기술유출진단서비스

Let the Data Speak

DEEPNINE

기술 유출을 막는 가장 확실한 방법,
보안데이터 분석기업 딥나인

01
서비스 소개

- 고객 문제점
- 문제 해결 방안
- 기존 보안솔루션 VS 딥나인 진단 서비스
- 서비스 프로세스
- 고객 문제점 해결사례
- 서비스 구성 및 비용안내

02
회사소개

DEEPNINE

퇴사자 이메일, 확인 해보셨나요?

기술 유출은 단 하루 만에 발생하지만, 이 사실을 발견하는 데는 평균 86일이 걸립니다

2024년 기술유출 300여건 중 58.3%가 재직 직원 및 퇴사자 소행이었습니다

이러한 유출사고로 기업들이 피해를 본 평균 손실액은 18억입니다

(출처: 글로벌 보안연구기관 Ponemon Institute, 중소벤처기업부 2024 기술보호실태조사)

정보 유출 주요 경로

인터넷

- 정보 유출이 가장 많은 경로
- 클라우드, 메신저, 이메일,
- 오피스365, 노션 등 생산성 툴

이동형 저장매체

- 대량의 정보유출 가능
- 외부 반출입 통제가 어려움

출력물

- 외부 반출입 통제가 어려움
- 보안 모니터링을 우회하는 수단으로 자주 활용

화면촬영

- 재택근무가 보편화된 후
- 보안 모니터링을 피해 대량의 정보를 유출하는 수단으로 활용

DEEPNINE

우리 회사의 기술 유출 위험, 얼마나 알고 계신가요?

간단한 체크리스트를 통해 우리 회사의 보안 현주소를 직접 확인해보세요

그룹웨어, 이메일 등 감사로그를 수집하거나, 정보유출 징후를 분석하지 않는다

USB, 외장하드와 같은 이동형 저장매체나 웹사이트를 통한 자료의 전송을 통제하지 않는다

퇴사자 보안점검, 계정 회수 등 보안 절차를 퇴사한 날 즉시 수행하지 않는다

중요 정보를 출력·반출하는 행위를 통제하지 않는다

외부업체, 전문가 등과 협업 시 NDA 체결, 자료 공유 통제 등 보안 관리 절차가 없다

위 5개 항목 중 2개 이상 해당되는 기업의 경우,

귀사의 내부 정보가 위험에 노출될 수 있습니다

무료 상담을 통해 지금 바로 기술유출 진단서비스를 도입해 보세요

아래 기업은 항목 중 하나라도 해당되면, 진단이 필요합니다.

- 혁신 기술 기업 - 기술 기반 스타트업 및 신생기업
- 성장형 기술기업 - 코스닥 등 기술특례 상장기업
- R&D 집약형 제조기업 - 연구개발 중심의 제조업체
- 국방·보안 관련기업 - 방위산업 및 보안업체
- 데이터 자산 기반 기업 – 고객정보, 거래·영업데이터가 경쟁력의 핵심인 기업

