NH농협은행

보안 지능화 대응 및 혁신 전략

농협은행 정보보안부문 김유경부장

목차

NH농협 보안의 터닝포인트

계속 되는 보안 사고 하지만…

“아플수록 더욱 성숙해진다.”

NH 보안 Rebuilding
(14년 ~18년)

금융권 최고수준의 보안 체계 구축을 목표로
정보보호 거버넌스, 단말보안,
인프라보안, 전자금융보안, 개인정보보호 영역에 대한
Rebuilding 추진

14년 정보보안부문 설립

「정보보안 부문 종합대책」104개 프로젝트 수행

NH농협은행

정보보호 프레임워크

NH 보안 지능화 및 혁신전략
(18년 ~ 현재)

Automatic & Intelligence

- 4차 산업혁명등 급변하는 IT환경변화 대응
- 지능화된 공격에 대응을 위한 보안 체계의 지능화
- 복잡해지는 공격징후 탐지 및 보안장비 운영 자동화

디지털 전환 시대의 보안

보안을 리스크 관리의 우선순위에 두고 "디지털 전환" 필요

4차 산업혁명 신기술 등장

AI, Cloud, Big Data, 5G, IoT

정확성↑ 신뢰성↑ 효율성↑

- 디지털 윤리 기준↓
- 신종 금융사기↑
- 신기술 기반 사이버위험 ↑

온오프라인 융합(Big-blur)

