
NH CERT 전략과
2021 보안 이슈 전망
2020.12.

## 0x01. Career

+ NH농협은행 CERT 팀장
+ ISMS-P 인증 심사원
+ 고려대학교 정보보호대학원 석사

## 0x02. Interest

+ Security : Hacking, A.I, Cloud, SOAR, Big Data, GDPR
+ ETC : Reading, Traveling, Climbing

# Contents

Ⅰ. ‘20 보안 위협

Ⅱ. NH CERT 전략

Ⅲ. ’21 보안 이슈

# ‘20 보안 위협

## 랜섬 디도스 공격

디지털데일리


[redacted] 올해 디도스 공격받았다

2020.10.05 21:24:08 / 이종현 bell@ddaily.co.kr

[디지털데일리 이종현기자] [redacted] 등이 올해 디도스(DDoS) 공격을 받은 것으로 알려졌다. [redacted] 까지 공격받았다.

가장 많이 발생한 공격 유형은 디도스 공격이다. 서버가 처리할 수 있는 용량 이상의 정보를 한 번에 보내 과부화를 발생시켜 접속 지연이나 서버 다운 등의 피해를 주는 디도스 공격은 전체 피해 37건 중 23건이다. 이어 정보유출 7건, 시스템 위·변조 5건, 악성코드 감염 2건 등이 뒤를 이었다.

NH농협은행

# ‘20 보안 위협

## 랜섬 디도스 공격 분석

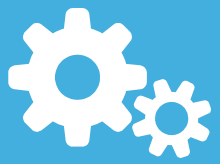
### 공격 방식

- Fancy Bear 등
- 사전 협박 메일
- 금전 요구
- 추가 공격 예고

### 공격 트래픽

- UDP 공격
- 2.5G ~ 70G
- DNS, NTP 등

### 공격 발생지



- 해외 트래픽 80%
- 미국,중국,러시아, 한국 순

### 대응 체계

- 자체 대응
- ISP 정책 적용
- 외부 디도스 대피소

NH농협은행

# ‘20 보안 위협

## Global Pandemic

- **71%의 기업들은 보안 위협과 공격이 증가**
- **55%의 보안전문가들은 피싱 공격을 주요 위협으로 선정**
- **95%의 응답자는 바이러스 확산으로 추가적인 IT보안 문제에 직면**

