DISARM Content Security for MS Exchange Online 사용자 매뉴얼

DISARM Content Security

for MS Exchange Online

Used by hundreds of thousands of users worldwide, DISARM is specially-built for securing content.
It provides a multi-layered security pipeline, combining traditional threat analysis with the market's most advanced sandbox and Content Disarm and Reconstruction (CDR) technologies. This combination ensures all content is fully sanitized before it even reaches user devices -- no matter if it contains yet unknown or evasive malware.
DISARM allows you to do so faster and with lower cost and complexity.

발행일 : 2024. 07

발행처 : 시큐레터 주식회사

목 차

DISARM

1. 기능

기능 1
“대시보드”

회사의 이메일 상태를 한눈에 확인하세요.
날짜 범위를 설정하기만 하면 필요한 정보를 얻을 수 있습니다.

1. 대시보드 - 상단 페이지

1. 이메일 통계치를 확인하고자 하는 기간을 설정합니다.

2. 가장 최근 탐지한 악성 메일을 간략히 표기합니다.

3. 1에서 설정한 기간 동안의 이메일 통계치를 확인합니다.

기능 1
“대시보드”

회사의 이메일 상태를 한눈에 확인하세요.
날짜 범위를 설정하기만 하면 필요한 정보를 얻을 수 있습니다.

1. 대시보드 - 첨부 내용, 악성 메일

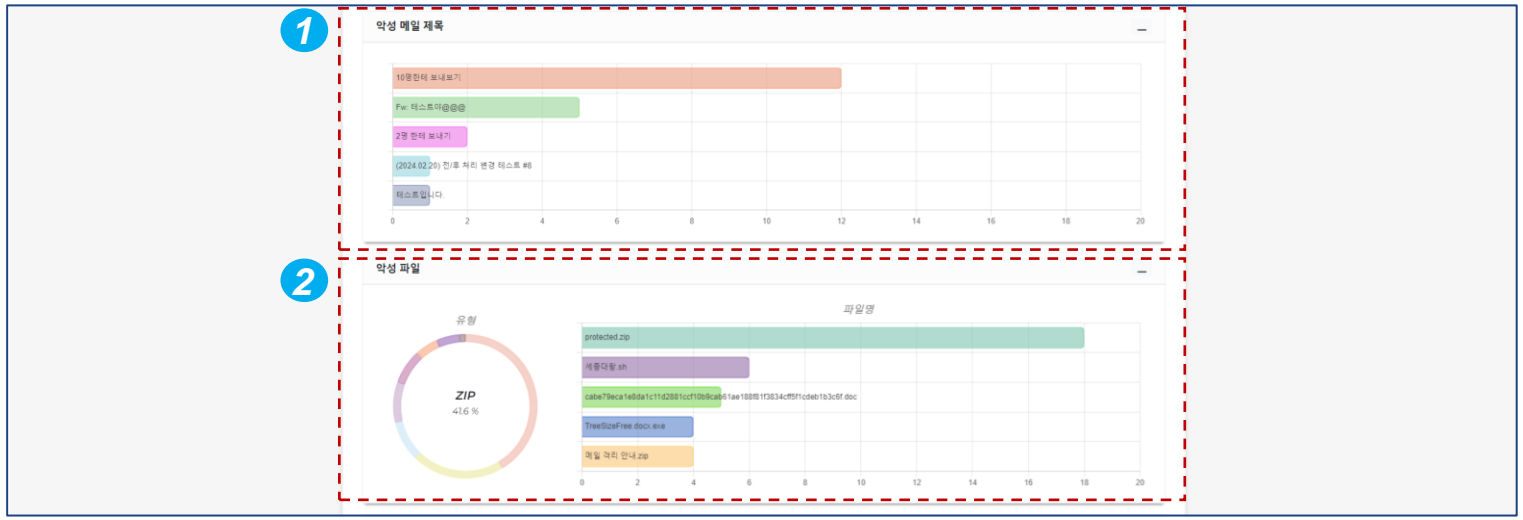
1. 설정한 기간 동안 유입된 첨부 파일의 탐지 결과 통계를 확인합니다.

2. 설정한 기간 동안 유입된 악성 메일의 통계를 확인합니다.
   가장 많이 탐지한 상위 5개의 악성 이메일 발신자 및 수신자 목록도 확인할 수 있습니다.

기능 1
“대시보드”

회사의 이메일 상태를 한눈에 확인하세요.
날짜 범위를 설정하기만 하면 필요한 정보를 얻을 수 있습니다.

1. 대시보드 - 악성 메일 제목, 악성 파일



1. 설정한 기간의 가장 많이 유입된 악성 이메일 제목 상위 5개를 확인합니다.

2. 설정한 기간 동안 유입된 악성 파일의 유형 통계와 가장 많이 유입된 악성 파일 상위 5개를 확인합니다.

기능 1
“대시보드”

회사의 이메일 상태를 한눈에 확인하세요.
날짜 범위를 설정하기만 하면 필요한 정보를 얻을 수 있습니다.

1. 대시보드 - 악성 행위, 무해화

1. 설정한 기간 동안 유입된 악성 행위 통계를 확인합니다.

2. 설정한 기간 동안 무해화 처리한 파일의 통계를 확인합니다.

기능 2
“로그 – 이메일”

DISARM은 자세한 분석 결과를 제공합니다. 로그 페이지에서 각 이메일, 파일 또는 URL별로 수신된 모든 이메일을 확인할 수 있습니다. 수신자의 개인정보 보호를 위해 이메일 본문 내용은 '악성'으로 탐지된 경우에만 확인할 수 있습니다.

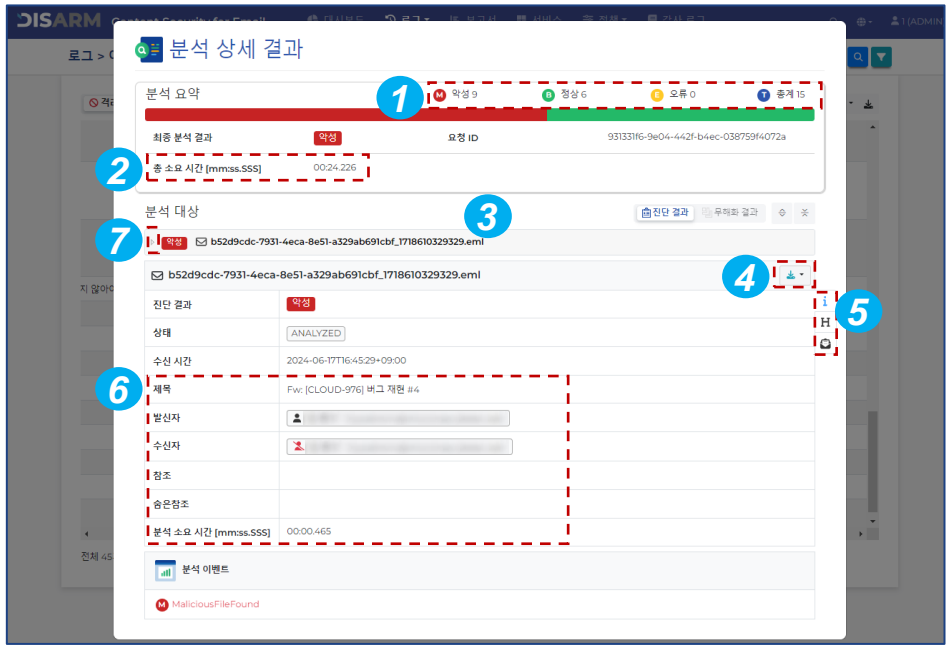
2. 로그 – 이메일

1. 로그를 보려는 기간 또는 필터를 설정합니다.
   *필터: 발신자, 수신자, 제목, 진단명
2. '격리'는 악성 이메일 로그를 표기하며, '전체'는 악성 포함 전체 이메일 로그를 표기합니다.
3. '새로 고침', '전체 화면', '컬럼 필터링', '텍스트 크기 변경', '목록을 CSV로 내보내기' 버튼입니다.
4. 각 이메일 로그를 클릭하면 자세한 진단 결과를 확인할 수 있습니다.
5. 이메일을 확인한 후 '메일 전송'을 클릭하여 수신자의 받은 편지함으로 전달합니다.
   *관리자 페이지에서 수동으로 전달된 메일에는 종이 비행기 아이콘이 표시됩니다.

기능 2
“로그 – 이메일”

로그 목록에서 이메일 중 하나를 클릭하면
자세한 진단 결과 정보를 확인할 수 있습니다.

