  - 지난 30일을 보는 경우 지난 90일 동안의 데이터에 대한 24시간 롤업
- 인쇄 버튼을 클릭하여 추세 차트를 인쇄하거나 PDF로 저장합니다.

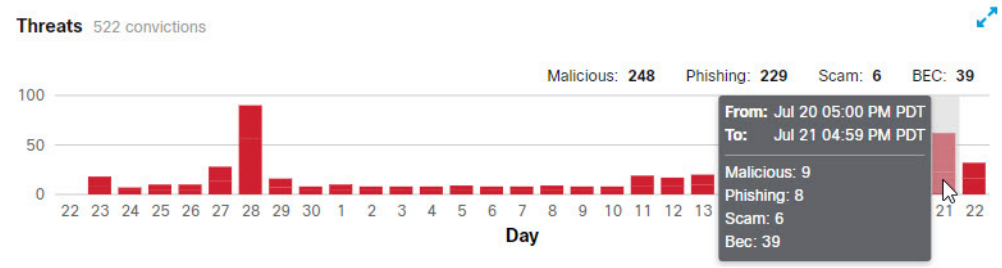
표준 시간대 정보

일별 차트의 각 막대는 1시간 동안의 데이터를 표시합니다. 이러한 차트는 브라우저의 현지 표준 시간대를 기준으로 합니다.



주 또는 월 차트의 각 막대는 24시간 하루에 대한 데이터를 보여줍니다. 날짜는 UTC 00:00부터 오후 11:59까지이며 이후 브라우저의 현지 시간으로 변환됩니다.

예를 들어 태평양 일광 절약 시간(PDT) UTC 07:00시에 월 차트의 막대는 태평양 시간으로 7월 20일 오후 5:00부터 7월 21일 오후 4:59분까지를 표시합니다.

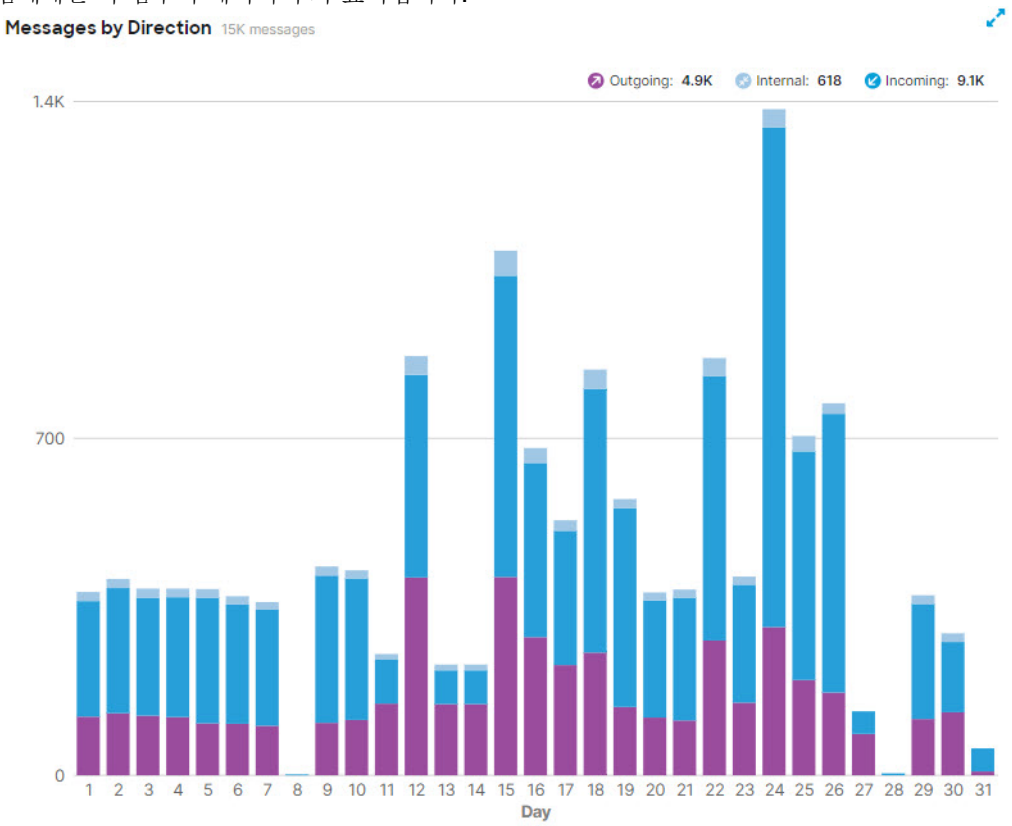


방향별 메시지

방향별 메시지 그래프는 총 이메일 트래픽을 보여줍니다. 메일은 다음 범주로 구분됩니다.

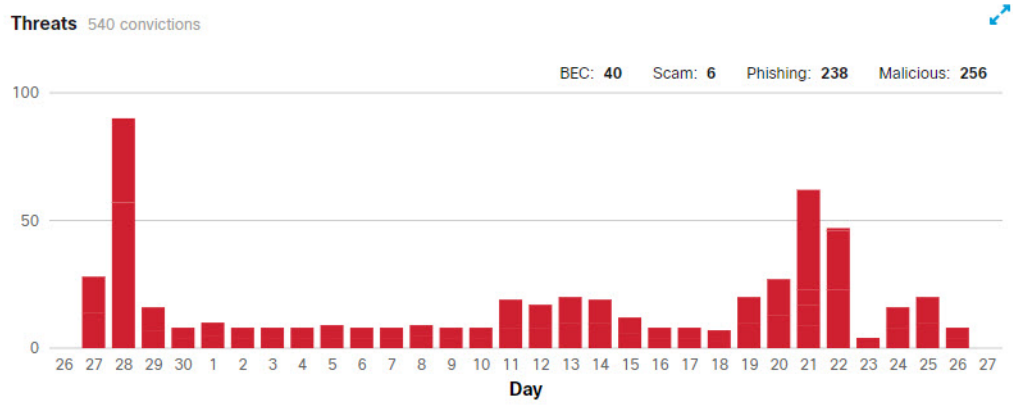
- **Outgoing(발신):** O365 테넌트 외부의 수신자에게 전송된 메일
- **Internal(내부):** O365 테넌트 내에서 전송된 메일
- **Incoming(수신):** O365 테넌트 외부에서 수신한 메일

범례에는 각 범주의 메시지 수가 표시됩니다.



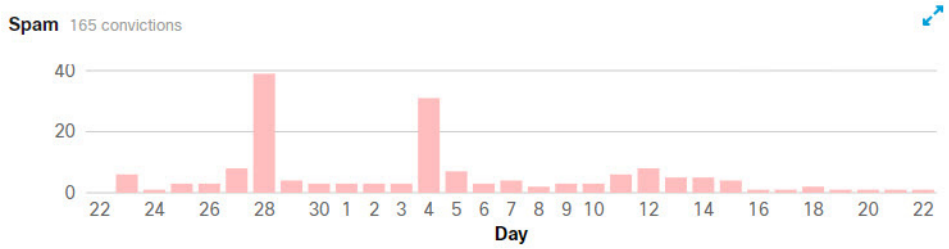
위협

Threats(위협) 그래프에는 위협으로 확인된 메시지의 스냅샷이 표시됩니다. 여기에는 BEC, 스캠, 피싱 및 악성이 포함됩니다. 범례에는 각 범주의 메시지 수가 표시됩니다. 데이터를 클릭하면 메시지 페이지로 이동합니다.



