

개인 식별 정보(PII)를 식별하고 매핑하여 접근 리스크를 벤치마킹하세요.

EPI-USE Labs의 SAP 데이터 프라이버시 진단 서비스



SAP® 시스템에는 방대한 양의 민감한 정보가 저장되며, 비즈니스 요구사항을 충족하기 위해 시스템 내에 커스터마이징된 기능이 존재할 수도 있습니다. 이러한 민감 데이터는 데이터 유출을 방지하고, 개인정보 보호 법규를 준수하기 위해 신중하게 관리되어야 합니다.

EPI-USE Labs는 고객의 개인 식별 정보(PII)를 이해하고 식별하며, 접근 권한 리스크를 진단할 수 있도록 지원합니다. 본 종합 서비스에는 다음이 포함됩니다.

데이터 디스커버리: SAP 데이터 디렉터리와 대한 분석

컨설팅 서비스: 데이터 디스커버리 결과 분석 및 PII 데이터 맵 정량화

기술 워크숍: EPI-USE Labs 데이터 프라이버시 전문가가 고객사의 기능·기술 팀과 함께 진행 (English only)

SAP 데이터 프라이버시 및 리스크 진단 분석: 상세 결과 보고서 제공

확장 디스커버리 보고서: SAP 접근관리 및 리스크를 분석하는 선택형 추가 서비스

왜 SAP 내 민감 데이터를 이해해야 할까요?

SAP 시스템에는 고객, 벤더, 임직원과 관련된 광범위한 민감 데이터가 저장되어 있습니다. 데이터 프라이버시를 고려할 때 SAP 데이터 모델을 함께 이해하는 것은 매우 중요합니다. SAP에서는 하나의 필드를 수정하면 시스템 전반의 여러 위치에 해당 값이 자동으로 반영되기 때문입니다. EPI-USE Labs의 경험에 따르면, 하나의 개인 식별 정보 값이 시스템 전반에 최대 100회까지 복제될 수 있습니다. 이러한 데이터 구조에서는 개인정보 보호 규정을 준수하기 위해 시스템 전체에서 값을 일관되게 변경해야 합니다. 또한, 오랜 기간 SAP를 사용해 온 많은 기업 사용자들은 데이터 저장 및 처리를 지원하기 위한 커스터마이징 기능을 개발해 왔으며, 커스텀 테이블을 포함한 이러한 요소들은 민감 데이터의 노출 범위를 더욱 확대합니다.