2. 로그 - 이메일 (이메일 탐지 결과 팝업 창)



1. 숫자는 분석된 요소의 진단 결과를 나타냅니다.
2. DISARM이 이메일을 수신하여 메일 서버로 전송하기까지 걸린 총 시간입니다.
3. MTA가 메일에 부여한 고유 ID입니다.
4. EML 파일을 파일 또는 압축 파일로 다운로드합니다.
5. 메일 정보, 헤더 값, 메일 본문을 확인합니다.
6. 이메일 제목, 발신자, 수신자 및 분석 시간을 확인합니다.
7. 작은 화살표를 클릭하면 첨부 파일과 해당 파일 분석 결과를 확인할 수 있습니다.
(다음 페이지에서 계속)

기능 2
“로그 – 이메일”

DISARM은 메일 본문 뿐만 아니라 첨부 파일에 대한 자세한 탐지 결과를 제공합니다.
시큐레터의 코어 기술인 ‘어셈블리 레벨 분석'을 통해 자체 악성코드 분석가를 보유한 듯한 경험을 해보실 수 있습니다.

2. 로그 - 이메일 (이메일 첨부파일 탐지 결과 팝업 창)

1. 파일명 또는 URL을 클릭하여 분석 결과를 확인합니다.

2. VT Link 버튼을 클릭하여 분석결과를 VirusTotal과 비교하거나 혹은 파일을 다운로드 할 수 있습니다.

3. 다양한 파일 정보를 확인합니다.

4. 각 분석 이벤트를 클릭하여 파일의 요소가 어떤 행위를 일으키는지 확인합니다.

5. DISARM은 동적 및 정적 엔진으로 추출한 더욱 상세한 분석 데이터를 제공합니다.
Dynamic Feature를 통해 시큐레터 코어 기술 '어셈블리 명령어 분석' 기법에서 도출된 결과를 볼 수 있습니다.

*각 기능은 분석된 파일에 해당되는 요소가 있는 경우에만 활성화됩니다.

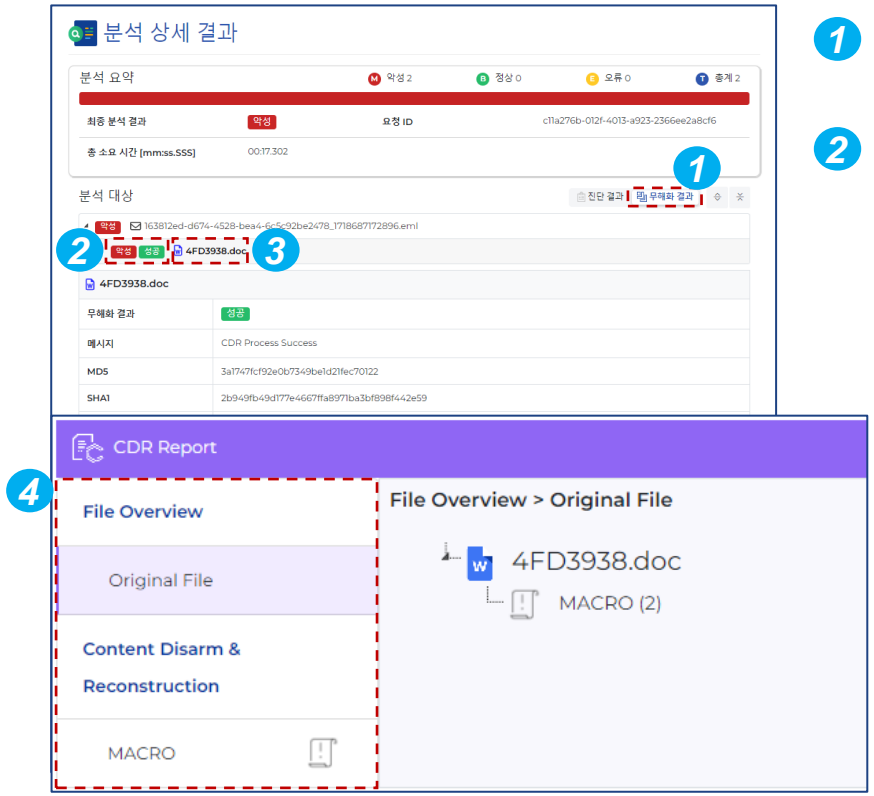
기능 2
“로그 – 이메일”

CDR(콘텐츠 무해화 솔루션)은 비즈니스 커뮤니케이션을 더욱 안전하고 효과적으로 만드는 DISARM의 큰 장점 중 하나입니다.

DISARM CDR은 하이퍼링크, 비주얼 베이직 매크로, 자바스크립트 등과 같은 파일 내부의 의심스럽거나 잠재적인 위협을 제거합니다.

DISARM CDR을 사용하면 안심하고 파일을 열 수 있습니다!

2. 로그 - 이메일 (이메일 첨부파일 무해화 결과 팝업 창)



1 ‘무해화 결과’를 클릭하여 무해화 분석 및 처리 결과를 확인합니다.

2 왼쪽 버튼은 ‘진단 결과’를, 오른쪽 버튼은 ‘무해화 결과’를 표시합니다.

결과	설명
성공	무해화 처리가 성공적으로 완료됨
실행하지 않음	파일이 무해화를 지원하는 확장자가 아님
제거할 콘텐츠 없음	파일 내 제거할 액티브콘텐츠 없음
실패	주로 잘못된 형식의 파일일 경우
지원하지 않음	주로 파일 형식이 구버전일 경우
재압축	CDR 성공 후 압축된 파일에 대해서만 표시됩니다. 모든 압축 파일의 확장자는 '.zip'으로 수정됩니다.

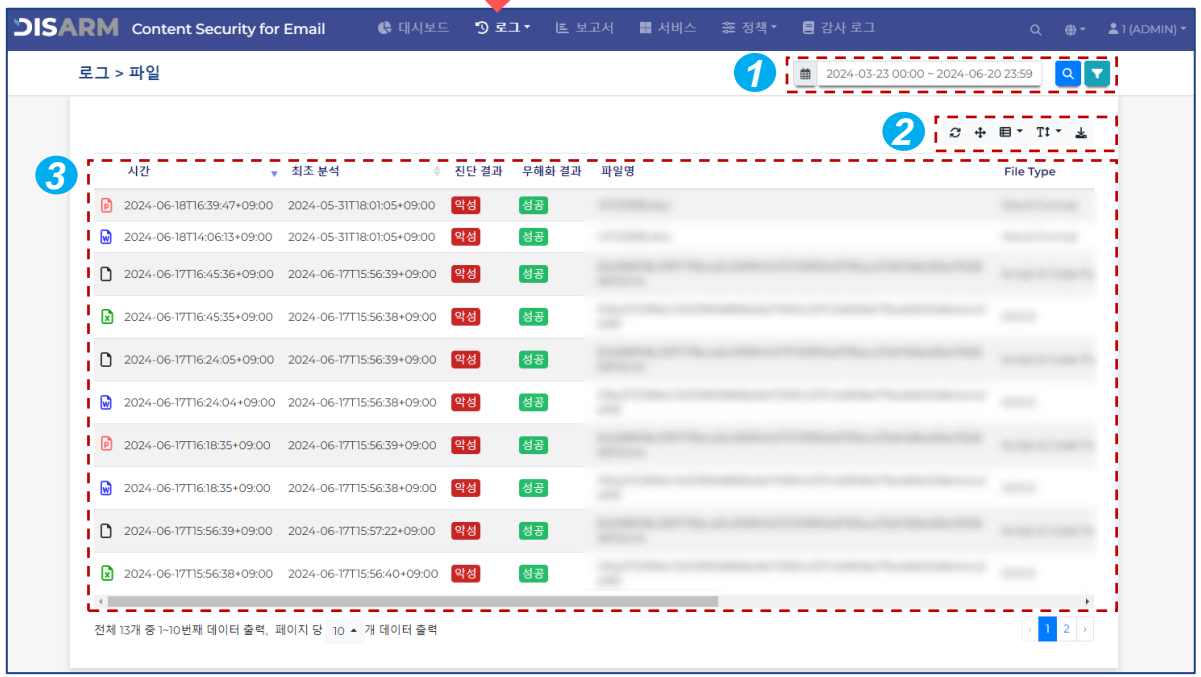
3 파일 이름을 클릭하면 자세한 CDR 결과를 볼 수 있습니다.

4 원본 파일에서 CDR이 제거한 내용을 보여줍니다.

