One Step
Ahead

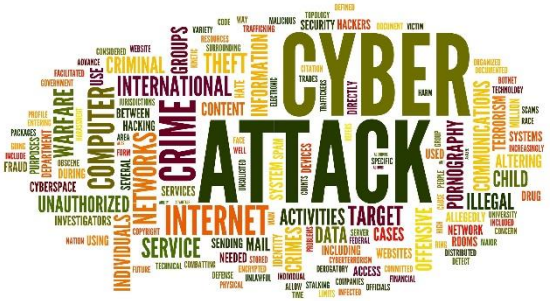
차세대 보안전쟁 AI vs 인간
공격과 대응

2017.04

IGLOOSECURITY

Contents

01 Cyber Attacks



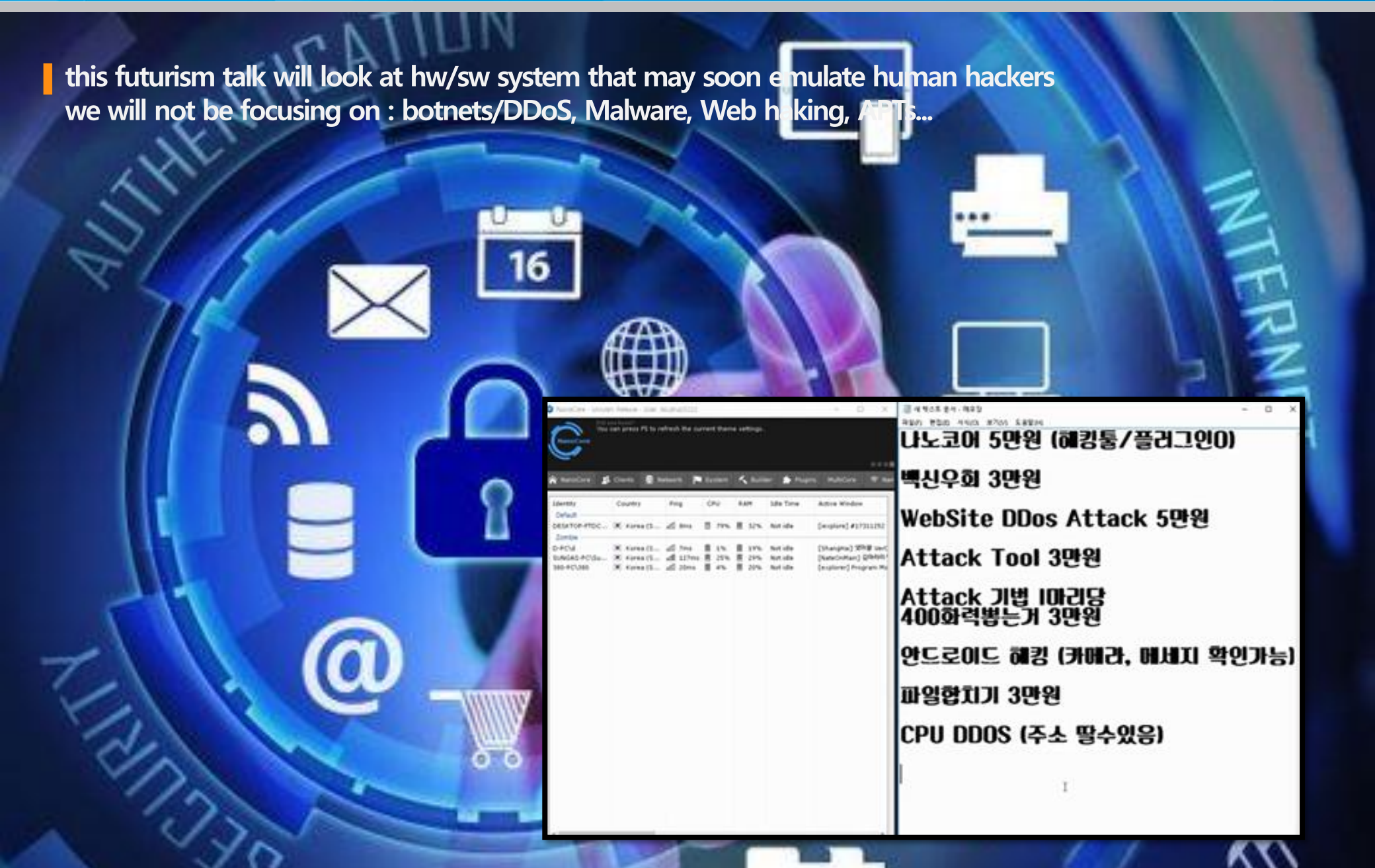
IGLOOSECURITY

1.1 Evolution of cyber attacks

[국가기반시설 / 사회기반시설]

1.1 Evolution of cyber attacks

- this futurism talk will look at hw/sw system that may soon emulate human hackers
  we will not be focusing on : botnets/DDoS, Malware, Web hacking, APTs...