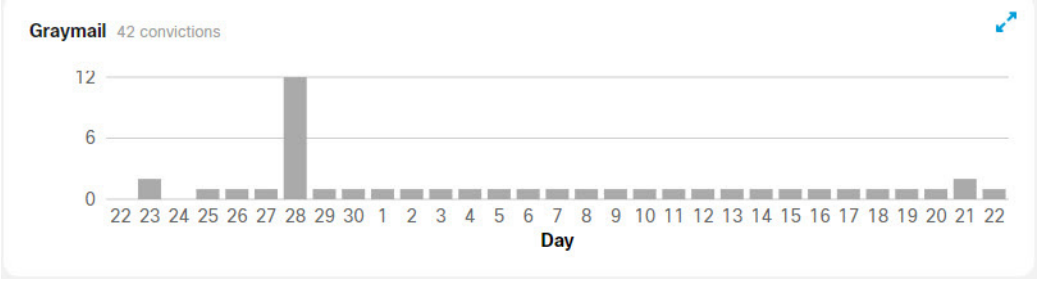
스팸

스팸 그래프에는 스팸으로 확인된 메시지의 스냅샷 이 표시됩니다. 범례에는 스팸으로 확인된 총 메시지 수가 표시됩니다.



그레이메일

그레이메일 그래프는 그레이메일로 확인된 메시지의 스냅샷을 보여줍니다. 범례에는 그레이메일로 확인된 총 메시지 수가 표시됩니다.

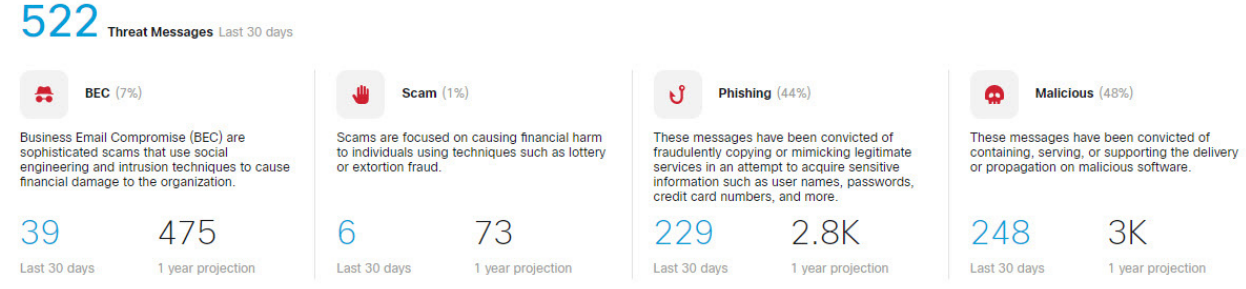


영향 보고서

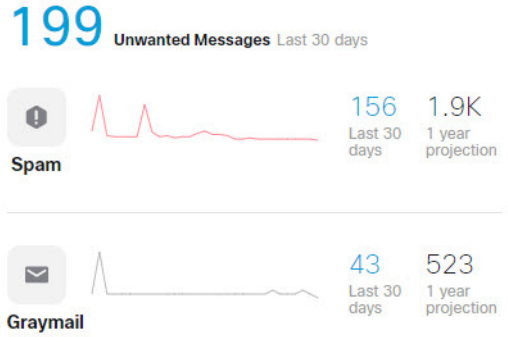
영향 보고서는 Secure Email Threat Defense가) 지난 30일 동안 제공한 혜택을 표시합니다. 보고서를 보려면 **Insights(인사이트) > Impact Report(영향 보고서)**를 선택합니다. 보고서에서 관심있는 데이터를 클릭하면 메시지 페이지의 데이터 상세정보로 이동합니다.

표시되는 데이터는 다음과 같습니다.

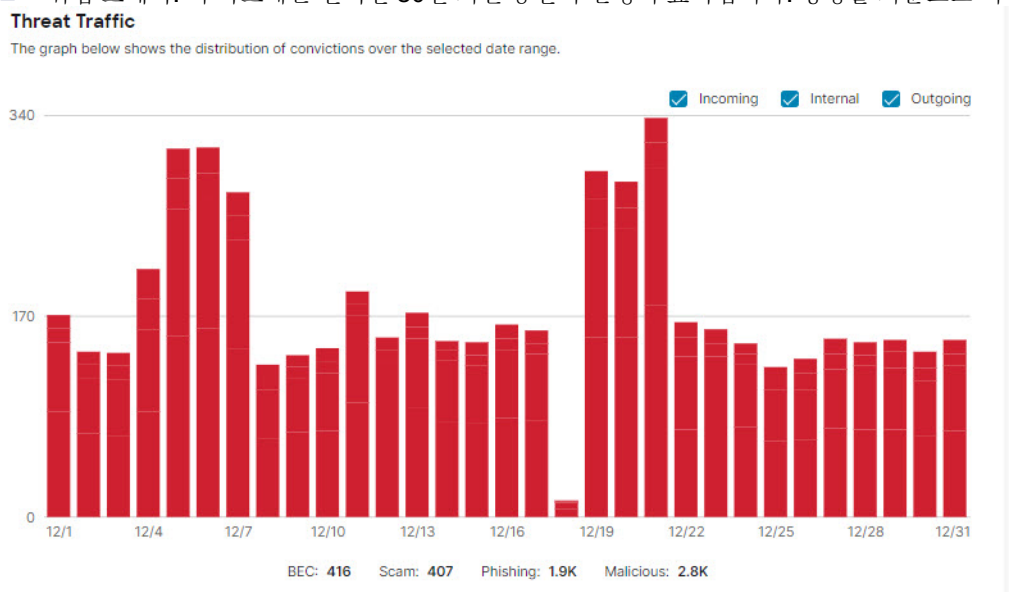
- 선택한 30일 기간 및 이 데이터의 1년 예측에 Secure Email Threat Defense가 포착한 위협 메시지. 1년 예측은 일별 평균에 365를 곱하여 계산됩니다.