민감 데이터를 이해하고, 식별하며, 매핑함으로써 얻을 수 있는 이점

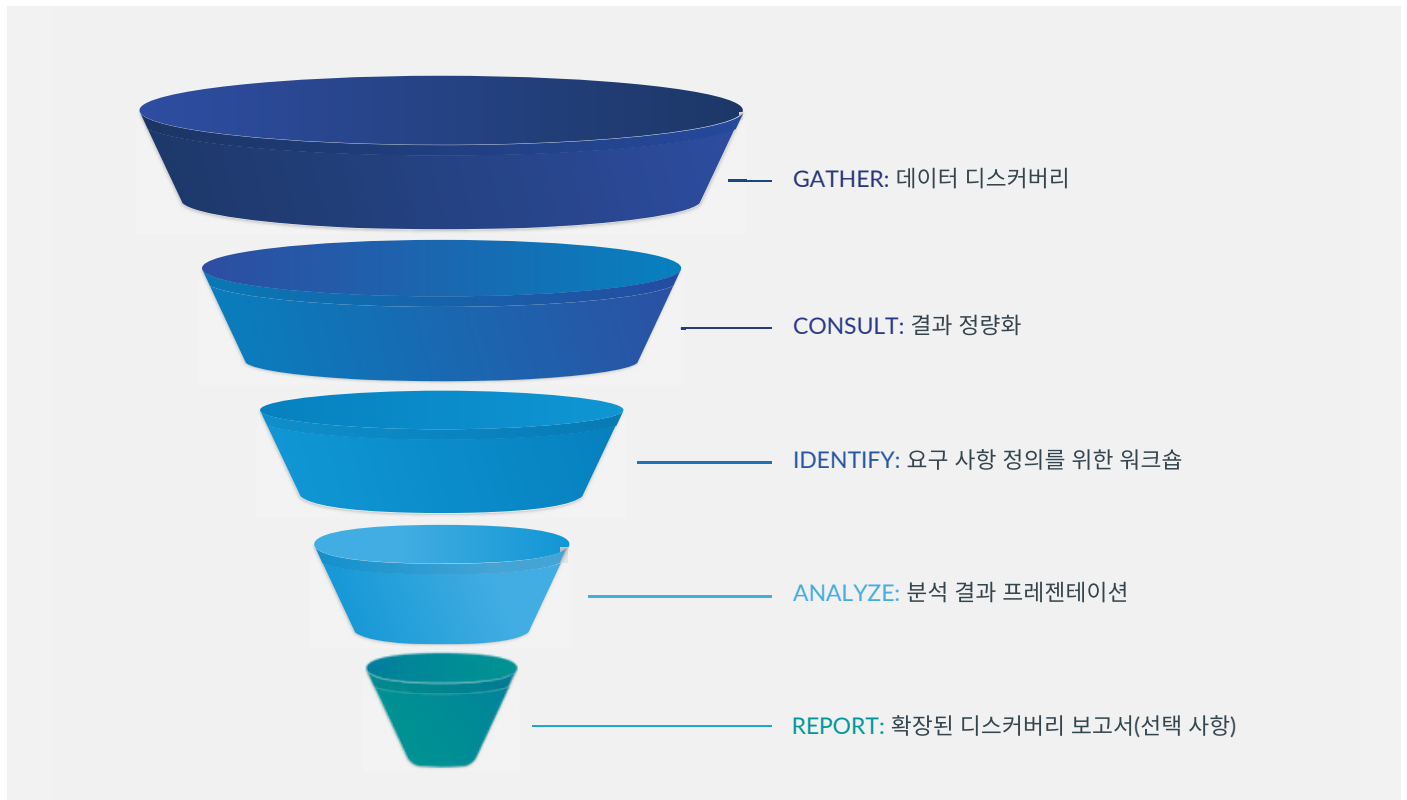
민감 데이터/PII 노출 리스크 최소화

데이터 보안 관리 강화

글로벌 개인정보보호 법규 준수

SAP 데이터 모델에 대한 수십 년간의 전문 도메인 경험을 바탕으로, EPI-USE Labs는 오브젝트와 시스템 전반에 걸쳐 민감 데이터를 일관성 있게 관리할 수 있도록 지원합니다.