기능 2
“로그 – 파일”

이메일로 수신된 모든 첨부파일을 각각의 탐지 결과와 함께 확인할 수 있습니다.

2. 로그 - 파일



1. 로그를 확인할 기간 또는 필터를 설정합니다.
   *필터: 분석 결과, 파일 유형, CDR 상태, 파일명, 진단명

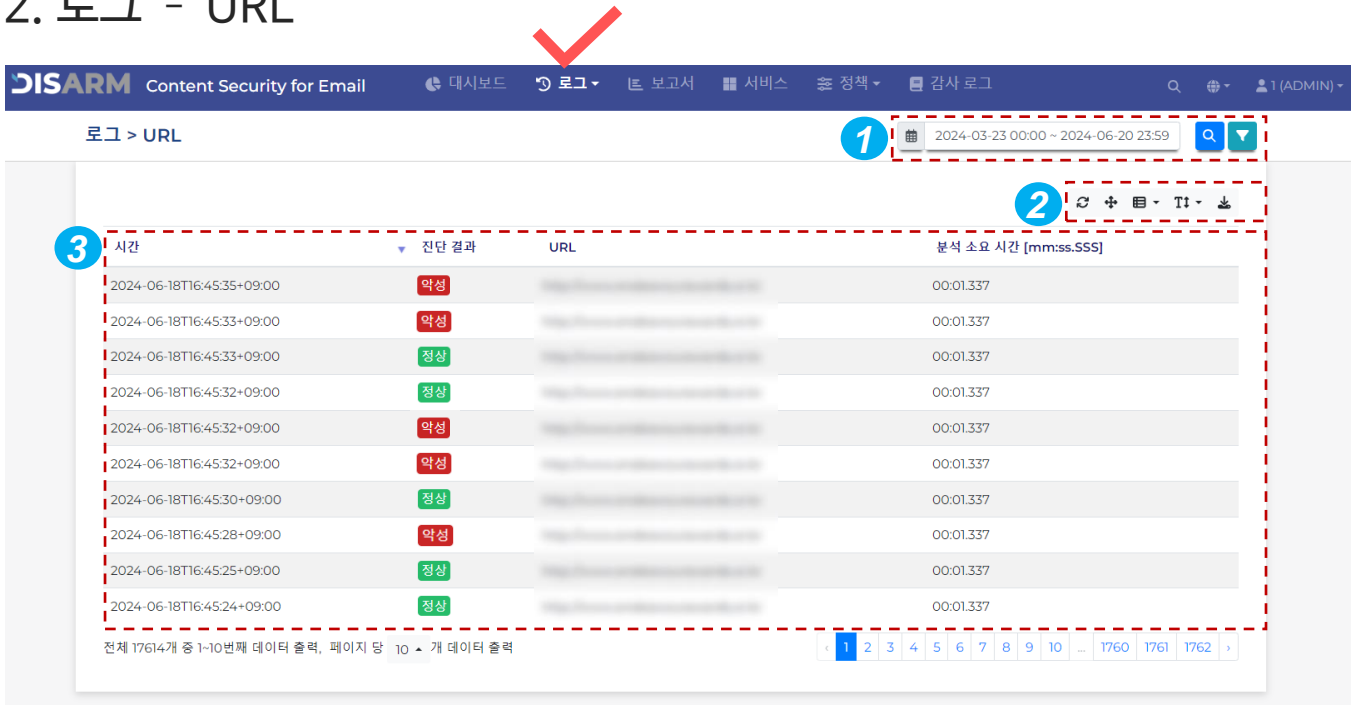
2. '새로 고침', '전체 화면', '컬럼 필터링', '텍스트 크기 변경', '목록을 CSV로 내보내기' 버튼입니다.

3. 각 이메일 로그를 클릭하면 자세한 진단 결과를 확인할 수 있습니다.
   *결과 팝업창은 10페이지 이메일 로그 자세히 보기와 항목이 동일합니다.

기능 2
“로그 – URL”

이메일 본문 혹은 첨부파일 내 포함된 모든 URL 을 각각의 탐지 결과와 함께 확인할 수 있습니다.

2. 로그 - URL



1. 로그를 확인할 기간 또는 필터를 설정합니다.
   *필터: 분석 결과, URL, 진단명

2. '새로 고침', '전체 화면', '컬럼 필터링', '텍스트 크기 변경', '목록을 CSV로 내보내기' 버튼입니다.

3. 각 이메일 로그를 클릭하면 자세한 진단 결과를 확인할 수 있습니다.
   *결과 팝업창은 10페이지 이메일 로그 자세히 보기와 항목이 동일합니다.

기능 3
“보고서”

이메일 보안 상태 보고서가 필요하신가요?
DISARM 보고서 페이지로 이동하여 전용 보고서를 쉽게 작성하세요!

3. 보고서

1. 날짜 범위를 지정하고 오른쪽에 있는 버튼을 클릭하여 보고서를 생성합니다.
(최대 31일 단위)

2. 버튼을 클릭하여 새 창에서 보고서 PDF로 저장하거나 하드 카피로 인쇄합니다.

3. 탐지 및 분석 결과 요약입니다.

4. 무해화 처리 결과 요약입니다.

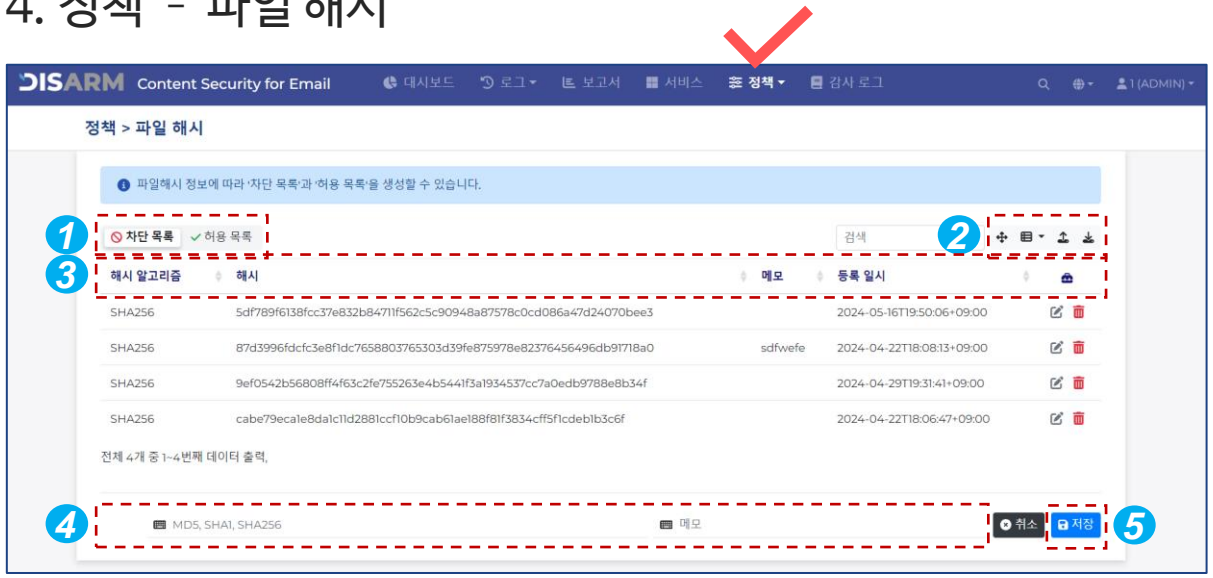
5. 탐지 및 분석 결과의 통계 차트입니다.

6. 카테고리별 상위 5가지 악성 및 CDR 정보를 확인합니다.

기능 4
“정책”

특정 파일 해시를 기반으로 기업의 블랙리스트와 화이트리스트를 만드세요.

4. 정책 - 파일 해시



1. '차단 목록'에 차단할 파일 해시를 추가하고 해당 파일이 포함된 이메일을 차단합니다.
   '허용 목록'에 추가된 파일 해시를 가진 첨부 파일은 분석하지 않습니다.

2. '전체 화면', '컬럼 필터링', '목록 한 번에 올리기', '목록을 CSV로 내보내기' 버튼입니다.

3. 아래 4에 입력한 파일 해시 정보를 표시합니다. *해시 알고리즘은 해시 정보 등록 시 자동으로 입력됩니다.