DEEPNINE

내부정보 유출에 대한 불안감, 딥나인이 해결합니다

서비스 도입 기대효과

내부자 정보유출 조기 차단

사용자 행위 분석(UBA)을 통해
정보유출 위험이 높은 인물을
조기에 식별하여,
정보유출 위협을 사전에 차단

4년간 정보유출 정황 탐지 실적

5,000+

보안솔루션 운영 효과 극대화

로그 데이터를 활용해
운영상 허점을 점검하고, 실효성
평가와 개선 방향을 제시하여
보안 투자 효과 극대화

내부조사+ 징계+자료 회수 실적

700+

내부 통제 활동 지원

문서·파일·기술자료 등 주요 자산의
직원간 과도한 공유나
외부 유출 징후를 식별하여,
감사팀의 내부통제 활동 지원

형사고발 등 법적조치 실적

10+

DEEPNINE

딥나인은 회사의 그룹웨어와 이메일 사용 기록과 같은 데이터를 분석해, 내부 정보 유출 위험을 조기에 진단합니다

위험은 조기에 식별되고, 기업의 핵심 정보자산은 안전하게 보호됩니다

Case-by-Case

건별 분석

- 핵심 인재의 갑작스런 퇴사로 정보유출이 우려될 때
- 72시간 내로 진단결과 제공
- 정보유출 확인 시 후속조치 지원

Regular Diagnostics

정기 진단

- 연 1회~4회 필요에 따라 정기 종합 진단 시행
- 회사 전체 정보유출 실태 파악 가능
- 임직원 개인별 정보유출 리스크 누적관리 가능

Weekly Monitoring

주간 모니터링

- 주간 정보유출 의심사례 탐지·보고
- 리스크가 높은 인원을 선별·순위화해 집중관리
- 기밀정보의 내외부 공유현황 상시 모니터링

필요한 순간, 즉시 서비스 사용 가능

1회/월/연 단위 필요한 기간만큼 사용

별도 시스템, 프로그램 불필요

분석 결과 수사기관에 증거로 제출 가능

DEEPNINE

대체 불가능한 전문성과 축적된 노하우

기존 보안 솔루션

설치 필요여부

- 모든 PC와 서버에 에이전트 프로그램 설치 필요
- 그룹웨어 등 교체시 보안솔루션과 호환성 확인 필요

작동 방식

- 차단 위주 사전 통제 방식
- 업무효율성 저하 및 직원들의 불편 초래
- 차단 우회가능

대응 시간

- 기업이 피해를 입고나서 유출을 인지하는 경우가 대부분

딥나인 진단 서비스

설치 필요여부

- 프로그램 설치 없음
- 기존 업무시스템이 보유한 로그데이터로 진단
- 그룹웨어 등 교체 시 별도 조치 불필요

작동 방식

- 사용자행위분석(UBA) 기반 정보유출 위험 식별
- 정보기관 노하우 적용한 정보 유출자 대응체계
- 통제가 아닌 모니터링에 집중, 자료 공유·반출에 불편함이 없음

대응 시간

- 유출 시도 초기 단계부터 포착·대응
- 긴급 상황 시 72시간내 유출진단

DEEPNINE

딥나인의 정보유출 식별 방식을 소개합니다

업무환경 파악
(정보유출 경로 파악)

핵심기술, 영업비밀 현황 점검
대내외 자료공유 현황 점검
사용 중인 그룹웨어 정보 확인
사용 중인 보안솔루션 정보 확인

→

로그 수집

업무메일 수발신 내역
문서중앙화 솔루션 사용 로그
그룹웨어 사용 로그
노션·메신저 등 사용 로그
보안솔루션 로그

→

내부정보 유출 진단 및 평가

자체 노하우로 수집한 로그 분석
정보유출 정황 추적
정보유출 위험 경로 점검

→

리포트 제출

정보유출 의심사례 보고
개인별 정보유출 리스크 평가보고
유출자료 회수 등 대책 보고
정보유출 취약점 및 대책 보고

진단 리포트 내용

- 정보유출 유출 정황, 개인별 정보유출 리스크 평가
- 국정원·경찰·공공기관 출신 보안·수사 출신 전문가의 교차 검증을 통해 평가 신뢰도 보장
- 정보유출자 색출, 경위조사 후 대응 수위(내부징계·법적조치 등) 가이드 및 수사기관 제출용 증거 지원
- 정보유출 경로(이메일, 클라우드, 메신저 등) 취약점 진단 및 보안대책 제안

DEEPNINE

1. 스타트업 : 핵심개발자 퇴사 후 기술정보 유출 정황 탐지 및 선제적 대응 사례

개요

- 기술 개발을 총괄하던 핵심 개발자가 퇴사 전 노트북을 포맷 후 반납
- 약 한 달 뒤, 유사 기술로 신규 창업한 사실이 확인되어, 기술유출 가능성에 대한 의심이 제기됨
- 노트북이 포맷된 상태로 반환되어 일반적인 디지털포렌식을 통한 분석이 불가능한 상황

딥나인 역할

- 딥나인은 퇴사자 계정의 이메일 및 그룹웨어 로그 1년치를 수집·분석
- 분석 결과, 회사내 핵심 기술문서에 대한 외부 발신 및 다운로드 정황이 다수 확인됨
- 관련 내용을 수사 증거로 활용 가능한 형태의 분석 리포트 제공

