다크웹 모니터링 서비스

제로다크웹 3.0

제로다크웹으로 다크웹 정보 유출 정보에 긴밀하게 대응하세요.



www.zerodarkweb.kr

JIRANSOFT

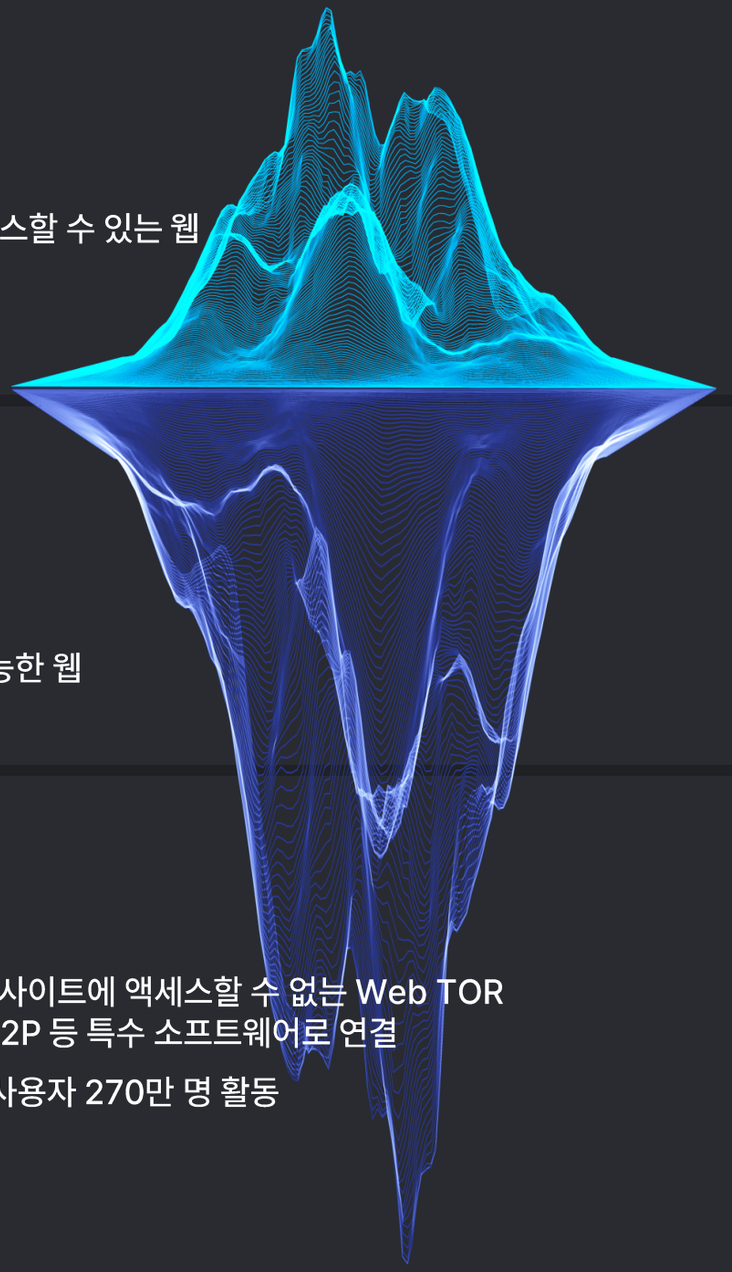
Darkweb 의 위협

다크웹에는 기업 및 개인정보, 악성코드와
랜섬웨어, 총, 금지 약물 등이 거래되고 있습니다.

주요 거래 품목과 가격:

- 시스템 접근용 익스플로잇: 평균 5,345달러
- 멀웨어 로더: 평균 3,566달러
- 구독 기반 스틸러: 평균 1,024달러
- 미국 신용카드: 10-40달러
- 독일 신용카드: 10-50달러

특히 AI 기반 공격이 442% 증가하며, 악성코드나 랜섬웨어 등 악의를 가진 프로그램이나, 다양한 사기성 도구 및 유출 정보를 활용하여 기업에 대한 공격으로 이어지고 있습니다.