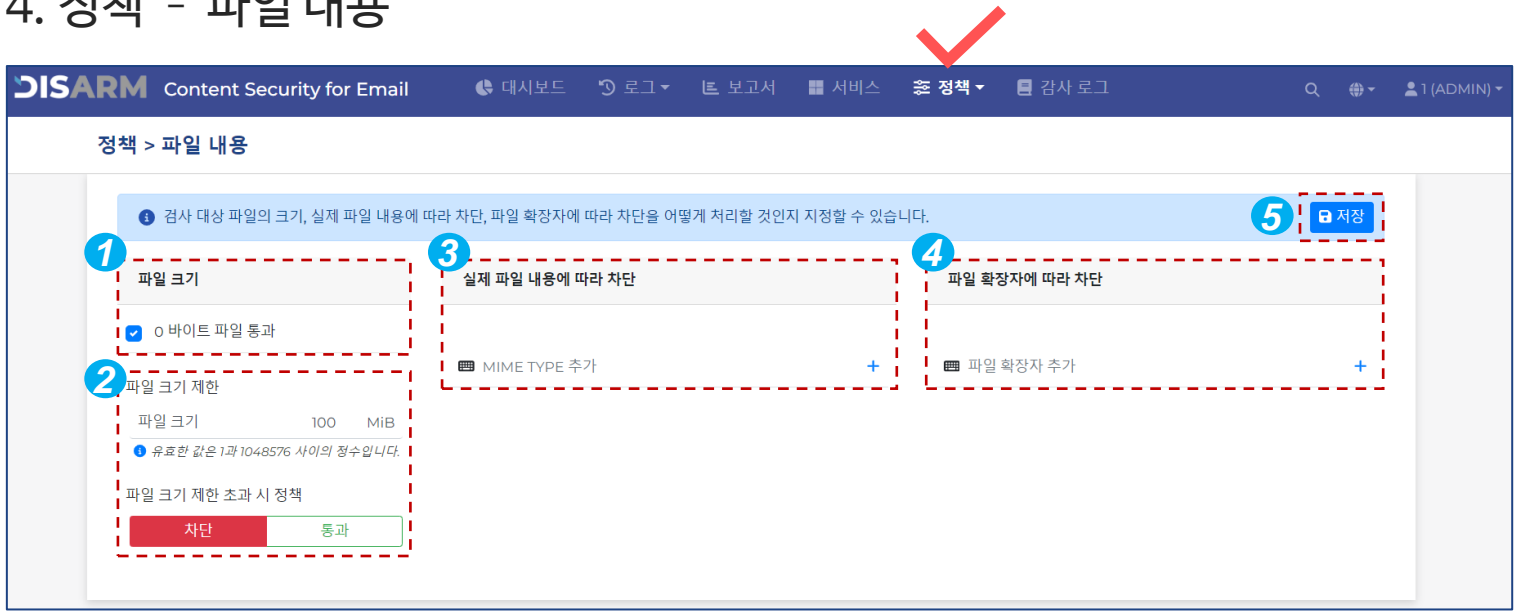
4. 등록한 파일 해시에 대한 정보를 함께 저장합니다.

5. '저장' 버튼을 클릭하여 업데이트한 내용을 적용합니다.

기능 4
“정책”

다양한 파일 정보를 기반으로 세부 정책을 설정합니다.

4. 정책 - 파일 내용

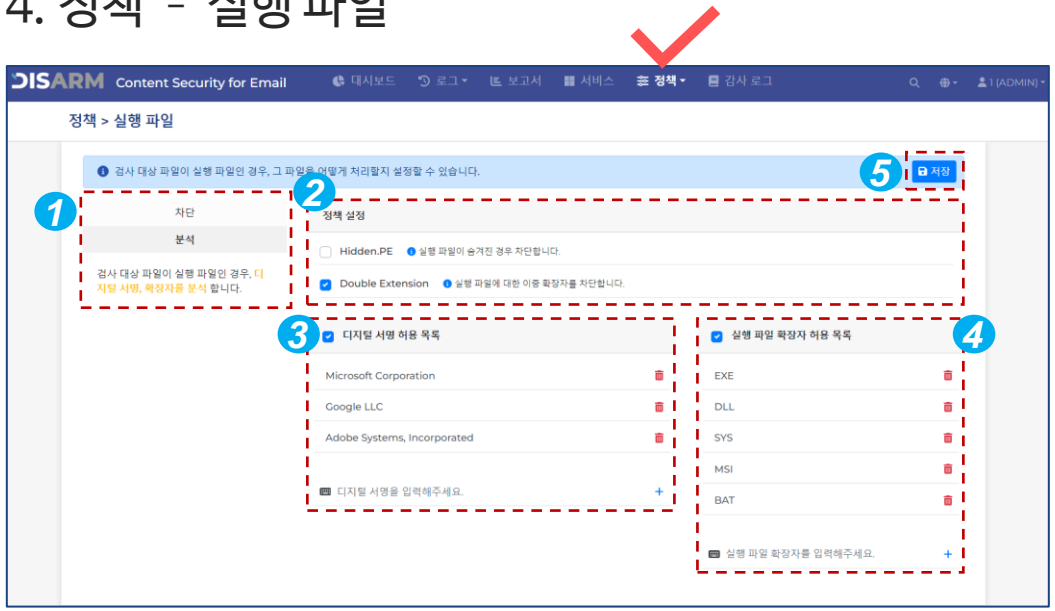


1. 체크박스를 활성화하면 0 바이트 사이즈의 파일 분석을 진행하지 않습니다.
2. 분석할 최대 파일 크기를 설정합니다.
   최대 파일 크기를 초과하는 파일을 차단하거나 분석을 진행하지 않도록 설정할 수 있습니다.
3. 차단할 MIME 타입을 추가하고, 해당 MIME 타입 파일이 첨부파일로 포함된 메일은 차단됩니다.
4. 차단할 파일 확장자를 추가하고, 해당 파일 확장자가 첨부파일로 포함된 메일은 차단됩니다.
5. ‘저장’ 버튼을 클릭하여 업데이트한 내용을 적용합니다.

기능 4
“정책”

EXE 또는 DLL과 같은 실행 파일을 분석하기 위해 DISARM은 사용자의 선호에 따라 다양한 설정을 제공합니다.

4. 정책 - 실행 파일



1. 실행 파일을 무조건 차단 혹은 분석 후 결과에 따라 처리할 지 선택합니다.
2. 숨겨진 실행 파일을 차단하려면 좌측 체크박스를 클릭합니다.
   실행 파일의 이중 확장자를 차단하려면 좌측 체크박스를 클릭합니다.
3. 특정 파일 디지털 서명을 분석하지 않고 통과시킬 수 있는 화이트리스트를 생성합니다. 이 목록에 등록되지 않은 다른 모든 서명을 차단합니다. 체크박스를 해제할 경우 모든 디지털 서명을 분석합니다.
4. 특정 실행 파일 확장자를 분석하지 않고 통과시킬 수 있는 화이트리스트를 생성합니다. 이 목록에 등록되지 않은 다른 모든 서명을 차단합니다. 체크박스를 해제할 경우 모든 실행 파일 확장자를 분석합니다.
5. ‘저장’ 버튼을 클릭하여 업데이트한 내용을 적용합니다.

기능 4
“정책”

암호화된 압축 파일이 포함된 이메일이 수신되면 DISARM은 미리 등록된 '비밀번호' 리스트를 사용하여 파일의 암호 해제를 시도합니다.
일치하는 비밀번호가 없는 경우, DISARM은 수신자에게 암호 요청 이메일을 보냅니다.

*암호 요청 이메일은 27페이지를 참조하세요.
*위 절차를 진행하려면 압축 파일 정책이 '차단'으로 설정되어 있어야 합니다.

4. 정책 - 암호화 파일

1. 암호로 보호된 문서 파일을 차단할지 분석 후 결과에 따라 처리할 지 선택합니다.
   *암호화 문서 파일을 분석하는 기능은 2024년 3분기에 제공될 예정입니다.
2. 암호화된 압축 파일(예: ZIP, EGG, 7Z 등) 처리 옵션 중 하나를 선택합니다.
3. 자주 사용하는 비밀번호를 등록하고 DISARM이 분석을 위해 자동으로 파일의 압축을 풀도록 합니다.
   *약 70개의 비밀번호가 기본으로 제공됩니다.
4. ‘저장’ 버튼을 클릭하여 업데이트한 내용을 적용합니다.

기능 4
“정책”

DISARM은 이메일 본문의 URL뿐만 아니라 첨부 파일에 포함된 URL도 철저히 검사하여 피싱 URL 이사용자에게 전달되기 전 사전에 차단합니다.