결과

- 고객사는 해당 분석 리포트를 바탕으로 퇴사자에게 기술정보의 반납 및 완전한 삭제를 요구
- 추가로, 기술정보 무단 보유·활용 시 손해배상 책임(00억원)이 발생한다는 확약서를 징구하여 법적 대응 기반 마련
- 이를 통해 기술유출로 인한 실질적 피해를 사전에 차단하고, 향후 형사 고발 등 법적 조치 시 활용 가능한 증거까지 확보

DEEPNINE

2. 방산기업 : 미 국방부 CMMC 인증준비 중 기술정보 유출 정황 탐지 및 대응 사례

개요

- 미 국방부 조달 요건인 CMMC 인증을 준비 중이던 방산기업, 인증 대비 사전 점검 차원에서 내부 정보유출 취약점 분석을 의뢰
- 분석대상 : 전현직 직원 000명의 그룹웨어, 이메일, 보안솔루션 등 각종 로그 데이터

딥나인 역할

- 방대한 로그에 대해 사용자행동분석(UBA) 기법을 활용, 이상행위를 1차 분석
- UBA분석 결과를 바탕으로 이상징후가 의심되는 인원을 선정, 심층 정밀 분석을 진행
- 그 결과, 설계도면 등 주요 기술정보의 외부 반출 정황이 포착되어 고객사에 보고

결과

- 딥나인의 분석 리포트와 CCTV 등 내부 보안자료를 종합하여 내부 감사 즉시 착수
- 해당 직원으로부터 무단 반출 자료를 회수하고, 내부 규정에 따라 징계 조치 실시
- 아울러, 형사 고발 등 법적 대응이 가능한 증거자료를 체계적으로 확보

DEEPNINE

3. 기술특례 상장사 : 퇴사 당일 클라우드 무단 접속 정황 탐지 및 즉각 대응 사례

개요

- 기술특례 상장을 준비 중이던 기업, 기술성 평가 완료 후 주요 투자자들로부터 보안강화 조치 이행을 요청받고 딥나인의 기술유출 모니터링 서비스를 도입하였음
- 상장 절차 진행 중 퇴사한 핵심 직원이 퇴사 당일 일부 기술자료 접근 등 이상 행위가 탐지됨

딥나인 역할

- 해당 직원의 재직 기간 중 생성된 로그데이터를 선제적으로 분석, 이상징후가 없음을 확인
- 퇴사 당일, 기밀정보 반납 및 삭제 확인서 징구 등 보안절차 안내와 보안교육 실시
- 퇴사 당일 진행한 추가 분석에서, 해당 직원이 같은 날 저녁 개인 기기를 통해 비정상적인 자료 접근 시도를 한 사실 포착
- 이상행위 확인 즉시 고객사 보안담당자에게 보고하고 추가 조치가 가능하도록 지원

결과

- 고객사는 즉시 퇴사자의 모든 업무용 계정을 차단하고, 변호사를 통해 내용증명을 발송
- 이후 휴대폰 포렌식 및 제3자 유출 여부에 대한 점검을 완료, 내부 절차에 따라 사건 종결

DEEPNINE

우리 회사에 꼭 맞는 플랜을 선택하세요

Insight Plan

인사이트 플랜

- ✓ 전체 임직원 대상 정보유출 리스크 진단
- ✓ 기존 보안솔루션 운용실태 진단
- ✓ 정보유통 경로 내부통제 현황 진단
- ✓ 정보유출자 대면조사
- ✓ 전체 임직원 대상 보안교육 제공
- ✓ 딥나인 제작 보안실무 가이드라인 제공

별도 문의

1개월 소요

Focus Plan

포커스 플랜

- ✓ 재직 직원, 퇴사자 등 특정 인원 1명에 대한 정보유출 리스크 진단
- ✓ 정보유출자 대면조사
- ✓ 퇴사자 보안교육 제공
- ✓ 기타 보안솔루션 운용실태 진단
- ✓ 퇴사자 3인 패키지(600만원, 1년 유효)

