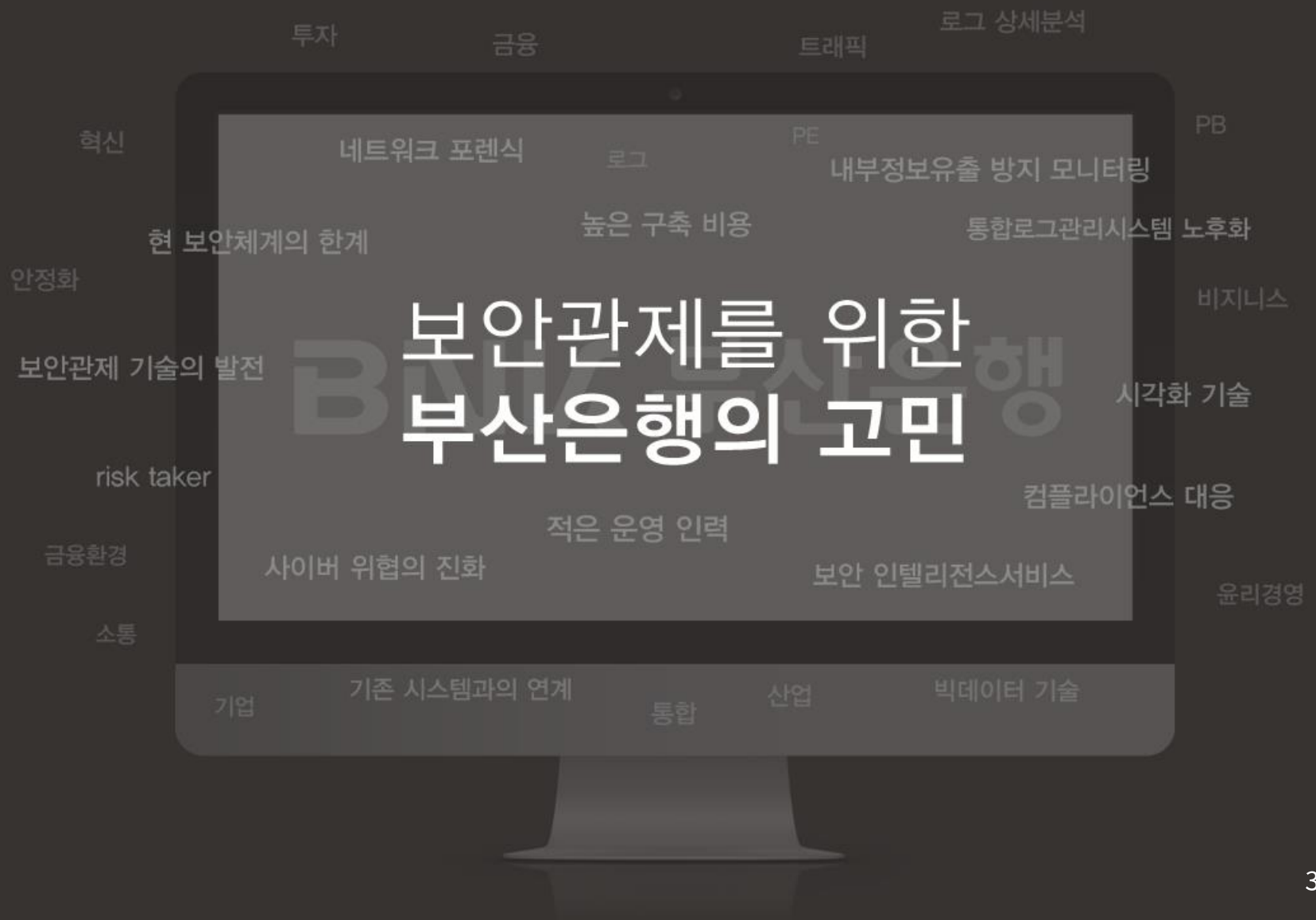
BNK 부산은행

위험관리 기반의
부산은행 정보보호 핵심 전략

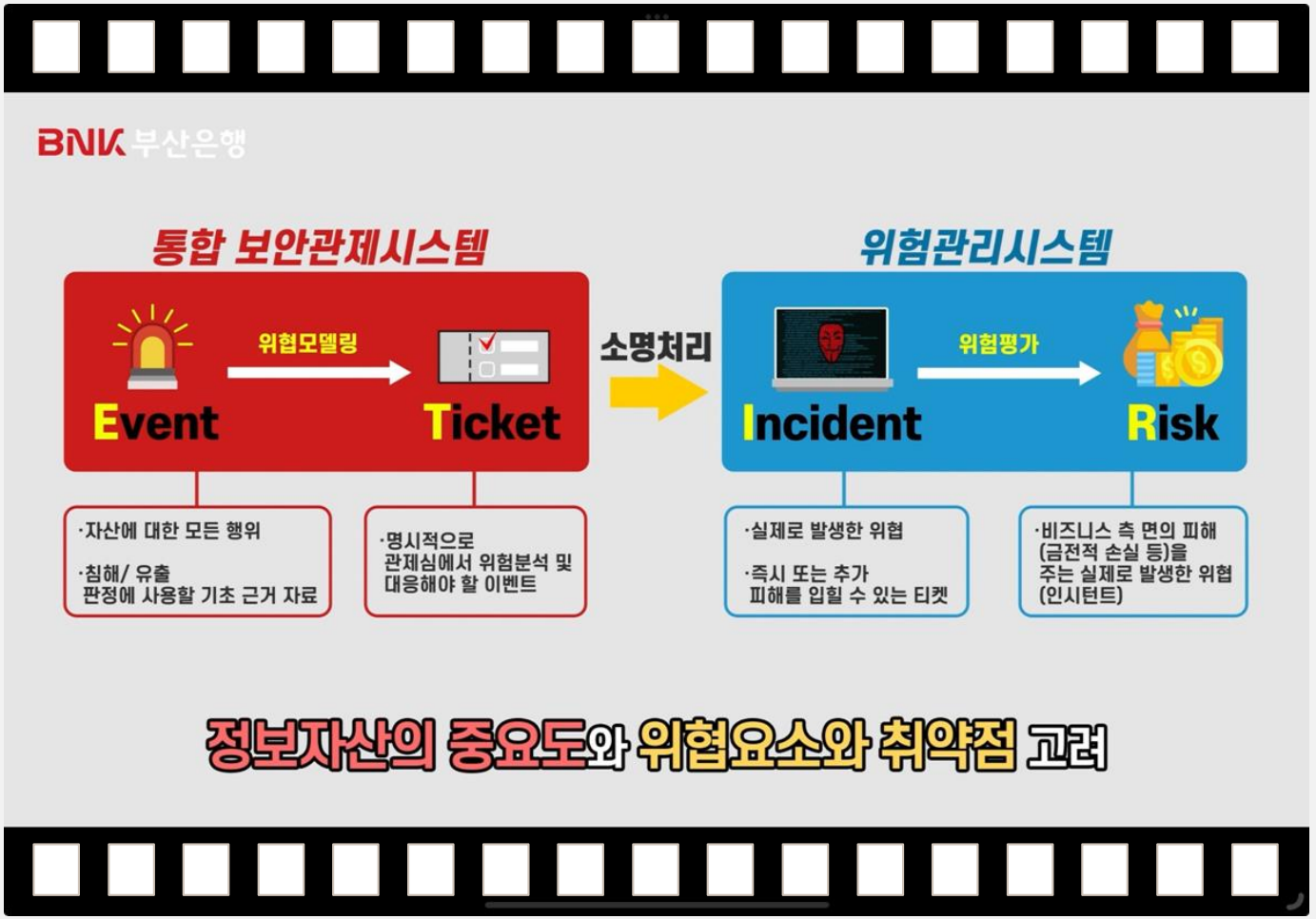
2023.12.07(목)