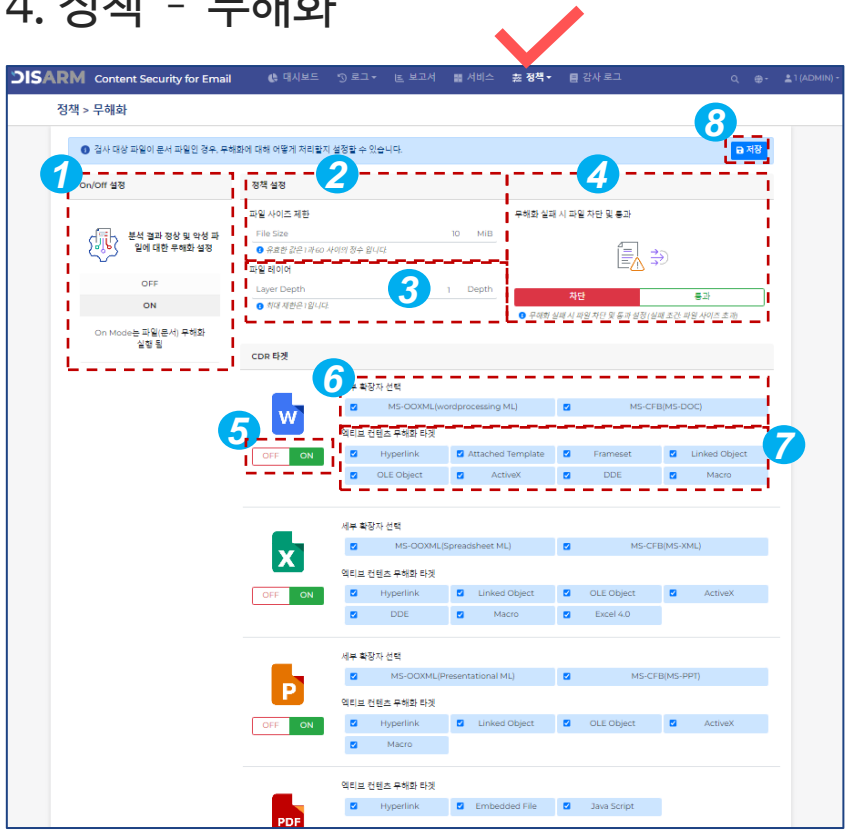
4. 정책 - URL 분석

1. 옵션 중 하나를 선택하여 URL 분석을 활성화할지 여부를 선택합니다.
2. URL 추출 대상 파일을 선택합니다.
3. 특정 URL을 리스트에 추가하여 분석 프로세스를 건너뛸 수 있습니다.
4. 차단할 URL을 추가합니다. 해당 리스트에 등록된 URL이 포함된 이메일은 차단됩니다.
5. ‘저장’ 버튼을 클릭하여 업데이트한 내용을 적용합니다.

기능 4
“정책”

DISARM 콘텐츠 무해화 (CDR) 을 사용하면 문서 파일에 포함된 잠재적 위협 없이 안심하고 문서 파일을 열 수 있습니다.

4. 정책 - 무해화

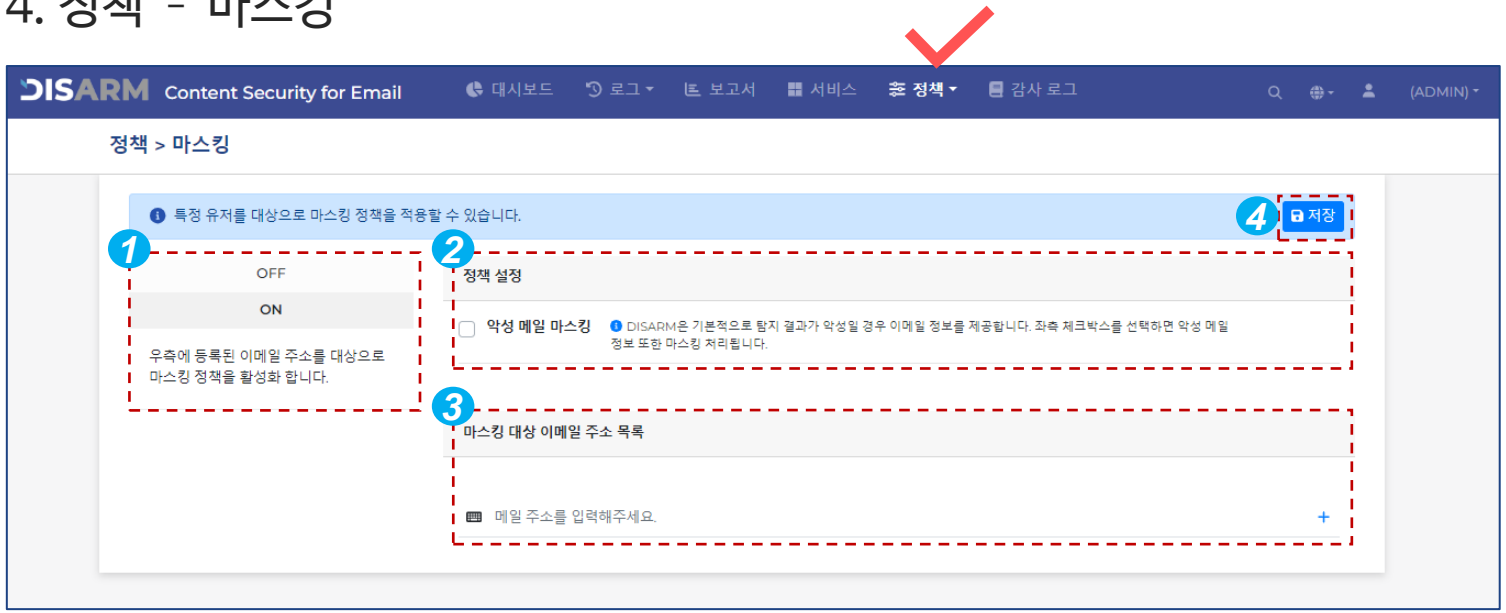


1. 옵션 중 하나를 선택하여 CDR 기능을 활성화하거나 비활성화합니다.
2. 무해화 할 최대 파일 크기를 설정합니다.
3. 문서 내 문서를 분석할 파일 레이어를 설정합니다.
4. 무해화 할 수 없는 파일에 대한 정책을 설정합니다.
   *무해화 실패는 주로 파일이 잘못된 형식의 파일일 때 발생합니다.
5. 파일 확장자 별 무해화 정책을 설정합니다.
   *OFF: 비활성화 / ON: 활성화
6. 파일 버전별로 CDR 정책을 설정합니다.
   *정확한 파일 확장자를 보려면 확장자 카테고리 위로 마우스를 가져가세요.
7. 제거할 액티브 콘텐츠를 선택합니다.
8. ‘저장’ 버튼을 클릭하여 업데이트한 내용을 적용합니다.

기능 4
“정책”

DISARM은 관리자에게 매우 상세한 수신 이메일 정보를 제공하지만, CEO, CFO 등과 같이 회사의 기밀 정보를 다루는 이메일 사용자의 정보는 관리자에게도 노출되지 않아야 합니다.
모든 사람의 받은 편지함을 안전하게 보호하되 VIP를 위한 기밀 정보는 숨기세요!