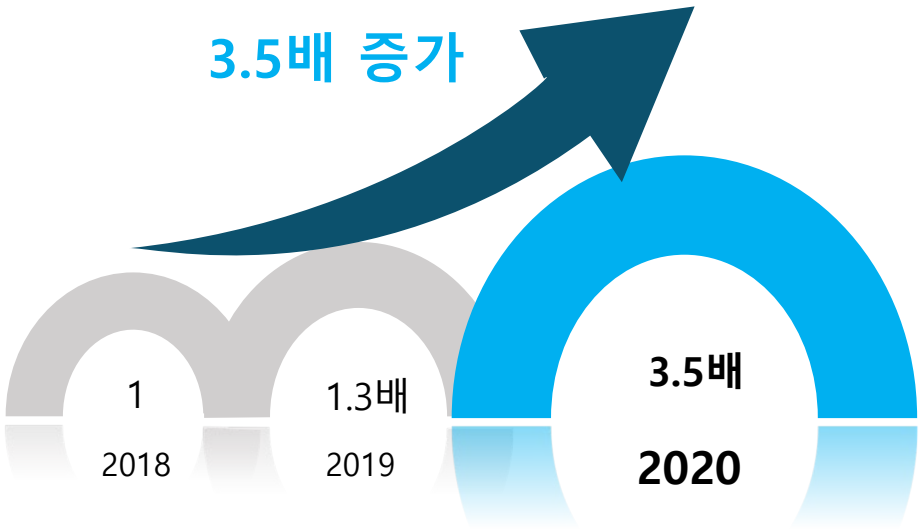
Source : 체크포인트

NH농협은행

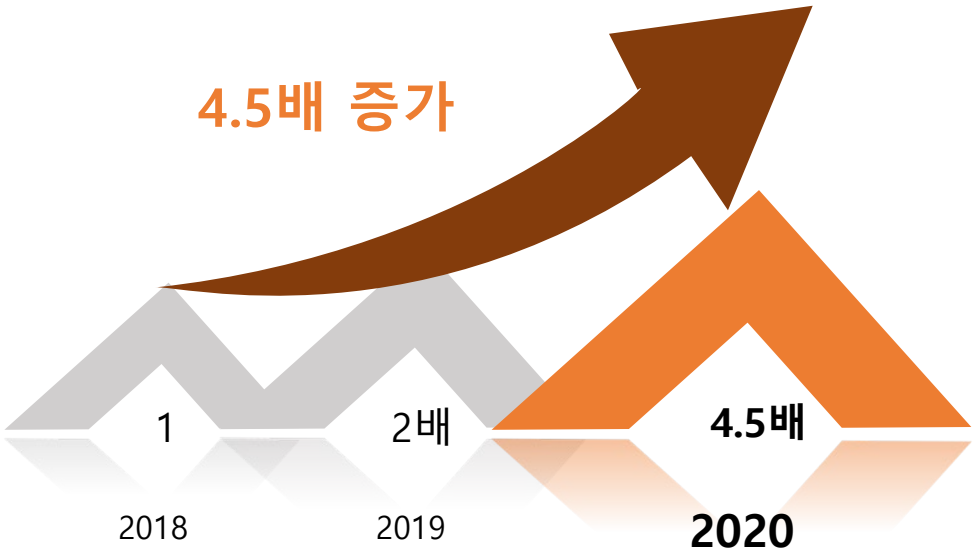
# ‘20년 보안 위협

## Scanning & Exploit

### ● Scanning




### ● Exploit

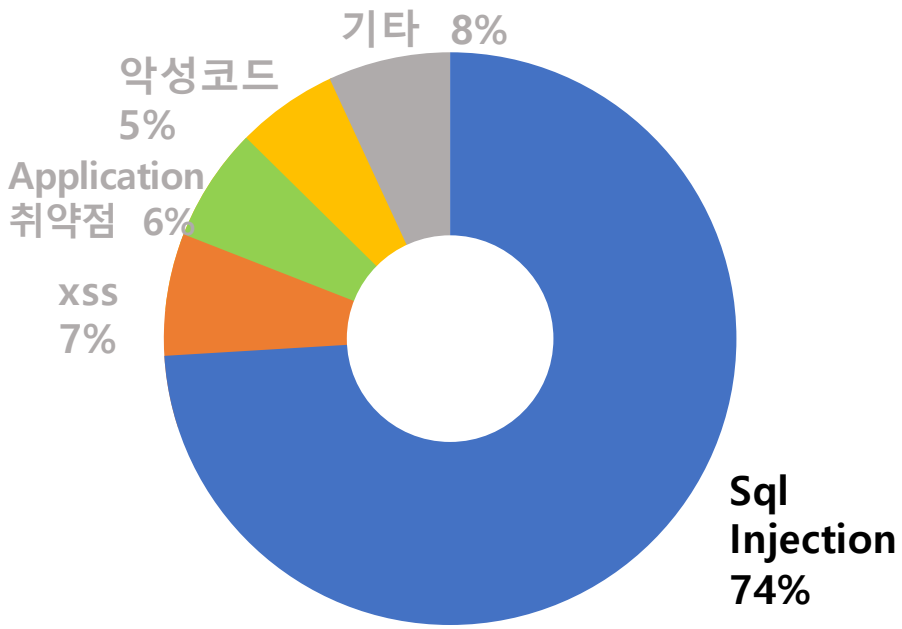



NH농협은행

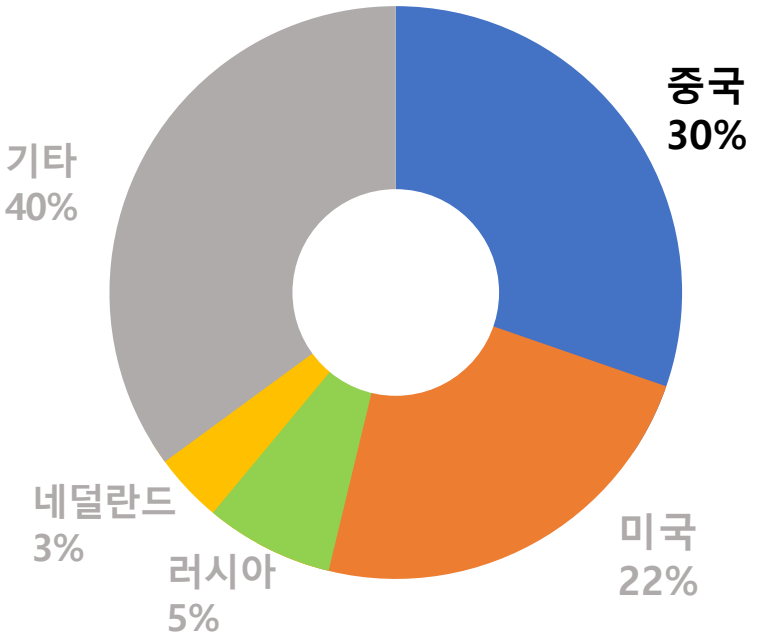
# ‘20년 보안 위협

## 침해시도 분석

• 침해시도 유형



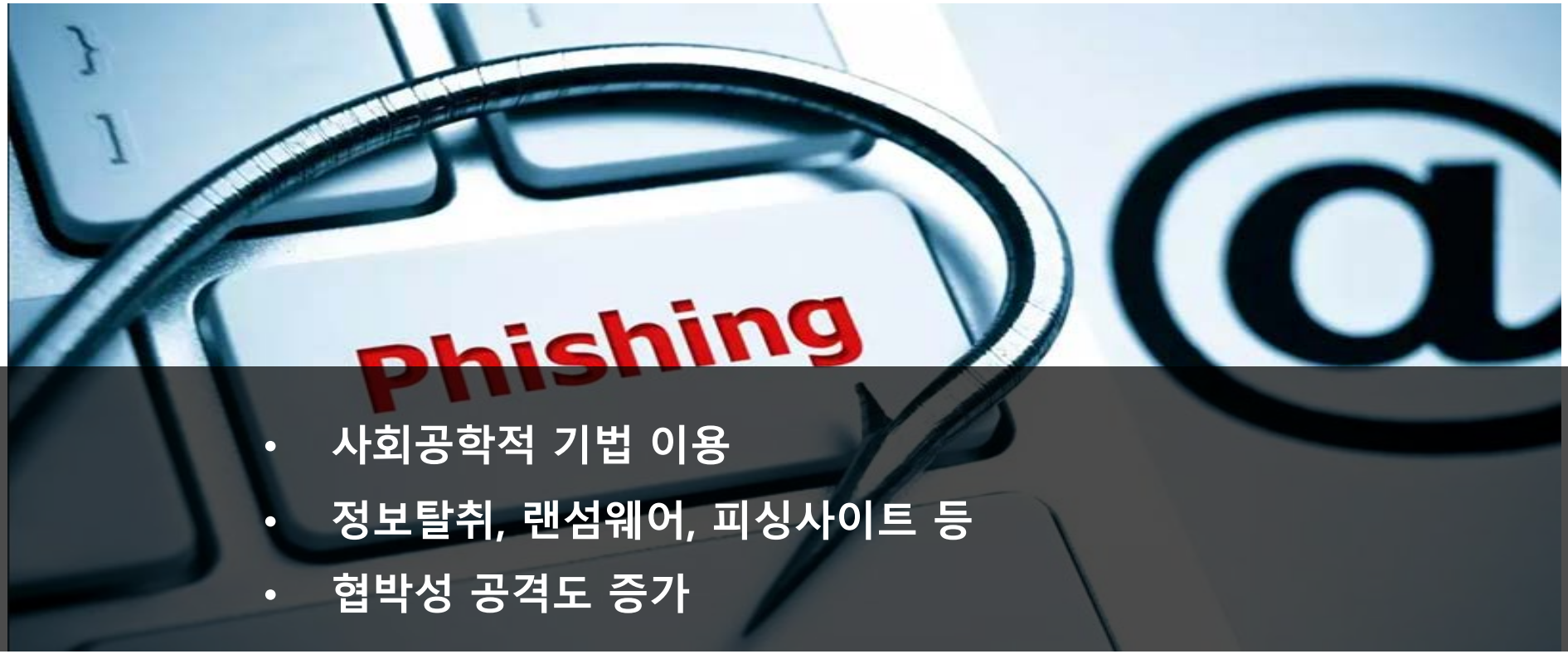

• 침해시도 국가