1.1 Evolution of cyber attacks

- 다양한 보안장비와 SNS, IoT 등으로 데이터 증가

탐지 및 대응시간 단축 필요

APT Attack

- 공격할 표적을 특정
- (초기) 정부, 군사기관
- (현재) 민간 기업도 포함
- 주 목적 : 정보 탈취

- 공격 조직은 목적 달성을 위해 각종 방어기술 우회
- 표적 대상이 공격당한 사실을 인지 못함

- 정해진 공격 기간 없음
- 평균 1~5년 정도 지속
- 공격 조직의 역량/목적, 표적 조직의 방어 역량에 따라 기간차 존재

200 Day

APT Attack - CyberKillChain

Reconnaissance

- 정보 수집
- 공개적으로 이용 가능한 인터넷 상의 정보를 수집

Delivery

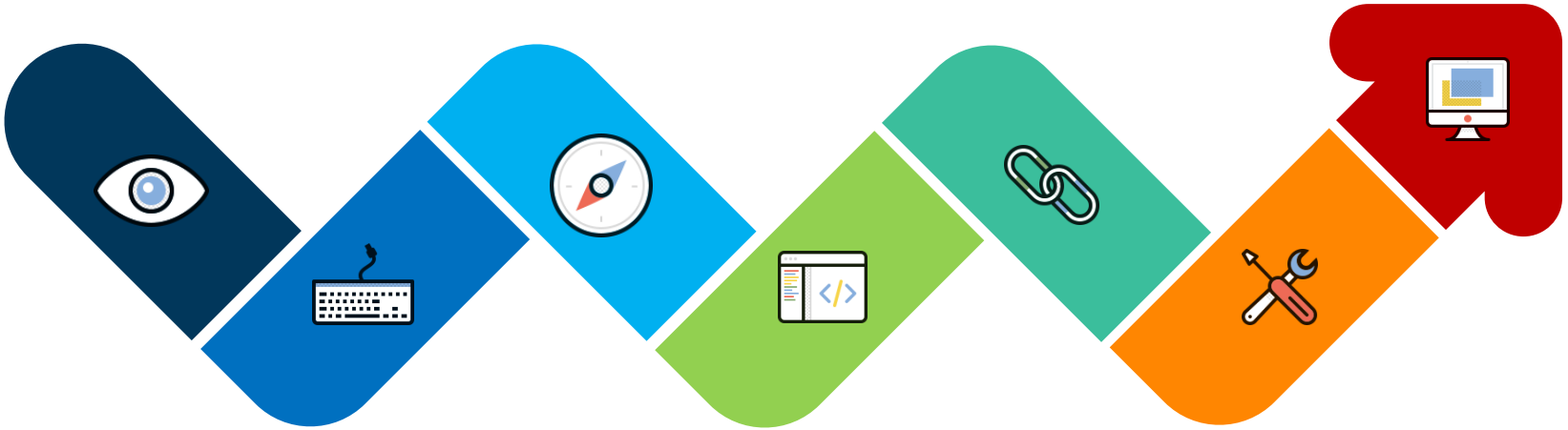
- 피해자에게 악성 페이로드를 전달
- 전자메일 등을 활용

Installation

- 추가 악성 코드설치
- 수개월간 정교한 공격 프로세스를 진행

Actions on objectives

- 실제 목표를 달성하기 위한 단계
- 목표 달성을 위해 수많은 단계를 필요로 하는 정교한 능동적 공격 프로세스



Weaponization

- Exploit 을 이용한 악성 페이로드 생성

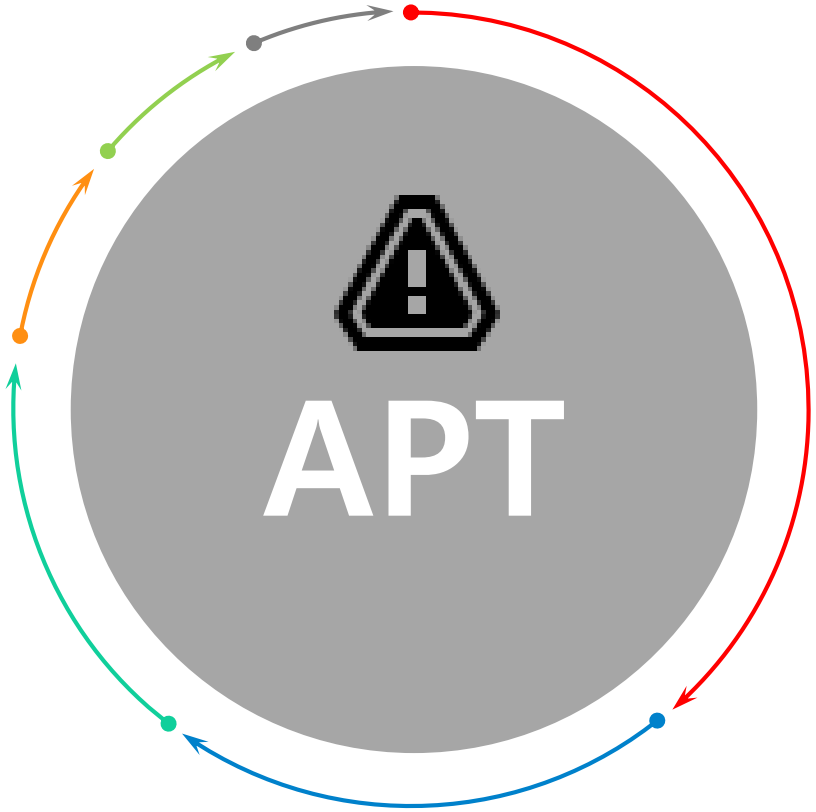
Exploitation

- 피해자 시스템의 취약점을 이용한 악성코드 실행

Command and Control

- 명령/제어 채널 생성
- 공격자가 원격으로 내부 자산을 작동시키기 위함

APT Attack by Country



- South Korea (37%)
- Southeast Asia (27%)
- Asia Pacific (27%)
- World Wide (15%)
- U.S. (13%)
- Europe (11%)

출처 : FireEye

1.3 APT Attack History [Domestic]

2011 - 2012

11.04 농협 전산망 마비

- 농협 내부서버 공격
- 275대 서버 파일 삭제

11.07 SK 정보유출

- Nate 내부서버 공격
- 회원정보 3,500만 유출

12.07 KT 정보유출

- KT 내부서버 공격
- 회원정보 870만 유출

1.3 APT Attack History [Domestic]

2013 - 2014

03.20 06.25 14.12

3.20 전산 대란

- 금융권, 방송사 홈페이지 공격
- 서버, PC, ATM 등 장애 발생
- 3월 20일 오후 2시 시스템 파괴

6.25 사이버 테러

- 정부, 공공기관 등 피해
- 홈페이지 변조, DDoS 공격

한국수력원자력 해킹

- 한수원 직원정보 및 기밀 기술자료 유출
- 이메일을 통한 악성코드 유포
- 감염 PC의 파일 삭제 및 MBR 파괴

1.3 APT Attack History [Domestic]

2015 - 2016

04.21 클리앙 랜섬웨어 유포

- 국내 커뮤니티 사이트에서 랜섬웨어 유포
- 사용자 컴퓨터 파일 암호화 및 금전 요구
- 랜섬웨어 유포방식 진화 (Email ➔ DBD)

09.15 코레일 전산망 해킹

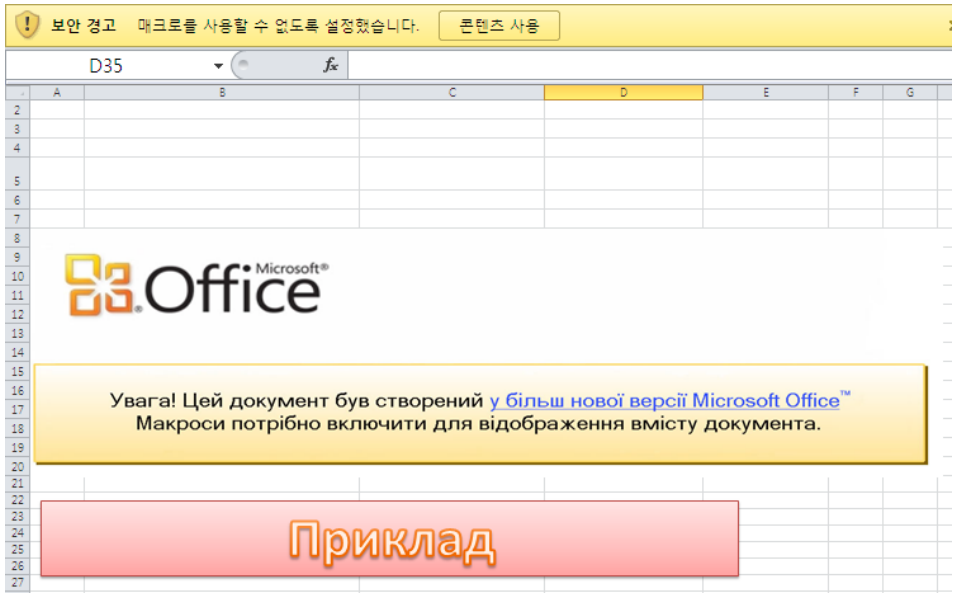
- 실제 해킹은 2013년 11월에 발생
- 주요 정보통신 기반시설 정보 유출

