SAMSUNG SDS

REAL 2019

REALIZE YOUR VISION
THROUGH DIGITAL TRANSFORMATION

2019 . 5 . 8 . WED . The Shilla Seoul

개인신용정보 오남용 모니터링 시스템 구축 및 활용 사례

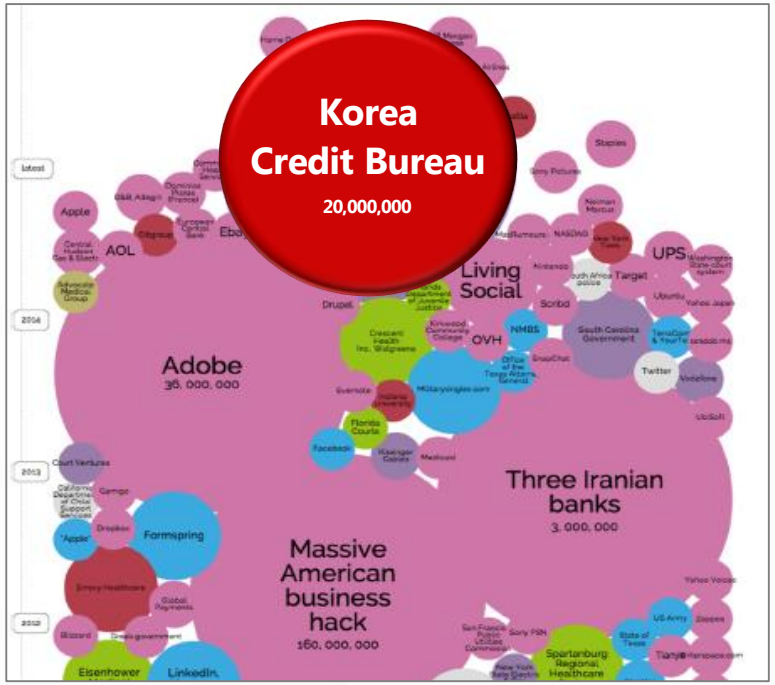
NH농협은행 IT보안부 김유경 부장

정보 유출이 기업에 미치는 영향

정보유출 사고는 기업에 막대한 피해를 입힐 수 있기 때문에 **기업 보안 관점에서 방지 체계 구축이 생존을 위한 필수 조건임**

2014.x.xx

World's Biggest Data Breaches and Hack



[20 Million People Fall Victim to South Korea Data Leak]

- The personal data of at least 20 million bank and credit card users in South Korea has been leaked, **one of the country's biggest ever breaches.**

Many major firms in the South have seen customers' data leaked in recent years, either by hacking attacks or their own employees.

In the latest case, an employee from personal credit ratings firm Korea Credit Bureau (KCB) has been arrested and accused of stealing the data from customers of three credit card firms while working for them as a temporary consultant.

* www.informationisbeautiful.net 참조

피해 상황

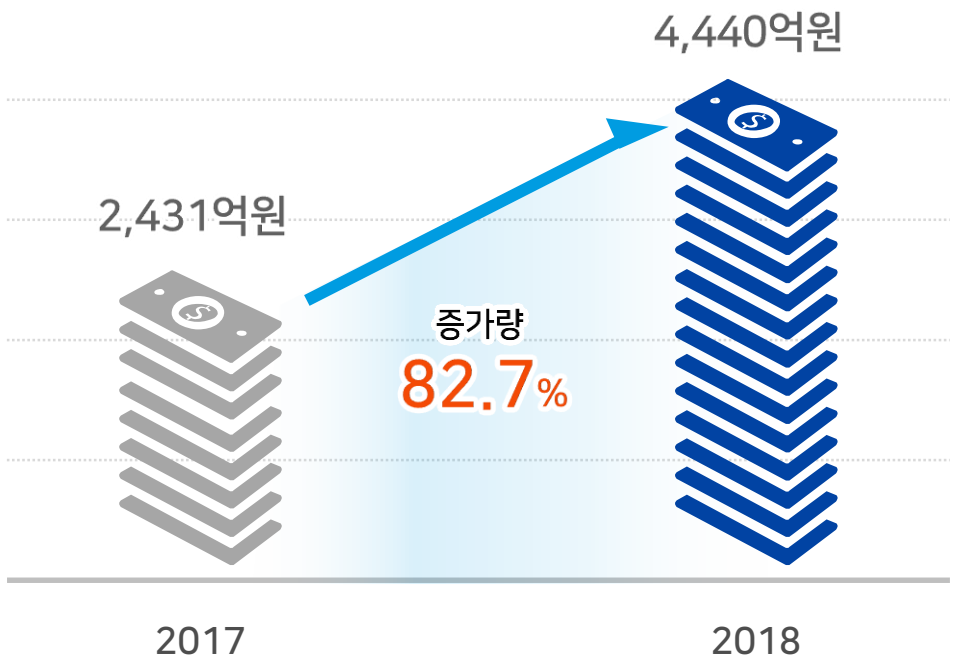
고객정보 유출건수	2500만 건
소송건수 및 소송액	126 건 (약 104억 원)
영업정지	3 개월
과징금	매출 1%
TRUST	신뢰도 하락