NH농협은행

# ‘20년 보안 위협

## 악성메일



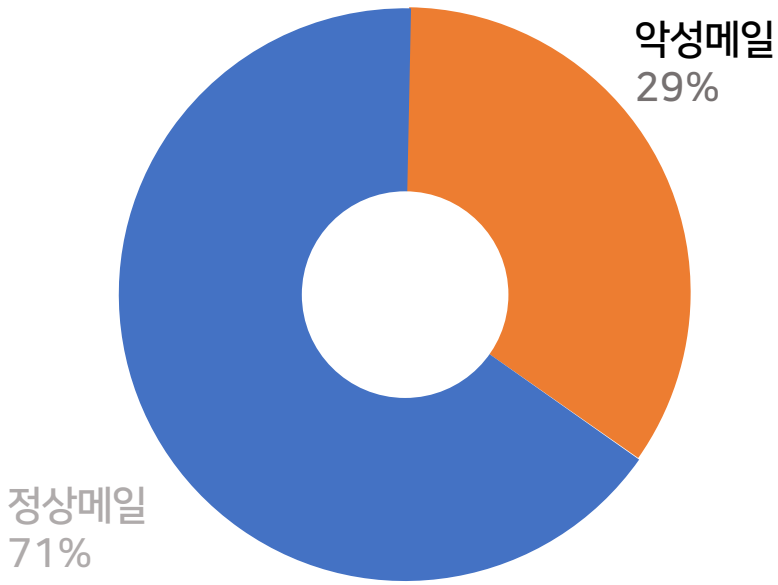

- 사회공학적 기법 이용
- 정보탈취, 랜섬웨어, 피싱사이트 등
- 협박성 공격도 증가

NH농협은행

# ‘20년 보안 위협

## 악성메일 분석

- 메일 분석




### 발송 국가

- 터키, 미국, 포르투갈 등

### 메일 제목

- 사회적 거리두기 단계
- 재난지원금 신청
- 코로나19 확진자 동선 안내 등

### 랜섬 협박 메일

- 중요정보 유출, 디도스 공격

NH농협은행

# NH CERT 전략

## 정보보안부문 연혁

**1. 기반마련**

- 정보보안부문 설립
- 73대 종합대책