금융-ICT 융합,
Big – Tech 기업 금융업 진출

금융 접근성↑ 시장 효율성↑

- 시장경쟁 가속화↑
- 금융규제 무력화↑
- 비즈니스 변화예측 어려움↑

디지털 경제 확대

일자리 변화
데이터 기반 경제 활성화

새로운 일자리 창출↑

- 디지털 디바이드(정보격차) ↑
- 데이터 거버넌스 복잡도↑
- 프라이버시 이슈↑

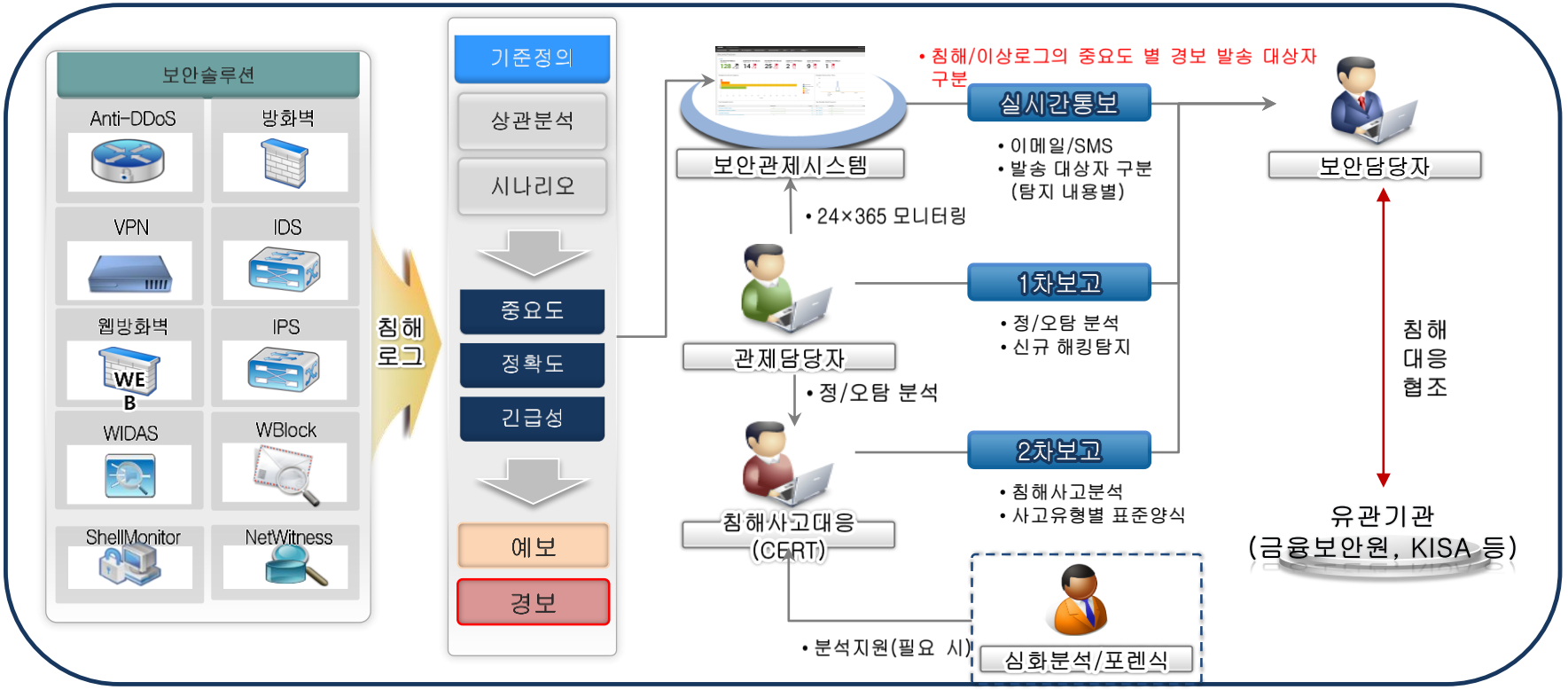
새로운 보안 위협

NH농협은행

차세대 보안관제 시스템

보안장비의 모든 log를 추출(1일 약 1.3TB)하여 빅데이터(Big-Data)로 저장, 보안위협의 실시간 추적 및상관 분석을 할 수 있는 차세대 관제 시스템

- 관제업무 프로세스 자동화
- 관제대상 장비 확대 중
- 다양한 탐지 및 분석 룰(Rule) 운영
- 분석 시간 단축 (1분 이내)