07.25 인터파크 개인정보 유출

- 인터파크 DB 서버 해킹
- 회원정보 1,030만건 유출

1.3 APT Attack History [Overseas]

BlackEnergy



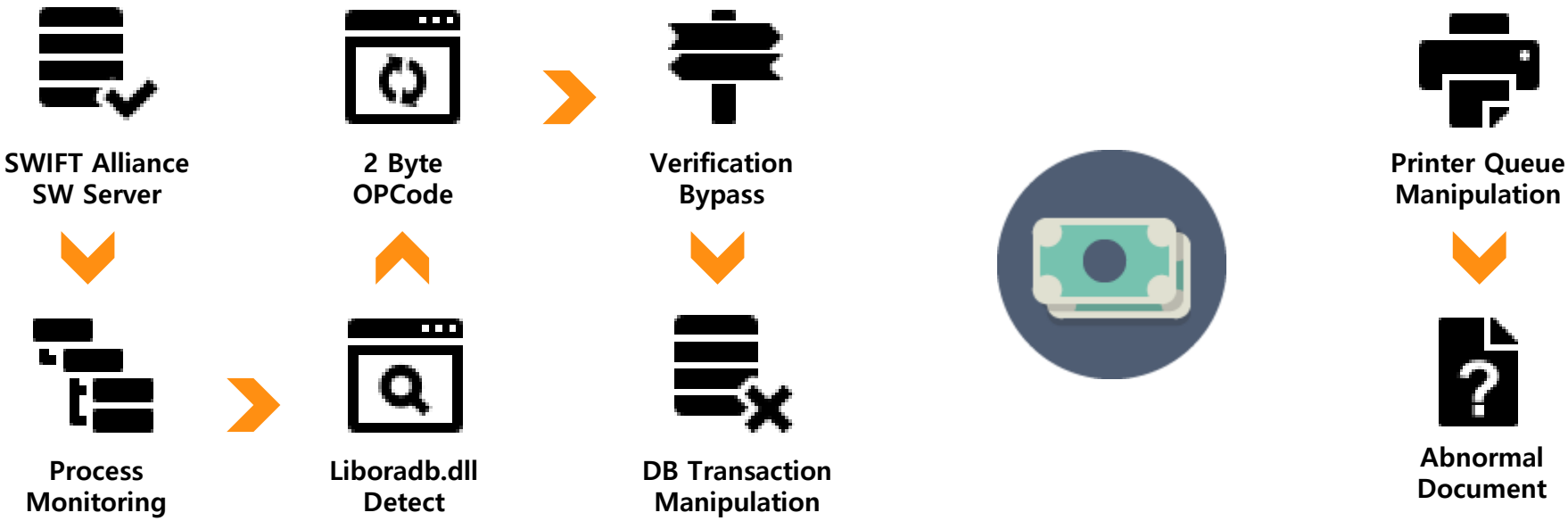

```
================================================================================
FILE: C:\BlackEnergy Smaple.xls
Type: OLE
--------------------------------------------------------------------------------
VBA MACRO Workbook________.cls
in file: C:\BlackEnergy Smaple.xls - OLE stream: u'_VBA_PROJECT_CUR/VBA/Workbook________'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Private a(768) As Variant
Private Sub Init0()
    a(1) = Array(77, 90, 144, 0, 3, 0, 0, 0, 4, 0, 0, 0, 255, 255, 0, 0, 184, 0, 0, 0, 0, 0, 0,
    a(2) = Array(136, 190, 95, 48, 204, 223, 49, 99, 204, 223, 49, 99, 204, 223, 49, 99, 163, 19
    a(3) = Array(11, 1, 6, 0, 0, 20, 1, 0, 0, 104, 0, 0, 0, 0, 0, 0, 64, 43, 0, 0, 0, 16, 0, 0,
    a(4) = Array(0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 64, 49, 1, 0, 28, 0, 0, 0, 0, (
    a(5) = Array(0, 0, 0, 0, 32, 0, 0, 96, 46, 114, 100, 97, 116, 97, 0, 0, 0, 32, 0, 0, 0, 48,
    a(6) = Array(0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, (
    a(7) = Array(0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, (
```

1.3 APT Attack History [Overseas]

방글라데시 중앙은행 해킹

1.3 APT Attack History [Overseas]

방글라데시 중앙은행 해킹



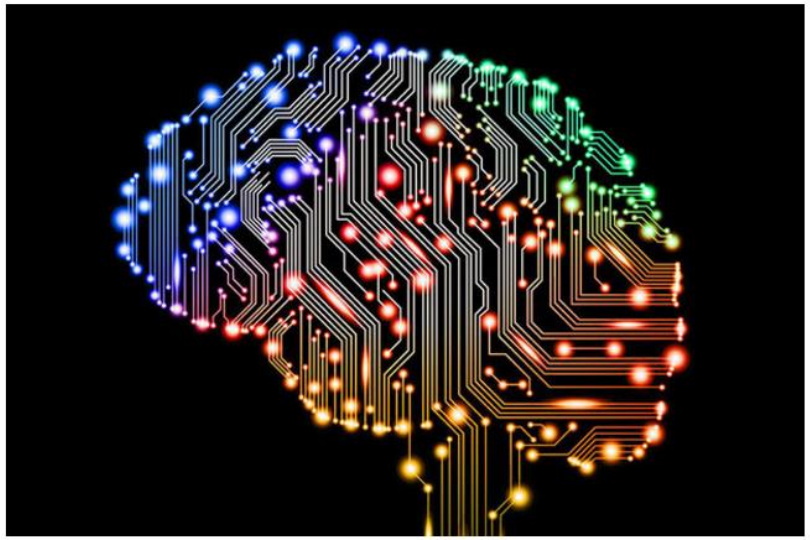
1.3 APT Attack History [Overseas]

2016 DEFCON24

보안 솔루션은 머신러닝으로 진화 중… 최신 사례 4가지

Maria Korolov | CSO

머신러닝의 발전으로 보안 시스템을 더 쉽게 훈련시킬 수 있게 된다. 또 변화에 더 유연하게 대응할 수 있게 된다. 머신러닝이 보안 분야에 적용되고 있는 최신 사례들을 정리했다.



보안업계, 머신러닝 기법 적용 활발…기계적 판단으로 허점 차단

기자] 보안업계가 머신러닝 기법을 도입한 제품 및 서비스 출시에 적극 나서고 있다.

최근 사람의 심리를 이용하는 '사회공학적 이메일 해킹' 기법 등 피해를 입는 기업들이 나타나면서 이에 대응할 수 있는 보안 솔루션 출시가 이어지고 있다.

사이버전은 속도전, 보안업계도 '머신러닝' 열풍

네트워크에서 엔드포인트에 이르는 모든 영역에서 보안 위협이 고도화됨에 따라 머신러닝(기계학습)을 보안 솔루션에 접목하고자 하는 시도가 주목받고 있다. 축적된 보안 인텔리전스를 기반으로 인공지능 대응 체계를 마련, 자동화된 방식으로 보다 신속하게 위협을 탐지하고 대응하기 위한 것이다.

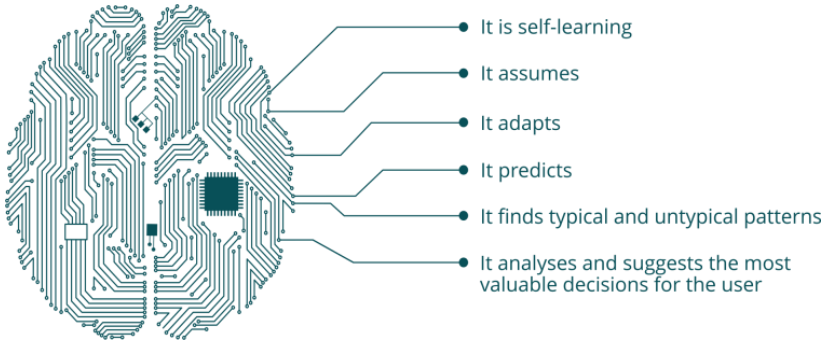
▲최근 주목받고 있는 머신러닝과 인공지능은 보안 분야에서도 뜨거운 화두 중 하나다.(사진= MS)

'머신러닝'으로 보안도 진화 중

국내외 보안 기업 머신러닝 적용에 '잰걸음'

2016년 11월 29일 오전 06:00

·기자] 보안 업계에 머신러닝 바람이 불고 있다. 최근 글로벌 보안 업체들은 새로운 악성코드, 알려지지 않은 위협을 감지하기 위해 보안 제품에 머신러닝을 적극 도입하고 있다.