* [더스쿠프] 카드3사 고객정보 유출사건 3년의 기록 참조

유출 정보 악용에 의한 대표적 피해 사례

최근 정보 유출을 통해 불법적으로 취득한 정보를 악용하는 사례가 증가하고 있어 이에 대한 기업의 대응이 절실한 상황임

유출된 개인정보로 인한 2차 범죄, 보이스 피싱 피해액 사상 최대 (전년比 82.7% ↑)



피해자도 30,919명에서 48,743명으로 약 58% 증가함

* [금융감독원] 2019 보이스피싱 피해 현황 참조

정보유출에 따른 기업 경쟁력 약화

그 외 국가 핵심기술에 대한 **정보유출 시도 지속 발생** 中

- [조선] 석유 시추선 핵심 설계도면 유출 (’16.11月)
- [화학] 태양전지 핵심 소재기술 해외 유출(’16.9月)
- [제조] 차량용 변속기 검사장비 기술 유출(’15.3月)
- [통신] 첨단 이동통신 중계기 기술 유출(’14.9月)

* [서울경제] 1,500억 투입한 알짜기술 뺏겨… 참조 ** [국가정보원] 산업보안 > 기술유출현황 참조

사전 탐지 및 예방을 위한 새로운 접근

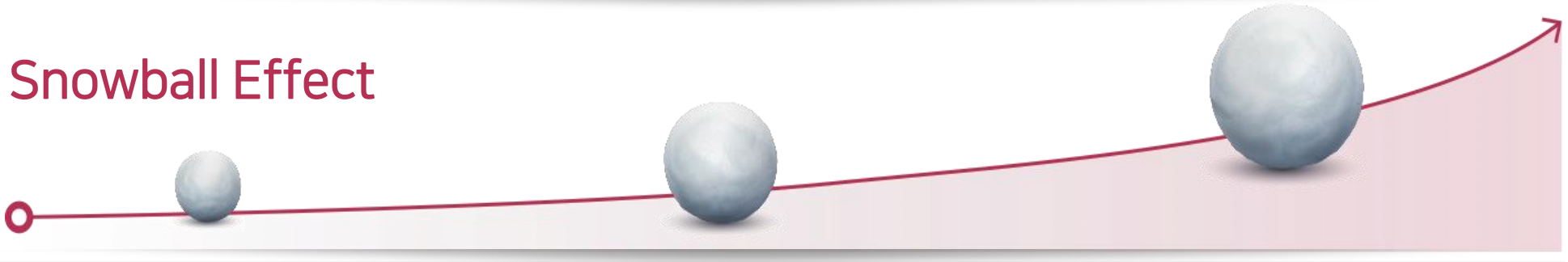
기존 차단 중심의 대응 방식과 달리 사전 탐지와 예방에 중점을 둔 새로운 접근 방식으로 추진이 필요함