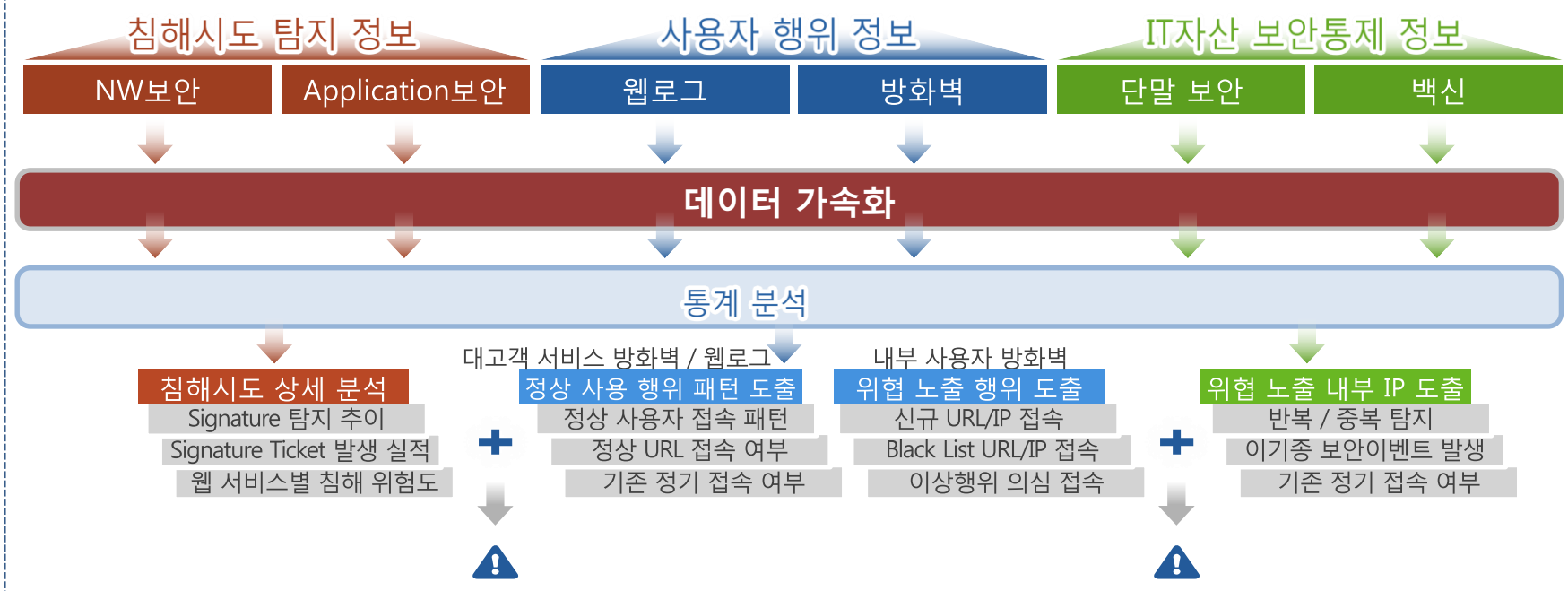
NH농협은행

차세대 보안관제 시스템 (2)

AI를 이용한 위협 탐지의 효과성 분석 중

– 당행 웹어플리케이션 및 방화벽 로그(20일, 4.5Tb)를 이용하여 공개 웹 서비스 신규 침해 위협 탐지 가능여부 검증 중

데이터 심화 분석을 활용한 침해시도 분석 절차



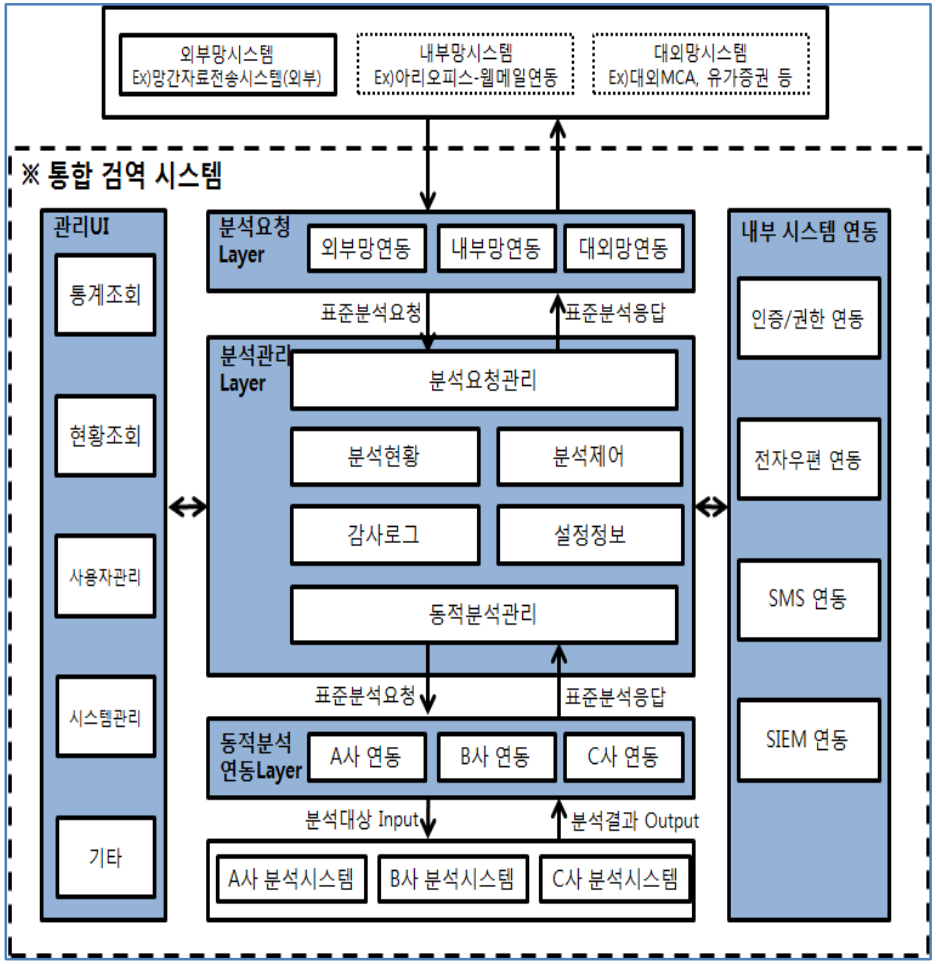
침해시도 탐지 정확도 향상 (시나리오 정교화)
침해시도 분석력 강화 (행위 분석 정보 제공)
침해탐지 검증 수단 (탐지 결과 사후분석 후 확대적용)