02 Security Machine Learning

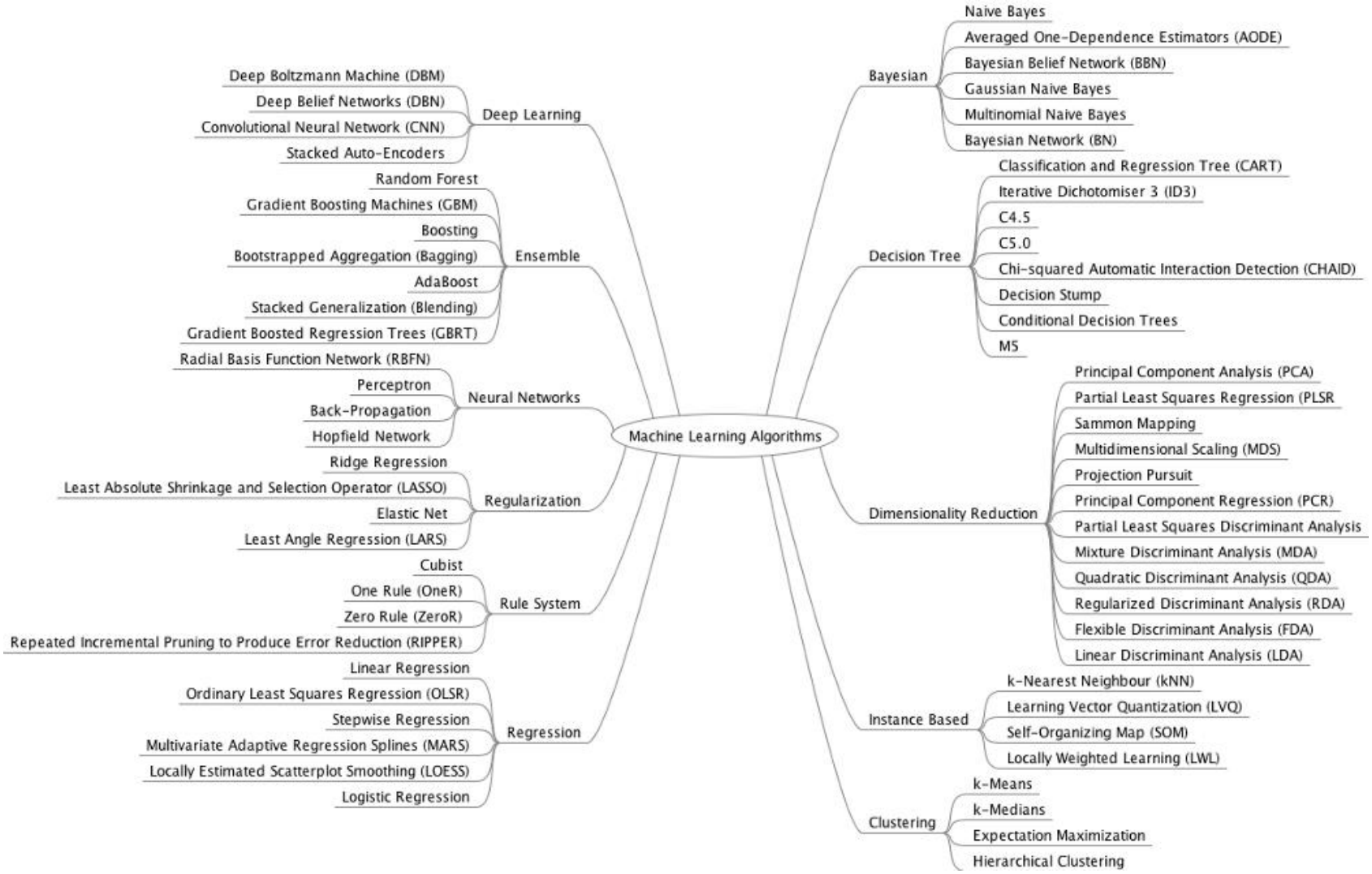
Machine Learning ? Deap Learning?

컴퓨터가 사람처럼 생각하고
판단하게 만드는 기술

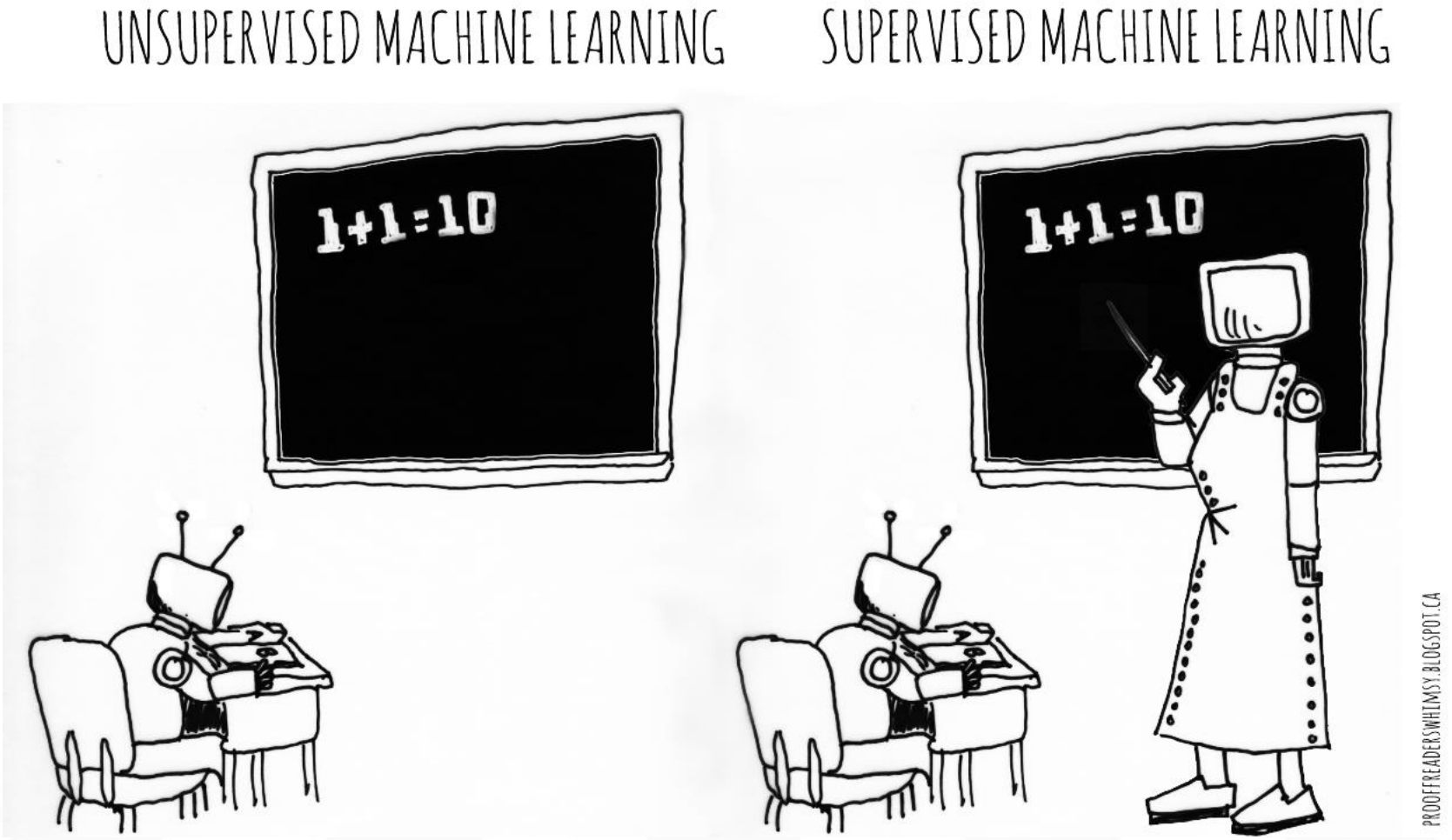
인간의 학습능력과 같은 기능을
컴퓨터에 부여하기 위한 기술

빅데이터 기반으로 스스로
학습하여 판단하는 기술

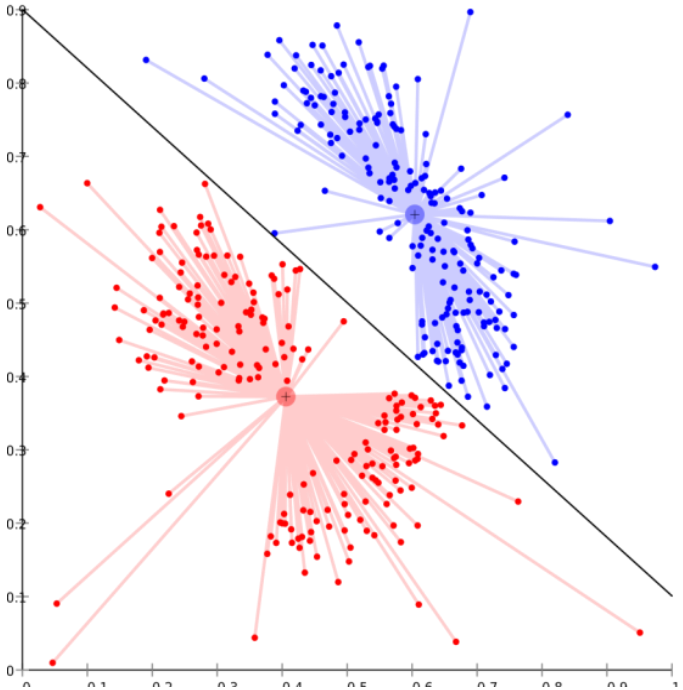
Machine Learning ? Deap Learning?