개인정보 유출과정

정보 접근 및 저장 → 경로 탐색 → **유출 시도** → 유통 및 활용

피해 정도

Snowball Effect

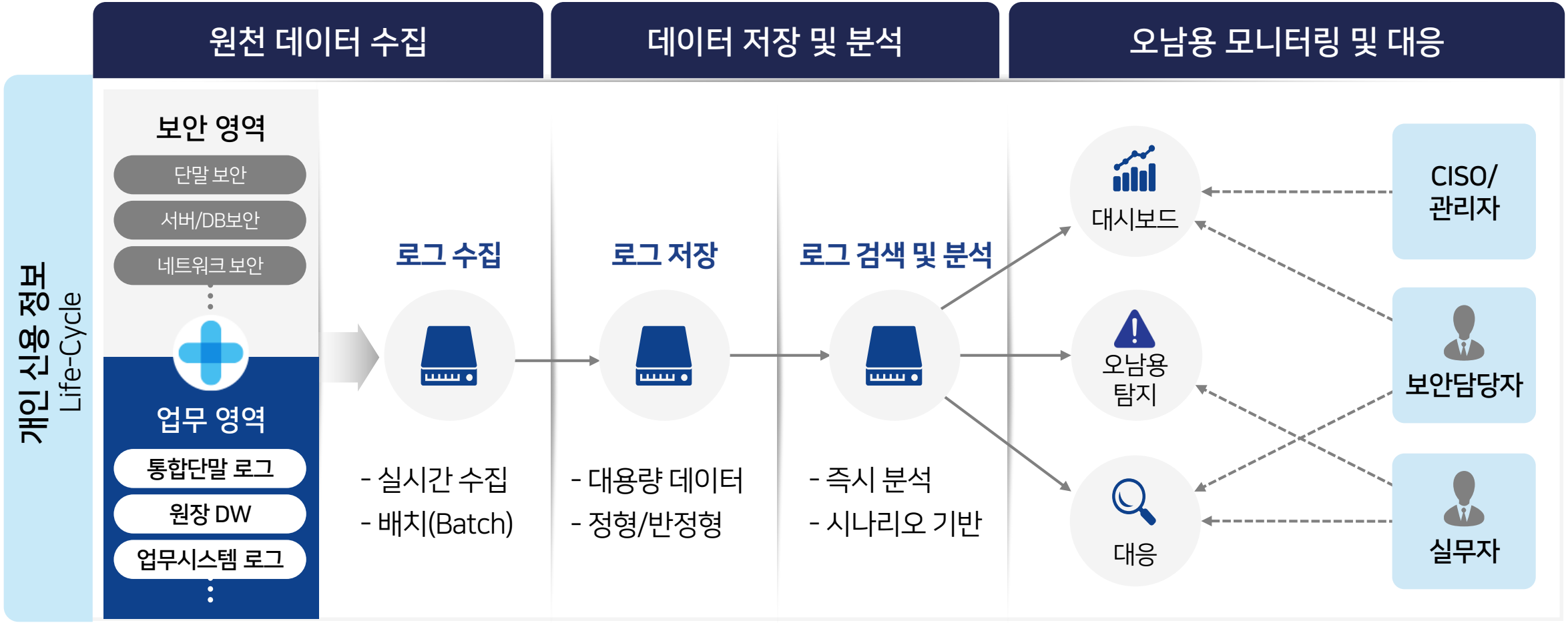


대응 방식

사전 탐지를 통한 예방 및 교육(TO-BE)	유출원인 원천차단(AS-IS)
임직원의 오남용 의심행위 모니터링	매체 제어, 네트워크 및 이메일 사용 통제