SURFACE WEB

4%

일반적으로 웹 에서 액세스할 수 있는 웹

DEEP WEB

90%

ID/PW 인증 후 사용 가능한 웹

DARK WEB

6%

일반 웹 브라우저에서는 사이트에 액세스할 수 없는 Web TOR (The Onion Router), I2P 등 특수 소프트웨어로 연결

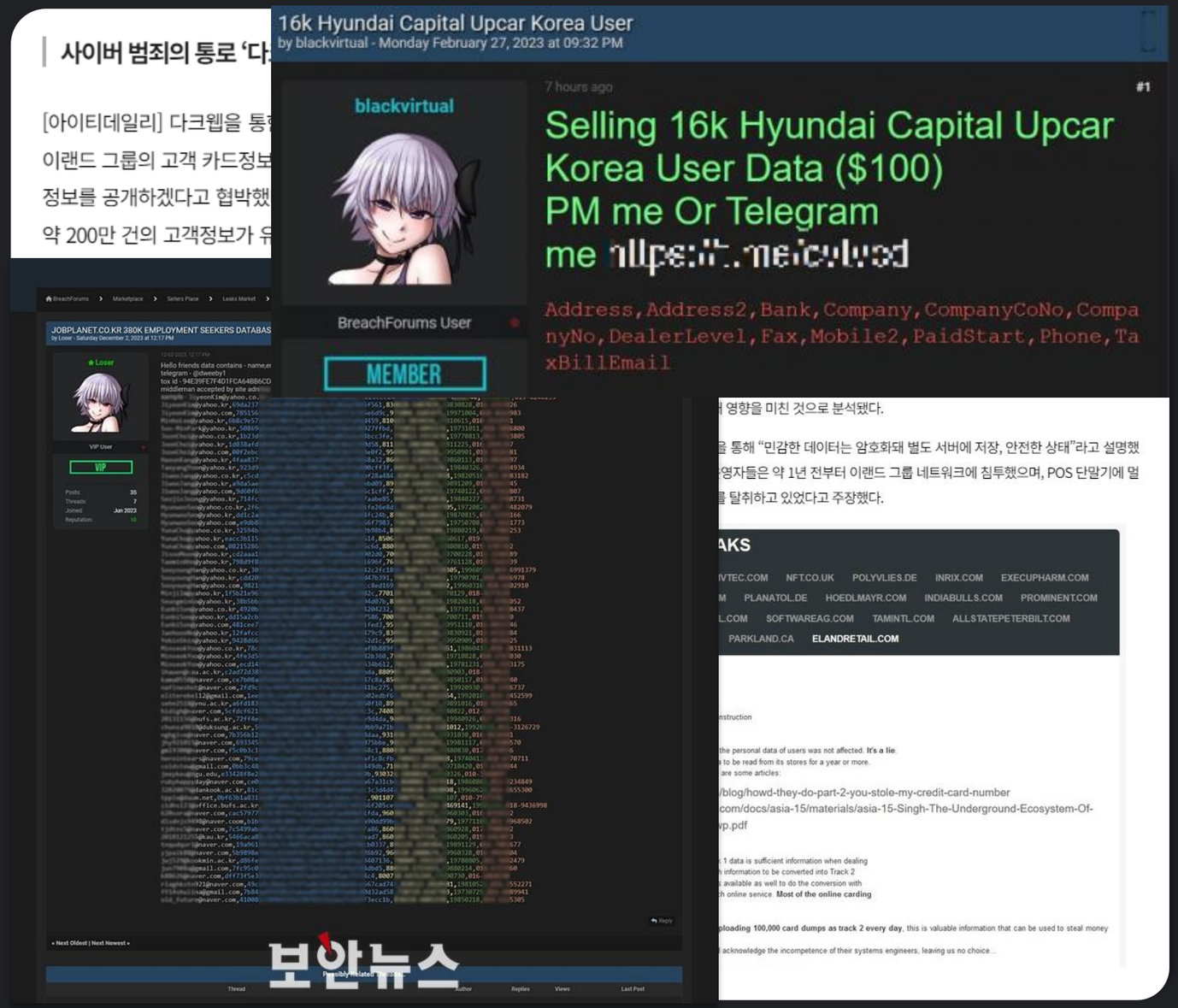
- 2025년 기준 일일 사용자 270만 명 활동

JIRANSOFT

Darkweb 기업 유출 사례

국내 주요 유출 사건

- 통신회사 초대형 데이터 유출
- 메신저 서비스 데이터 유출로 151억 원 과징금 (국내 최대 기록)
- 페이먼트 서비스 해외 결제사와 무단 고객 데이터 공유
- LockBit 랜섬웨어로 제조업체 전체 시스템 암호화
- Underground 그룹이 부품업체 745GB 데이터 탈취
- 취업정보 사이트 개인정보 데이터, 다크웹에 유출
- 금융서비스 이용자들 정보 유출
- 계열사를 향한 지속적인 해커 공격
- 랜섬웨어 그룹의 모 그룹 공격 사례



사이버 공격 트렌드 변화

크리덴셜 스터핑 (Credential Stuffing) 공격의 폭발적 증가

최신 공격 현황:

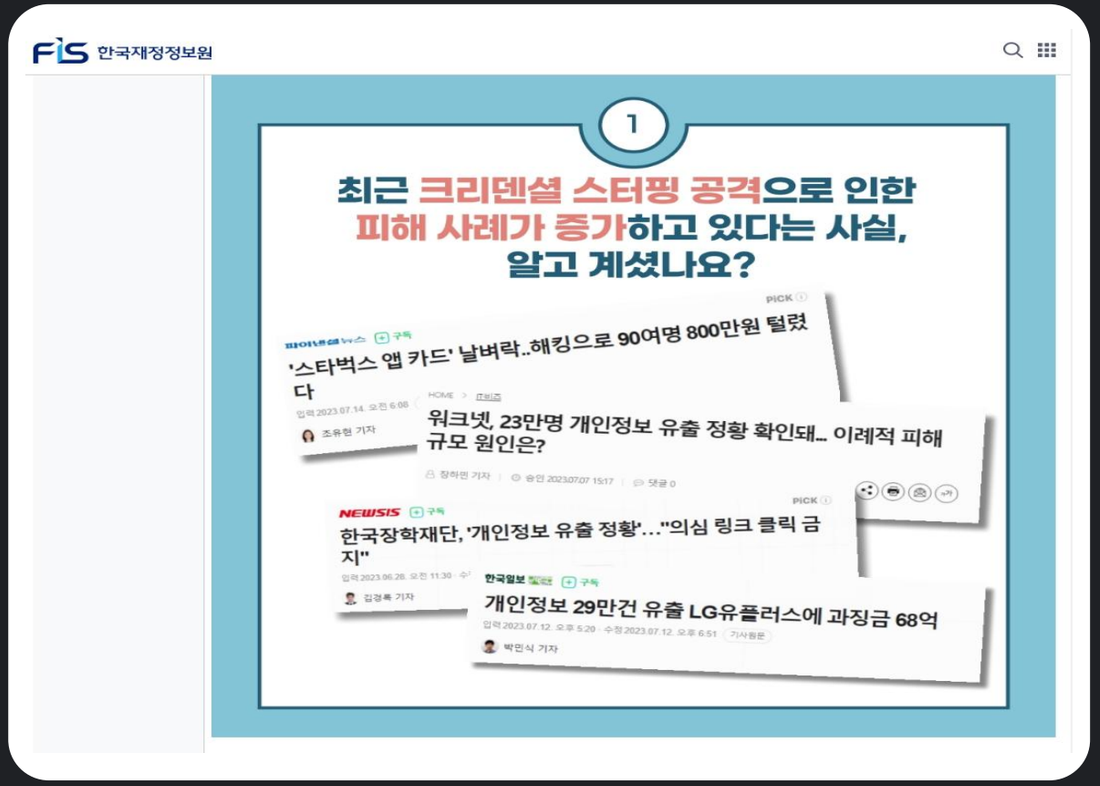
- 전 세계 월 260억 건의 크리덴셜 스터핑 시도
- 18개월간 48% 증가한 공격 빈도
- 인증 요청의 19.4%가 크리덴셜 스터핑 공격

공격 성공률과 피해:

- 성공률: 0.1% (낮지만 규모로 인해 효과적)
- 사용자의 85%가 여러 서비스에서 동일 비밀번호 재사용
- 평균 침입-확산 시간 48분으로 단축 (최단 51초 기록)

인포스틸러 멀웨어 현황:

- RedLine Stealer: 43% 점유율, 4억7천만 개 비밀번호 탈취
- 전체 2,300만 대 호스트에서 21억 개 크리덴셜 탈취

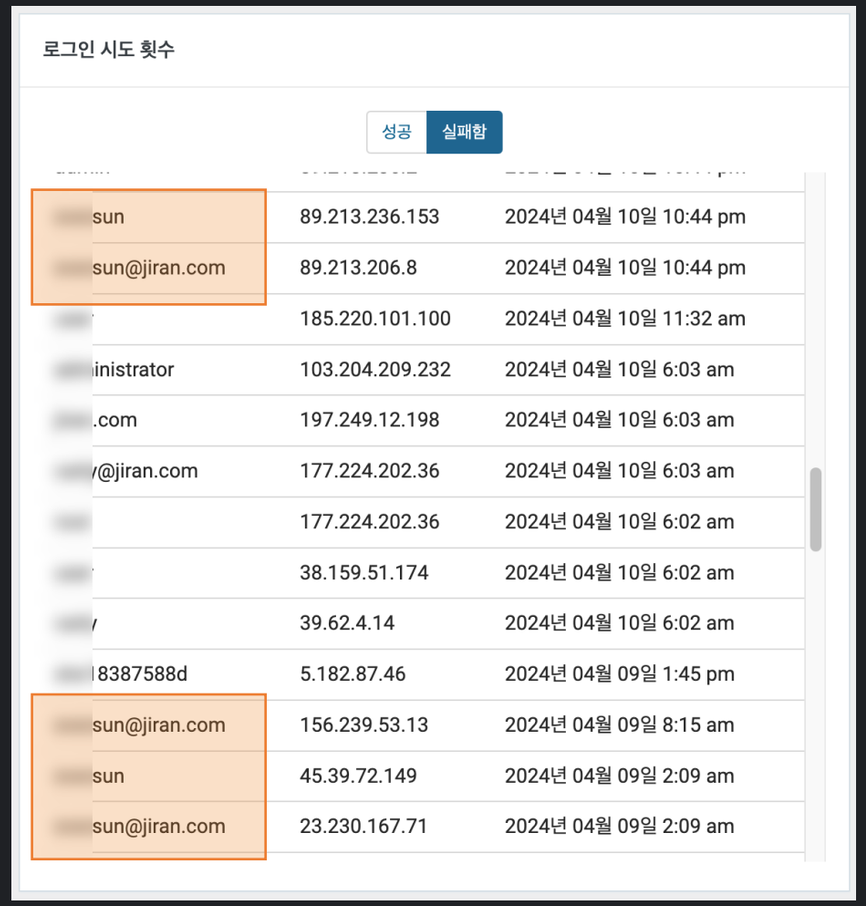


23년 8월 한국재정정보원

JIRANSOFT

크리덴셜 스터핑 예시 – 자사 웹사이트 관리자 페이지

보이지 않는 곳에서 크리덴셜 스터핑은 실제로 일어나고 있습니다.