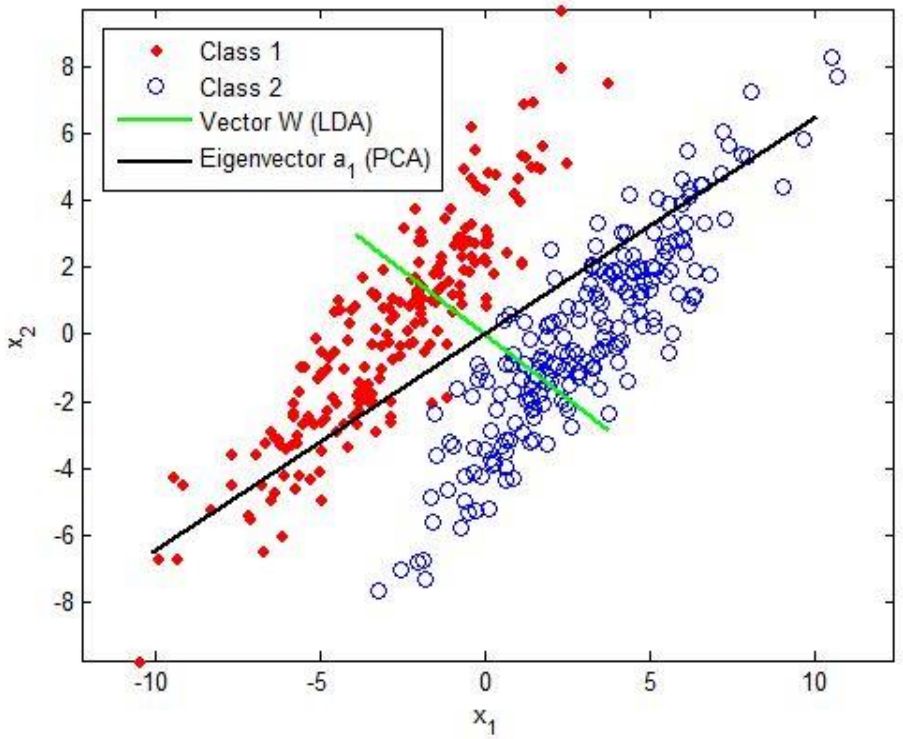


Unsupervised Learning + Supervised Learning



Unsupervised Learning

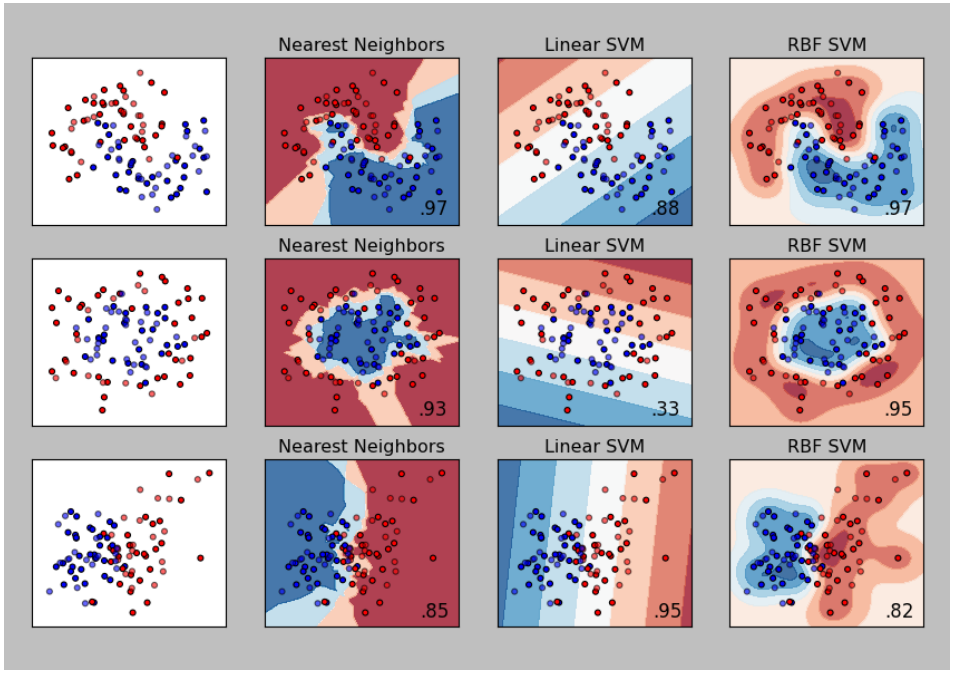


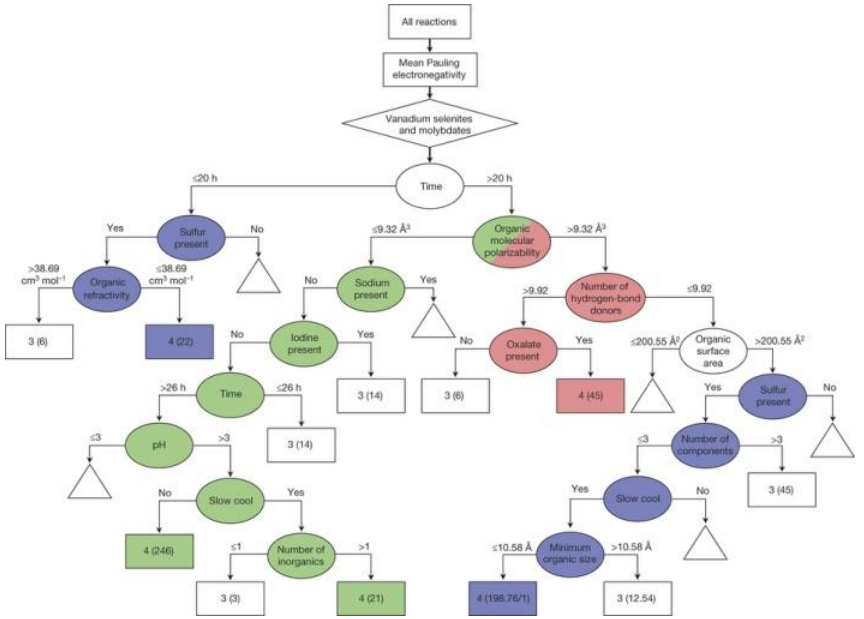


- 예) 군집화 (Clustering, 비슷한 관측치끼리 군집)