- 시스템, 장비, 규정 등

**2014**

**2. 성숙단계**

- 31대 고도화 계획
- 보안위협 신속 대응
- 빅데이터 기반 관제

**2016**

**3. 질적전환**

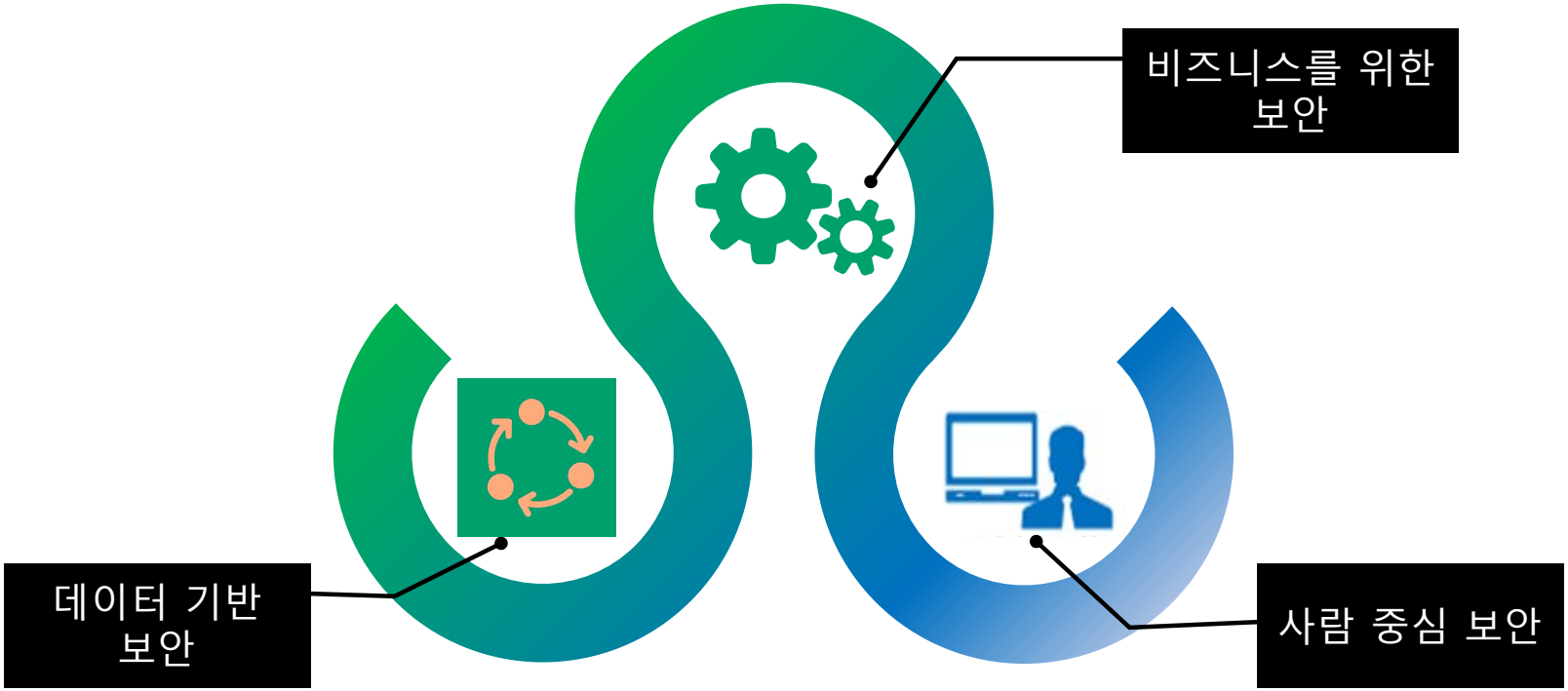
- 32대 지속가능한 전략
- 안전한 디지털 금융
- AI, SOAR 관제 고도화

**2019 ~**

NH농협은행

# NH CERT 전략

## 지속 가능한 정보보안 전략 - 32개 과제




NH농협은행

# NH CERT 전략

## 정보보안부문 조직


- 은행장(CEO) 직속
- 정보보안부문(부행장) : 2부 1단 9팀
- 정보보호부 (CPO), IT보안부 (CISO)