부산은행 정보보호부
CISO 배진호 상무

목차


투자
금융
트래픽
로그 상세분석
혁신
네트워크 포렌식
로그
PE
PB
내부정보유출 방지 모니터링
높은 구축 비용
현 보안체계의 한계
통합로그관리시스템 노후화
안정화
비지니스
보안관제를 위한
부산은행의 고민
보안관제 기술의 발전
시각화 기술
risk taker
컴플라이언스 대응
적은 운영 인력
금융환경
사이버 위협의 진화
보안 인텔리전스서비스
윤리경영
소통
기업
기존 시스템과의 연계
통합
산업
빅데이터 기술

동영상 시청


BNK 부산은행
통합 보안관제시스템
위협모델링
Event
Ticket
·자산에 대한 모든 행위
·침해/ 유출
판정에 사용할 기초 근거 자료
·명시적으로
관제심에서 위험분석 및
대응해야 할 이벤트
소명처리
위험관리시스템
위협평가
Incident
Risk
·실제로 발생한 위협
·즉시 또는 추가
피해를 입힐 수 있는 티켓
·비즈니스 측 면의 피해
(금전적 손실 등)을
주는 실제로 발생한 위협
(인시던트)
정보자산의 중요도와 위협요소와 취약점 고려

보안의 혁신적인 재설계(Redesign Security)

- SWOT분석으로 조직의 현황을 파악하고, “보안을 혁신적으로 재설계 한다”라는 목표 수립

Strength

- 독자적인 정보보호 통합 플랫폼 구성
- 업무효율화를 위한 관제 운영
- 실시간 빅데이터 기술 적용
- 다차원 시각화 기술을 적용한 데이터 추적
- 보안관제 상황정보 구성

Weakness

- 적은 운영 인력
- 높은 시스템 구축 비용
- 주 52시간 근무제 시행으로 업무시간 축소
- 국내 최초 시도에 따른 시행착오 불가피
- 임직원의 낮은 보안 인식

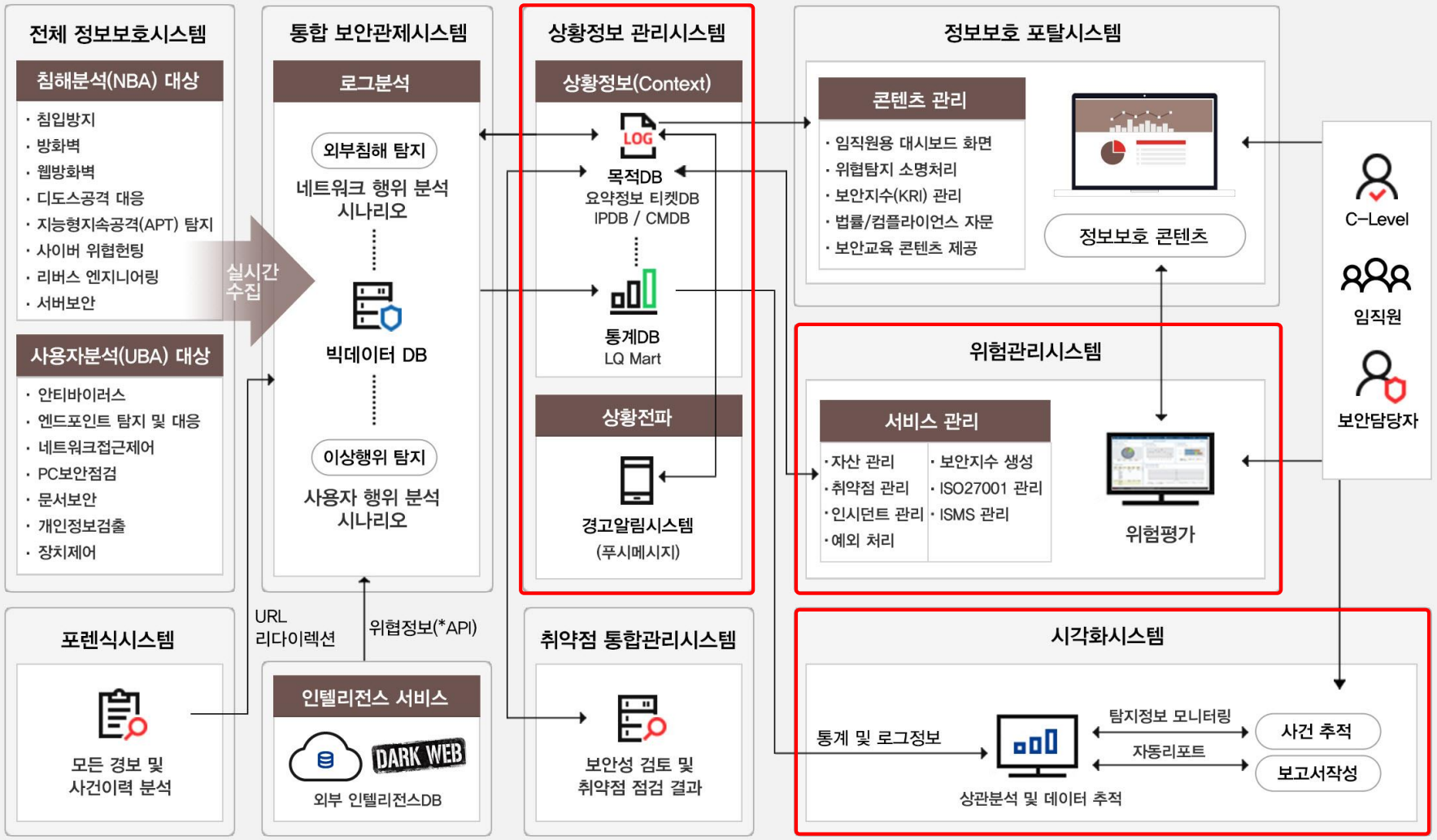
Opportunity

- 4차 산업혁명 시대의 도래
- 빅데이터 기술의 발전
- 사무실 내 정보보호 관제센터 구축
- 전문 관제 및 취약점 점검 인력 충원
- 위험관리 프로세스 적용