자사 홈페이지 관리자 페이지 로그인 시도 기록



제로다크웹 리포트에 검출된 유출 계정

JIRANSOFT

국내 100대 기업의 DarkWeb 정보 유출 상황

(제로다크웹이 국내 기업의 다크웹 정보 유출 현황을 조사)

1. 조사 대상 100개사 중, 99개사에서 다크웹에 정보 유출됨을 확인 (99%)
2. 사내문서 유출 케이스 : 87개사 (87%)
3. 해킹 우려 PC 건수 : 81개사, 15,028건
4. 메일 어카운트 정보 유출 건수 : 1,052,537건



참고 사항
- 대상 : 국내 주요 100대 기업 (시가총액 기준)
- 어카운트 정보는ID (e-mail) 와 패스워드가 페어로 유출된 케이스를 1건 유출로 판단
- 문서 유출은 건수까지 확인하지 않았으며, 유출 유무만 조사
- 해킹의 우려가 있는 PC의 수량
- 유출된 어카운트 정보는 다크웹에 유출된 원본 그대로이고, 데이터의 진위 및 유효성 (로그인 가능 여부) 는 검증하지 않음

JIRANSOFT

제로다크웹 3.0

복잡한 보안 상황을 간단하게 파악하고, 어디서부터 손써야 할지 명확한 우선순위를 제시받아
효율적으로 보안 업무를 처리할 수 있습니다.

JIRANSOFT

제로다크웹3.0의 주요 기능

웹 도메인(URL) 유출 탐지 (신규 기능)

우리 회사 도메인과 관련된 모든 위험을 24시간 자동으로 감시하여 큰 사고가 되기 전에 미리 알려줍니다.

요약 보고

바쁜 경영진도 몇 초 만에 우리 회사 보안 상황의 심각성을 파악하고 즉시 의사결정을 내릴 수 있습니다.

유출 상세

각각의 유출 사건마다 무엇을 어떻게 해야 할지 구체적인 해결 방법을 제시받아 헤맬 필요 없이 바로 대응할 수 있습니다.

유출 대응 이력

과거 대응 사례를 통해 새로운 사건 발생 시 검증된 해결 방법을 빠르게 적용하여 처리 시간을 단축할 수 있습니다.

글로벌 사이버 공격 동향

전 세계 사이버 공격 트렌드를 미리 파악하여 우리나라에 상륙하기 전에 대비책을 마련할 수 있는 경쟁 우위를 확보합니다.

웹 도메인(URL) 유출 탐지 (신규 기능)

회사 관련 모든 웹사이트와 서비스의 보안 상태를 하나의 화면에서 통합 관리하여 완벽한 보안 관리가 가능합니다.

각 서비스마다 위험도를 색깔로 구분해 우선순위를 즉시 판단할 수 있고, 단계별 가이드로 보안 전문가가 아니어도 체계적인 보안 강화 작업을 수행할 수 있습니다.



주요 모듈



도메인 탐색 필터

어떤 도메인이 가장 위험한지 한눈에 파악할 수 있어 대응 우선순위를 명확하게 정할 수 있습니다.

위험 수준별로 색상 구분되어 표시되므로 보안 담당자가 어떤 도메인부터 먼저 처리해야 할지 즉시 판단 가능합니다. 도메인별 메모 기능으로 과거 대응 이력과 특이사항을 기록해두면, 팀원 간 정보 공유와 업무 인수인계가 훨씬 수월해집니다.



유출 피해 증감 추이

보안 투자가 실제로 효과를 보고 있는지, 유출 상황이 개선되고 있는지를 그래프로 명확하게 확인할 수 있습니다.

특정 시점에 급격한 유출 증가가 있었다면 그 원인을 찾아 재발 방지 대책을 세울 수 있고, 지속적인 감소 추세라면 현재 보안 정책이 효과적임을 입증할 수 있어 경영진 보고 시 객관적인 근거자료로 활용 가능합니다.



유출 상세 정보

실제로 어떤 계정과 비밀번호가 유출되었는지 구체적으로 확인할 수 있어 즉시 비밀번호 변경이나 계정 정지 등의 대응 조치를 취할 수 있습니다.

유출된 정보가 어느 도메인에서 나온 것인지 정확히 알 수 있어 해당 시스템의 보안 취약점을 찾아 보완할 수 있고, 피해 범위를 정확히 파악하여 고객이나 임직원에게 적절한 안내와 대응책을 제공할 수 있습니다.



유출 상세 정보 필터링

수천 건의 유출 정보 중에서 내가 지금 당장 확인해야 할 것만 골라서 볼 수 있어 업무 효율성이 크게 향상됩니다.

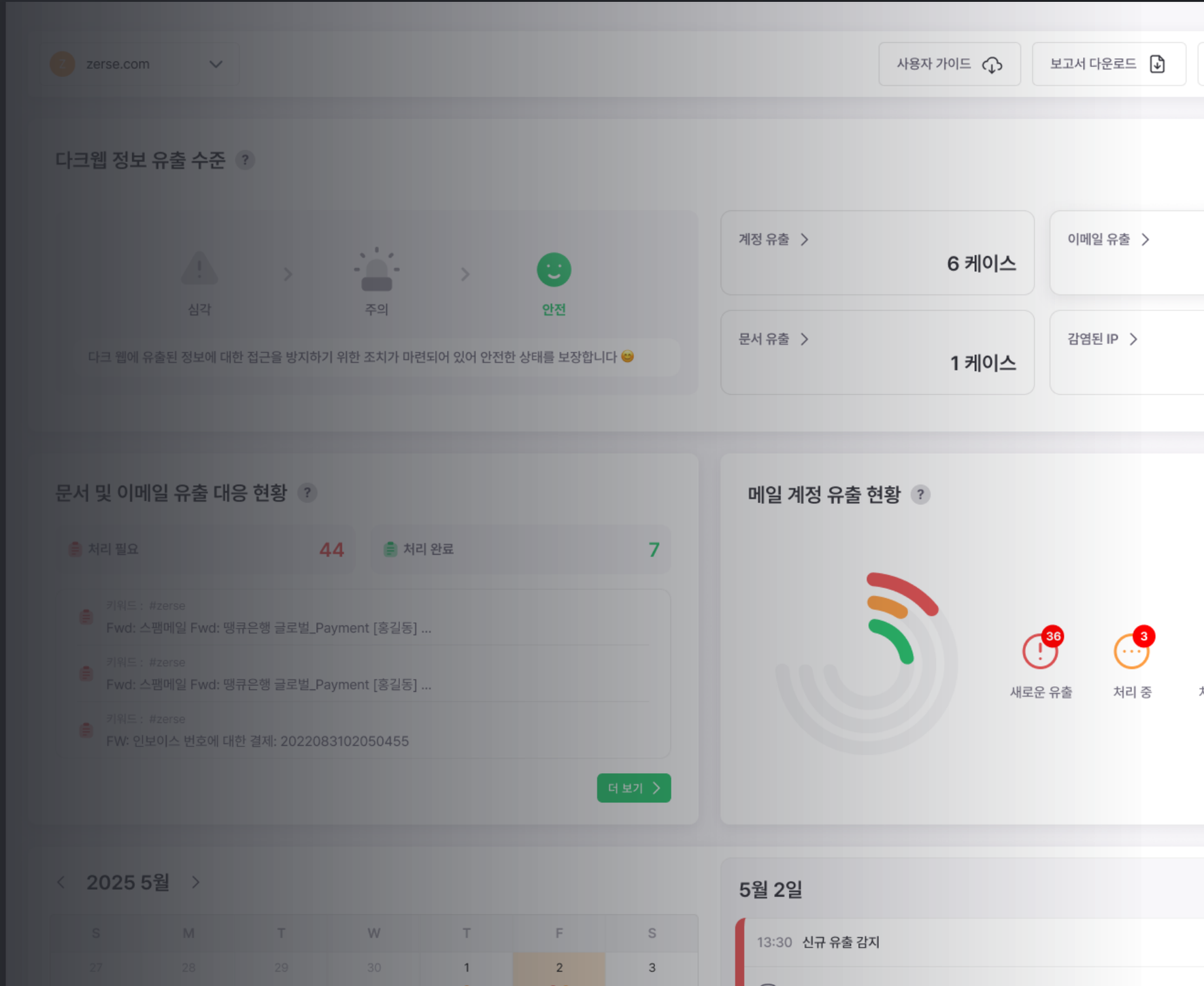
예를 들어 최근 1주일간 심각 등급의 새로운 유출만 보고 싶다면 몇 번의 클릭으로 해당 정보만 필터링할 수 있어, 중요한 것을 놓치지 않고 신속하게 대응할 수 있습니다.