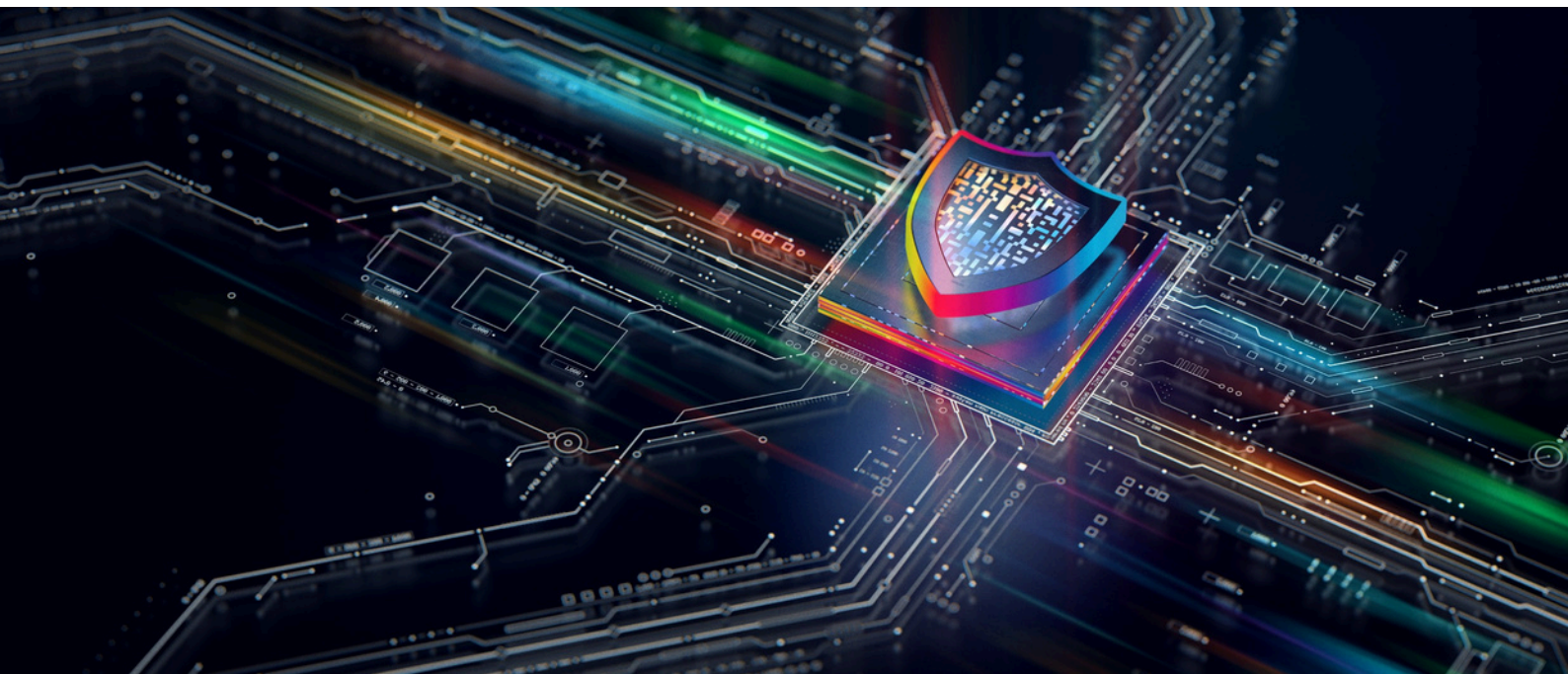
종합적인 SAP 데이터 프라이버시 진단 서비스



GATHER: 데이터 디스커버리

SAP 데이터 관리 자체에 특화된 SAP 독립적 개발 파트너로서, 당사는 오브젝트 간 및 시스템 간 통합을 상세히 정의한 자체 독점으로 보유한 비즈니스 오브젝트 정의(Business Object Definitions)를 개발해 왔습니다. 이 상세한 테이블 매핑을 기반으로, 모든 표준 SAP PII 필드에 대한 필드 레벨 통합 맵을 구축했습니다.

이 맵을 활용하여 SAP 시스템 내 데이터 디렉토리를 분석하는 데이터 디스커버리 프로그램을 설계했습니다. 이 프로그램은 민감 데이터 요소에 대한 와일드카드 검색을 수행하고, PII를 포함할 가능성이 있는 테이블 및 필드 목록을 생성합니다. 이후 해당 테이블이 실제로 데이터가 채워져 있는지 검증합니다.



CONSULT AND IDENTIFY: 컨설팅 서비스 및 데이터 프라이버시 워크숍

당사의 데이터 프라이버시 전문가들이 귀사의 기능 조직과 함께 워크숍을 진행하여, 다음을 포함한 모든 PII 데이터 유형에 대한 요구 사항을 정의합니다.

운영 데이터 보존 요구 사항 (데이터 유형별)	예를 들어, 직원이 비활성 상태가 되면 즉시 은행 정보 및 가족 정보를 삭제하고, 연락처 정보는 5년 후 삭제, 10년 후에는 완전 비식별 처리합니다.
마스킹/삭제 (Redaction)	데이터 주체가 삭제 대상 요건을 충족했을 때, 운영 시스템에서 어떤 조치를 취해야 하나요?
공개(Disclosure)	SAP 데이터 중 어떤 데이터가 정보주체 열람 요청(Subject Access Request) PDF에 포함되어야 하나요?
비운영 데이터 스크램블링	데이터 유형별로 어떤 조치를 취해야 하며, 예외 사항이나 조건이 있습니까?
랜드스케이프 검토 및 시스템 데이터 상속	어떤 시스템이 스크램블된 데이터를 수신하며, 스크램블링이 이에 어떤 영향을 미칩니까?

당사의 숙련된 컨설턴트들은 글로벌 다양한 산업 분야에서의 경험을 보유하고 있습니다. 이들은 데이터 프라이버시의 복잡성을 이해하고 있으며, 풍부한 경험을 귀사와 공유할 수 있습니다.