Threat

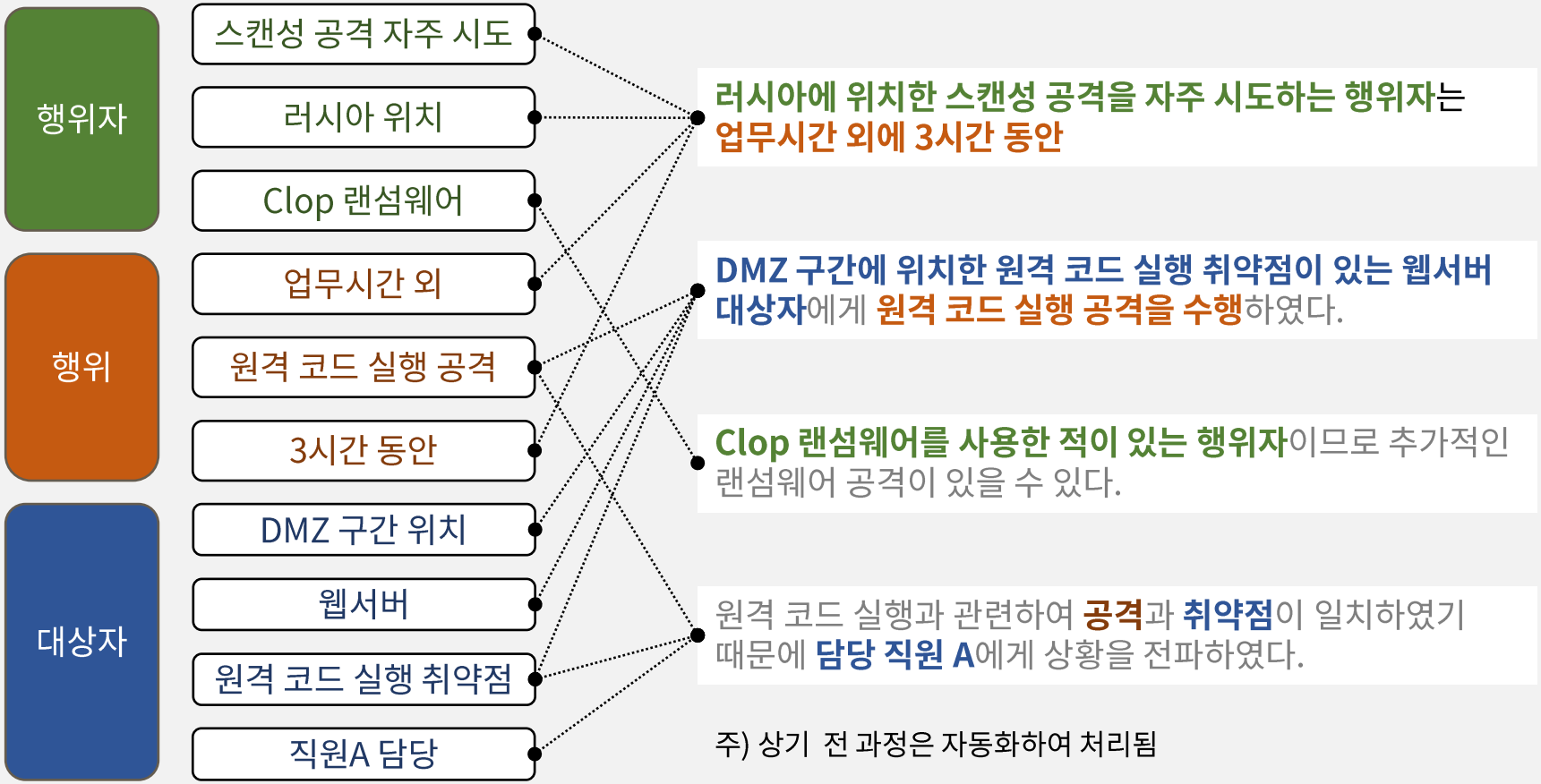
- 고도화된 사이버 위협
- 지속적인 개인정보 유출 사고
- 금융 사고·사기로 소비자 신뢰 하락
- 팬더믹으로 인한 원격 근무에 대한 위협
- 신기술을 이용한 새로운 보안 위협

독자적인 '부산은행 정보보호 통합 플랫폼' 구성 Special



상황정보(Context) 예시

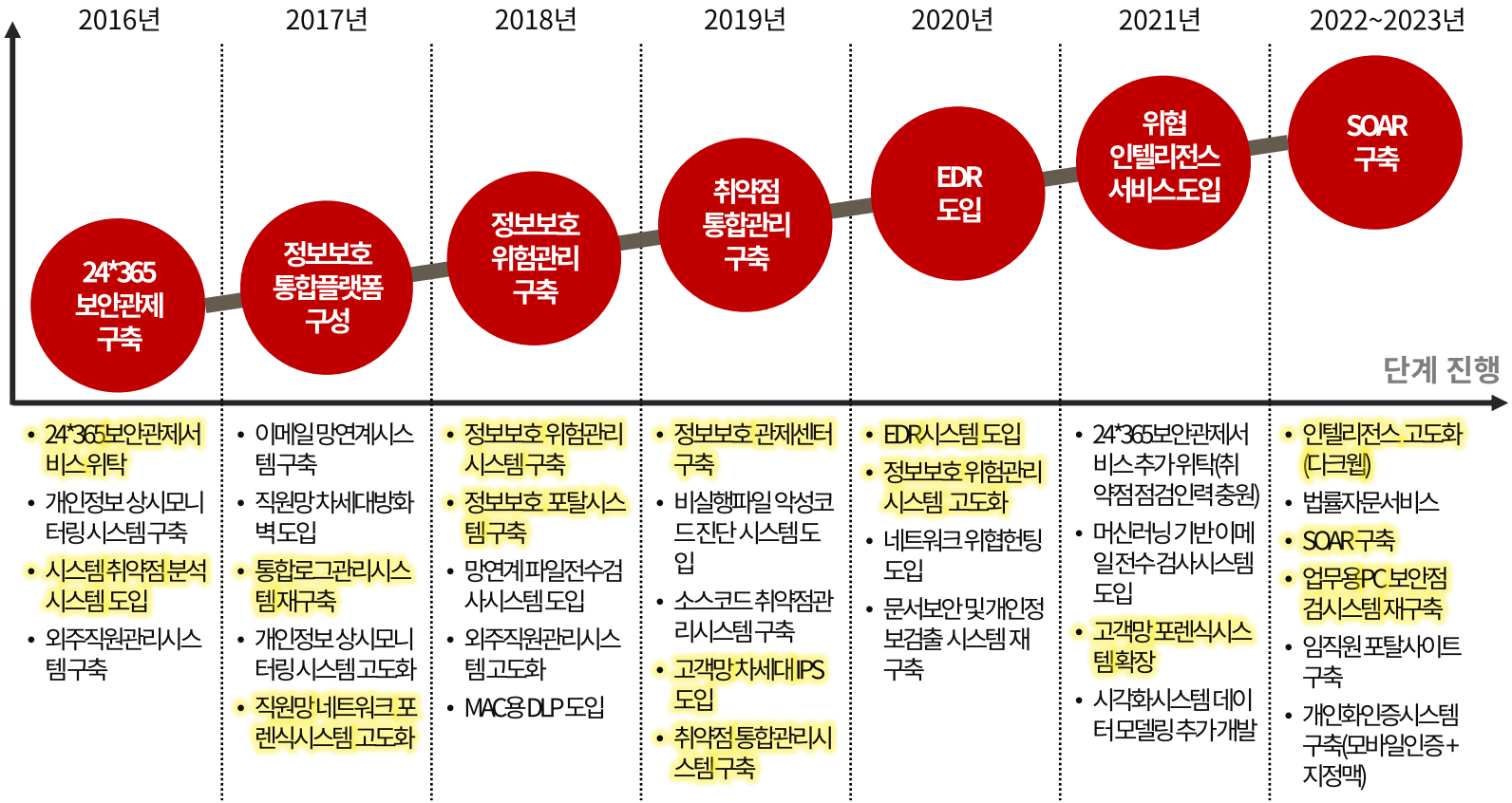
- 상황정보를 활용함으로써 분석 과정에서 수작업으로 확인해야 할 다양한 상황을 정보화 하고 이를 규칙적으로 처리할 수 있는 기틀이 마련됨



주) 상기 전 과정은 자동화하여 처리됨

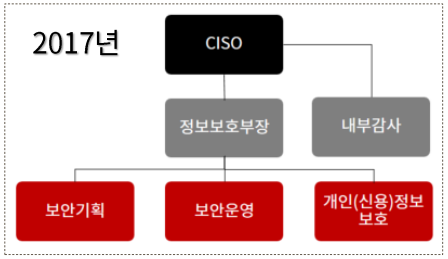
정보보호 인프라 연도별 구축 현황

- 지난 7년간 정보보호 통합 플랫폼 구성 아래 장기적 관점으로 사업 추진



부산은행 정보보호부의 직무 체계 개편 Special

- 효율적인 실시간 위험관리를 위해 위험 3요소(자산, 위협, 취약점)를 반영한 조직 구성 필요
- 2018년부터 One Team 구성(보안기획 + 보안관제 + 보안진단)으로 협업