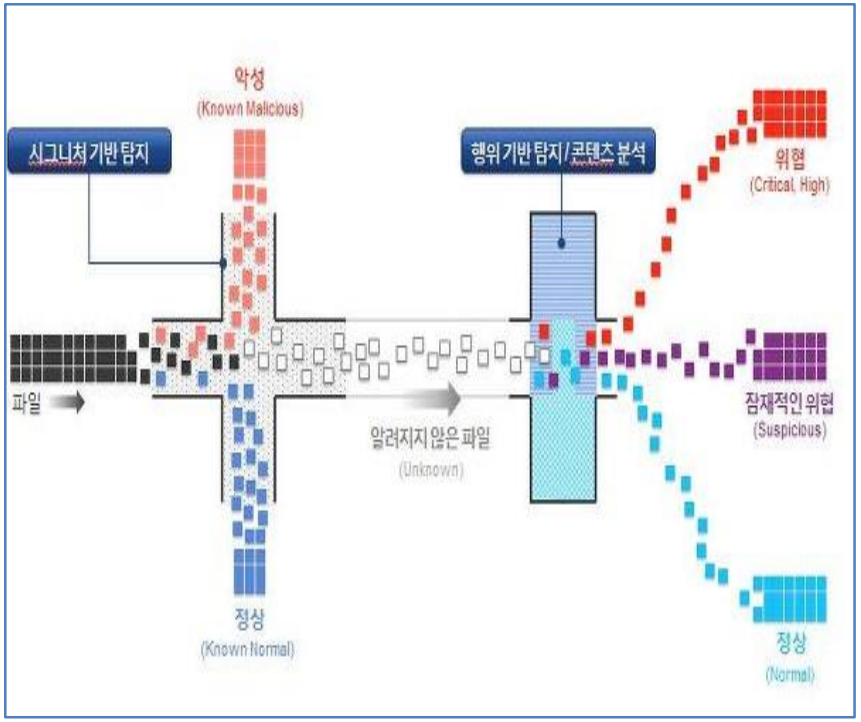
APT 공격 위협 노출 사용자 도출(순위 도출, 임계치)
동일 탐지 건에 대한 탐지 확산(교차 검증)

NH농협은행

악성코드 통합 검역시스템

인터넷, 팩스, 대외망을 통한 유입 파일 및 내부 그룹웨어에서 유통되는 모든 파일에 대한 악성 코드를 전수 검사를 하는 시스템 (SandBox를 이용한 교차 분석 수행)