NH농협은행

# NH CERT 전략

## 주요 보안대응 체계


- 빅데이터 분석
- 위협 인텔리전스

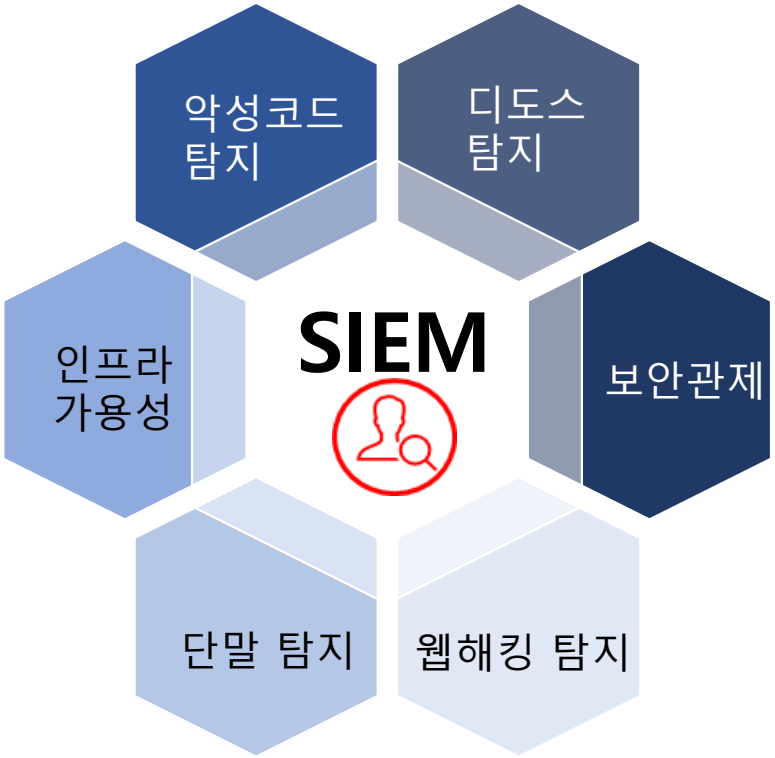

- 파일 통합 검역
- E.D.R


- Red Teaming
- 개인정보 오남용 모니터링

NH농협은행

# 보안 관제 - SIEM

## 빅데이터 분석



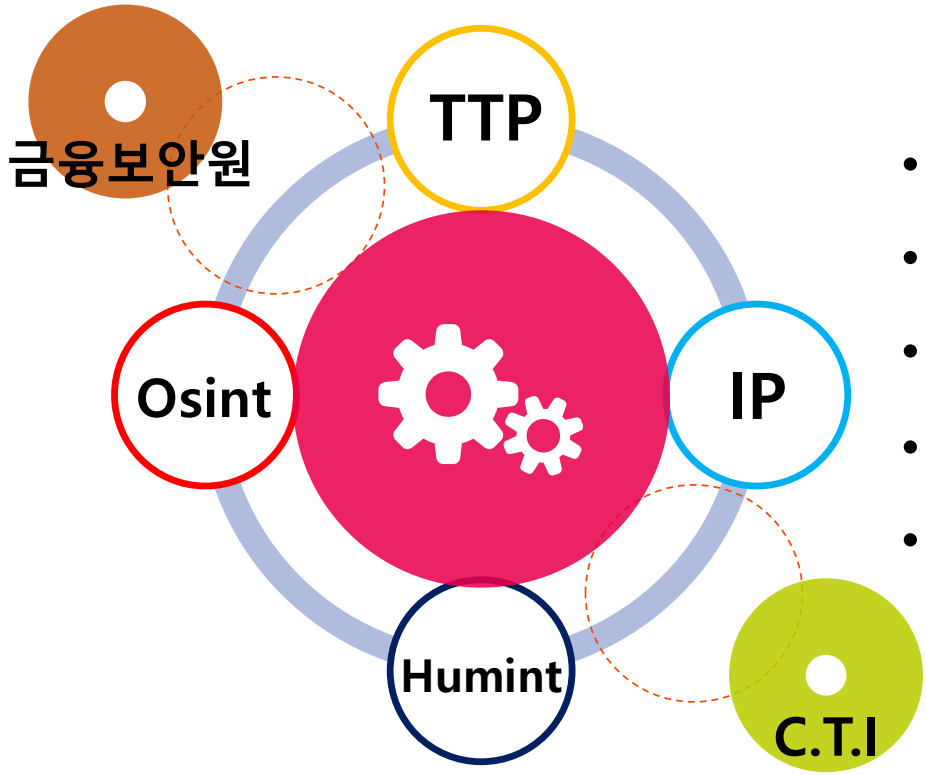


- 일일 최대 수 TB 실시간 수집
- 이벤트 간 상관 분석
- 침해 유형별 탐지 시나리오
- IT인프라 전반 가시성 확보

NH농협은행

# 보안 관제 - SIEM

## 위협 인텔리 전스

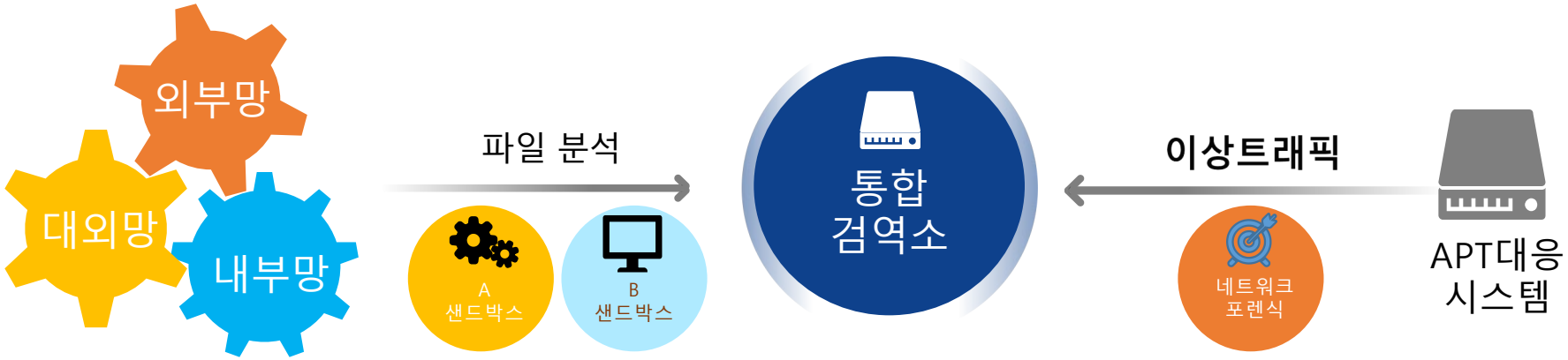



- SIEM과 실 시간 연계
- Emerging 공격 대응
- Attack Correlation과 Profiling
- 공격자의 TTP 분석/대응
- 고도화된 기법의 보안솔루션 우회 탐지