JIRANSOFT

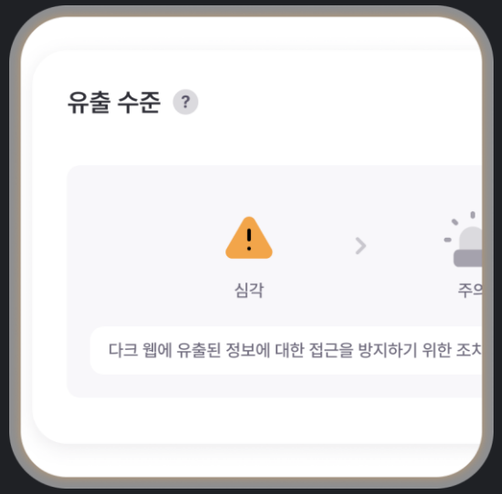
요약 보고

5분만 투자하면 회사 보안 상황 전체를 파악하고 필요한 조치를 즉시 결정할 수 있습니다.

신호등처럼 '심각', '주의', '안전'으로 표시되어 보안 지식 없이도 상황 파악이 쉽고, 달력과 지도로 문제 발생 패턴을 직관적으로 확인해 경영진 보고 시 의사결정 속도를 향상시킬 수 있습니다.



주요 모듈



유출 수준

복잡한 보안 전문 용어 없이도 우리 회사의 현재 상황이 얼마나 심각한지 신호등처럼 간단하게 알 수 있습니다.

심각이면 즉시 비상 대응 체계를 가동하고, 주의면 예방 조치를 강화하며, 안전이면 현재 보안 정책을 유지하면 되어 비전문가도 쉽게 상황을 판단하고 대응할 수 있습니다.



메일 계정 유출 현황

전체 유출 건수 중에서 아직 처리하지 못한 것이 얼마나 되는지, 현재 처리 중인 것이 몇 건인지 한눈에 파악할 수 있어 업무량 관리와 인력 배치 계획을 세우기 쉽습니다.

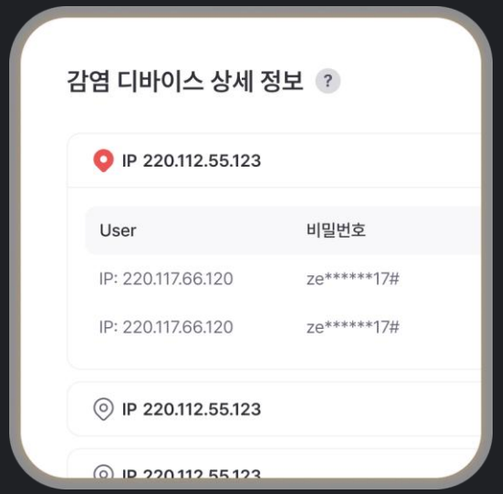
처리 완료 비율을 통해 팀의 대응 성과를 객관적으로 측정할 수 있고, 경영진에게 보안팀의 업무 효율성을 입증할 수 있는 지표로 활용 가능합니다.



파일 탐지 유출 탐지 현황

메일 첨부 파일의 유출 여부 및 탐지 상황에 대한 정보를 제공하여, 첨부 파일을 통한 데이터 유출 위험을 관리할 수 있도록 지원합니다.

특정 키워드에 대한 정보 유출 상태 및 안전 여부를 모니터링하고 관리함으로써, 중요한 정보의 보안 상태를 체계적으로 추적합니다.



멀웨어 감염에 대한 상세 보고서

어느 지역에서 멀웨어 감염이 가장 많이 발생하는지 지도로 시각화되어 공격 패턴을 쉽게 파악할 수 있습니다.

감염된 컴퓨터에서 어떤 계정 정보가 탈취되었는지 구체적으로 확인할 수 있어 해당 계정의 비밀번호를 즉시 변경하거나 접근을 차단할 수 있고, 감염 경로를 분석하여 동일한 방식의 재감염을 방지하는 보안 대책을 수립할 수 있습니다.

JIRANSOFT

주요 모듈



유출 유형별 건수

바쁜 업무 중에도 몇 번의 클릭만으로 원하는 정보에 바로 접근할 수 있어 시간을 크게 절약할 수 있습니다.

예를 들어 '문서 유출 100건'이라는 버튼을 클릭하면 문서 유출 관련 정보만 필터링되어 표시되므로, 복잡한 메뉴를 찾아 헤맬 필요 없이 즉시 필요한 작업을 시작할 수 있어 업무 효율성이 크게 향상됩니다.



유출 현황 - 타임라인

특정 날짜에 무슨 일이 있었는지 쉽게 되돌아볼 수 있어 사고 원인 분석이나 대응 효과 검증에 유용합니다.

예를 들어 지난주 화요일에 갑자기 유출이 증가했다면 그날 있었던 시스템 업데이트나 외부 공격과의 연관성을 찾을 수 있고, 성공적으로 대응한 날의 방법을 다른 상황에도 적용하여 대응 품질을 향상시킬 수 있습니다.



유출 현황 – 캘린더

월간 보안 상황을 달력 형태로 한눈에 파악할 수 있어 주기적인 패턴이나 특정 요일의 취약점을 쉽게 발견할 수 있습니다.