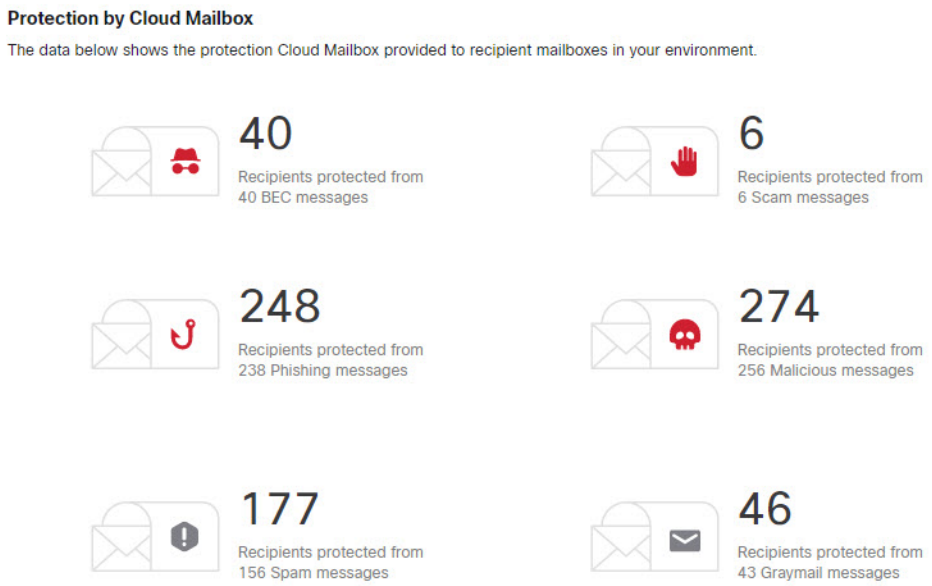
- 원치 않는 메시지. 이 차트는 선택한 30일 기간의 스팸 및 그레이메일과 이 데이터의 1년 예측을 보여줍니다. 1년 예측은 일별 평균에 365를 곱하여 계산됩니다.



- 위협 트래픽. 이 차트에는 선택한 30일 기간 동안의 판정이 표시됩니다. 방향을 기준으로 이 차트를 필터링할 수 있습니다.



- Secure Email Threat Defense에 의한 보호. 이 차트는 환경의 수신자 사서함에 제공되는 보호 Secure Email Threat Defense를 보여줍니다.



- 주요 타겟. 이 차트에는 선택한 30일 기간 동안의 위협 메시지의 상위 10개 내부 타겟이 표시됩니다.

Top Targets

The statistics below indicate the addresses which received the most threat messages over the previous 30 days.

	Recipient	BEC	Scam	Phishing	Malicious	Totals
1	[redacted]	1	0	109	107	217
2	[redacted]	0	0	36	36	72
3	[redacted]	0	0	15	30	45
4	[redacted]	0	0	16	22	38
5	[redacted]	0	0	17	17	34
6	[redacted]	0	0	10	19	29
7	[redacted]	0	0	14	14	28
8	[redacted]	0	0	9	18	27
9	[redacted]	0	0	14	9	23
10	[redacted]	12	0	0	0	12

- 내부 위협 발신자. 이 차트는 위협 메시지의 상위 10개 내부 발신자를 보여줍니다.

Internal Threat Senders

The internal addresses listed here were seen sending malicious or phishing messages from within the organization.

	Sender	Number of Messages Sent
1	[redacted]	54
2	[redacted]	50
3	[redacted]	16
4	[redacted]	2

영향력이 큰 직원 목록

경영진과 같은 중요 인사는 다른 타겟을 공격하기 위해 사칭될 위험이 있습니다. 영향력이 큰 직원 목록은 Secure Email Threat Defense가 사칭 공격으로부터 조직을 방어하는 데 도움이 됩니다.

관리자는 표시 이름과 발신자 이메일 주소에 대한 심층 조사를 위해 최대 100명의 목록을 생성하여 Talos로 전송할 수 있습니다. 개인에 대해 구성된 정보에서 벗어나는 경우 위협 판결을 받은 메시지의 판결 세부정보 패널에서 '기술'로 식별됩니다.

영향력이 큰 직원 목록에 사용자 추가

영향력이 큰 직원 목록에 사용자를 추가하려면 다음 단계를 완료하십시오.

1. **Administration(관리) > High Impact Personnel(영향력이 큰 직원)**을 선택합니다.
2. **Add New Personnel(새 직원 추가)** 버튼을 클릭합니다.
3. 사용자 정보를 입력합니다. 이름, 성, 이메일 주소가 필요합니다.
4. **Submit(제출)**을 클릭하여 목록에 사용자 추가를 완료합니다.

영향력이 큰 직원 목록에서 사용자 정보 업데이트

영향력이 큰 직원 목록에서 사용자 정보를 수정하려면 다음 단계를 완료하십시오.

1. **Administration(관리) > High Impact Personnel(영향력이 큰 직원)**을 선택합니다.
2. Actions(작업) 열에서 **Edit(편집)** 버튼을 클릭합니다.
3. 필요에 따라 사용자 정보를 업데이트합니다. 이름, 성, 이메일 주소가 필요합니다.
4. 사용자 정보 편집을 완료하려면 **Submit(제출)**을 클릭합니다.

영향력이 큰 직원 목록에서 사용자 제거

영향력이 큰 직원 목록에서 사용자를 제거하려면 다음 단계를 완료하십시오.

1. **Administration(관리) > High Impact Personnel(영향력이 큰 직원)**을 선택합니다.
2. Actions(작업) 열에서 **Delete(삭제)** 버튼 을 클릭합니다.
3. 제거 확인 대화 상자에서 **Delete(삭제)**를 클릭하여 작업을 완료합니다.

영향력이 큰 직원 목록에서 사용자 제거

사용자 관리

Administration(관리) > User(사용자) 페이지에서 사용자 어카운트를 관리합니다.

Secure Email Threat Defense 사용자 인증 관리를 위해 Cisco Security Cloud Sign On(이전 SecureX sign-on)을 사용합니다. Security Cloud Sign On에 대한 자세한 정보는 https://cisco.com/go/securesignon를 참조하십시오.

참고: 기존 Cisco XDR, Cisco Secure Malware Analytics(이전 Threat Grid) 또는 Cisco Secure Endpoint(이전 AMP) 고객인 경우, 기존 Security Cloud Sign On 자격 증명으로 로그인해야 합니다. 기존 사용자가 아닌 경우 새 Security Cloud Sign On 어카운트를 생성해야 합니다.

Security Cloud Sign On에 다른 유형의 어카운트로 로그인할 수 있지만 Security Cloud Sign On 어카운트를 사용하여 시스코 보안 제품 어카운트로 연결을 유지하는 것이 좋습니다.

다중 어카운트 액세스

동일한 Security Cloud Sign On 어카운트를 사용하여 여러 Secure Email Threat Defense 인스턴스에 액세스할 수 있습니다. 이렇게 하면 별도의 Security Cloud Sign On 어카운트를 사용하여 로그아웃했다가 다시 로그인할 필요 없이 각 인스턴스를 더 쉽게 추적할 수 있습니다.

새 사용자 생성, 50페이지의 단계를 수행하여 추가 Secure Email Threat Defense 인스턴스에 사용자를 추가합니다. 동일한 Security Cloud Sign On 어카운트를 사용하는 어카운트를 사용자 메뉴에서 사용할 수 있습니다. 이 액세스는 동일한 지역(북미, 유럽, 호주 또는 인도)에 있는 Secure Email Threat Defense 인스턴스로 제한됩니다.