4. 정책 - 마스킹

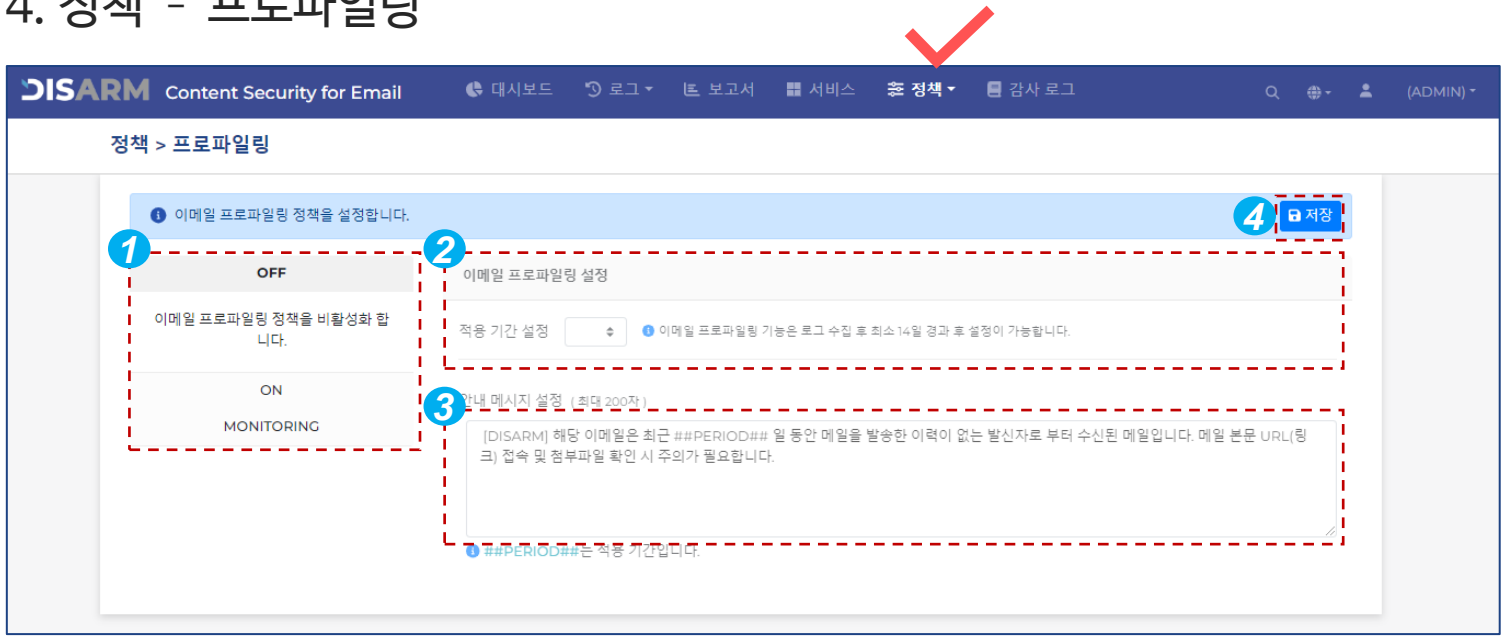


1. 옵션 중 하나를 선택하여 마스킹 기능을 활성화하거나 비활성화합니다.
2. 체크박스를 클릭하여 악성 메일에 대한 정보도 숨김 처리합니다.
3. 마스킹 정책을 적용할 이메일 주소를 등록합니다.
4. ‘저장’ 버튼을 클릭하여 업데이트한 내용을 적용합니다.

기능 4
“정책”

이전에 연락한 적이 없거나 오랫동안 연락하지 않은 발신자의 메일은 주의를 요합니다. 특히 이메일에 URL이나 첨부 파일이 포함되어 있다면 더욱 그렇습니다.
DISARM은 수신자에게 특정기간 수신 기록이 없는 이메일에 대한 알림을 주는 프로파일링 배너 기능을 제공합니다.

4. 정책 - 프로파일링



1. 옵션 중 하나를 선택하여 마스킹 기능을 활성화하거나 비활성화합니다.
   모니터링 모드는 프로파일링 대상 메일에 대한 로그만 서버에 남기고, 수신자에게 배너는 띄우지 않습니다.

2. 프로파일링 정책을 적용할 기간을 선택합니다.
   *DISARM을 처음 사용하는 경우 프로파일링을 활성화하더라도 왼쪽에서 선택한 기간이 지날 때까지 배너가 표시되지 않습니다.

3. 수신자 이메일의 상단 배너에 표시할 문장을 작성합니다.

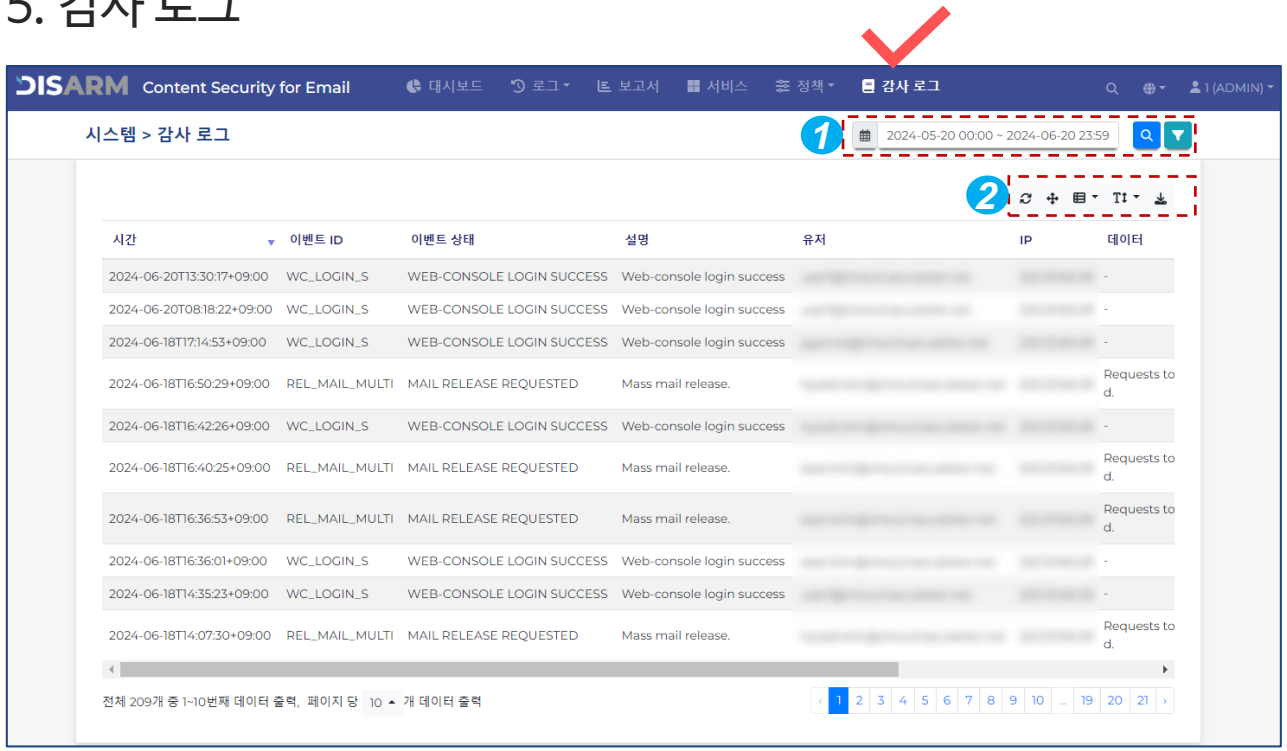
4. ‘저장’ 버튼을 클릭하여 업데이트한 내용을 적용합니다.

기능 5
“감사 로그”

지정된 기간 동안 관리자 페이지에서 수행된 작업의 로그를 표시합니다.

관리자 페이지에서 누가 언제 무엇을 수행했는지 자세히 확인 할 수 있습니다.

5. 감사 로그



1. 로그를 확인할 기간 또는 필터를 설정합니다.
   *필터: 이벤트 ID, 이벤트 상태, 설명, 유저, IP

2. '새로 고침', '전체 화면', '컬럼 필터링', '텍스트 크기 변경', '목록을 CSV로 내보내기' 버튼입니다.

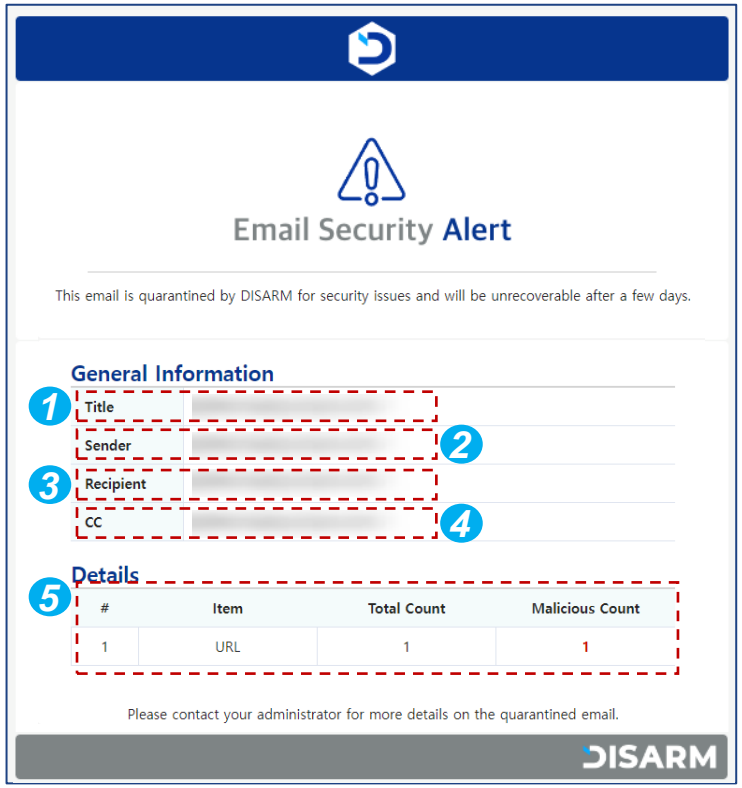
2. 알림 메일

알림 메일 1
“악성 메일”

악성 이메일이 수신자의 받은 편지함에 도달하기 전에 선제적으로 차단되면 사용자는 알림 메일을 받게 됩니다.