  차원축소 (Dimensionality Reduction, 데이터간의 연관 규칙을 찾음) 등

Supervised Learning

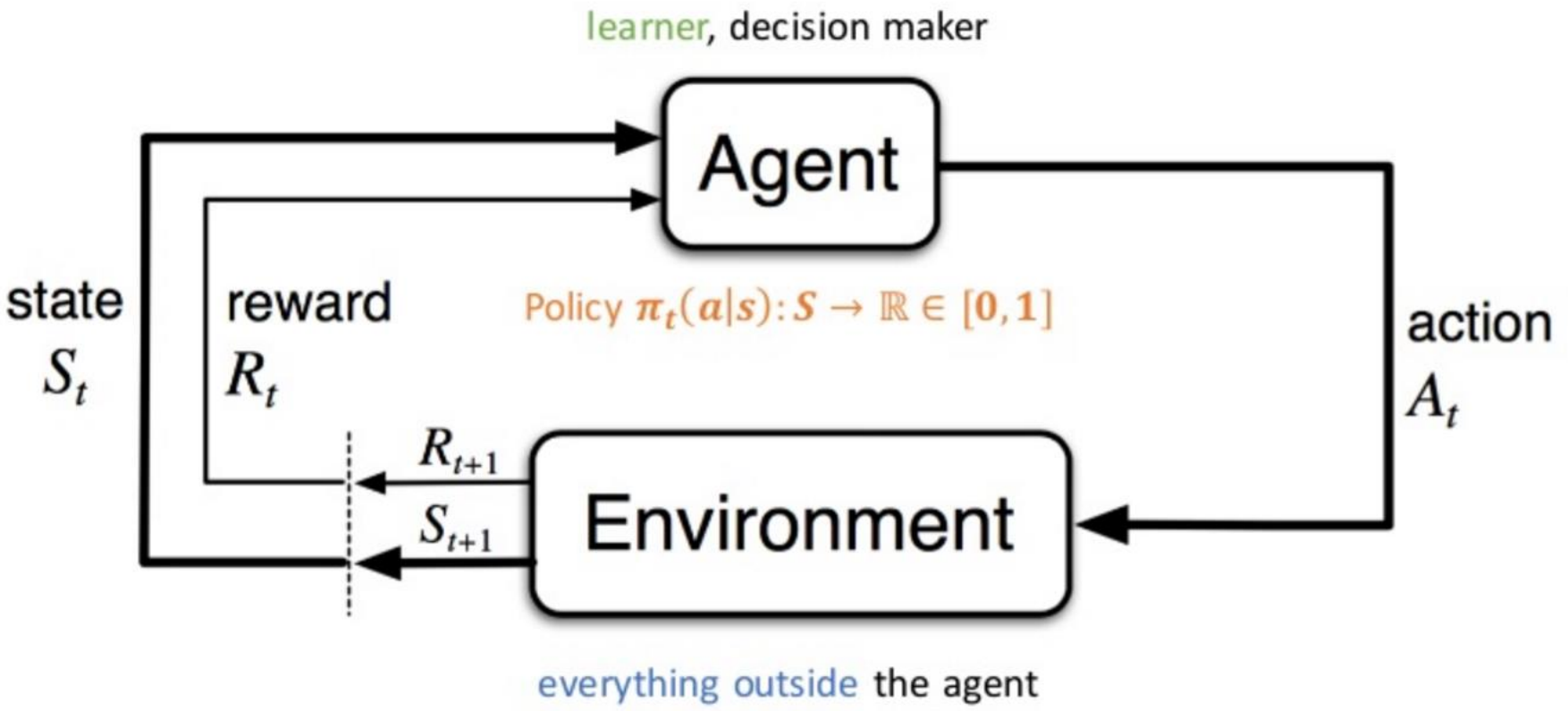




- 예) 회귀분석 (Regression Analysis, 데이터의 함수 관계 예측)
- 의사결정나무 (Decision Tree, 데이터 속성에 따라 나무 형태의 의사결정 학습 모델을 만들고 , 반복을 통해 최종 결정을 도출) 등

Reinforcement Learning

- 상태(State)에서 어떤 행동(Action)을 취하는 것이 최적인지를 학습
- 행동을 취할 때마다 외부 환경에서 보상(Reward)이 주어지며, 보상을 최대화 하는 방향으로 학습이 진행
- 예) 컴퓨터 체스, 복잡한 로봇의 제어 등



The Iris flower Data set

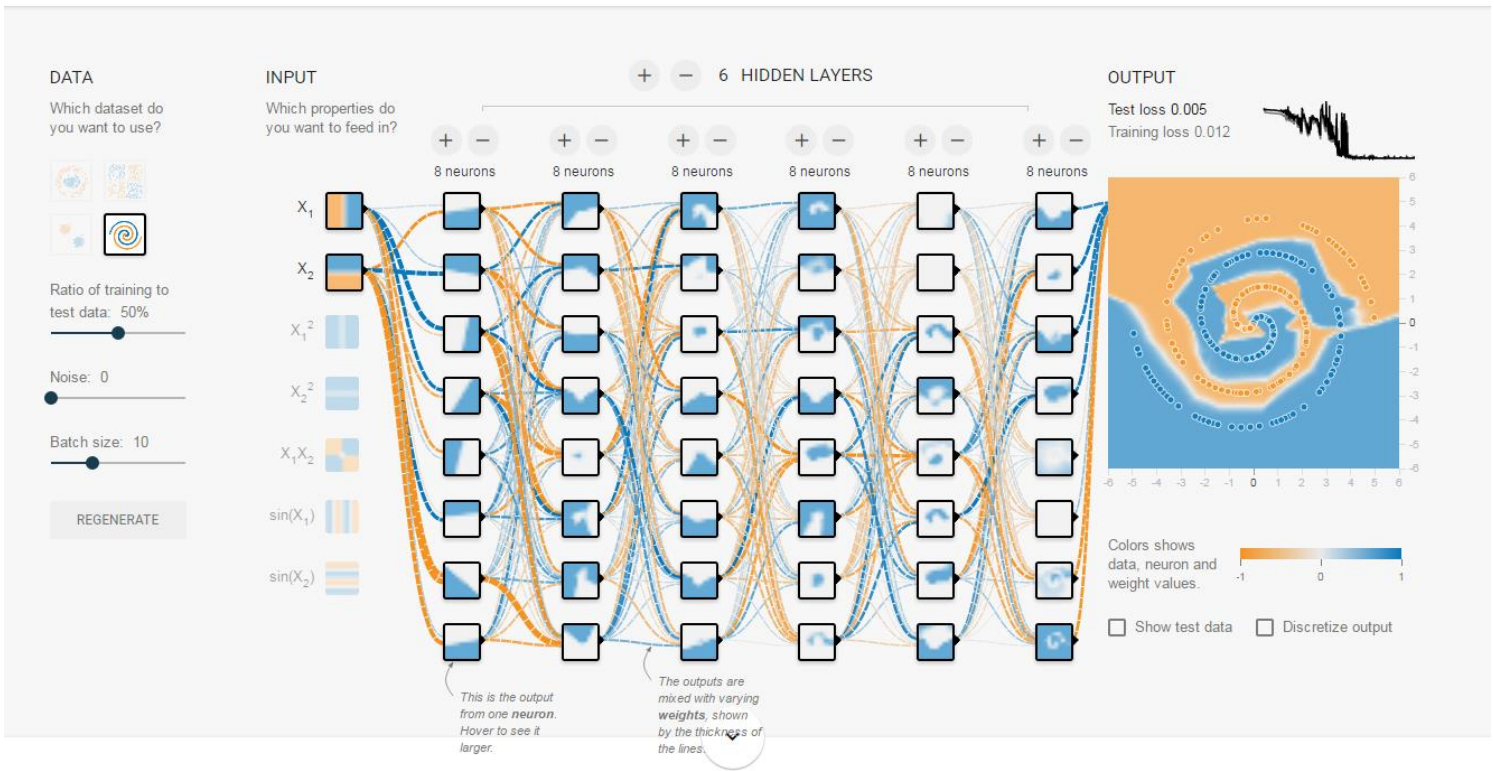
- Iris (붓꽃)종의 3 종류의 꽃 50개씩의 꽃잎 (petal)과 꽃잎받침 (sepal)의 넓이와 높이를 측정한 데이터
- R을 설치하면 기본으로 깔려 있는 몇 개의 데이터 중 하나, 간단하지만 정확하고 적절한 개수의 샘플로 사용처가 매우 높음
- 꽃잎과 꽃잎받침의 수치만을 가지고 기계가 어떤 꽃의 정보인지 자동으로 판단하게 하는 모델

Machine Learning Service

Microsoft
Project Oxford

```
Detection Result:
JSON:
[
  {
    "faceId": "48cdf8c8-841c-4d33-b875-1710a3fc6542",
    "faceRectangle": {
      "width": 228,
      "height": 228,
      "left": 460,
      "top": 125
    },
    "faceLandmarks": {
      "pupilLeft": {
        "x": 507,
        "y": 204.9
      },
      "pupilRight": {
        "x": 609.8,
        "y": 175.4
      },
      "noseTip": {
```