NH농협은행

# 위협 정보 통합 검역소

## 파일 통합 검역




- 유통되는 모든 파일에 대한 통합 검역 – Zero Trust
- 이기종 샌드박스 활용, 정적 & 동적분석 활용 위협 탐지
- 악성코드 및 비정상트래픽 대응시스템 연계 통합보안관리효과 극대화

NH농협은행

# 위협정보 통합 검역소

## Endpoint Detection and Response


- Endpoint Hardening 공격 표면 최소화
- SIEM 연계 상관 분석
- Prevention, Detection, Response

NH농협은행

# 상시 보안 점검

## Red Teaming

- Red Team과 Blue Team이 상호 협업 및 견제
- Threat Hunting
- IT인프라, 어플리케이션 정기/상시 취약점 점검

NH농협은행

# 상시 보안 점검

## 개인정보 오남용 모니터링

**정책**
권한, 접근제어,
인사정보 연동


**보안솔루션**
PC, 서버/DB,
NW

- 개인신용정보 생애주기(Lief Cycle) 관리 통합 보안체계
- 빅데이터 기반 사용자 행위 분석
- 정보보호 점검 활동의 효율적 수단 제공으로 점검 고도화

NH농협은행

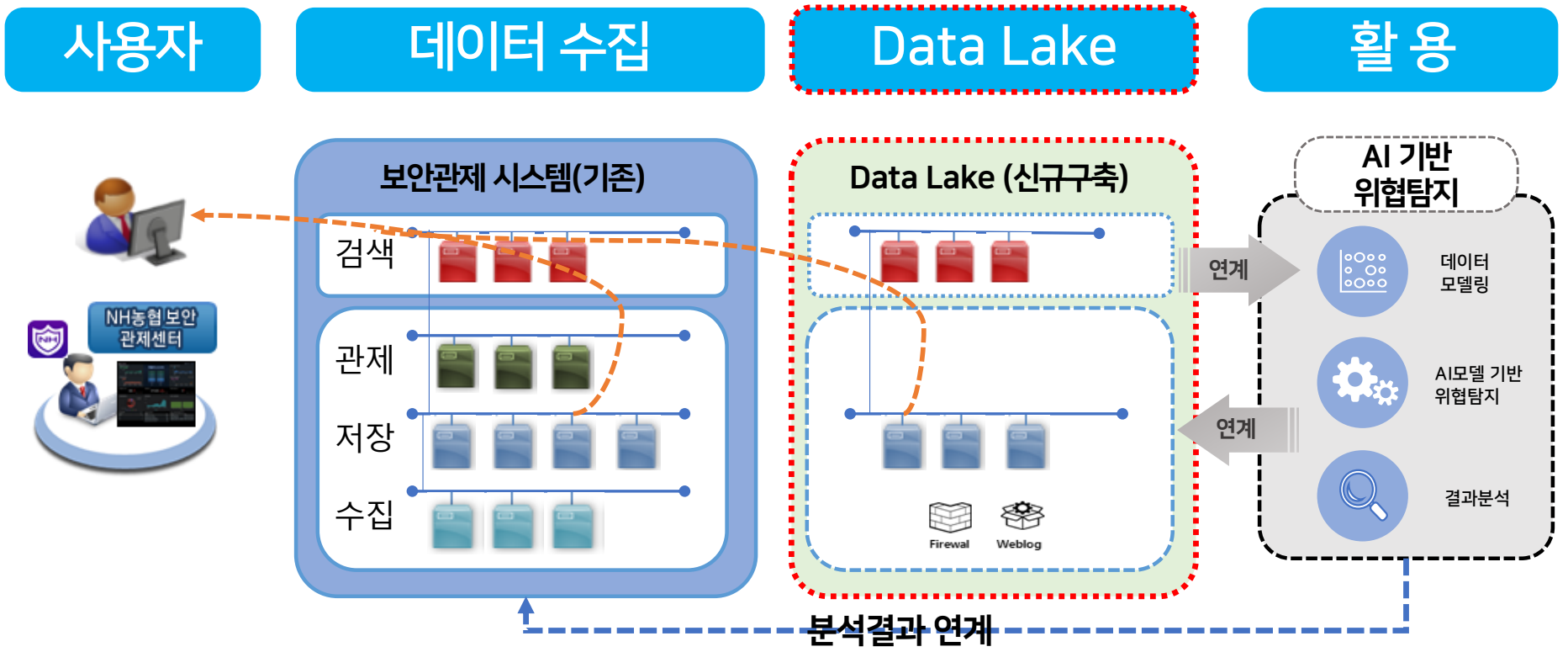
# NH CERT 전략

- 1단계: 보안 데이터 레이크