*한국어 버전은 2024년 3분기에 제공될 예정입니다.

1. 수신자 악성 탐지 알림 메일

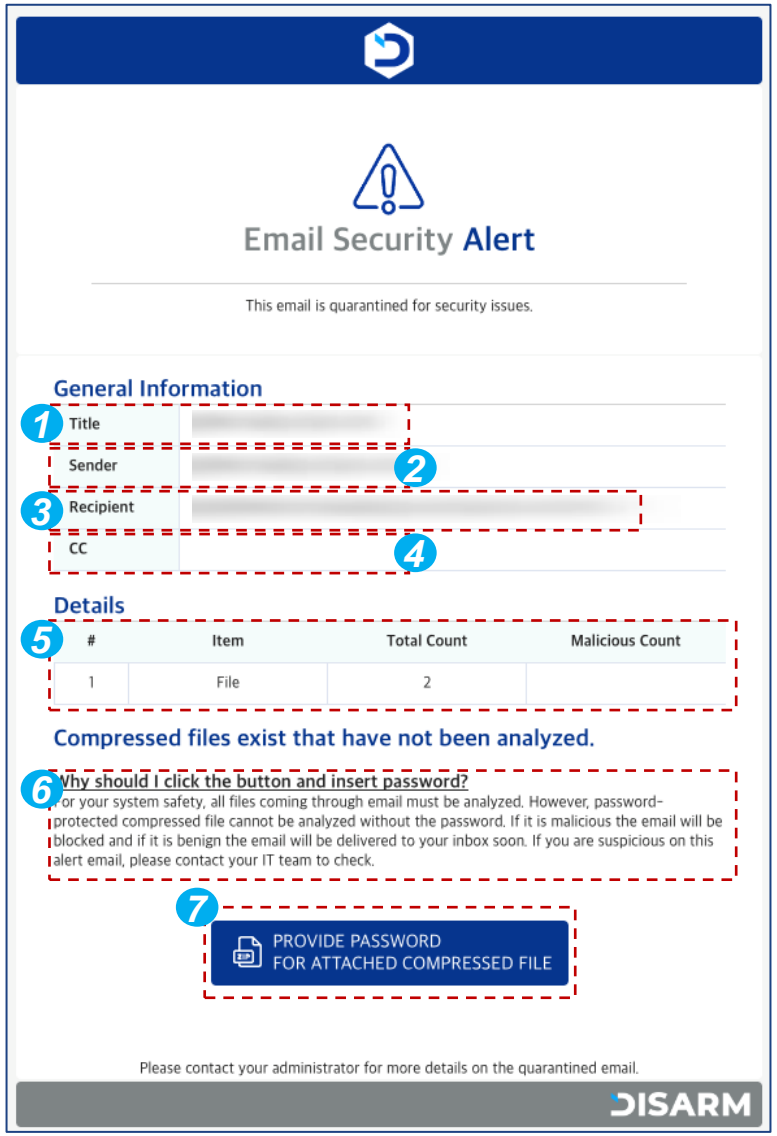


1. 차단된 악성 메일의 제목
2. 차단된 악성 메일의 발신자
3. 차단된 악성 메일의 수신자
4. 차단된 악성 메일의 참조 수신자
5. 차단된 메일에 포함된 악성 콘텐츠 내용

알림 메일 2
“암호 요청 메일”

암호 요청 메일을 수신하면 DISARM이 메일을 분석 할 수 있도록 암호화 압축 파일의 비밀번호를 입력합니다.
비밀번호가 입력되면 DISARM은 압축 파일의 악성 여부를 판단하기 위한 분석 프로세스를 시작합니다.

2-1. 암호 요청 메일

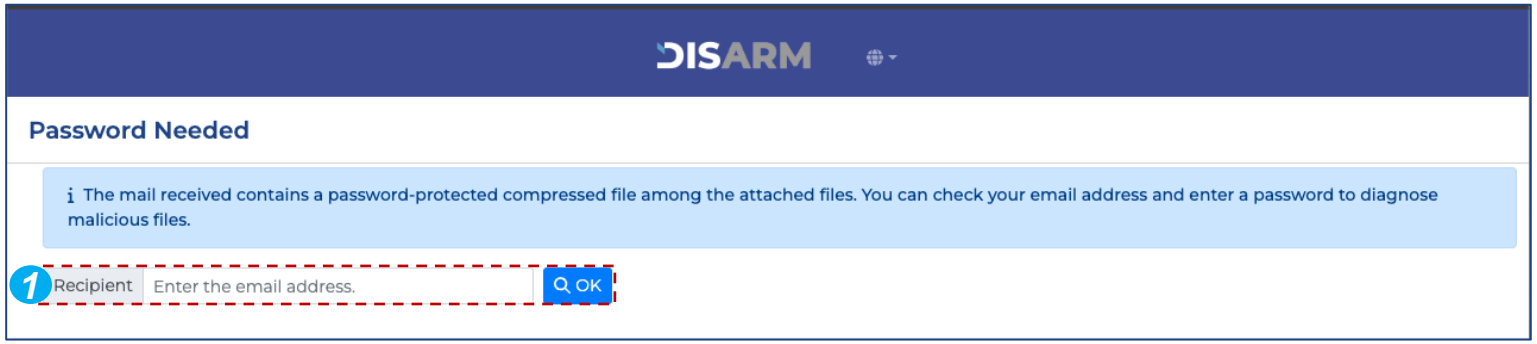


1. 분석할 메일의 제목
2. 분석할 메일의 발신자
3. 분석할 메일의 수신자
4. 분석할 메일의 참조 수신자
5. 분석할 메일에 포함된 콘텐츠 내용
6. 비밀번호 제공의 필요성 및 절차에 대한 설명
7. 버튼을 클릭 후 열린 새 페이지에 비밀번호를 입력

알림 메일 2
“암호 요청 메일”

암호 요청 메일을 수신하면 DISARM이 메일을 분석 할 수 있도록 암호화 압축 파일의 비밀번호를 입력합니다.
비밀번호가 입력되면 DISARM은 압축 파일의 악성 여부를 판단하기 위한 분석 프로세스를 시작합니다.

2-2. 암호 요청 메일

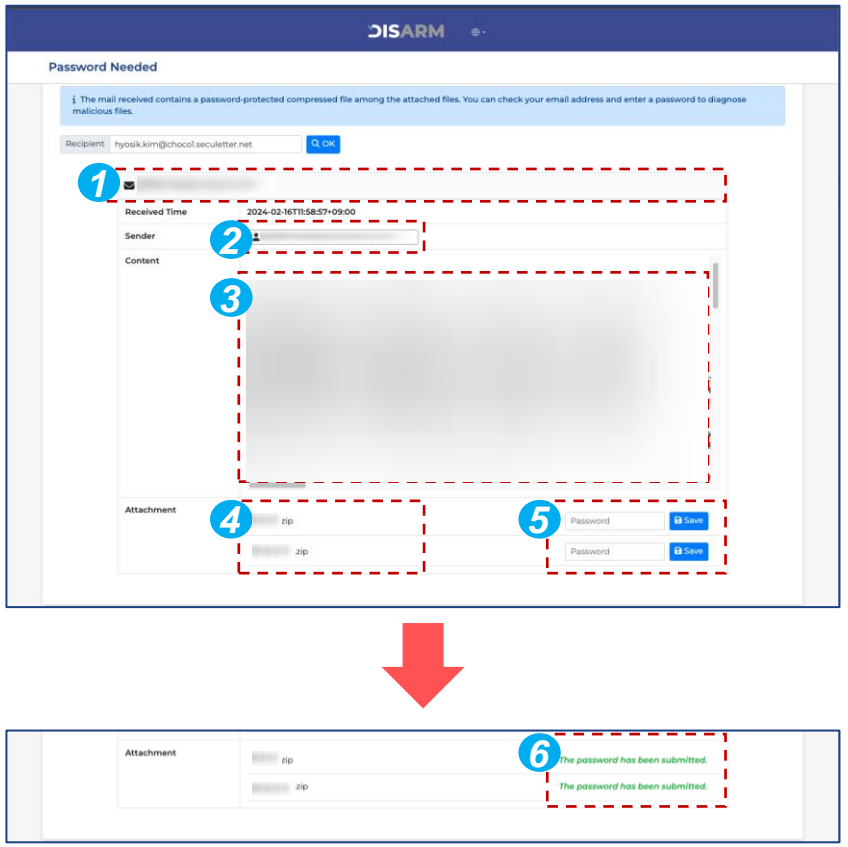


1 수신자의 이메일 주소를 기입한 후 ‘OK ' 를 클릭합니다.