CISO
CISO, CPO, CIAP

위험관리 담당

정보보호부장
업무 총괄

내부감사
일/월/분기 감사, 특명감사

보안기획
기획, 보안성심의, 정보보호위원회 등

보안관제
정보보안 통합 관제

보안진단
취약점점검, 모의훈련

보안운영
정보보호 시스템 운영, 주요정보 모니터링

개인(신용)정보보호
개인,신용정보 관리

위험관리
이슈관리, 위험평가/관리

사고대응
사고관리/조사, 포렌식

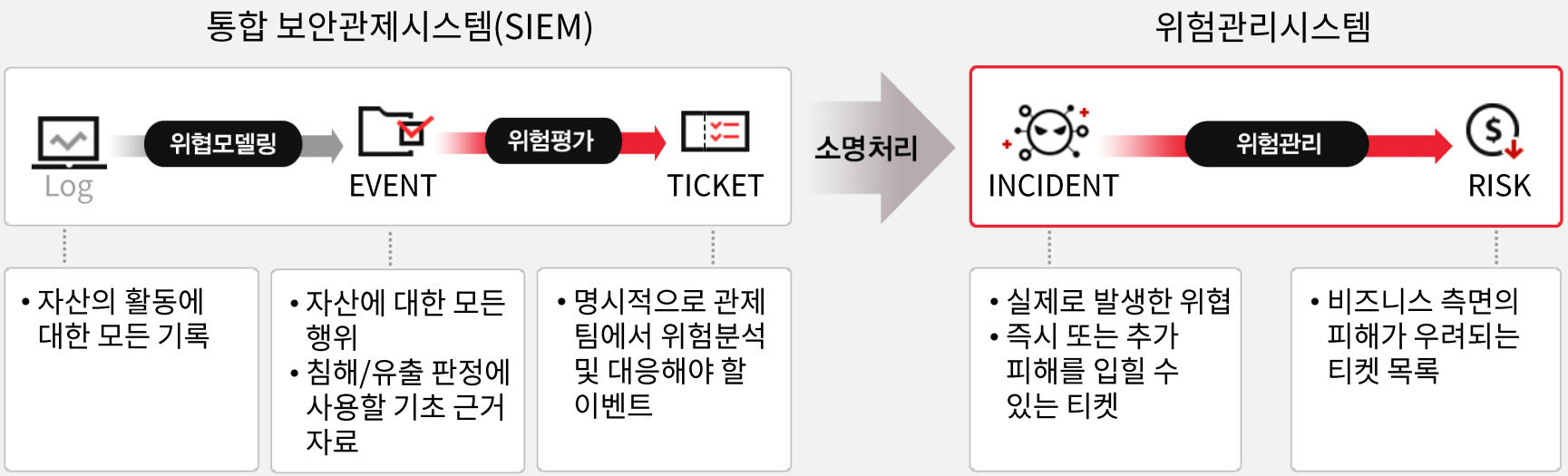
침해대응
정보보호 시스템 운영, 사이버위협 탐지 대응

내부통제
정보보호 시스템 운영, 비즈니스 연속성 관리

- 영국의 CESG(Communications-Electronics Security Group) 참고

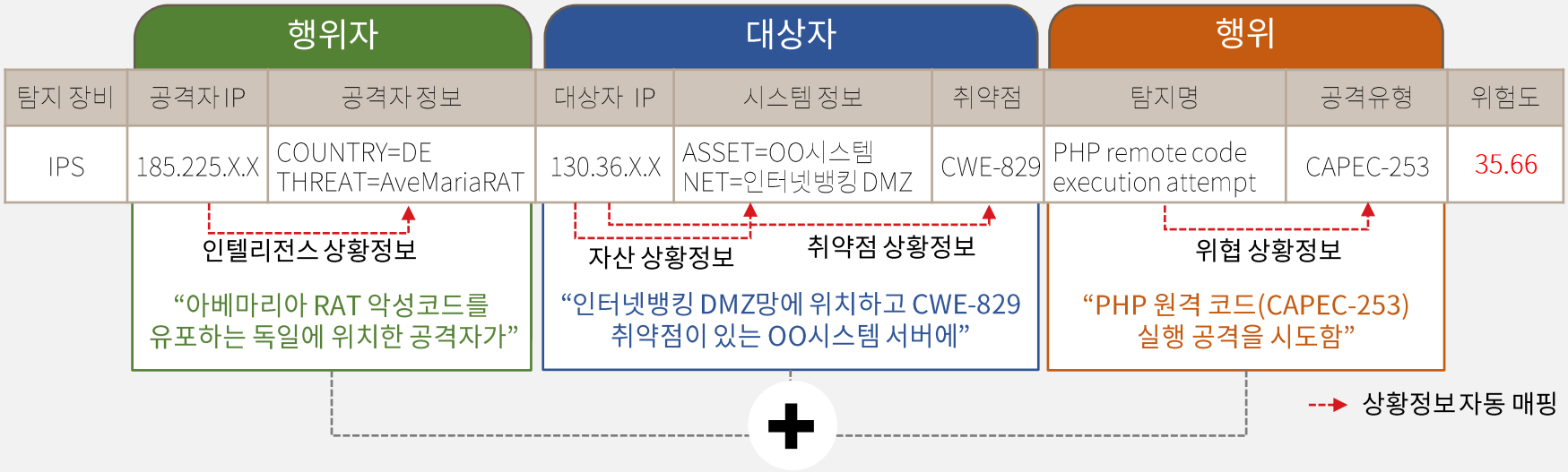
정량적 위험관리를 위한 'ETIR 모델' 개발 Special

- 통합 보안관제시스템과 위험관리시스템을 하나의 프로세스로 연동하여 관리
- 위험관리시스템을 통해 자산에 피해를 주는 위험을 비즈니스 관점에서 정량적 위험 지표로 파악



- ETIR(Event, Ticket, Incident, Risk) 모델: 위협 정보로부터 위험 관리 과정까지를 일원화한 모델
- 정량적 위험관리를 통한 정확한 판단 기준으로 외부 위협에 대응하여 보안관제 업무 효율 향상

ETIR 모델링을 통한 티켓 처리 예시



소명 내용	• 아베마리아 RAT 악성코드를 유포하는 독일에 위치한 공격자가 인터넷뱅킹 DMZ망에 위치하고 CWE-829 취약점이 있는 OO시스템 서버에 PHP 원격 코드(CAPEC-253) 실행 공격을 시도함 • CWE-829 취약점을 가진 자산은 CAPEC-253 공격으로 인한 악성코드 감염 가능성이 높음
조치 내용	• 공격자IP : 방화벽 차단 • IPS 정책 : 탐지 모드 → 차단 모드 변경 • 네트워크 포렌식 : 악성코드 감염 여부 확인
기대 효과	• 방화벽 차단 : 동일 공격자의 다른 유형 공격 차단 • IPS 차단 : 동일 유형 공격 차단으로 유사 공격자 차단

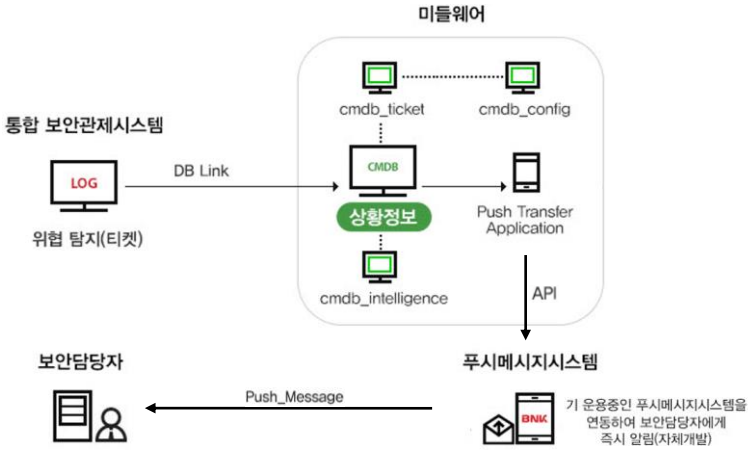
• 과거에 공격 이력이 많은 행위자나 악성코드에 자주 감염되었던 대상자는 사고 발생가능성에 대한 점수를 높여 중요 이벤트의 위험도가 높아지도록 재조정(Rebalancing)함