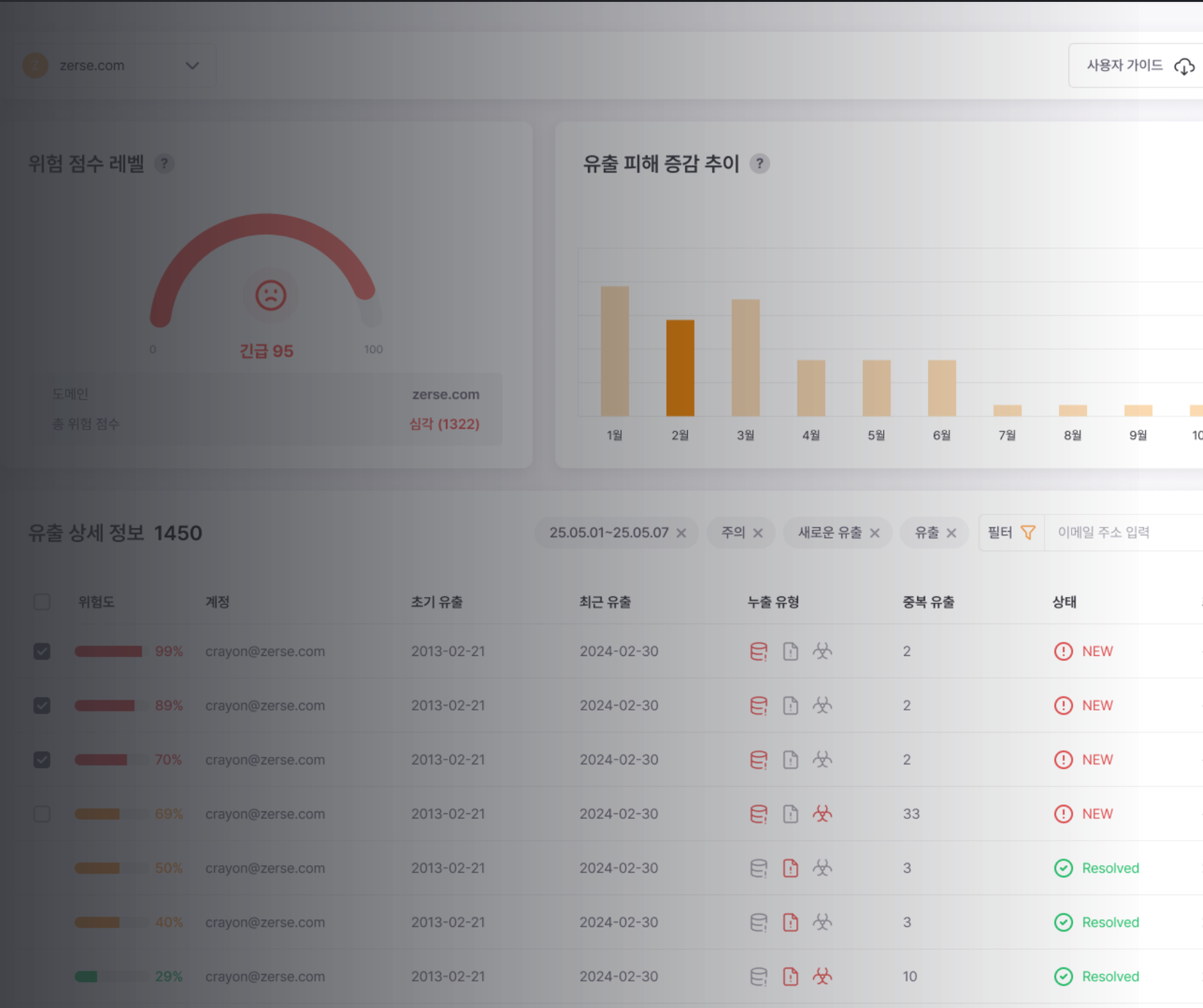
예를 들어 매주 금요일마다 유출이 증가한다면 주말 전 보안 점검을 강화하거나, 월말에 집중적으로 공격이 발생한다면 해당 시기에 모니터링을 강화하는 등 데이터 기반의 예방 전략을 수립할 수 있습니다.

JIRANSOFT

유출 상세

유출 정보의 심각도와 리스크 스코어(위험 점수)를 제공하며, 대응 추이와 피해 증감을 시각화합니다.

위험도를 점수화해 우선순위를 쉽게 정하고, 월별·연도별 유출 증감 추이로 보안 투자 효과를 객관적으로 확인할 수 있습니다.



주요 모듈



유출 위험 수준

마치 자동차 속도계처럼 우리 회사의 현재 위험도를 직관적으로 확인할 수 있어 비전문가도 상황의 심각성을 쉽게 이해할 수 있습니다.

숫자가 높을수록 위험하다는 것을 누구나 알 수 있고, 경영진에게 보고할 때도 복잡한 설명 없이 한 장의 그래프만으로 현재 상황과 투자 필요성을 명확하게 전달할 수 있습니다.



유출 상세 정보

어떤 계정이 언제, 어떤 방식으로 유출되었는지 엑셀처럼 정리된 표로 한눈에 확인할 수 있어 대응 계획을 세우기 쉽습니다.

색깔로 위험도가 구분되어 표시되므로 빨간색인 것부터 우선 처리하면 되고, 아직 처리하지 않은 것과 이미 해결한 것이 명확히 구분되어 업무 진행 상황을 쉽게 파악할 수 있습니다.



유출 피해 증감 추이

작년 대비 올해 상황이 나아지고 있는지, 특정 월에 왜 유출이 급증했는지를 쉽게 파악할 수 있어 장기적인 보안 전략 수립에 도움이 됩니다.

보안 시스템 도입 전후의 효과를 객관적으로 비교할 수 있고, 계절적 패턴이나 특별한 이벤트와의 연관성을 찾아 예방 조치를 강화할 시기를 정확히 판단할 수 있습니다.



유출 상세 정보 필터링

내가 담당하는 업무나 관심 있는 정보만 골라서 볼 수 있어 업무 집중도가 높아집니다.

예를 들어 '이번 주 심각 등급 미처리 건'만 필터링하면 오늘 해야 할 일만 명확하게 보이고, 필터 상태가 화면에 표시되어 현재 어떤 조건으로 보고 있는지 헷갈리지 않아 실수를 줄일 수 있습니다.

JIRANSOFT

주요 모듈



이메일 및 파일 유출 탐지 보고서

한 건의 유출 사고에 대한 모든 정보를 하나의 페이지에서 완전히 파악할 수 있어 사건 전체를 체계적으로 이해하고 대응할 수 있습니다.

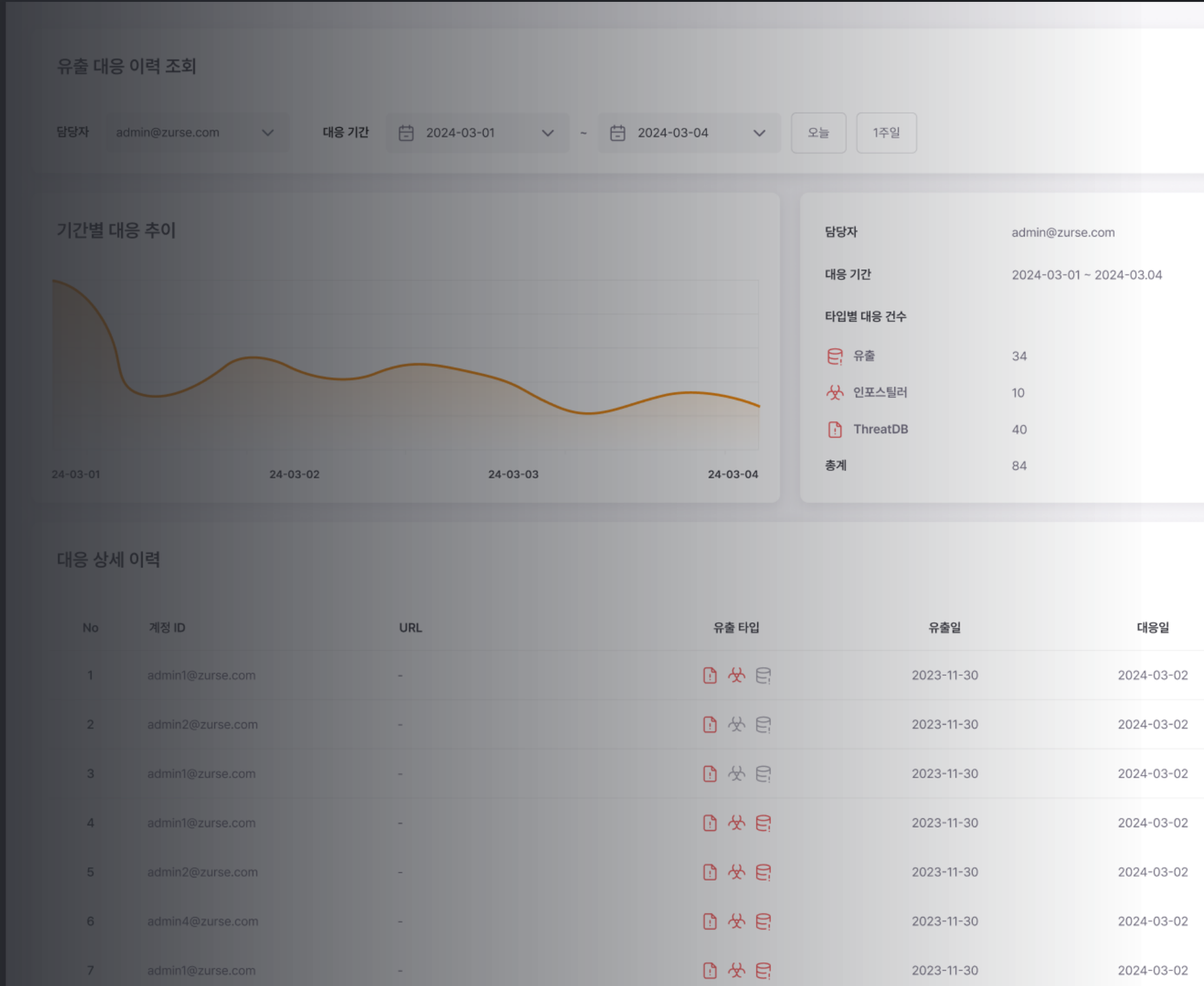
이 계정이 과거에도 유출된 적이 있는지, 몇 개의 비밀번호가 노출되었는지, 언제 해결했는데 또 유출되었는지 등을 시간 순서대로 추적할 수 있어 근본적인 보안 취약점을 찾아 해결할 수 있습니다.