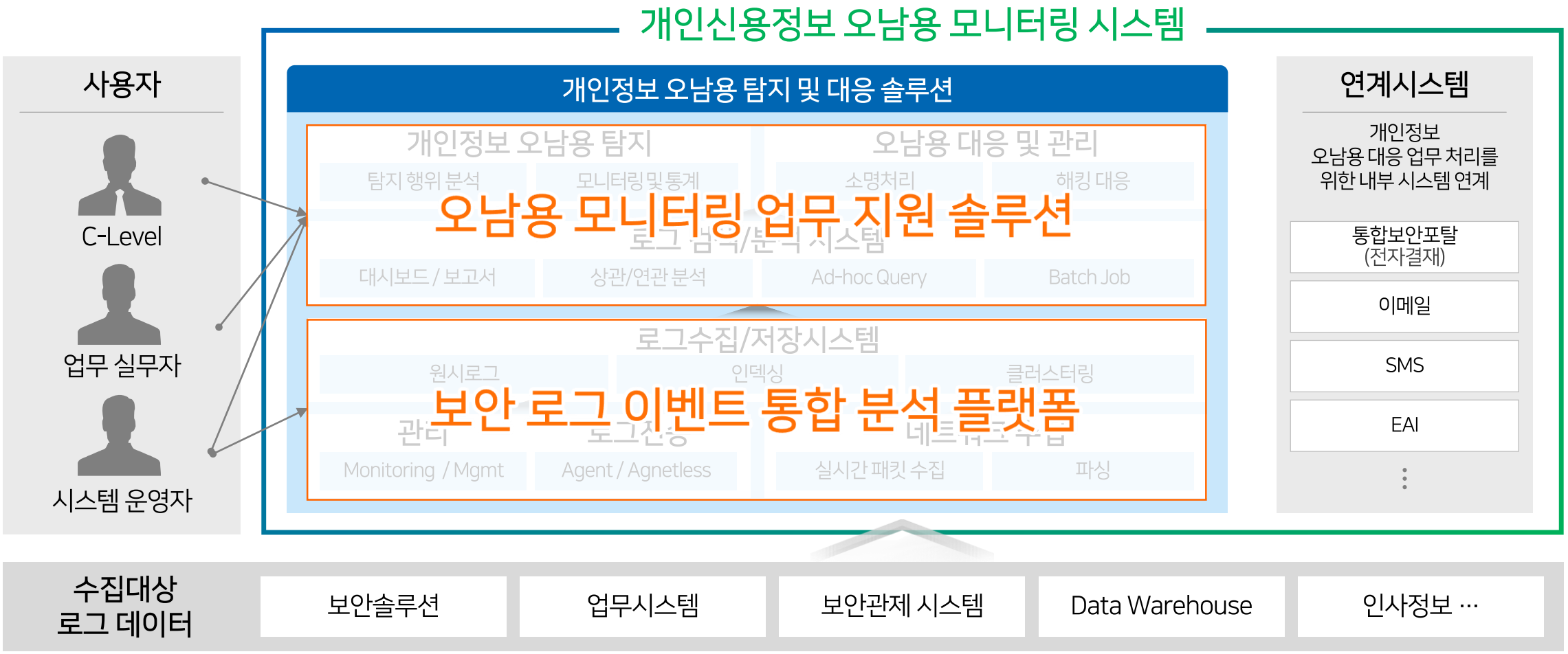
빅데이터 기반 사용자 행위 분석 체계

개인신용정보 Life-Cycle 전 과정에 대한 로그를 빅데이터 플랫폼에 수집/저장하여 오남용 모니터링 및 대응 활동 수행



개인신용정보 오남용 모니터링 시스템 개요

보안 로그 이벤트 통합 분석 플랫폼 + 오남용 모니터링 업무 지원 솔루션 → **개인신용정보 오남용 모니터링 시스템**



탐지 유형별 대응 프로세스 체계화

임직원의 오남용 의심행위 탐지 결과를 유형별로 분류, **유형별 특징에 따라 조치 및 대응 절차 수행**

임직원 유출

- **일반 처리** : 이메일 알림, 전사 게시 등
- **소명 처리** : 사유 입력 → 개인정보 담당자 승인
- **현장 점검** : 소명 처리 後 추가 현장 방문, 테마 점검 등