업무 효율화를 위한 프로세스 자체 개발

- 중요 기능(위협 알림)을 효율적으로 자체 구현하기 위해 오픈소스 API 활용
- 반복적으로 수행하는 업무를 자동화하여 업무 효율성 증대

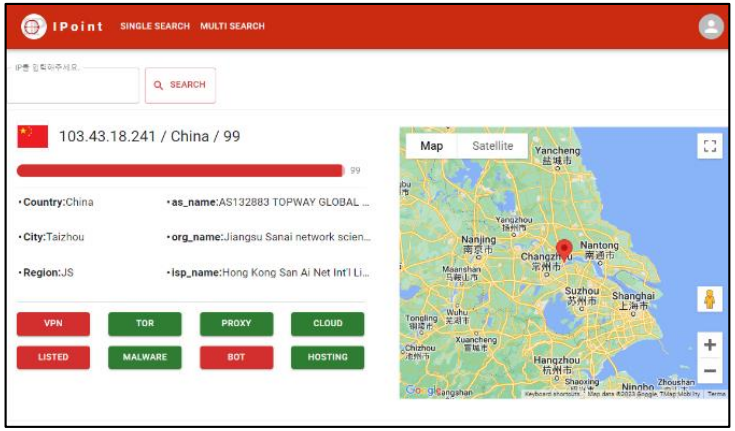
경고 알림 프로세스

- SIEM에서 식별된 위협 정보 중 실시간 대응이 필요한 이벤트 또는 파급력이 높은 위협 도출
- 담당자 그룹에게 알림을 공유하기 위해 텔레그램 API 활용하여 서비스 구현



위협IP 평판 통합 조회 프로세스

- IP 평판 조회 사이트(abuseup 등 6개)를 활용해 정보 통합 및 다수의 IP 일괄 조회 기능 구현(웹)
- 일일 6시간 소요되는 침해지표 검증 및 분석 업무가 30분 이내 수행 가능(IP 300개 기준)



논문 발표 및 기술 백서 출간

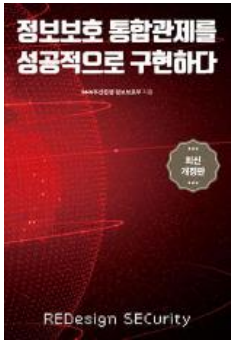
- 2018년부터 4편의 논문 발표와 4번의 국내 금융보안원 및 KISA 공모전 수상
- '정보보호 통합관제' 백서 출간, 전 금융권과 공유하며 수년간 축적한 노하우 공유 금융보안 ESG 실천 높은 평가

논문 발표

- 2019년, ‘ETIR 모델 기반 SOAR 금융보안 관제 설계 및 구축’
- 2020년, ‘정량적 위험 관리를 위한 실시간 위협 분석체계 설계 및 구축
- 2021년, ‘공격 단계 식별을 통한 APT 공격 탐지 프로세스 설계 및 구축’
- 2022년, ‘금융기관 임직원 PC 취약점 점검 고도화 및 위험관리 방안’

기술 백서 출간

- 2019년, ‘정보보호 통합관제를 혁신적으로 재설계하다’



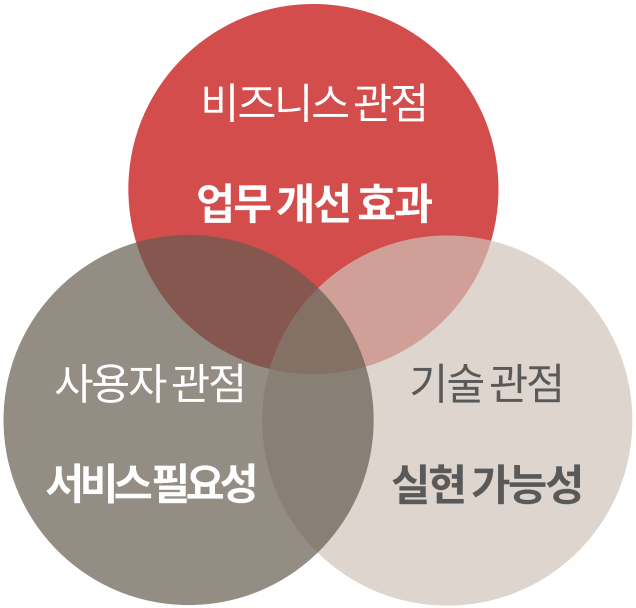
- 2023년, ‘정보보호 통합관제를 성공적으로 구현하다’

협력 社와의 PoC(개념 증명)를 통한 신기술 적용

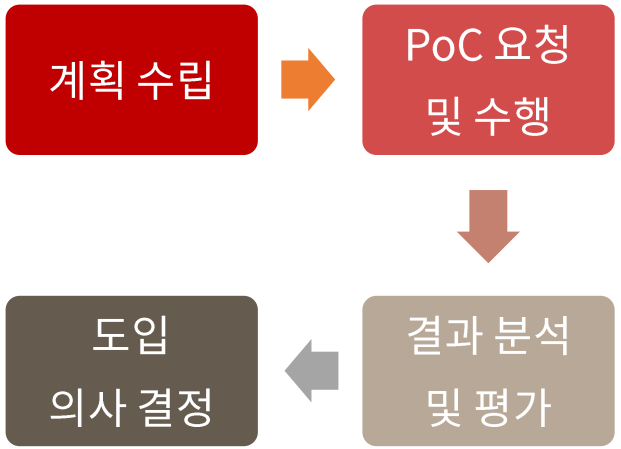
- 신기술 적용 또는 신제품에 대한 사전 검증, 도입 위험 완화 및 사용자 반응 확인
- 부산은행 전략인 '패스트 팔로어'를 기반으로 업무에 따라 '퍼스트 무버'를 병행하여 수행
  - 사례: 리스크 기반 보안체계, 외주직원 관리, 취약점 통합관리, STIG*기반 PC취약점 점검 등

* STIG(Security Technical Implementation Guides, 보안기술 구현 가이드) : 사이버 보안 요구 사항으로 구성된 표준 가이드

PoC에 필요한 3개의 관점



PoC 절차



가시성 확보를 위한 신기술 적용

- 비즈니스 관점의 위험을 평가하기 위해서는 모든 데이터(업무 로그, 자산 취약점, 위협 정보 등)에 대한 빅데이터 분석으로 높은 가시성 확보
- 빅데이터를 쉽고 섬세하게 처리 가능하고 복잡도 높은 데이터 이해를 위한 시각화 적용

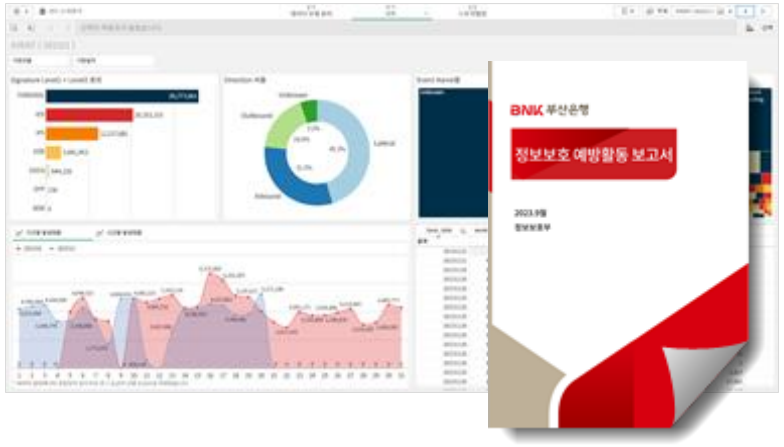
빅데이터 분석

- 자유도가 높은 명령어(SQL문 형태)와 대시보드를 제공하는 빅데이터 시스템 채택
- 위험관리를 위한 추가 기능 요청 및 반영을 위해 국내 전문 솔루션 도입