JIRANSOFT

유출 대응 이력

과거 대응 사례 축적으로 새로운 문제 발생 시 검증된 해결 방법을 즉시 활용해 대응 시간 단축과 실수 최소화가 가능합니다.

성공·실패 사례 학습으로 신입 직원의 빠른 업무 적응이 가능하고, 반복 문제의 근본 원인 발견을 통해 예방 중심 보안 체계로 발전시킬 수 있습니다.



주요 모듈



유출 대응 이력 필터링

특정 담당자의 업무 성과나 특정 기간의 대응 효율성을 쉽게 분석할 수 있어 인사 평가나 프로세스 개선에 활용할 수 있습니다.

예를 들어 김과장이 지난달에 처리한 건들만 보거나, 연말 바쁜 시기의 대응 품질을 점검할 수 있어 팀 관리와 업무 개선 방향을 데이터 기반으로 결정할 수 있습니다.



기간별 대응 추이

우리 팀이 시간이 지나면서 더 잘해지고 있는지, 언제 업무량이 몰리는지를 그래프로 확인할 수 있어 인력 배치나 교육 계획을 세우는 데 도움이 됩니다.

대응 건수가 늘어나는 시기를 미리 예측해서 추가 인력을 배치하거나, 처리 시간이 단축되고 있다면 팀의 역량 향상을 객관적으로 입증할 수 있습니다.



유출 대응 현황

누가 어떤 종류의 업무를 몇 건씩 처리했는지 한눈에 보여주어 업무 배분이 공평한지, 특정 직원에게 업무가 편중되지 않았는지 쉽게 파악할 수 있습니다.

각 담당자의 전문 분야나 처리 속도를 고려한 업무 할당 계획을 세울 수 있고, 팀원들의 개별 성과를 객관적으로 평가할 수 있는 자료로 활용 가능합니다.



유출 대응 상세 이력

과거에 비슷한 사건이 발생했을 때 어떻게 해결했는지 참고할 수 있어 대응 시간을 단축하고 실수를 줄일 수 있습니다.

새로운 팀원이 들어왔을 때 과거 사례를 통해 학습할 수 있고, 재발하는 유출 패턴을 발견해서 근본 원인을 찾아 예방 조치를 강화할 수 있는 소중한 자료로 활용할 수 있습니다.

JIRANSOFT

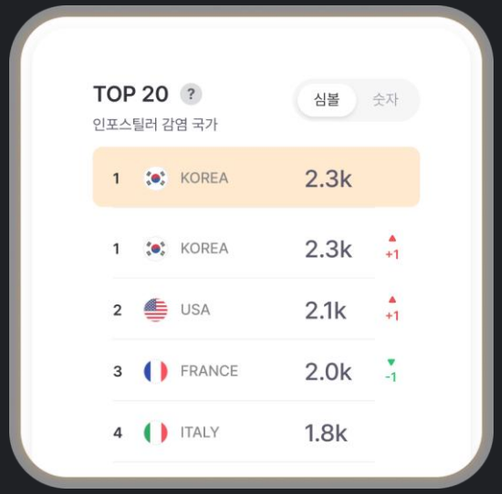
글로벌 사이버 공격 동향

전 세계 사이버 공격 트렌드를 미리 파악해 우리나라 상륙 전에 대비책을 마련할 수 있고, 해외 지사나 협력업체의 위험도를 사전 확인하여 맞춤형 방어 전략을 수립할 수 있습니다.

글로벌 비즈니스 기업이라면 진출 예정 국가의 사이버 보안 환경을 미리 평가해 사업 계획에 보안 리스크를 반영할 수 있습니다.



주요 모듈



TOP 20 인포스틸러 감염 국가

우리 회사가 해외 지사나 협력사와 업무할 때 어느 나라가 더 위험한지 미리 알 수 있어 추가 보안 조치를 준비할 수 있습니다.

특정 국가에서 접속하는 사용자에 대해 보안 점검을 강화하거나, 해외 출장 시 사용할 기기의 보안 설정을 더욱 철저히 할 수 있어 글로벌 비즈니스 환경에서의 보안 리스크를 효과적으로 관리할 수 있습니다.



그룹별 공격 비중

어떤 해커 그룹이 가장 활발하게 활동하고 있는지 알 수 있어 해당 그룹의 공격 방식에 맞는 방어 전략을 미리 준비할 수 있습니다.

예를 들어 특정 그룹이 이메일 공격을 주로 한다면 이메일 보안을 강화하고, 다른 그룹이 웹사이트 해킹을 많이 한다면 웹 보안에 더 투자하는 등 효율적인 보안 투자 계획을 세울 수 있습니다.



그룹의 공격 현황

우리와 같은 업종의 다른 회사들이 어떤 공격을 받고 있는지 알 수 있어 '우리도 비슷한 공격을 받을 수 있다'고 미리 대비할 수 있습니다.

최근에 어떤 새로운 공격 방식이 등장하고 있는지 실시간으로 파악할 수 있어, 뉴스나 보고서로 알려지기 전에 선제적으로 보안 패치나 대응책을 마련할 수 있는 경쟁 우위를 확보할 수 있습니다.



국가별 피해 규모

글로벌 확장을 계획하고 있다면 어느 나라가 사이버 보안 측면에서 더 안전한지 판단할 수 있어 사업 진출 전략 수립에 도움이 됩니다.

또한 전 세계적인 사이버 공격 동향을 파악하여 우리나라의 상대적 위험도를 이해하고, 국가 차원의 보안 정책 변화나 국제 협력 필요성을 객관적으로 평가할 수 있는 근거자료로 활용할 수 있습니다.