사용자 역할

RBAC(역할 기반 액세스 제어)를 사용하면 사용자가 애플리케이션 내에서 다양한 수준의 제어 또는 액세스를 갖도록 할 수 있습니다. Secure Email Threat Defense 사용자는 다음 표에 설명된 역할에서 생성할 수 있습니다.

표 1 사용자 역할

Role(역할)	설명
슈퍼 관리자	이 사용자는 Secure Email Threat Defense의 모든 기능에 액세스할 수 있습니다. 설정 및 정책을 변경하고, 메시지를 재분류 및 조치하고, EML 파일을 다운로드하고, 이메일 메시지 미리보기를 볼 수 있습니다.
관리자	이 사용자는 슈퍼 관리자의 모든 기능을 사용할 수 있지만, 슈퍼 관리자 또는 관리자를 생성, 수정 또는 삭제할 수는 없습니다.
Analyst	이 사용자는 검색 및 인사이트 기능을 사용할 수 있습니다. 메시지를 재분류하고 조치할 수 있지만, 사용자 사서함에서 메시지를 삭제할 수는 없습니다. 어카운트 설정 또는 정책을 변경하거나 신규 사용자를 생성, 편집, 삭제할 수 없습니다. 또한 EML 파일을 다운로드하거나 이메일 메시지 미리보기를 볼 수 없습니다.
읽기 전용	이 사용자는 검색 및 인사이트 기능을 사용할 수 있습니다. 메시지를 재분류하거나 조치하거나, 어카운트 설정 또는 정책을 변경하거나, 신규 사용자를 생성할 수 없습니다. 또한 EML 파일을 다운로드하거나 이메일 메시지 미리보기를 볼 수 없습니다.

표 2 역할별 기능 액세스

기능 그룹	기능	Role(역할)
관리	사용자 추가/편집	■ 슈퍼 관리자 ■ 관리자
	관리자 생성/ 편집/삭제	■ 슈퍼 관리자
직장	Google 애널리틱스 토글	■ 슈퍼 관리자 ■ 관리자
	알림 이메일 보기	■ 슈퍼 관리자 ■ 관리자
	회귀 알림 이메일 편집	■ 슈퍼 관리자 ■ 관리자
	감사 로그 다운로드	■ 슈퍼 관리자 ■ 관리자 ■ Analyst ■ 읽기 전용
	격리 폴더 보기	■ 슈퍼 관리자 ■ 관리자
	알림 보기	■ 슈퍼 관리자 ■ 관리자 ■ Analyst ■ 읽기 전용
정책	정책 편집	■ 슈퍼 관리자 ■ 관리자
	도메인 가져오기	■ 슈퍼 관리자 ■ 관리자
	메시지 규칙 수정	■ 슈퍼 관리자 ■ 관리자 ■ Analyst
검색	홈페이지에서 검색	■ 슈퍼 관리자 ■ 관리자 ■ Analyst ■ 읽기 전용

표 2 역할별 기능 액세스

기능 그룹	기능	Role(역할)
메시지	확장 보기	■ 슈퍼 관리자 ■ 관리자 ■ Analyst ■ 읽기 전용
	보고서 보기	■ 슈퍼 관리자 ■ 관리자 ■ Analyst ■ 읽기 전용
	EML 다운로드	■ 슈퍼 관리자 ■ 관리자
	이메일 미리보기 보기	■ 슈퍼 관리자 ■ 관리자
재분류 및 조치	재분류	■ 슈퍼 관리자 ■ 관리자 ■ Analyst
	메시지 이동	■ 슈퍼 관리자 ■ 관리자 ■ Analyst
	메시지 격리	■ 슈퍼 관리자 ■ 관리자 ■ Analyst
	메시지 삭제	■ 슈퍼 관리자 ■ 관리자
	조치 오류 로그 보기	■ 슈퍼 관리자 ■ 관리자 ■ Analyst ■ 읽기 전용

표 2 역할별 기능 액세스

기능 그룹	기능	Role(역할)
Cisco XDR	대시보드 인증	■ 슈퍼 관리자 ■ 관리자
	리본 인증	■ 슈퍼 관리자 ■ 관리자 ■ Analyst ■ 읽기 전용
API	API 탭 액세스	■ 슈퍼 관리자 ■ 관리자
	API 키 액세스	■ 슈퍼 관리자 ■ 관리자
	API 자격 증명 생성	■ 슈퍼 관리자 ■ 관리자

새 사용자 생성

새 사용자를 생성하려면 다음 단계를 완료합니다.

1. **System Administration(시스템 관리) > Users(사용자)**를 선택합니다.
2. **Add New User(새 사용자 추가)**를 클릭합니다.
3. 사용자의 자격 증명을 입력하고 역할을 선택한 다음 **Create(생성)**를 클릭합니다.

   참고: 사용자의 이메일 주소는 Security Cloud Sign On 어카운트에 사용하는 주소와 일치 *해야* 합니다.

사용자가 **Welcome toCisco Secure Email Threat Defense**라는 제목의 이메일을 수신합니다. 사용자는 이메일의 지침에 따라 Security Cloud Sign On 어카운트를 설정하고(아직 없는 경우) 로그인해야 합니다.

사용자 편집

사용자의 역할을 업데이트 할 수 있습니다. 사용자의 이메일 주소는 편집할 수 없습니다. 사용자가 이름을 변경하면 자신의 Security Cloud Sign On 어카운트에서 업데이트해야 합니다.

사용자 역할을 편집하려면 다음을 수행합니다.

1. **System Administration(시스템 관리) > Users(사용자)**를 선택합니다.
2. 작업 열 아래의 연필을 클릭합니다.
3. 사용자 편집 대화 상자에서 사용자의 새 역할을 선택하고 **Save changes(변경 사항 저장)**를 클릭합니다.

사용자 삭제

사용자를 삭제하려면 다음 단계를 완료합니다.

1. **System Administration(시스템 관리) > Users(사용자)**를 선택합니다.
2. 작업 열에서 X 아이콘을 클릭합니다.
3. 삭제 확인 대화 상자에서 **Delete(삭제)**를 클릭하여 작업을 완료합니다.

삭제가 완료되었음을 알리는 상태 메시지가 표시됩니다. Secure Email Threat Defense에서 사용자 어카운트가 삭제되지만 Security Cloud Sign On 어카운트는 삭제되지 않습니다. 여러 Secure Email Threat Defense 인스턴스에서 사용자를 삭제하려면 각 인스턴스에 대해 다음 단계를 완료해야 합니다.

사용자 삭제

사용자 설정

개별 사용자 프로파일에 대한 설정은 **User(사용자)** (프로파일 아이콘) - **User Settings(사용자 설정)**에서 액세스할 수 있습니다.

세부 사항

세부 사항 섹션에는 사용자 이름, 역할 및 조직이 포함됩니다.