자체 구성한 위험관리 대시보드

빅데이터 시각화

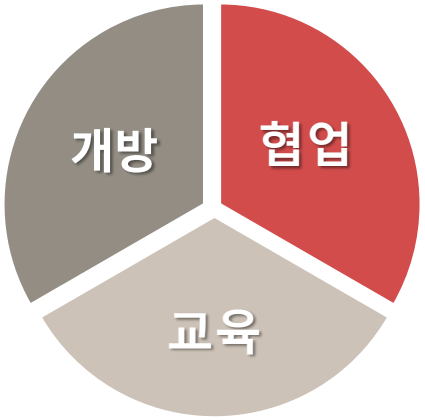
- 시각화시스템의 상관분석, 스토리텔링 등을 이용하여 셀프 분석 및 통합 보고서 구현
- 화이트&그레이 기법을 통한 쉬운 데이터 필터링과 다양한 그래프를 통한 다차원 시각화 표현



보안 역량강화를 위한 커뮤니티 행사

- 보안분야에 종사하는 직원들의 교류와 최신 보안 트렌드에 대한 이해 증진을 위한 행사
- 개방, 협업, 교육을 주제로 누구나 참여할 수 있는 개방적인 행사

오픈 클래스 : SEC



행사명		주요 내용	주기
Security Company Seminar	보안기업 설명회	보안 전문가와 함께 새로운 기술과 제품 등 다양한 주제를 다루는 발표 설명회(부산은행, 경남은행, 그룹사 정보보호 및 IT담당자)	월별
Engineer's Day	엔지니어 데이	부산은행과 관련 있는 협력 社들의 엔지니어, 비즈니스 담당자와의 커뮤니티 행사	연별
Cooperation Class	직원 지식 및 경험 소개	직원들이 업무 수행으로 얻은 지식이나 경험, 개선사항, 자기계발을 통해 습득한 지식 등을 공유	수시

- 보안 역량 향상 및 최신 보안 동향에 대한 이해도 증진
- 직원 간 지식 공유, 협력업체와의 네트워킹 및 외부 전문가와의 협력 강화

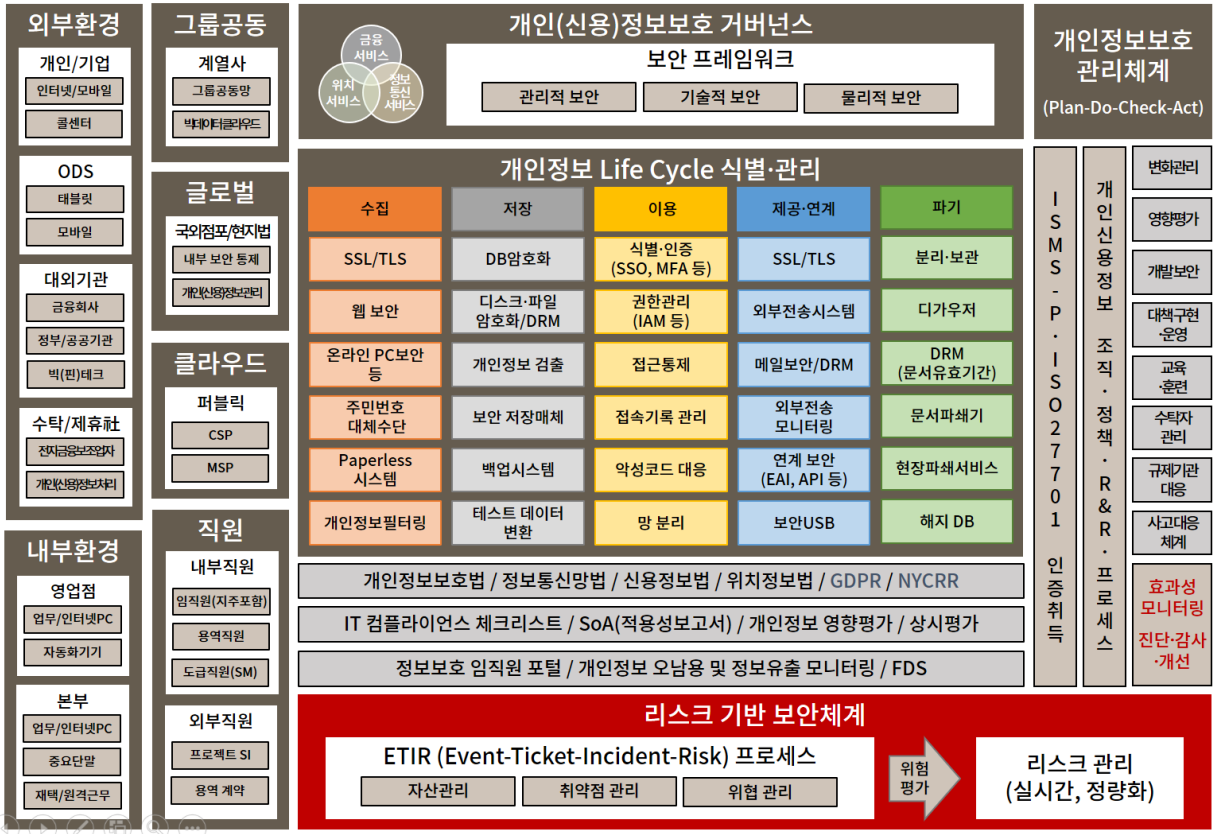
부산은행 정보보호부의 사업 방향

- 리스크 기반 보안체계의 정보보안 업무영역 청사진(Blueprint)

- KB국민은행 정보보호부 청사진 참고

부산은행 정보보호부의 사업 방향

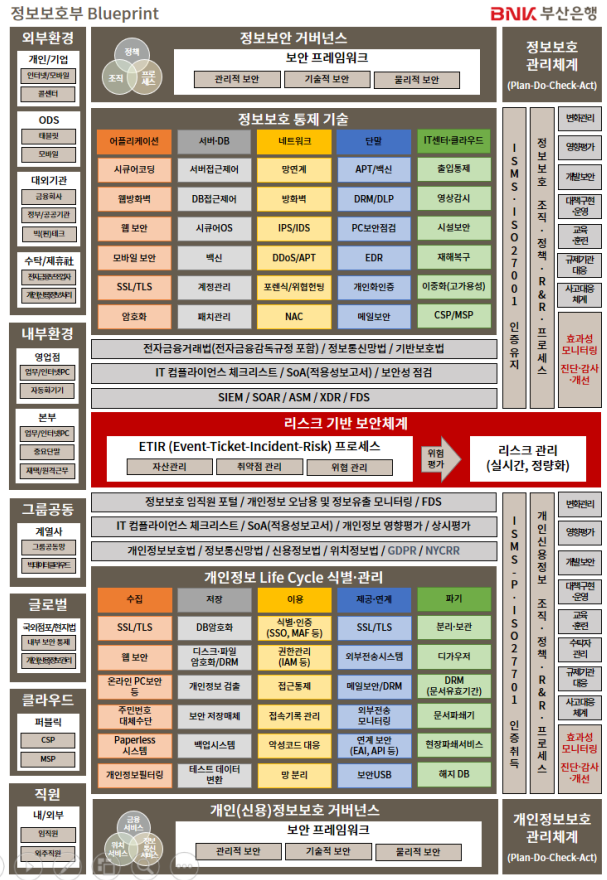
- 리스크 기반 보안체계의 개인(신용)정보보호 업무영역 청사진(Blueprint)



- 제이엔시큐리티 김경하 대표 '개인(신용)정보 보호 주안점' 발표자료 참고

부산은행 정보보호부의 사업 방향 Special

- 정보보안과 개인(신용)정보보호 업무영역을 통합한 부산은행 정보보호부의 청사진(Blueprint)



- 정보보호부는 정보보안과 개인(신용)정보보호 업무영역으로 나뉘어 운영

- 정보보안은 외부 위협 대응을 위한 사이버 보안
- 개인(신용)정보보호는 임직원의 정보유출 및 오남용 방지를 위한 내부통제

- 사이버 보안 대응 통합 보안체계 기반으로 내부 임직원의 이상징후를 파악할 수 있는 내부통제 체계를 포함한 고도화

- 빅데이터 기술의 발전으로 데이터 가시성 확보 및 통합 운영에 따른 인력 효율화와 다양한 관점의 상관 분석 가능

사이버공격의 패러다임 전환(개인 → 국가)