Machine Learning Service



2.2 Machine Learning Service



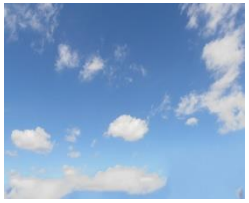














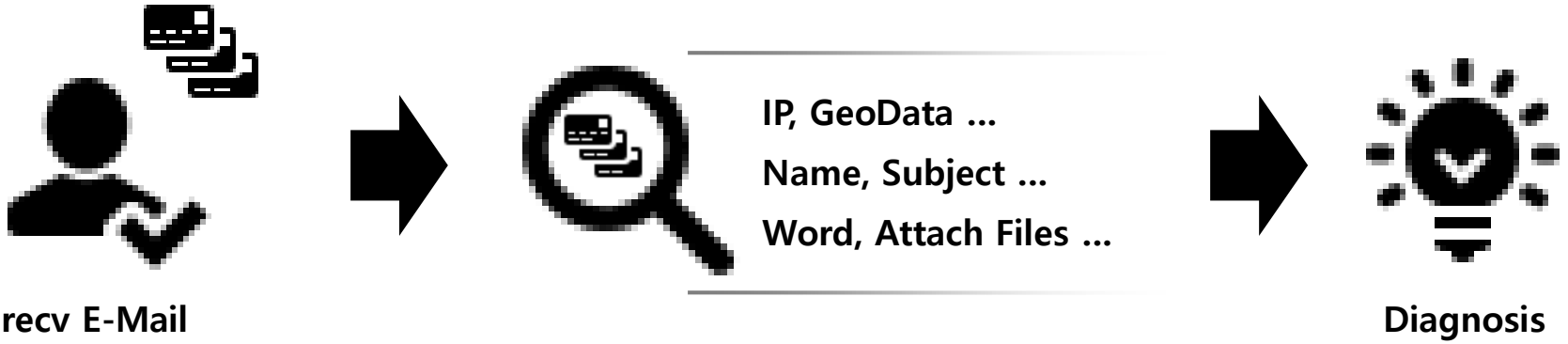

IGLOOSECURITY

Machine Learning Security Service

Detect Malware

Find SpearPhishing

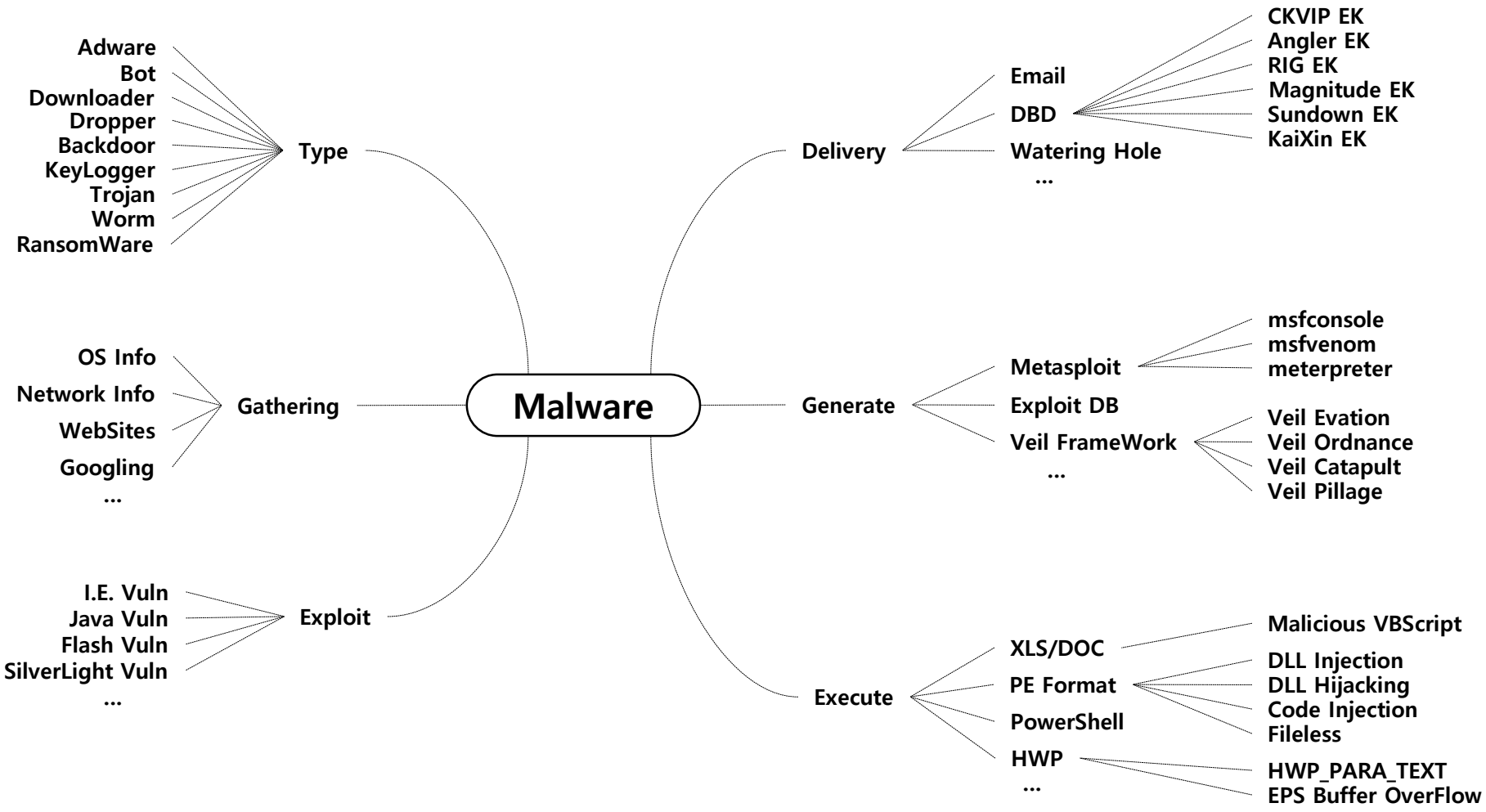
Prevention
BruteForce Attack



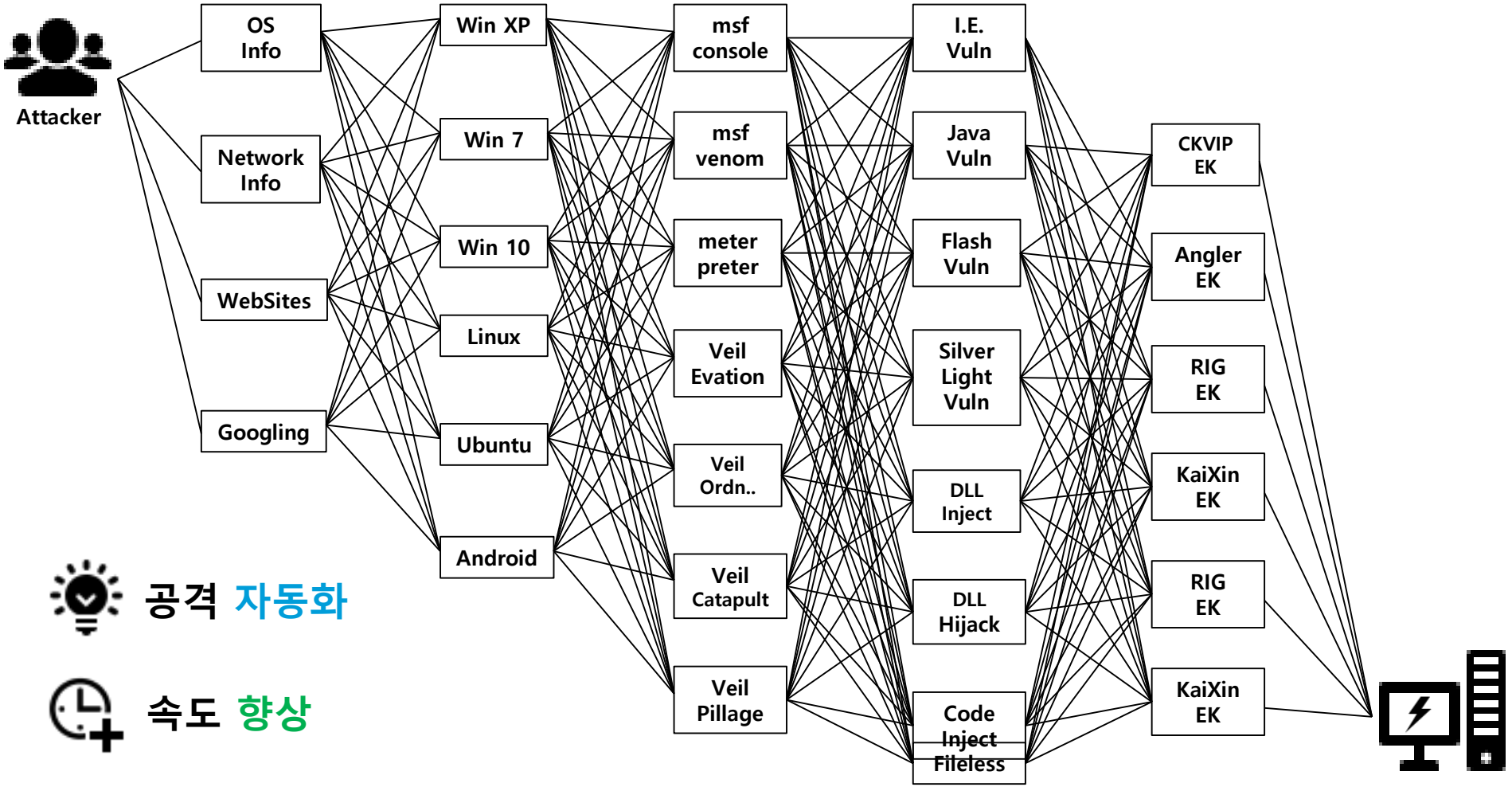
recv E-Mail

Diagnosis

Malware Threat using Machine Learning



APT using Machine Learning

