

출처를 모르는 문서는, 등급을 매길 수 없습니다

문서의 출처를 자동으로 식별해 업무 시스템별 보안 등급을 관리하는 출처 기반 등급 관리 솔루션

파일 메타데이터와 다운로드 기록을 교차 분석해 문서의 출처를 자동 식별하고, 업무 시스템에 등급을 지정하면 해당 문서 전체에 자동 태깅합니다. 수십만 건을 수작업 없이 국가망 보안체계(N2SF) 등급 기준에 맞춰 관리합니다.

InfoDiscovery 동작 원리



1 출처 식별

메타데이터 · 다운로드 기록 분석



2 현황 확인 · 등급 지정

웹 콘솔에서 시스템에 등급



3 자동 태깅

기준 · 신규 문서 일괄 태깅



4 보안 연동

DRM 등 등급 기반 보호

내용은 열지 않고 문서의 출처부터 가려냅니다

파일 메타데이터와 다운로드 기록만 읽기 전용으로 분석해, 어느 업무 시스템에서 나온 문서인지 자동으로 식별합니다.

시스템 하나에 등급을 매기면 문서 전체가 따라옵니다

문서를 일일이 분류하지 않습니다. 업무 시스템 단위로 한 번에 등급을 적용해 수십만 건을 정리합니다.

IT팀도 몰랐던 시스템까지 한눈에 드러냅니다

흩어진 시스템·문서 분포는 물론, 외부 클라우드·메신저·다운로드 경로 같은 사각지대(Shadow IT)까지 가시화합니다.

매긴 등급은 그대로 보호로 이어집니다

태깅된 등급을 기반으로 DRM 등 문서보안 솔루션과 연동해 암호화·접근제어를 자동 적용합니다.



Visibility

업무 시스템 현황 가시화

어떤 시스템이 몇 개 쓰이는지, 문서가 어디에 퍼져 있는 조직 전체 현황을 명확히 파악합니다.

Compliance

N2SF 등급 의무 충족

국가망 보안체계(N2SF)의 정보시스템 등급 분류 원칙에 맞춰 등급 관리 의무를 효율적으로 충족합니다.

Efficiency

분류 비용 절감

수십만 건을 수작업 없이 시스템 단위로 일괄 등급 관리해 분류에 드는 시간과 비용을 줄입니다.

InfoDiscovery 주요 특징

01 출처 식별 방식

읽기 전용 · 메타데이터 · 내용 비열람

문서 내용을 열지 않고 파일 메타데이터와 브라우저 다운로드 기록만 읽기 전용으로 교차 분석합니다. 내용 노출 없이 정확하고 비용 효율적입니다.



02 보안 등급 관리 & 자동 태깅

C/S/O 등급 · 자동 배포 · 일괄 · 감사 추적

업무 시스템에 C/S/O 보안 등급을 지정하면 전사 에이전트에 자동 배포되어 기존·신규 문서에 자동 태깅됩니다. 등급 변경 사유가 기록되어 감사 추적이 가능합니다.

*기밀(C·Classified)·민감(S·Sensitive)·공개(O·Open)



03 운영 이력 & 통계

위험 지수 · 신규 유입 추이

위험 지수, 신규 유입 추이 등 운영 통계를 제공해 등급 관리 현황과 변화를 지속적으로 모니터링합니다.



04 N2SF 등급 분류 대응

정보시스템 등급 분류 · 의무 대응

정보시스템의 등급을 그 시스템이 처리하는 업무정보의 등급과 동일하게 분류하는 N2SF 원칙을 준용해, 강화되는 등급 관리 의무에 대응합니다.

*N2SF (National Network Security Framework)