- 최근 해킹 공격은 개인이 아닌 국가(북한, 러시아, 중국 등)의 지원을 받는 해킹그룹에서 시도하고 있음
- 국가 배후 해킹 조직의 사이버 안보 위협 고조로 선제 대응 필요

- 러시아는 우크라이나를 침략('22.2월)하면서 우크라이나의 핵심시설(전력, 통신 등)을 대상으로 사이버공격 수행
- 북한 해킹그룹(안다리엘)은 한국항공우주산업(KAI)을 공격('22.6월)하여 전투기 설계도면 등 기술정보를 탈취함
- 중국 해킹그룹(샤오치잉)은 국내 12개 기관(건설정책연구원 등)을 공격('23.1월)하여 개인정보 탈취 및 홈페이지를 변조함

- 금융보안원, SK쉴더스 등과 통합보안관제시스템을 공동으로 운영하여 침해 사고를 예방하고 있음
  (24시간 보안관제로 매일 평균 2천 건의 공격을 받으며, 이 중 의미 있는 공격으로 20여건 처리함)

BNK 부산은행

은행권 내부통제 개선방안 ('22.10.19 금융감독원 발표)

- 사고 취약 업무프로세스 고도화 방안 中 시스템 접근통제 고도화 추진
- 금융사고 재발 방지를 위한 내부통제 강화를 추진하고 금융사고에 대한 적시 대응체계 마련

고도화 추진 방향

- 은행은 시스템 접근·요청·승인 시 권한 없는 자가 접근할 수 없도록 기존 비밀번호 방식 대신 개인화된 인증방식 적용 추진
  - 개인이 소유한 기기를 기반으로 인증(신분증, 모바일 OTP, QR코드 인증 등) 하는 방식
  - 생체인식(지문, 홍채, 안면 인식 등) 인증 방식
  - 기타 상기에 준하는 수준의 수단으로 은행이 선택한 방식

관리실태 점검 강화

- (접근권한 관리 의무 명시) 은행은 사고예방대책에 시스템 인증 기기 관리 사항(신분증 또는 핸드폰 등 인증 기기 대여·공유 금지)을 명시
- (점검 실시) 부점 자전 감사 또는 명령 휴가 검사 시 이에 대한 관리실태 점검

이행 시기

- 예산 등 감안 중요 시스템은 '24.1월, 기타 시스템은 '24.7월 시행

금융보안규제 선진화 계획 ('23.2.24 금융감독원 발표)

- 디지털 금융혁신 下 새로운 리스크에 효과적으로 대응을 위한 금융보안체계, 보안규정 및 관리·감독 방식의 선진화 추진
- 現 금융보안 규제는 급변하는 디지털 환경변화와 보안리스크에 효과적으로 대응하기 곤란

- 금융위원회(전자금융과) 주도의 총괄 TF와 업계 TF로 구성하여 규제개선 로드맵 도출
  - 총괄TF : 금융위원회, 금융감독원, 금융보안원 실무진으로 구성, 민간자문위원회 설치・운영
  - 업계TF : 시장 이해관계자의 의견을 수렴・전달하는 채널로 활용

보안 거버넌스 개선	보안 규제 정비	관리・감독 선진화
• 금융보안을 금융회사 등의 전사적 차원에서 준수하는 핵심가치로 제고 • 보안체계를 리스크 기반의 '자율보안체계'로의 전환 추진	• 목표·원칙 중심으로 규제를 전환하고, 세부사항은 가이드 형태로 전환 • 자율보안체계 미 구축, 보안사고 발생 시 사후 책임 강화	• 규정 위반여부 감독 중심 → 자율보안체계 이행 등 검증 중심으로 전환 • 금융회사 등의 보안 거버넌스 구축 지원 강화

- 이미 정량적 위험관리를 통한 통합보안관제 체계를 구축・운영하고 있으며, 최근 '정보보호 통합관제' 백서를 출간해 금융보안원 회원사 및 대학교 등에 배포하여 수년간 축적한 관련 노하우를 공유함

제2차 금융분야 보이스피싱 대책 ('23.2.28 금융감독원 발표)

- 보이스피싱과 같은 민생침해 범죄가 증가할 수 있어 정부는 보이스피싱 엄단을 국정과제로 발표, 대응

- 가상자산을 이용한 보이스피싱 피해구제를 위해 가상자산사업자 및 가상자산에도 통신사기피해환급법을 적용하고, 숙려기간 등을 도입해 가상자산 현금화에도 대응
- 금융회사와 간편송금업자간 보이스피싱 관련 계좌정보를 공유하여, 간편송금을 이용한 보이스피싱의 신속한 피해구제 도모
- 계좌의 일부 지급정지를 허용하여, 통신사기피해환급법상 지급정지 절차를 악용한 통장 협박*의 피해자 구제

  * 계좌가 공개된 자영업자 등에게 소액 송금 후 자영업자 등의 계좌 지급정지

- 24시간 대응체계를 구축하여 은행권 보이스피싱 대응 강화

- 부산은행은 고객 모바일에 '악성 앱 및 명의도용 탐지사기방지 서비스'를 최근 11월 2일부터 시행하고, 보이스피싱 범죄 근절을 위해 더욱 보안을 강화하고 있음

2024 디지털금융 및 사이버보안 이슈 전망 ('23.11.02 금융보안원 발표)

- 정보보호 조직이 통제하는 기술적 영역을 벗어나 임직원 모두 필수적으로 보안을 체득하고 일상에서 이를 적용할 수 있도록 금융보안 프렌들리(Friendly) 전략을 수립·이행할 필요
- 급변하는 금융IT 환경변화에 맞춰 정부는 목표·원칙 중심의 규제, 위험기반 보안을 강조하는 자율보안체계로의 전환을 추진

※ 가트너(Gartner)는「'23년 9가지 주요 사이버 보안 트렌드」에서 '27년까지 기업의 절반이 '인간중심' 보안 설계를 채택할 것으로 전망(보안을 인간중심으로 설계하여 편의성과 자율성을 보장하면서도 일정 보안수준을 유지)

디지털 금융 정책	보안 위협	IT 혁신
• 더 이상 거스를 수 없는 패러다임, 자율보안체계 전환 • 깨지지 않는(anti-fragile) 탄력성, 사이버복원력 • 클라우드 마이그레이션, 하드웨어 넘어 소프트웨어로	• 공격 채널의 다양화, 영역을 넘나드는 hybrid 위협 고조 • S/W 공급망 공격 성행, SBOM의 중요성이 강조 • 피싱 범죄, '내 얼굴과 목소리 까지도?' 딥페이크 기술 악용	• 모든 것을 담는다, 디지털 지갑 경쟁 가속화 • AI의 안전성과 신뢰성 확보, 책임감 있는 AI 구현 • 사물과 디지털금융의 만남, 금융 사물 인터넷(FoT)

2024년도 부산은행 정보보호 주요 전략

잠재적 위협대응으로 위험 감소

- 사이버 해킹 및 정보유출사고 ZERO 달성
- 오픈소스 활용을 위한 보안 취약점 관리
- 공격 표면의 리스크 관리를 위한 ASM 운영
- 위협 탐지·사고 대응을 통합한 XDR 운영