- 2단계: 인공지능 보안관제
- 3단계: (SOAR)사이버보안 종합 관제

NH농협은행

# NH CERT 전략

## 1단계 : 보안 데이터 레이크



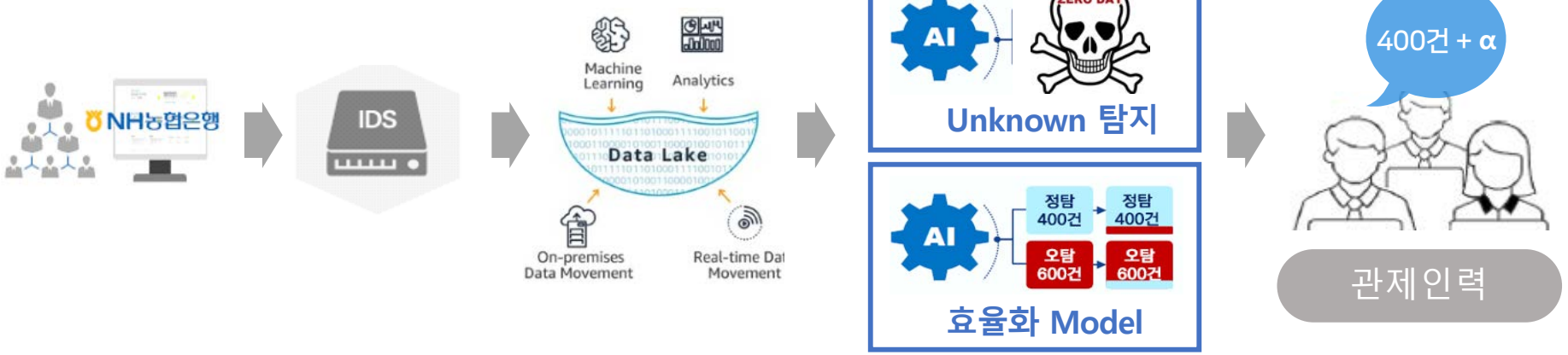

NH농협은행

# NH CERT 전략

## 2단계 : 인공지능 보안관제

Raw Data > IDS Data > Data Lake > AI 적용 > 분석/대응

접속 100만건 | 탐지 1,000건 | 연관 Data 500만건 | AI 분류 400건 + α | 분석 1,000건




- Attack Protection에서 Attack Prevention으로

NH농협은행

# NH CERT 전략

## 3단계 : (SOAR)사이버보안 종합 관제

위협정보 수집/분류 자동화 (Automation)

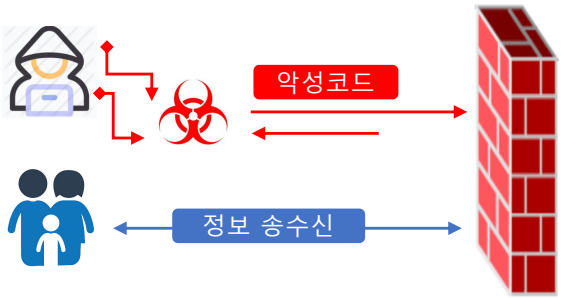
보안 관제 프로세스 조직화 (Orchestration)

이벤트 분류/워크로드 정교화 (Management)

보안사고 대응 표준/신속화 (Response)

**(사이버보안관제센터) 사이버보안 종합 관제 체계, SOAR**

### (외부관제) 외부 침해위협 모니터링



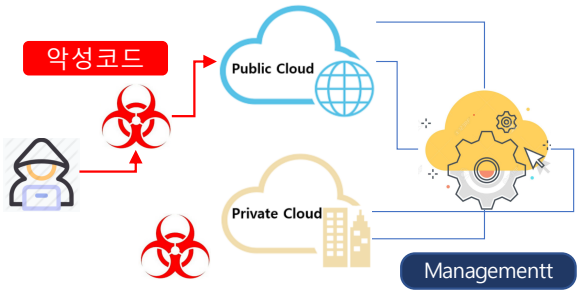

오픈뱅킹, 마이데이터, 이상행위(FDS)