환경설정

환경설정 섹션에는 XDR 리본 인증 및 테마 모양 설정이 포함됩니다.

XDR 리본

Secure Email Threat Defense 은(는) Cisco XDR 리본과 통합됩니다. 리본을 사용하면 시스코 보안 제품 간을 탐색하고, 케이스북에 액세스하고, 관찰 가능 개체를 검색하고, 인시던트를 볼 수 있습니다. XDR 리본은 사용자별로 권한이 부여됩니다. 자세한 내용은 Cisco XDR, 61페이지를 참고하십시오.

테마

밝거나 어두운 배경에서 Secure Email Threat Defense을(를) 볼 수 있습니다. 모드를 전환하려면 **User(사용자)**(프로파일 아이콘) > **User Settings(사용자 설정)** > **Preferences(환경설정)** > **Theme(테마)**로 이동합니다. 이 가이드의 이미지는 일반적으로 밝은 색 테마로 표시됩니다.

환경설정

관리 설정

이 섹션에서 설명하는 관리 설정은 **Administration(관리) > Business(비즈니스)**에서 액세스할 수 있습니다.

어카운트

어카운트 섹션에는 다음이 표시됩니다.

- Microsoft 365 테넌트 ID
- 저널 주소
- 비즈니스 ID
- 격리 폴더 ID
- 지원 구독 ID

라이선스

라이선스 섹션에는 다음 정보가 표시됩니다.

- 라이선스 유형
- 시트 수
- 시작 날짜(제품군에 속하지 않는 독립형 비즈니스의 경우)
- 종료 날짜(제품군에 속하지 않은 독립형 비즈니스의 경우)

환경설정

환경설정 섹션에는 알림 이메일 주소, 감사 로그에 액세스, Google 애널리틱스 설정 및 비즈니스 레벨 Cisco XDR 통합 인증이 포함되어 있습니다.

알림 이메일

알림 이메일 주소는 Secure Email Threat Defense에서 알림 이메일을 보내는 주소입니다. 예를 들어, 시스템 업데이트, 새로운 기능, 예약된 유지 보수 등에 대한 알림을 전송할 수 있습니다. 처음에는 첫 번째 사용자의 이메일 주소로 설정됩니다.

알림 이메일 주소로 회귀적 판정에 대한 알림을 보낼지 여부를 선택할 수 있습니다. 메시지에 회귀적 판정이 적용되면 이메일이 전송됩니다.

감사 로그

감사 로그는 모든 보안 이벤트를 추적하고, 보안 인시던트를 추적하고, 그 영향을 시각화합니다. 지난 3개월(각 월에 대해 별도)에 대한 감사 로그를 CSV 파일로 내보낼 수 있습니다. 감사 로그를 다운로드하려면 드롭다운에서 날짜 범위를 선택하고 **Download CSV(CSV 다운로드)**를 클릭합니다. CSV는 이벤트 범주, 시간과 날짜, 수행한 작업, 사용자 이메일과 IP, 이벤트 상태 및 메타데이터에 대한 정보를 제공합니다.

Google 애널리틱스

Secure Email Threat Defense을 설정하고 이용 약관에 동의할 때 Google Analytics가 처음으로 활성화 또는 비활성화됩니다. 활성화하면 시스코는 발신자, 수신자, 주체, URL을 포함하는 개인 식별이 불가능한 사용 데이터를 수집하고 이 데이터를 Google 애널리틱스와 공유할 수 있습니다. 이 데이터를 통해 Secure Email Threat Defense이(가) 요구 사항을 충족하는지 확인할 수 있습니다.

Cisco XDR

Secure Email Threat Defense 은(는) Cisco XDR과 통합됩니다. XDR을 사용하면 다른 시스코 보안 제품의 데이터와 함께 Secure Email Threat Defense 정보를 볼 수 있습니다. 이 설정에 대한 자세한 내용은 **Cisco XDR, 61페이지**을 참고하십시오.

메시지 규칙

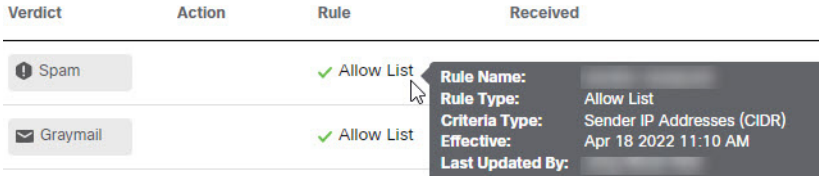
메시지 규칙을 사용하면 일부 유형의 메시지를 교정하거나 검사하지 않도록 지정할 수 있습니다. 다음을 생성할 수 있습니다.

- 허용 목록 규칙
- 판정 재정의 규칙
- 분석 규칙 우회

참고: 인증 없음 모드에서는 비즈니스에 대해 허용 목록 및 판정 재정의 규칙을 사용할 수 없습니다.

Administration(관리) > Message Rules(메시지 규칙) 페이지에서 메시지 규칙을 생성하고 관리합니다.

분석 우회 규칙은 허용 목록 및 판정 재정의 규칙보다 우선합니다. 메시지가 규칙의 영향을 받으면 메시지 페이지의 메시지 규칙 열에 표시됩니다. 적용된 규칙을 확인하려면 규칙 열의 항목 위에 커서를 올려놓습니다.



참고: 규칙이 하위 도메인에 자동으로 적용되지는 않습니다. 도메인은 규칙에 표시된 것과 정확히 일치합니다.

허용 목록 규칙

허용 목록 규칙을 사용하면 특정 발신자 이메일 주소, 발신자 도메인 또는 발신자 IP 주소에서 오는 위협, 스팸 및/또는 그레이메일 메시지의 조치를 차단할 수 있습니다. 메시지는 계속 분석되지만 자동 치료는 적용되지 않습니다. 예를 들어 Secure Email Threat Defense에서 특정 발신자의 항목을 스팸으로 확인하지만 사용자의 받은 편지함에는 해당 항목을 보관하려는 경우, 허용 목록 규칙을 생성하여 해당 메시지를 조치하는 모든 정책 을 재정의할 수 있습니다. 허용 목록 규칙은 전체 정책 설정에 대한 예외 역할을 합니다. 허용 목록 규칙과 일치하는 메시지는 영향 보고서에 계속 나타납니다.

허용 목록 규칙:

- 위협, 스팸 및/또는 그레이메일에 적용합니다.
- 허용된 발신자 이메일 주소, 발신자 도메인 또는 발신자 IP 주소(IPv4 또는 CIDR 차단)를 지정합니다.
- 규칙당 최대 50개의 기준을 가질 수 있습니다. 즉, 50개의 이메일 주소, 도메인 또는 주소입니다.

활성 규칙은 20개로 제한됩니다. 규칙을 비활성화하거나 삭제할 수 있습니다.

판정 재정의 규칙

판정 재정의 규칙을 사용하면 규칙에서 지정한 기준과 일치하는 위협, 스팸 및/또는 그레이메일 판정을 재정의할 수 있습니다. 메시지가 중립 판정으로 표시되며 조치되지 않습니다. 판정이 재정의된 메시지는 영향 보고서에 표시되지 않습니다.