전자금융 대면 거래 사기 예방 확대

- 악성 앱 및 명의도용 탐지사기방지서비스 시행
- 보이스피싱 피해방지 모니터링 강화
- 대외기관과의 공조체계 수립

내부통제 강화로 보안의식 고취

- 개인화인증시스템 구축으로 금융사고 예방
- 임직원 정보보호 포털사이트 운영을 통한 내부통제 강화
- 제로 트러스트 업무환경 구축

개인(신용)정보관리 보안 강화

- 개인신용정보 위·수탁 및 제휴업체 관리 시스템 구축
- 개인정보 모니터링시스템 확대 구축
- 수탁사 대상 보안 전수 점검 및 교육 실시

내부 임직원 내부통제 강화

- 향후 통합보안관제 체계를 계속 안정화하고, 이를 기반으로 외부 보안 위협 뿐만 아니라 내부 임직원의 이상징후를 파악할 수 있는 내부통제 체계를 포함해 고도화 예정

자율보안체계 수립

- 규칙(Rule)에서 원칙(Principle) 중심의 감독규정 정비에 대응하기 위한 내부통제 영역 위험관리 기반으로 확대

프렌들리 전략

- 정보보호 임직원 포털사이트 운영(구축 완료)
  - 직원별 보안활동지수 및 이상징후 소명 처리
  - 숏컷 드라마 형식의 교육 영상 제작으로 친근감 있는 교육 환경 구현

제로트러스트 환경 구성

- ID통합, 모바일 통합인증 및 지정맥 인증 등 개인화 인증시스템 운영(구축중)
  - Identity 식별, 인증 로깅부터 단계별 추진

안전한 오픈소스(OSS) 활용을 위한 보안 취약점 관리 개선

- 로그4j는 대표적인 오픈소스* 프로그램이며, 제품 내에 패키지 형태로 포함되어 취약점이 발견될 경우 해당 프로그램 사용 여부를 상세히 파악하기가 쉽지 않음

* 저작권자가 소스코드를 공개하여 누구나 자유롭게 사용, 수정, 재배포할 수 있는 자유로운 소프트웨어

- 오픈소스 취약점 점검 솔루션을 도입하여 소프트웨어 개발 생명주기(SDLC)와 상호 연계하고, 자체 보안성 점검절차에서 취약점과 관련된 보안 위협을 지속적으로 관리함

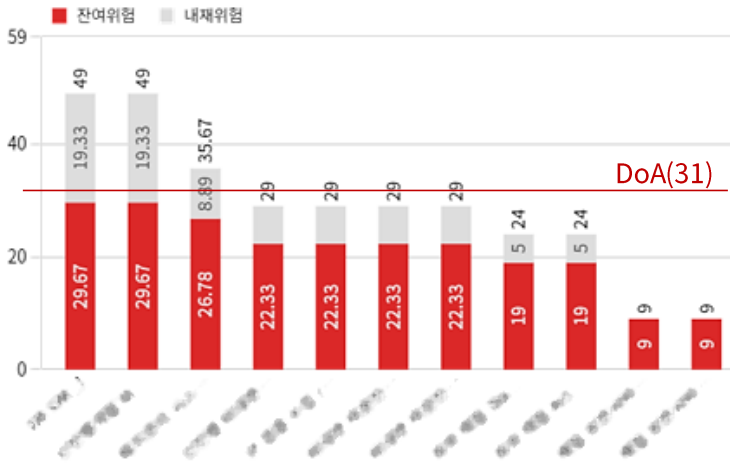
공격 표면의 보안 리스크 관리를 위한 ASM(공격표면관리) 운영

- 가트너는 최근 기업에 대한 성공적인 공격의 1/3이상이 외부와 연결된 자산으로부터 시작되며, 공격표면* 관리(ASM: Attack Surface Management)는 CIO, CISO에게 필수 과제라고 전망

  * 공격표면 : DMZ구간 등 인터넷 기반의 모든 정보자산을 말함

① 자산 식별	② 취약점 점검
네트워크 IP 대역별 스캐닝 후 비식별 자산 검출, 전산 등록 및 중요도 평가 실시	공개된 결함 목록(CVE)의 보안 취약점 점검 및 자산 담당자 조치 요청
④ 위험 관리	③ 위협 탐지
자산의 위험평가 수행 및 지속적인 위험관리를 통해 위험도 감소	외부 공격에 대한 보안위협, 실시간 탐지 및 차단 자동화

☞ 분기감사 적용 예정(절차 검증 완료)



[부산은행 DMZ구간 자산별 위험도 Top]

- 공격자들은 열려 있는 단 하나의 포트로도 침투할 수 있기 때문에 외부에 공개된 정보자산을 평가하고 취약점을 점검해 관리하는 공격표면 관리가 필요하게 됨
- 노출 가능성이 있는 모든 곳에서 기업의 중요 정보자산을 지속적으로 검색하고, 보호해야 할 자산을 분류해 취약점 진단, 다크웹 상에서의 기밀정보 유출 여부를 탐지해야 함

위협 탐지·사고 대응을 통합한 XDR(확장된 감지·대응) 고도화

- XDR(eXtended Detection and Response)은 보안 분석가가 대상을 명확히 하고 효과적인 방식으로 위협에 대응하는데 필요한 종합적인 가시성과 상황 인식을 제공


SIEM


Threat Intelligence


NDR


IDS & Malware Analysis


SOAR

X(eXtended)	D(Detection)	R(Response)
• STIG*기반 PC보안점검시스템 구축 및 EDR 연계로 위협 도출 - 임직원 자체 점검 항목 : 28개 - 보안정책 점검 항목 : 225개	• AI기술 이용한 상관분석으로 그레이 영역 보완 • 제로데이 공격 대응을 위한 위협헌팅 검토 후 도입	• SOAR 도입으로 수동조치대비 100배 효율 증가 예상 • 잔존위험 감소로 수용 가능한 위험수준(DoA) 감소 기대

- XDR은 단일 솔루션 제품이 아닌 보안의 범위를 넓혀 조직의 엔드포인트, 서버, 애플리케이션 등의 다양한 제품을 보안 운영 시스템에 통합한 위협 탐지 및 사고 대응 도구임(2018년 가트너 소개)

Zero Trust(제로 트러스트) 업무환경 구축

- 경계 기반 보안 모델에서 사용자, 자산, 리소스에 초점을 맞추는 방어 전략으로 전환
- 완전하게 인증되고 인가된 사용자 및 디바이스에 한해 접근할 수 있도록 함

구분	아키텍처 설명	부산은행 추진 현황
ID 및 정책관리	• 접근 주체, 자원 정보 관리를 위해 타 시스템과 연계 • ID Life Cycle 관리 및 ID 상태 변화에 따른 정책 반영 • 접근통제 정책 관리를 위한 다양한 속성, 보안상태 관리	• 윈도우 AD기반 ID 통합 진행
인증/인가	• 내·외부에서 24시간 접속 가능한 인증/인가 서비스 구현 • Context 기반 인증/인가 처리 • 다양한 인증 표준, SSO, MFA 등을 구현	• 개인화 인증(MFA) 적용 및 로깅 • Context(상황정보) 고도화 진행
접근 통제	• 접근 권한 세분화(마이크로 세그먼테이션) 설정 • 접근 통제 게이트웨이, 에이전트를 통해서만 자원 접근 허용 • 모든 내·외부 통신 암호화 • 내부 자원의 외부 노출 차단, 자원의 보안상태 관리 및 유지	• 모든 외부 통신 구간 암호화 진행 (내부는 단계적 적용 예정) • 접근통제시스템 고도화 예정
가시화	• 사용자 행위, 자원에서 발생하는 모든 데이터 저장 및 분석 • 다양한 데이터 분석을 통한 가시성 확보 • 위험 관리에 기반한 사고 대응 전개	• SOAR 도입 진행 • 시각화시스템 고도화 진행 • UEBA* 고도화 예정

* UEBA(User and Entity Behavior Analytics): 사용자 행동에 초점을 맞춰 위험을 탐지 및 대응하는 솔루션

- 제로 트러스트 구현을 위한 보안 요건은 업무 환경에 미치는 변화를 고려해야 함
- 보안 요건을 달성하기 위해서는 기존 시스템, 신규 도입 기술, 서비스, 솔루션과의 융합을 고려해 구현

질의 응답

감사합니다.