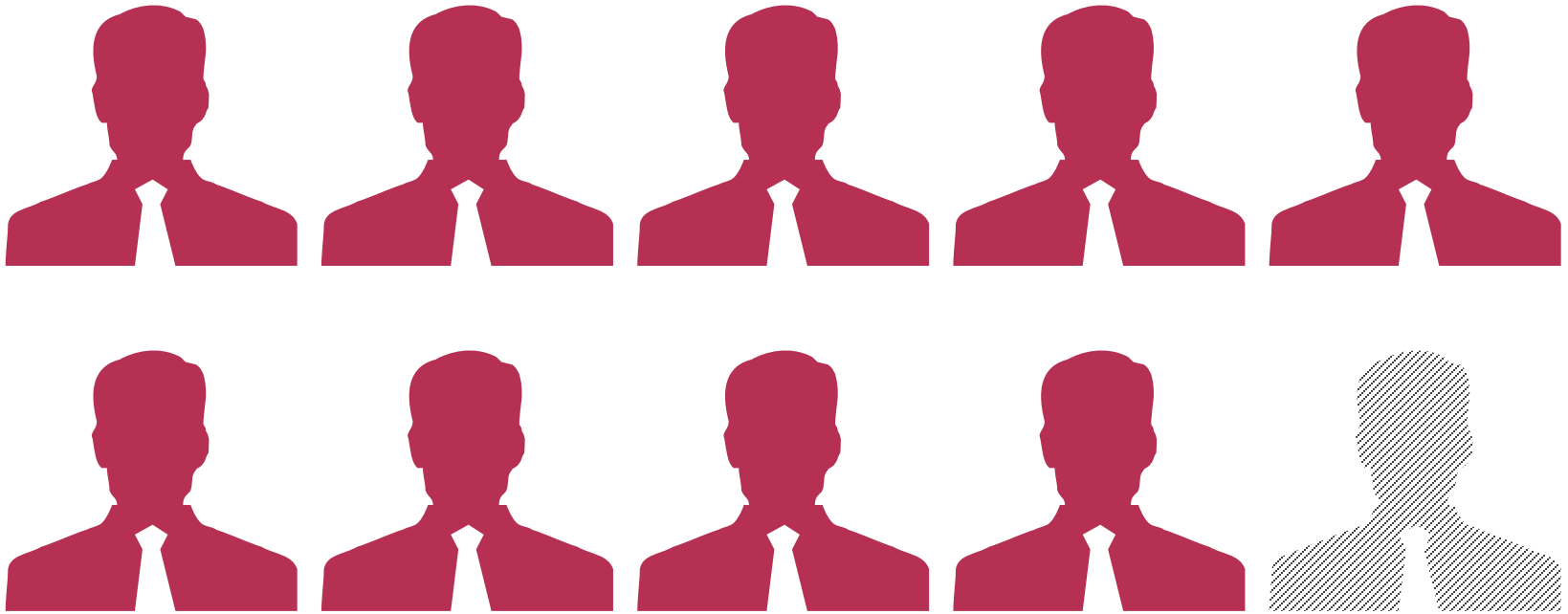
외부 해킹 시도

- **정책 적용** : 매체제어/차단 및 불필요한 권한 회수
- **사용자 행위분석** : 대상 확인 → 보안관제실 유의 모니터링
- **즉시 차단** : 해킹 탐지 → 단말, NW 등 즉시 차단 수행

적중율 높은 오남용 모니터링 시스템 확보

소명 요청 건 中 93%가 실제 오남용 행위인 것으로 최종 판정 → **실효성과 정확성이 검증된 모니터링 체계 구축 달성**

개인정보 오남용 행위 적중율



93%

소명요청 건 中
오남용 최종 판정

정책/기능 모니터링을 통한 기업 보안 수준 향상

시나리오 기반의 보안솔루션 정책적용 현황 모니터링을 통해 **당행 환경에 최적화된 기업 보안 역량 수준 확보**

보안솔루션의 정책적용 모니터링

정책
권한, 접근제어,
인사정보 연동

보안솔루션
PC, 서버/DB,
NW

0

해킹에 의한
개인정보 유출

오남용 모니터링 역량 강화를 위한 중점 추진 과제

- **임직원 업무 특성 프로파일링** : Outlier 탐지 강화
- **일간 외에 주간/월간 누적 시나리오 개발** : 임계치 한계 극복
- **다수 시나리오 연계 분석** : 이상행위 탐지 적중률 Up
- **자동화 & 자동화 & 자동화** : 궁극의 모니터링

조기 경보(Early Warning)

단일 솔루션 → 단일 행위 → 단편적 보안대응

단일솔루션, 단일 행위 중심의 보안

지상레이더 vs 공중조기경보기

입체적, 다각적 모니터링

NH농협은행

데이터 통합

체계적 분석

입체적 보안대응

Thank you

Q&A

SAMSUNG SDS

Realize your vision

www.samsungsds.com