건당 250만원

3일 소요

Monitoring Plan

모니터링 플랜

- ✓ 주간 정보유출 모니터링
- ✓ 퇴사자 정보유출 위험분석
- ✓ 정보유출자 대면조사
- ✓ 퇴사자 화상 보안교육
- ✓ 전체 임직원 보안교육
- ✓ 월간 진단리포트
- ✓ 딥나인 제작 보안실무 가이드라인 제공

월 구독형 : 100만원부터

최종 비용은 사용자 수와 데이터 종류에 따라 상담 후 결정됩니다

DEEPNINE

플랜별 구성 비교

구분	포커스	인사이트	모니터링
자가진단표	●	●	●
내부정보 유출 위험 진단 리포트	●	●	●
정보유출자 대면조사 (국정원·경찰 출신 조사전문가 투입)	●	●	●
퇴사자 보안교육	●	●	●
기존 보안솔루션 운용 실태 점검		●	●
메신저·이메일 등 사내 정보유통 경로 실태 점검		●	●
보안담당자 전용 보안실무 가이드라인 제작		●	●
전 임직원 보안교육 (연1회)		●	●
전 사업장 현장 보안감사 (연1회) (물리보안·시설보안·인원보안·보안제도 등 분야별 점검)		●	●
보안정책, 보안이슈 상시 자문			●

DEEPNINE

딥나인은 국가 안보, 사이버 수사, 공공 감사, 산업기술 보호 등 서로 다른 분야에서 실무를 경험한 전문가들이 함께하는 보안데이터 분석 조직입니다

구성원 각각이 다른 기관과 환경에서 축적해 온 실전 경험은, 단순한 기술 분석을 넘어 위협을 '식별하고 대응할 수 있는' 실행력 있는 보안 전략으로 이어집니다

특히 국가기관에서 축적한 감사 및 보안 실무 역량을 바탕으로, 딥나인은 감사로그·보안로그 등 행위 기반 메타데이터를 분석해 내부자 위협과 기술 유출의 징후를 정밀하게 식별하는 데 특화되어 있습니다.

우리는 보안을 단순한 시스템 문제가 아닌, 사람과 행위, 그리고 그 흔적의 해석으로 접근합니다.

딥나인은 로그와 데이터의 맥락 속에서, 사람의 의도를 읽어냅니다.

대표

김재형

- 국가정보원 근무
- 민간군사기업 창업&부사장
- 위즈노트 유한회사(현 딥나인) 창업&대표

고문

강원선

- 국가정보원 근무
- 한국산업기술보호협회 기술보호센터장
- 명지대학교 산업보안센터장

고문

이선응

- 국가정보원 근무

이사

강구민

- 성균관대학교 법학박사
- 특검 디지털 포렌식 수사팀장
- 성남시 감사관실 조사관
- 국가정보원, 특허청 자문위원

이사

김무석

- 성균관대학교 과학수사학 박사
- 특검 디지털 포렌식 수사관
- 경찰청 사이버수사국 수사관

DEEPNINE

다양한 업종의 고객을 통해 쌓아온 분석 경험과 노하우를 바탕으로 우리는 “AI 기반 기술유출 진단 플랫폼”으로 성장합니다

2020

도전의 시작

- 위즈노트 유한회사 설립
- 해외안전 및 보안 컨설팅 시작

2021

변화의 전환점

- 영업비밀 보호 컨설팅 시작
- **기술유출 진단체계 개발 착수**

2022-23

분석기술 기반 성장

- 사용자행동분석 기법 도입
- 천만 건의 데이터 분석 경험
- **자체 분석기법 상용화 성공**

2024

분석기술 고도화

- 정부기관 출신 포렌식 전문가 영입
- 개인별 정보유출 리스크 평가체계 고도화
- **기술유출 진단 서비스 출시**

2025

전략적 도약

- (주)필라넷과 기술유출 진단 AI 공동개발
- ‘딥나인’으로 사명 변경
- **25년 9월, 기술유출진단 플랫폼 “딥나인” 출시**

우리 기업의 핵심기술과 영업비밀이 잘 보호되고 있는가?

이 질문에 확신할 수 없다면, 지금 딥나인이 필요한 시점입니다.

기술유출 진단, 지금 바로 시작해보세요.

https://www.deepnine.io

master@deepnine.io