JIRANSOFT

전체 기능

웹 도메인(URL) 유출 탐지

다크웹을 통한 정보 유출의 수준을 평가하고, 메일 계정 및 첨부 파일의 유출 현황을 분석합니다.
멀웨어 감염에 대한 상세 정보와 일자별 유출 및 대응 정보를 제공합니다.

모듈	기능
도메인 유출 모니터링	등록된 도메인의 다크웹/유출 사이트 내 노출 여부 실시간 감시, 신규 유출 알림
서브도메인 유출 탐지	메인 도메인과 연관된 모든 서브도메인의 유출 정보 추적, 서브도메인별 위험도 분석
도메인 관련 이메일 유출	@도메인 형식의 이메일 계정 유출 현황, 부서별/직급별 유출 분포 분석
도메인 기반 필터링	특정 도메인/서브도메인 선택을 통한 맞춤형 유출 정보 조회, 위험 수준별 정렬
유출 경로 추적	도메인 정보가 유출된 경로와 출처 분석, 유출 시점과 확산 범위 파악
도메인 보안 점검	도메인 관련 보안 취약점 진단, DNS/SSL 인증서 만료 알림, 피싱 사이트 유사 도메인 탐지
유출 도메인 상세 정보	유출된 도메인별 상세 현황(유출 건수/유형/위험도), 연관 이메일 계정 목록, 대응 권장사항
도메인 유출 알림 설정	특정 도메인 유출 시 실시간 알림 설정, 알림 수신자 관리, 알림 빈도 조절

전체 기능

도메인 유출 탐지

다크웹을 통한 정보 유출의 수준을 평가하고, 메일 계정 및 첨부 파일의 유출 현황을 분석합니다.
멀웨어 감염에 대한 상세 정보와 일자별 유출 및 대응 정보를 제공합니다.

모듈	기능
다크웹 정보 유출 수준	유출 정보의 심각도 평가 (심각 / 주의 / 안전)
유출 위험 수준	0~100 수치 반원 그래프, 심각/주의/안전 분류, 도메인명과 위험수준 표시
메일 계정 유출 현황	메일 계정 유출 상태 파악 (신규 유출 / 대응 중인 유출 / 대응 완료된 유출 / 유출 합계), 도넛형 진행률 그래프
원클릭 숏컷	계정 유출/이메일 유출/문서 유출/감염된 아이피 유형별 원클릭 페이지 이동, 유출 건수 표시
문서/이메일 유출 대응 상태	처리 필요/완료 건수 표시, 최근 3건 미리보기, 더보기 버튼
도메인 탐색 필터	서브도메인별 정렬, 위험 수준 필터링(위험/주의/안전), 유출 건수 표시, 메모 기능
멀웨어 감염에 대한 상세 보고서	아이피 기반 목록/지도 제공, 최신순/유출순 정렬, 대응 여부 필터링, 아코디언 형태 상세 정보(사용자명/비밀번호/스틸러경로/스틸러타입), 해결하기/해결완료 버튼
유출 현황 - 타임라인	일자별 데이터 표시, 타임라인 요약정보/공지사항/일일 대응 현황, 유형별(유출/감염/복합) 신규/재유출 건수
유출 현황 - 캘린더	일자 클릭 시 해당 날짜 유출 데이터 실시간 표시, 상호작용 캘린더
이메일 및 파일 유출 탐지 보고서	헤더(제목/닫기버튼), 위험 점수 %/도넛그래프, 타입 라벨(유출/감염/복합), 대응/대응취소 버튼, @형식 이메일/해결날짜, 고유 비밀번호 목록/악성코드 감염 목록 아코디언, 이력 아코디언(유형/URL/비밀번호/유출일자/해결일자/해결 상태)

전체 기능

유출 상세

유출된 정보의 심각도와 관련된 리스크 스코어를 제공하며, 유출 대응의 추이와 피해 증감을 시각화합니다.
또한, 기간별 대응 현황과 유출된 계정의 상세 정보 리스트를 필터링하여 보여줍니다.

모듈	기능
위험 점수	유출 정보에 대한 위험도 점수 제공
보고서 다운로드	상세 보고서 다운로드
유출 대응 추이 그래프	유출 대응 및 피해 증감 추이 시각화
피해 증감 추이 그래프	유출 대응 및 피해 증감 추이 시각화
기간별 대응 현황	유형별 / 당일 대응 / 월간 누적 대응 / 연간 누적 대응 현황 제공
유출 상세 정보 목록	전체 건수 표시, 위험 점수 3색상 진행 막대 + %, 계정 아이디 @이메일 형식, yyyy-mm-dd 날짜 형식, 유출 유형 아이콘(유출/감염/복합), 대응 상태(신규/해결/검토중), 페이지 구분
유출 피해 증감 추이	월별 막대그래프, 연도 표시, 좌우 화살표(<,>) 클릭으로 이전/이후 연도 이동
유출 상세 정보 필터링	필터 버튼 클릭 시 팝업, 기간/날짜/위험도(심각/주의/안전)/대응단계(새로운유출/처리중/처리완료)/유형(유출/감염/복합) 태그 선택, 초기화/취소/적용 버튼, 테이블 상단 태그 표시
유출 정보 상세 보기	위험 점수 / 이메일 계정 / 대응 완료일 / 대응 후 재유출 여부 / 유출된 비밀번호 / 로그인 URL / 감염된 장치 정보 제공, 권장 사항 제공
유출 이력	순서 / 유출 유형 / URL / 비밀번호 / 유출 일자 / 대응 일자 / 대응 여부

전체 기능

유출 대응 이력

각 유출 사건에 대한 대응 작업의 이력과 관리자별 대응 현황을 추적합니다.
이를 통해 조직의 보안 대응력을 평가하고 개선할 수 있는 인사이트를 제공합니다.

모듈	기능
유출 대응 이력	담당자별 대응 현황 필터링, 기간내 대응 현황 필터링
기간별 대응 추이 그래프	기간별 대응 추이 시각화
관리자 대응 현황	담당자 / 대응 기간 / 타입별 대응 건수 정보 제공
대응 상세 이력	순서 / 아이디 / URL / 유출 타입 / 유출일 / 대응일 정보 제공

글로벌 사이버 공격 동향

전 세계에서 가장 큰 영향을 받은 TOP 20 인포스틸러 감염 국가와 해커 그룹의 활동을 분석합니다.
이는 글로벌 보안 환경에 대한 광범위한 이해를 지원하며, 특정 공격자 그룹에 대한 심층적인 인사이트를 제공합니다.

모듈	기능
TOP 20 인포스틸러 감염 국가	순위 / 유출량 제공
사이버 공격 그룹 활동 분석	해커 그룹간 공격 비중
해커 그룹의 활동 분석	공격목표 사이트 정보 제공, 공격 발견 날짜 정보 제공, 공격 사이트의 산업군 정보 제공, 공격 그룹이 공격한 다른 국가의 피해 규모 정보 제공

제로다크웹은 숫자로 말합니다.