알림 메일 2
“암호 요청 메일”

암호 요청 메일을 수신하면 DISARM이 메일을 분석 할 수 있도록 암호화 압축 파일의 비밀번호를 입력합니다.
비밀번호가 입력되면 DISARM은 압축 파일의 악성 여부를 판단하기 위한 분석 프로세스를 시작합니다.

2-3. 암호 요청 메일



1. 분석할 메일의 제목
2. 분석할 메일의 발신자
3. 분석할 메일의 본문 내용
4. 분석할 메일에 첨부된 암호화 압축 파일 제목
5. 비밀번호 입력 칸
6. 비밀번호를 입력하면 섹션 5가 변경되어 그림과 같이 메시지가 표시됩니다.

3. FAQ & Contact Info

FAQ

Q. DISARM 서비스를 설치하면 Microsoft 365에 제로 트러스트 CDR 이 어떻게 적용되나요?

A: 구독자가 수신한 이메일은 DISARM 서비스가 먼저 악성 여부 분석 및 첨부파일 무해화 과정 수행 후 안전한 메일로 변경하여 Microsoft 365 '받은편지함'으로 전달합니다.
구독자는 메일 본문 상단 알림 배너를 통해 콘텐츠 무해화가 완료되었음을 알 수 있으며, 악성 이메일의 수신될 경우 DISARM 에서 격리시킨 후 탐지 결과를 사용자에게 알림 메일로 안내합니다.

Q. 조직에 이미 Microsoft 365 보안이 있는 경우 어떻게 해야 하나요?

A: Microsoft 365에서 제공하는 보안 솔루션이 있더라도 조직의 보안 강화를 위해 DISARM 도입을 추천합니다.
Microsoft 365 의 보안 기능은 시그니처 기반 보안(예: Anti-Virus, SPAM 등)을 제공하기 때문에 보안 기능을 우회하는 '알려지지 않은 신·변종 악성코드/랜섬웨어(Unknown Threat)'가 유입될 경우 탐지·차단이 어렵습니다.
이와 달리 DISARM은 알려진 보안 위협 뿐만 아니라 알려지지 않은 보안 위협까지도 독자적인 리버스 엔지니어링 기술을 통해 모두 탐지해 선제 차단합니다. 또한 콘텐츠 무해화 기술을 통해 모든 비즈니스 콘텐츠(MS Office, HWP, PDF, JPG, PNG 등)를 사이버 공격이 불가능하도록 무해화 시키기 때문에 더욱 안전한 Microsoft 365를 사용할 수 있습니다.

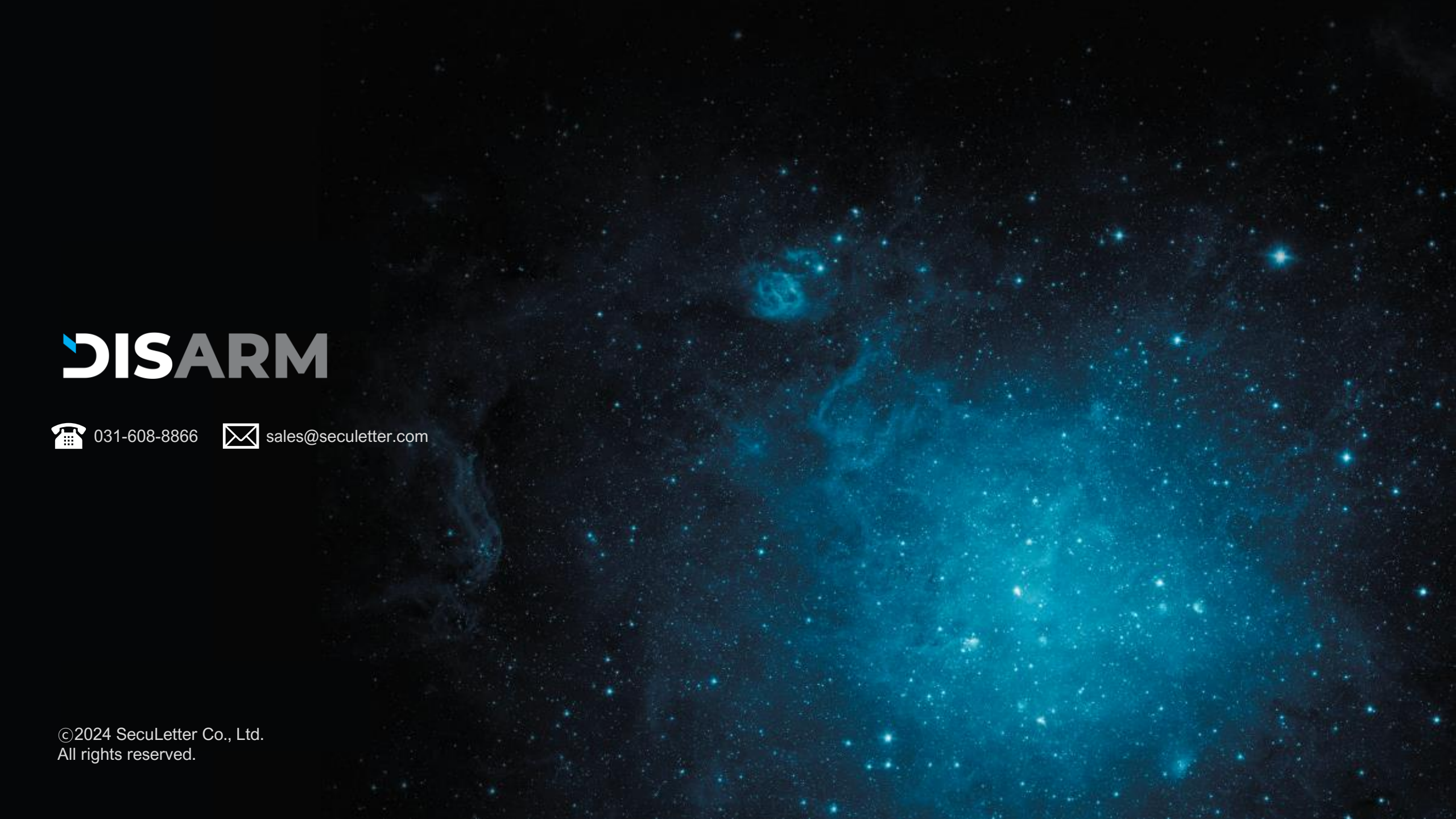
FAQ

Q. Microsoft 365에서 제공하는 추가적인 보안 강화 서비스 구독 대신 DISARM을 선택해야 하는 이유는 무엇인가요?

A: Microsoft 365 에서 제공하는 별도의 보안 서비스 'Office 365용 Microsoft Defender Plan 1 / Plan 2' 을 추가로 구독하면, 더욱 향상된 피싱 탐지 및 다양한 보안 기능이 제공됩니다.
하지만 Microsoft에서 제공하는 보안 기능은 DETECT (탐지) 방식 위주로 구성되어 있습니다. 이는 최신 변종 해킹 공격을 탐지하지 못할 수 있습니다.
반면에 시큐레터는 이메일 보안 전문 기업으로서 제로 트러스트 철학을 반영한 보안을 제공하기 때문에 DISARM은 해킹 및 피싱 공격 원천 방어에 특화되어 있습니다.

Q. Microsoft 365에서는 탐지하지 못하고 DISARM 에서만 탐지한 사례가 있나요?

A: 계정 탈취 목적을 가진 최신 악성 피싱 이메일 탐지 사례가 있습니다. Microsoft 365는 해당 메일을 정상으로 판별하여 메일 수신함으로 보냈지만 DISARM은 악성으로 탐지하여 메일 수신함에 메일이 수신되기 전에 차단했습니다. 그림보기



☎ 031-608-8866 ✉ sales@seculetter.com