### (내부관제) 개인정보 유출위험 모니터링


침투 이후 내부망 공격

내부자 정보유출

### (클라우드 관제) Multi Cloud 모니터링




비인가 접근, 시스템 환경 설정 오류

NH농협은행

# ‘21 보안 이슈 전망

## 보안 4대 키워드

1.
Cloud Security

2.
Third Party Risk

3.
Zero Trust for
W.F.A*

*Work from Anywhere

4.
Innovation &
Security Balance

NH농협은행

# ‘21 보안 이슈 전망

## Cloud Security

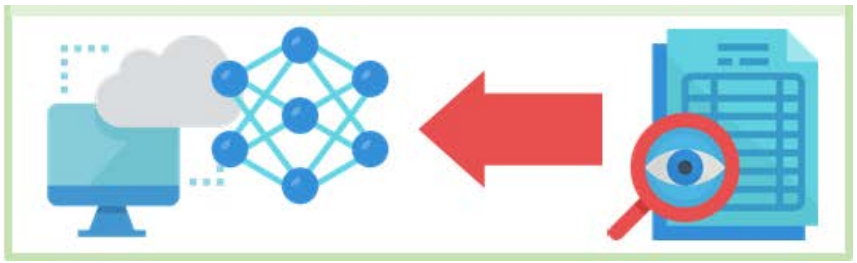

- Different Challenge
- 소유에서 공유중심으로 변화
- Monitoring & Controlling

NH농협은행

# ‘21 보안 이슈 전망

## Third Party Risk

**클라우드 등 제3자 리스크 증대**



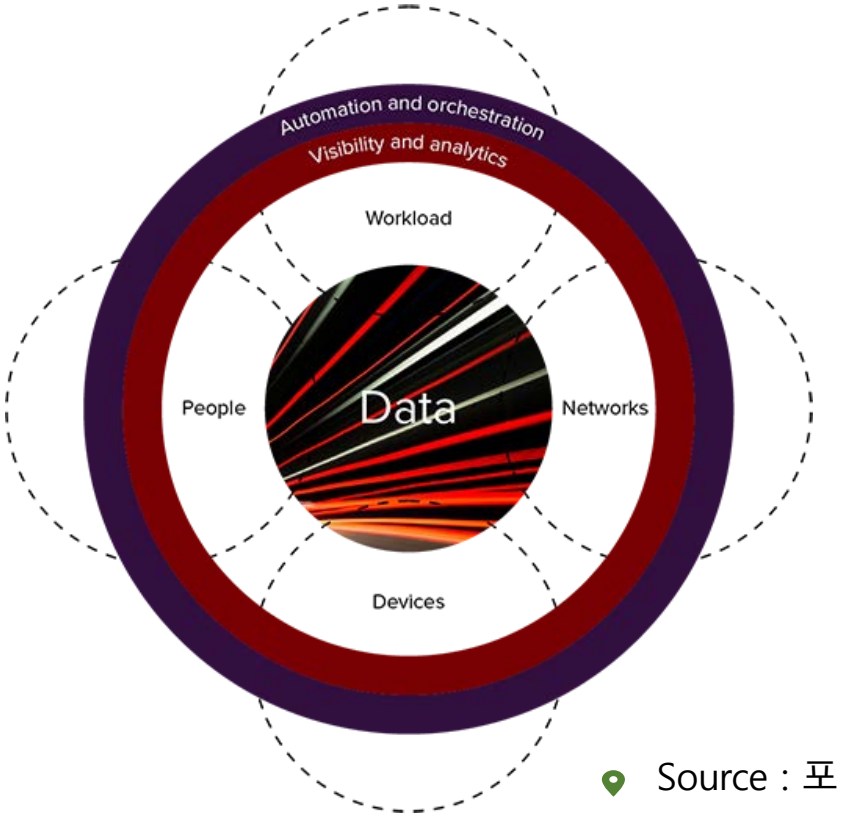
**IT아웃소싱 확대 등 리스크 증대**


- 클라우드 등 제3자 서비스 이용 증가
- 위탁의 증가로 공급망 복잡도 증가
- 다양한 공급망을 통한 해킹 가능성

NH농협은행

# ‘21 보안 이슈 전망

## Zero Trust for W.F.A




- 급격한 비대면 문화의 확산
- 보안경계를 ID로 내려오게 함
- 데이터, 사람, 네트워크, 워크로드 등 전반
- 보안정책이 진화하는 방향이고, 긴 여정

Source : 포레스트

NH농협은행

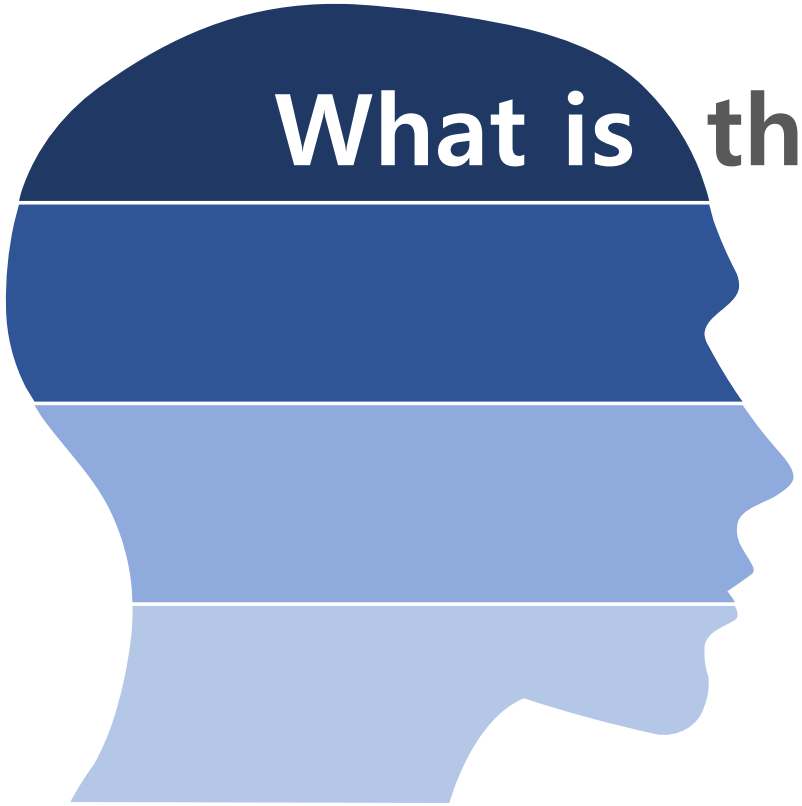
# ‘21 보안 이슈 전망

## Innovation & Security Balance


- 사이버 위협의 유형과 범위 확대
- 신기술 리스크 = 사이버 리스크
- 디지털 성숙도와 사이버 보안 성숙도의 균형

NH농협은행

# ‘업’의 본질은 무엇인가?



What is the Essence of Security?

NH농협은행


금융의 모든 순간
NH농협금융
Q & A
엄마의 은행에서 딸의 은행으로
세대를 이어 함께하는 은행
NH농협은행