판정 재정의 규칙:

- 위협, 스팸 및/또는 그레이메일에 적용합니다.

- 허용된 발신자 이메일 주소, 발신자 도메인 또는 발신자 IP 주소(IPv4 또는 CIDR 차단)를 지정합니다.
- 규칙당 최대 50개의 기준을 가질 수 있습니다. 즉, 50개의 이메일 주소, 도메인 또는 IP 주소입니다.

활성 규칙은 20개로 제한됩니다. 규칙을 비활성화하거나 삭제할 수 있습니다.

분석 규칙 우회

분석 우회 규칙을 사용하면 기준과 일치하는 피싱 테스트 또는 보안 사서함 메시지에 대한 분석을 우회 할 수 있습니다. 규칙 기준을 충족하는 메시지는 모든 엔진 분석을 우회하므로 엔진의 간섭 없이 보안 테스트를 처리할 수 있습니다. 첨부 파일 및 링크는 Secure Email Threat Defense로 열리거나 검사되지 않습니다.

참고: 우회 분석 규칙을 테스트용으로 생성하는 경우, 취약성을 방지하기 위해 적절한 기간이 지난 후에 규칙을 재고해야 합니다.

피싱 테스트 규칙:

- 지정된 발신자 이메일 주소, 발신자 도메인 또는 IP 주소(IPv4 또는 CIDR 차단)에서 오는 모든 수신 메시지에 적용합니다 . 메시지는 분석되지 않습니다.

  참고: 특정 발신자 인프라 를 우회하는 경우에는 발신자 IP 주소/CIDR 기준만 사용하는 것이 좋습니다. IP 주소는 발신자 이메일 주소 또는 도메인처럼 쉽게 스푸핑되지 않습니다.

- 규칙당 최대 50개의 기준을 가질 수 있습니다.

보안 사서함 규칙:

- 지정된 수신자 이메일 주소의 수신 메시지에 적용합니다. 메시지는 분석되지 않습니다.

  참고: 지정된 수신자가 메시지의 유일한 수신자인 경우 보안 사서함 규칙이 적용됩니다. 다른 수신인이 BCC(숨은 참조)로 복사되거나 포함되는 경우, 메시지는 분석 엔진을 우회하지 않습니다

- 규칙당 최대 50개의 기준을 가질 수 있습니다.

활성 우회 분석 규칙은 20개로 제한됩니다. 규칙을 비활성화하거나 삭제할 수 있습니다.

우회 규칙 생성 및 사용에 대한 권고

우회 규칙을 생성하고 사용할 때 다음과 같은 중요한 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 주의합니다.
- 우회 규칙에서 발신자 도메인 또는 이메일 주소를 사용하려면 조직의 업스트림 에지 이메일 제어에서 발신자 이메일 인증이 강력하게 적용되고 지정된 발신자 도메인 또는 발신자 이메일 주소가 우회 규칙과 일치하려는 모든 메시지의 최종 반환 경로 헤더와 정확히 일치하는지 별도로 검증해야 합니다.

메시지 규칙 추가

메시지 규칙을 추가하는 단계는 규칙 범주에 따라 약간 다릅니다.

새 허용 목록 또는 판정 재정의 규칙 추가

새 규칙을 생성하려면 다음 단계를 완료합니다.

1. **Administration(관리) > Message Rules(메시지 규칙)**를 선택합니다.
2. 생성할 규칙 범주를 선택합니다. **Allow List(허용 목록)** 또는 **Verdic Override(판정 재정의)**를 선택합니다.
3. **Add New Rule(새 규칙 추가)** 버튼을 클릭합니다.
4. 규칙 이름을 생성합니다. 각 규칙에는 고유한 이름이 있어야 합니다.
5. 기준 유형을 선택합니다. 발신자 이메일, 발신자 도메인, 발신자 IP 주소(IPv4) 또는 발신자 IP 주소(CIDR)를 선택할 수 있습니다.
6. 허용하거나 재정의할 항목을 쉼표로 구분하여 입력합니다.
7. 허용하려는 판정에 따라 스팸, 그레이메일 및/또는 위협을 선택합니다.
8. **Submit(제출)**을 클릭해 규칙 생성을 마칩니다.

규칙이 목록에 추가됩니다. 변경 사항이 적용되려면 최대 20분이 걸립니다.

새 우회 분석 규칙 추가

새 규칙을 생성하려면 다음 단계를 완료합니다.

1. **Administration(관리) > Message Rules(메시지 규칙)**를 선택합니다.
2. **Bypass Analysis(분석 우회)**를 선택합니다.
3. **Add New Rule(새 규칙 추가)** 버튼을 클릭합니다.
4. 규칙 이름을 생성합니다. 각 규칙에는 고유한 이름이 있어야 합니다.
5. 생성할 규칙 유형을 선택합니다(**Phish Test(피싱 테스트)** 또는 **Security Mailbox(보안 사서함)**).
6. 피싱 테스트 규칙의 경우, 기준 유형을 선택합니다(발신자 이메일 주소, 발신자 도메인, 발신자 IP 주소(IPv4) 또는 IP 주소(CIDR)). 그런 다음 쉼표로 구분하여 항목을 입력합니다.

   보안 사서함 규칙의 경우, 수신자 이메일 주소를 쉼표로 구분하여 입력합니다.
7. **Submit(제출)**을 클릭해 규칙 생성을 마칩니다.

규칙이 목록에 추가됩니다. 변경 사항이 적용되려면 최대 20분이 걸립니다.

참고: 우회 분석 규칙을 테스트용으로 생성하는 경우, 취약성을 방지하기 위해 적절한 기간이 지난 후에 규칙을 재고해야 합니다. 우회 규칙을 생성하고 사용할 때 유의해야 할 중요한 주의 사항을 참조하십시오.

규칙 편집

참고로 활성화된 규칙만 편집할 수 있습니다. 규칙을 편집하려면 다음을 수행합니다.

1. **Administration(관리) > Message Rules(메시지 규칙)**를 선택합니다.
2. 편집할 규칙 유형을 선택합니다.
3. 작업 열에서 편집하려는 규칙 옆에 있는 연필 아이콘을 클릭합니다.
4. 원하는 대로 변경한 다음 **Save Changes(변경 사항 저장)**을 클릭합니다.

규칙이 업데이트되었습니다. 변경 사항이 적용되려면 최대 20분이 걸립니다.

규칙 활성화 또는 비활성화

기존 규칙 활성화 또는 비활성화하려면 다음을 수행합니다.

1. **Administration(관리) > Message Rules(메시지 규칙)**를 선택합니다.
2. 활성화 또는 비활성화할 규칙 유형을 선택합니다.
3. 작업 열에서 상태를 변경할 규칙 옆의 활성화 또는 비활성화 아이콘을 클릭합니다.

규칙의 상태가 업데이트되었습니다. 변경 사항이 적용되려면 최대 20분이 걸립니다.