본 서비스에는 라이선스 비용이 발생하지 않으며, 일반적인 SAP ECC 프로젝트는 2주 기간 동안 총 5일이 소요될 것으로 예상합니다.

- 3일: 데이터 디스커버리 및 기술적 시스템 분석
- 1일: 비즈니스 및 컴플라이언스 팀과의 워크숍
- 1일: 문서화 및 결과 프레젠테이션

대면 워크숍을 권장하지만, 원격 또는 현장 방식 모두 가능합니다.

ANALYZE: SAP 데이터 프라이버시 및 리스크 진단 분석

결과물은 심층적인 SAP 데이터 프라이버시 및 리스크 평가 분석 문서로 정리되며, 이를 통해 귀사의 비즈니스 부서, 컴플라이언스 팀, 데이터 보호 책임자(DPO)가 SAP 환경 내 리스크 수준을 이해할 수 있도록 지원합니다.

해당 내용은 프로젝트 이해관계자와의 후속 미팅에서 발표되며, 제공 범위에 대한 비용 개요도 함께 제시됩니다.



REPORT:

Enhanced Discovery Report (선택적 추가 서비스)

추가로 2일의 투입을 통해, 전략적 파트너인 Soterion과 함께 Enhanced Discovery Report를 제공합니다. 본 보고서는 SAP 시스템 내 데이터 프라이버시 리스크와 접근 권한 리스크를 모두 고려합니다. Soterion은 SAP를 위한 비즈니스 중심의 GRC(Governance, Risk and Compliance) 솔루션 구축에 집중하여, 리스크에 대한 비즈니스 책임성을 강화합니다.

SAP 시스템에서 파일을 추출하여, 로컬 데이터센터에 호스팅된 Soterion의 임시 인스턴스에 로드한 후 분석을 수행하고 결과를 제공합니다.

Soterion은 표준 접근 권한 리스크 규칙(rule-set)을 보유하고 있습니다. 이미 GRC 솔루션을 운영 중이든 아니든 관계없이, 사전 구성된 해당 규칙을 통해 컴플라이언스 상태를 측정할 수 있습니다.

본 고급 서비스에서 제공되는 주요 인사이트는 다음과 같습니다.

개인정보 데이터 액세스 리스크	직무 분리 (SOD)	국가 간(법적 관할권 간) 데이터 액세스	중요 트랜잭션 리스크
대부분의 GRC 솔루션은 직무 분리(SOD) 및 부정 방지에 초점을 맞추고 있습니다. Soterion은 이러한 기능을 수행할 뿐만 아니라, PII 데이터에 접근 가능한 사용자를 식별 및 분석하기 위한 규칙도 구현합니다.	예를 들어, 지급 요청과 승인 권한을 모두 보유한 사용자는 누구입니까? Soterion은 시스템 내에서 상충되는 접근 권한을 보유한 모든 사용자를 식별합니다.	미국 사용자가 유럽 직원 또는 고객 데이터에 접근할 수 있습니까? 또는 그 반대의 경우는 어떻습니까? 그렇다면, 데이터 실드(Data Shield)를 구성할 경우 어떤 사용자에게 영향을 미치게 됩니까?	테이블 유지 보수에 직접 접근 권한이 있거나, 프로그램을 직접 실행할 수 있는 사용자는 누구입니까? 벤더 및 고객 마스터 데이터 유지 보수는 적절한 사용자로 제한되어 있습니까?

이러한 보고서를 포함하여, EPI-USE Labs와 Soterion은 데이터 프라이버시 및 접근 권한 리스크 전반에 대한 벤치마크 리스크 진단을 제공하며, 해당 리스크를 해결하기 위한 권고 사항도 함께 제시합니다.



글로벌 소프트웨어 솔루션 및 매니지드 서비스 기업인 EPI-USE Labs는 SAP 및 SAP SuccessFactors 시스템의 성능, 운영, 보안을 극대화할 수 있도록 지원합니다. 고객들은 EPI-USE Labs가 어떻게 비즈니스 운영을 혁신했는지를 매일같이 이야기합니다. 귀사의 비즈니스 과제를 어떻게 해결할 수 있는지 알아보려면 문의해 주세요.

epiuse.com | sales@labs.epiuse.com
EPI-USE Labs는 Group Elephant의 멤버입니다.