일 평균 검사건수 : 약 00,000건

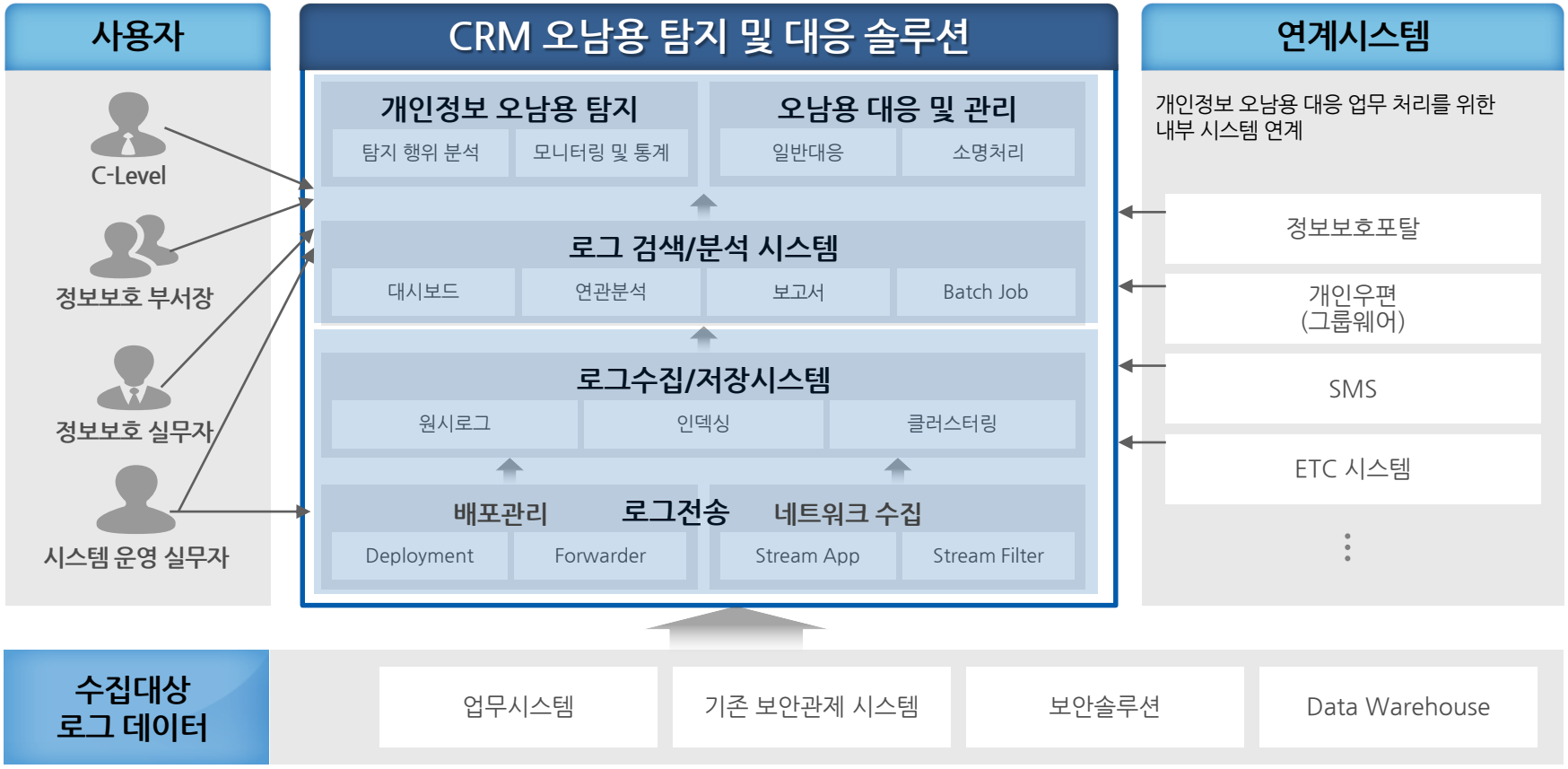
악성파일 의심건수 : 약 0,000건

NH농협은행

개인정보 오남용 모니터링 시스템

내부 업무 중 발생 가능한 개인신용정보 오/남용을 탐지하고 사후관리하기 위한 빅데이터를 이용한 모니터링 시스템

– 개인정보 오남용 시나리오 수립(000개), 오남용 탐지,판정,대응 프로세스 수립



NH농협은행

개인정보 오남용 모니터링 시스템(2)

개인정보 오남용 탐지 및 대응 프로세스

오남용 모니터링	소명	조치 및 사후관리	
빅데이터 기반 오남용여부 정밀분석 업무시스템 로그 (통합업무시스템등) + 보안시스템 로그 (단말보안시스템등)	직원소명 (정보보호포탈)	정상	종결
		미흡	조치, 사후관리

효과 분석

- **소명 요청건 중 OO%가 실제 오남용 행위로 판정**
- **OOO 사무소 현장점검 결과 개인정보 출력 00%감소**
- **사무소별 고객정보 조회량 00%감소**

단말 이상행위 탐지(EDR)(1)

단말 이상행위 탐지(EDR)(2)

침해 사고 지표 (IOC), 머신러닝, 규칙기반 악성코드 검사(YARA), 행위기반엔진(XBA)를 이용하여 단계별 위협을 탐지하여, File less를 포함한 다양한 형태의 악성행위를 탐지

당행 단말 Data를 M/L엔진을 이용한 학습을 통하여 정합성 향상을 위한 마이그레이션 중

이제는?

Security By Desine