규칙 삭제

규칙을 삭제하려면 다음을 수행합니다.

1. **Administration(관리) > Message Rules(메시지 규칙)**를 선택합니다.
2. 삭제할 규칙 유형을 선택합니다.
3. 작업 열에서 삭제하려는 규칙 옆에 있는 삭제 아이콘을 클릭합니다.

규칙이 삭제되었습니다.

Microsoft 허용 목록 및 안전한 발신자

Secure Email Threat Defense 는 스팸 및 그레이메일 메시지에 대해 Microsoft 365의 스팸 필터 허용 목록에 추가된 발신자 및 도메인을 준수합니다. MS 허용 목록은 악성 또는 피싱 판정에 적용되지 않습니다. 자세한 내용은 Cisco Secure Email Threat Defense FAQ: Secure Email Threat Defense 및 Microsoft 365를 참조하십시오.

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.

Cisco XDR

Cisco XDR은 시스코 보안 제품을 통합 플랫폼에 연결합니다. Secure Email Threat Defense Cisco XDR 및 Cisco XDR 리본과 통합됩니다.

- XDR을 사용하면 다른 시스코 보안 제품의 데이터와 함께 Secure Email Threat Defense 정보를 보고 조치를 취할 수 있습니다.
- XDR 리본을 사용하면 시스코 보안 제품 간을 탐색하고, 케이스북에 액세스하고, 관찰 가능 개체를 검색하고, 인시던트를 볼 수 있습니다.

이 문서에 제공되지 않은 XDR에 대한 자세한 내용은 Cisco XDR 설명서 https://docs.xdr.security.cisco.com/ 를 참조하십시오.

XDR

Secure Email Threat Defense 는 Cisco XDR 대시보드에서 볼 수 있는 다음 타일을 제공합니다.

- 방향별 메시지: 총 이메일 트래픽을 방향별로 표시합니다. 메일은 발신, 내부, 및 수신으로 나뉩니다.
- 위협: BEC, 스캠, 피싱 또는 악성으로 확인된 메시지의 스냅샷을 표시합니다.
- 스팸: 스팸으로 확인된 메시지의 스냅샷을 표시합니다.
- 그레이메일: 그레이메일로 확인된 메시지의 스냅샷을 표시합니다.

XDR 대시보드에 대한 내용은 Cisco XDR 설명서 https://docs.xdr.security.cisco.com/ 를 참조하십시오.

Cisco XDR 인증 Secure Email Threat Defense

Secure Email Threat Defense에 대해 Cisco XDR 인증하기 전에 Cisco XDR 어카운트가 있어야 하며 Cisco XDR 조직의 구성원이어야 합니다. 자세한 내용은 Cisco XDR 설명서 https://docs.xdr.security.cisco.com/ 를 참조하십시오.

참고: Secure Email Threat Defense 어카운트는 한 번에 하나의 Cisco XDR 조직에만 통합할 수 있습니다.

Secure Email Threat Defense 슈퍼 관리자 및 관리자는 Secure Email Threat Defense 인스턴스에 대해 Cisco XDR 모듈을 인증할 수 있습니다.

1. **Administration(관리) > Business(비즈니스)**를 선택합니다.
2. **Preferences(환경설정) > Extended Detection and Response(확장 탐지 및 응답)**에서 **Authorize XDR Integration(XDR 통합 인증)**을 클릭합니다.
3. 인증 플로우를 완료합니다.

XDR 구성에 성공했다는 배너가 표시됩니다.

이제 Secure Email Threat Defense 타일을 XDR 대시보드에 추가할 수 있습니다. 이 작업을 수행하는 방법에 대한 자세한 내용은 Cisco XDR 설명서 https://docs.xdr.security.cisco.com/Content/Control-Center/configure-dashboards.htm 를 참조하십시오.

XDR 인증 취소 Secure Email Threat Defense

참고: 슈퍼 관리자 또는 관리자라면 누구나 이 작업을 수행할 수 있습니다. Secure Email Threat Defense 인스턴스에 대한 XDR 인증한 사용자가 수행할 필요는 없습니다.

XDR 인증을 취소하려면 다음을 수행합니다.

1. **Administration(관리) > Business(비즈니스)**를 선택합니다.
2. **Preferences(환경설정) > Extended Detection and Response(확장 탐지 및 응답)**에서 **Revoke Authorization (인증 취소)**을 클릭합니다.

XDR 구성이 성공적으로 업데이트되었음을 알리는 배너가 표시됩니다.

XDR 리본

XDR 리본은 페이지 하단에 있으며, 사용자 환경에서 Secure Email Threat Defense과 다른 시스코 보안 제품 사이를 이동할 때에도 계속 유지됩니다. 모든 Secure Email Threat Defense 사용자는 XDR 리본을 사용하도록 인증할 수 있습니다. 리본을 사용하여 시스코 보안 애플리케이션 간을 이동하고, 케이스북에 액세스하고, 관찰 가능 개체를 검색하고, 인시던트를 볼 수 있습니다.

XDR 리본에 대한 자세한 내용은 Cisco XDR 설명서 https://docs.xdr.security.cisco.com/Content/Ribbon/ribbon.htm를 참조하십시오.

피벗 메뉴

리본을 인증하면 XDR 피벗 메뉴가 Secure Email Threat Defense 메시지 보고서 내에 추가됩니다. 이러한 메뉴를 통해 구매한 시스코 보안 제품에 따라 각 관찰 가능 항목에 대한 추가 정보에 액세스할 수 있는 중앙 지점을 제공합니다.

마찬가지로, Secure Email Threat Defense와 XDR의 통합을 통해 피벗 메뉴를 사용하여 XDR에서 Secure Email Threat Defense에 액세스할 수 있습니다. 피벗할 수 있는 관찰 가능 개체는 다음과 같습니다.

- 이메일 주소
- 이메일 메시지 ID
- 이메일 제목
- 파일 이름
- 발신자 IP
- SHA 256
- URL

피벗 메뉴를 다음에 사용할 수 있습니다.

- 피벗 메뉴에서 직접 특정 관찰 항목과 관련된 메시지를 격리합니다. 이 방법으로 격리된 항목은 Secure Email Threat Defense에서 XDR을 사용하여/XDR 사용자가 수동으로 복구했음을 나타냅니다.
  - **참고:** 피벗 메뉴에서 격리하는 메시지는 100개까지로 제한됩니다.
- Secure Email Threat Defense에서 검색을 시작합니다.

XDR 피벗 메뉴에 대한 자세한 내용은 XDR 설명서 https://docs.xdr.security.cisco.com/Content/pivot-menu.htm)를 참조하십시오.

XDR 리본 인증

XDR 리본은 사용자 레벨에서 인증됩니다. 리본 내에서 또는 사용자 환경설정 메뉴에서 리본에 대한 인증할 수 있습니다.

참고: 리본에 인증하려면 XDR 어카운트를 활성화해야 합니다. Cisco XDR 인증 Secure Email Threat Defense, 61페이지의 지침을 따르거나 XDR의 다른 모듈을 통합하여 이 작업을 수행할 수 있습니다.