다크웹에 정보가
유출된 기업의 비율
77%

3,220억

건의 데이터

880억

건의 유출 계정

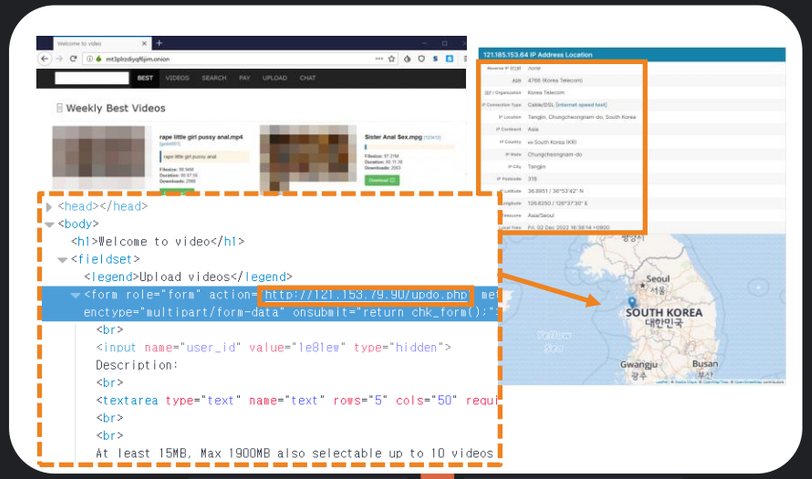
98.5만

샘플 리포트로 발견된
유출 정보의 수

*Extracted data: 164,767,319,997
+ Account-specific data: 58,522,819,911 (23.4.24.)

JIRANSOFT

제로다크웹이 수집하는 데이터



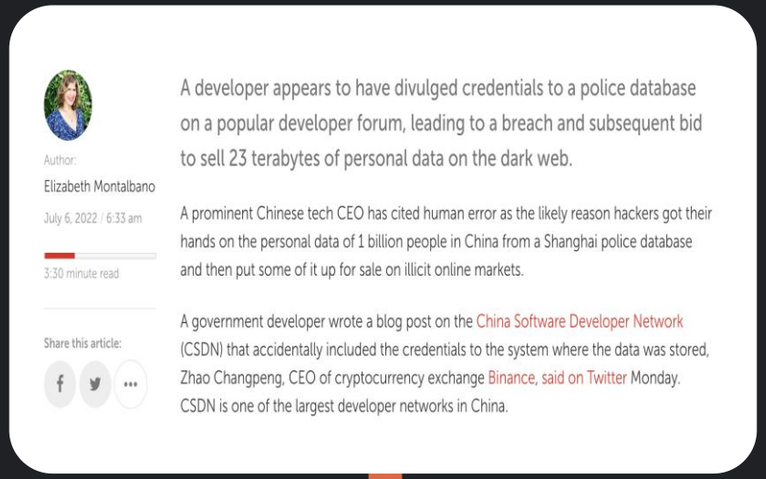

200 million Twitter users' email addresses allegedly leaked online

By Lawrence Abrams

January 4, 2023 03:16 PM

Image: AI generated at Dall-E

A data leak described as containing email addresses for over 200 million Twitter users has been published on a popular hacker forum for about $2. BleepingComputer has confirmed the validity of many of the email addresses listed in the leak.


Author:
Elizabeth Montalbano

July 6, 2022 / 6:33 am

3:30 minute read

Share this article:

A developer appears to have divulged credentials to a police database on a popular developer forum, leading to a breach and subsequent bid to sell 23 terabytes of personal data on the dark web.

A prominent Chinese tech CEO has cited human error as the likely reason hackers got their hands on the personal data of 1 billion people in China from a Shanghai police database and then put some of it up for sale on illicit online markets.

A government developer wrote a blog post on the China Software Developer Network (CSDN) that accidentally included the credentials to the system where the data was stored, Zhao Changpeng, CEO of cryptocurrency exchange Binance, said on Twitter Monday. CSDN is one of the largest developer networks in China.

IP Address
Web Domain
Images
Cryptocurrency Address

Geolocation
Web Domain
Text
Backlinks

ID
Email
Leaked Source

Password
Domain
Leaked Date

ID
Email
Leaked IP

Password
Domain
Leaked Date

ZERODARKWEB PARTNER DATA WAREHOUSE

JIRANSOFT

USE CASE (정보 보호를 위해 고객사의 이름은 비공개 처리되었습니다.)

자동차 부품 제조 KR

"해당 고객사는 자동차 관련 제조 산업 분야의 글로벌 기업으로, 자사의 기술 정보와 제품 설계 데이터의 불법 유출 및 다크웹 상의 거래를 탐지하고 효과적으로 대응하고자 제로다크웹을 도입함."

디지털 마케팅 및 핀테크 JP

"해당 고객사는 데이터 보안과 정보 유출 방지를 핵심 과제로 삼고 있음. 제로다크웹의 가격 경쟁력과 유출 데이터 탐지의 정확성을 높이 평가하여 도입을 결정함. 제로다크웹을 통해 고객 데이터 보호, 내부 정보 유출 방지, 그리고 사이버 위협에 대한 실시간 대응 능력을 강화하고 있음."

반도체 제조업 ID

"해당 고객사는 첨단 반도체 제조 및 설계에 주력하는 기업으로, 기술적 정보와 설계도면의 보안을 중시함. 반도체 설계 및 제조 과정에서 발생하는 민감한 정보와 지적 재산권 보호를 위해 제로다크웹을 도입함. 제로다크웹을 통해 다크웹에서의 기술 유출 탐지 및 대응, 그리고 사내 정보 보안 강화에 주력하고 있음."

유선 통신업 KR

"해당 고객사는 국내 대기업 계열사로 앱, 게임 및 콘텐츠를 유통하고 있음. 콘텐츠의 다크웹 유통 탐지와 사내 정보 유출 탐색 및 대응을 위해 제로다크웹을 도입함."

USE CASE (정보 보호를 위해 고객사의 이름은 비공개 처리되었습니다.)

응용 소프트웨어 개발 및 공급업 KR

"해당 고객사는 금융 결제 시스템 구축과 다국어 번역 서비스를 중심으로 메타버스, 블록체인 등의 신기술 발굴에 주력하고 있음. 다크웹 유출에 대해 선제적인 대응을 위해 제로다크웹을 도입함"

패션 브랜드 JP

"해당 고객사는 글로벌 패션 브랜드로, 고객 개인정보와 브랜드 이미지 보호를 중시함. 제로다크웹을 통해 고객 데이터 보안 강화, 브랜드 평판 모니터링, 그리고 잠재적 위협에 대한 선제적 대응에 주력하고 있음."

전자상거래 소매 중개업 KR

"해당 고객사는 온라인 도서유통을 발판으로 음악, Ebook등의 다양한 문화상품의 판매 및 유통을 하고 있음. 취급 중인 콘텐츠의 다크웹 유통을 탐지하고 대응하고자 제로다크웹을 도입함."

자동차 인테리어 부품 제조업 KR

"해당 고객사는 자동차 인테리어 산업을 선도하는 글로벌 기업으로, 사내 정보 유출 탐색 및 대응을 위해 제로다크웹을 도입함."

제로다크웹은 고객과 함께합니다.



실제 긴급 알림 보고서

정보유출로 인한 해킹 위험성, 취약점이 발견되는 경우에도
제로다크웹 서비스는 사용자에게 취할 수 있는 연락 수단을 동원해
긴급 알림을 제공합니다.

최근 케이스

- 메타 표준화 페이지 노출 정황
- 특정 리포지토리 취약점 이슈 탐지
- 깃 서버 도메인 탐지

JIRANSOFT

궁금한 점은 언제든 편히 연락주세요.

문의 메일:
officesales@jiran.com

샘플 리포트 신청:
https://www.zerodarkweb.kr/

JIRANSOFT

CONFIDENTIALITY NOTE: The information transmitted, including attachments, is intended only for the person(s) or entity to which it is addressed and may contain confidential and/or privileged material. Any review, retransmission, dissemination or other use of, or taking of any action in reliance upon this information by persons or entities other than the intended recipient is prohibited. If you received this in error, please contact the sender and destroy any copies of this information.

© 2025, ZERO-SECURITY. All rights reserved. Powered by StealthMole