XDR 리본 내에서 인증

리본 내에서 XDR 리본을 인증하려면 다음을 수행합니다.

1. **Get XDR(XDR 가져오기)**을 클릭합니다.
2. 애플리케이션 액세스 인증 대화 상자에서 **Secure Email Threat Defense 리본 인증을** 클릭합니다.

이제 XDR 리본에 인증되었습니다. XDR 구성이 성공적으로 업데이트되었음을 알리는 배너가 표시됩니다.

Secure Email Threat Defense 사용자 설정에서 인증

사용자 설정 메뉴에서 XDR 리본에 인증하려면 다음을 수행합니다.

1. **User(사용자)** (프로파일 아이콘) > **User Settings(사용자 설정)**을 선택합니다.
2. **Preferences(환경설정)** > **XDR 리본**에서 **Authorize XDR Ribbon(XDR 리본 인증)**을 클릭합니다.
3. 애플리케이션 액세스 인증 대화 상자에서 **Cisco Secure Email Threat Defense 리본 인증**을 클릭합니다.

이제 XDR 리본에 인증되었습니다. XDR 구성이 성공적으로 업데이트되었음을 알리는 배너가 표시됩니다.

XDR 리본 인증 취소

XDR 리본은 사용자 레벨에서 인증됩니다. 리본 내에서 또는 사용자 환경설정 메뉴에서 인증을 취소할 수 있습니다.

XDR 리본 내에서 인증 취소

리본 내에서 XDR 리본 인증을 취소하려면

1. XDR 리본에서 **Settings(설정)** > **Authorization(인증)** > **Revoke(취소)**를 선택합니다.
2. 취소 대화상자에서 **Confirm(확인)**을 클릭합니다.

XDR 리본이 Secure Email Threat Defense 사용자 어카운트에 대해 더 이상 인증되지 않습니다.

Secure Email Threat Defense 사용자 설정에서 인증 취소

사용자 설정 메뉴에서 XDR 리본 인증을 취소하려면 다음을 수행합니다.

1. **User(사용자)** (프로파일 아이콘) > **User Settings(사용자 설정)**을 선택합니다.
2. **Preferences(환경설정)** > **XDR Ribbon(XDR 리본)**에서 **Revoke XDR Ribbon(XDR 리본 인증 취소)**을 클릭합니다.

XDR 리본이 Secure Email Threat Defense 사용자 어카운트에 대해 더 이상 인증되지 않습니다. XDR 구성이 성공적으로 업데이트되었음을 알리는 배너가 표시됩니다.

API

Secure Email Threat Defense API를 사용하면 안전하고 확장 가능한 방식으로 프로그래밍 방식으로 액세스하고 데이터를 사용할 수 있습니다. 자세한 내용은 API 설명서 https://developer.cisco.com/docs/message-search-api/를 참조하십시오.

Secure Email Threat Defense 비활성화

메시지 소스: Microsoft 365

Microsoft를 메시지 소스 로 하는 경우, Secure Email Threat Defense을 비활성화하는 경우에는 두 가지 주요 작업이 있습니다.

- Microsoft 365 관리 센터에서 Secure Email Threat Defense 저널 항목 삭제
- Microsoft Azure 테넌트에서 Secure Email Threat Defense 애플리케이션 삭제

Secure Email Threat Defense저널 규칙 삭제

Secure Email Threat Defense 저널 규칙을 삭제하려면 다음을 수행합니다.

1. Microsoft 365 관리 센터 https://admin.microsoft.com/AdminPortal/Home#/homepage로 이동합니다.
2. **Admin centers(관리 센터)** > **Compliance(컴플라이언스)** > **Data lifecycle management(데이터 라이프사이클 관리)** > **Exchange(legacy)(교환(레거시))** > **Journal rules(저널 규칙)**으로 이동합니다.
3. Secure Email Threat Defense 저널 규칙을 선택한 다음 **Delete(삭제)**를 클릭합니다. 저널 규칙을 삭제하려면 **Yes(예)**를 선택합니다.

Azure에서 Secure Email Threat Defense 애플리케이션 삭제

Azure에서 Secure Email Threat Defense 애플리케이션 을 삭제하려면 다음을 수행합니다.

1. portal.azure.com으로 이동합니다.
2. **Enterprise applications(엔터프라이즈 애플리케이션)**을 검색하고 선택합니다.

   참고: Azure에서 이전 보기를 사용하는 경우 이를 **App registrations(앱 등록)**이라고 할 수도 있습니다.
3. **Cisco Secure Email Threat Defense** 및/또는 **Cisco Secure Email Threat Defense (Read Only)** 애플리케이션을 찾아 선택합니다.
4. 왼쪽 창에서 **Properties(속성)**를 선택합니다.
5. **Delete(삭제)** 버튼을 클릭한 다음 **Yes(예)**를 선택하여 Secure Email Threat Defense 앱을 삭제한다고 확인합니다.

메시지 소스: 게이트웨이

게이트웨이를 메시지 소스로 사용할 때 Secure Email Threat Defense를 비활성화하려면 다음 두 가지 작업을 수행합니다.

- Secure Email Threat Defense로 메시지 전송을 중지하도록 게이트웨이 구성
- Microsoft Azure 테넌트 에서 Secure Email Threat Defense 애플리케이션을 삭제 합니다(인증 없음 모드인 경우 필요하지 않음).

메시지 전송을 중지하도록 게이트웨이 구성

Secure Email Threat Defense로 메시지 전송을 중지하도록 게이트웨이를 구성하려면 다음을 수행합니다.

1. Secure Email Cloud Gateway 콘솔에서 **Security Services(보안 서비스)** > **Threat Defense Connector((위협 방어 커넥터))**로 이동합니다.
2. **Threat Defense Connector((위협 방어 커넥터))**가 현재 **Disabled(비활성화)**되어 있습니다.

Azure에서 Secure Email Threat Defense 애플리케이션 삭제

Azure에서 Secure Email Threat Defense 애플리케이션을 삭제하려면 다음을 수행합니다.

1. portal.azure.com으로 이동합니다.
2. **Enterprise applications(엔터프라이즈 애플리케이션)**을 검색하고 선택합니다.

   참고: Azure에서 이전 보기를 사용하는 경우 이를 **App registrations(앱 등록)**이라고 할 수도 있습니다.
3. **Cisco Secure Email Threat Defense** 및/또는 **Cisco Secure Email Threat Defense (Read Only)** 애플리케이션을 찾아 선택합니다.
4. 왼쪽 창에서 **Properties(속성)**를 선택합니다.
5. **Delete(삭제)** 버튼을 클릭한 다음 **Yes(예)**를 선택하여 Secure Email Threat Defense 앱을 삭제한다고 확인합니다.

FAQ(자주 묻는 질문)

자주 묻는 질문은 Cisco Secure Email Threat Defense FAQ에서 확인할 수 있습니다.