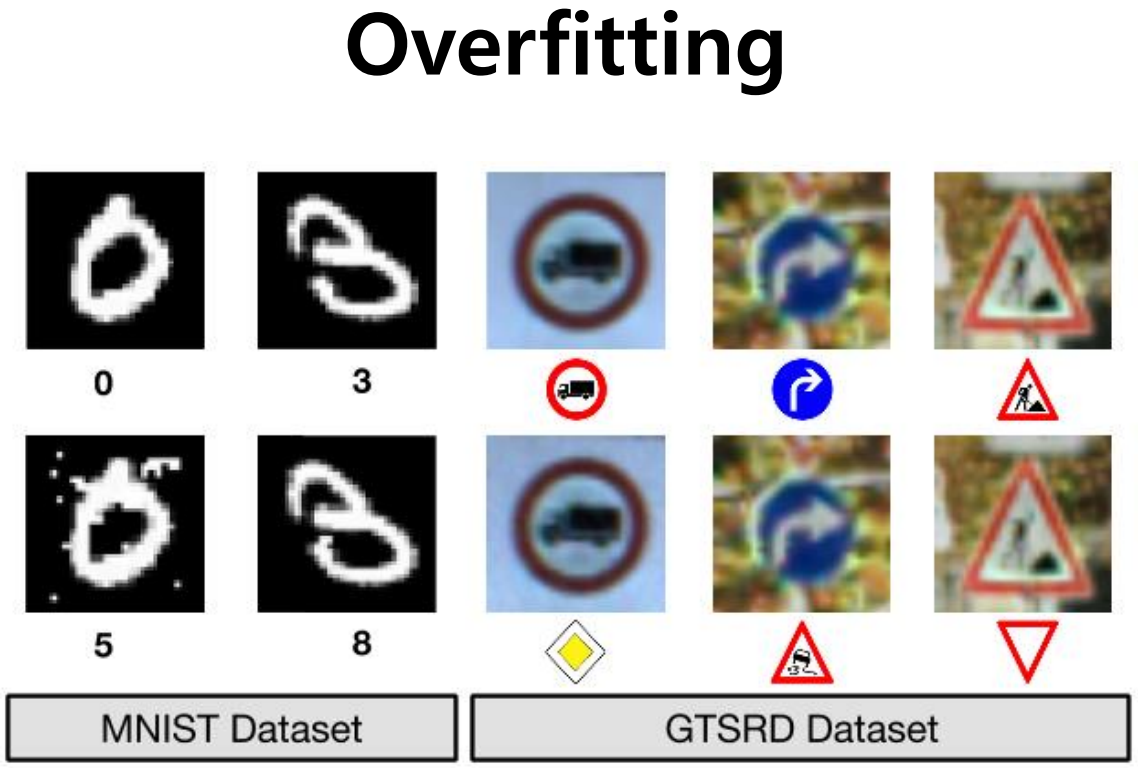


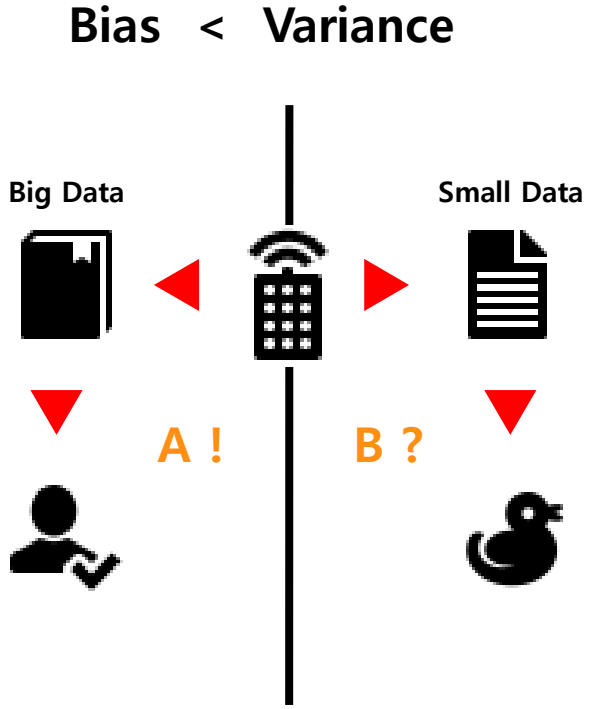
공격 자동화

속도 향상

위협 증대

Machine Learning Vulnerability #1





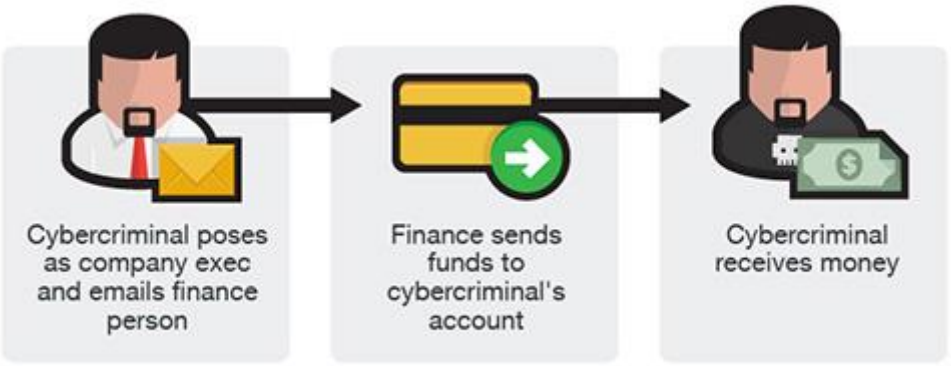
Machine Learning Vulnerability #2

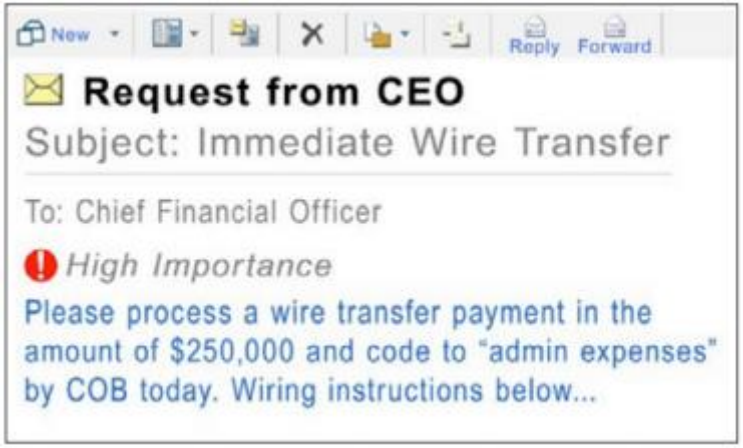
Machine Learning Hacking Case

B **Business**

E **Email**

C **Compromise**





Machine Learning Hacking Case

[BEC Attack Scenario Concept]

출처 : Intel Security

Data Collection

Data Breaches
Social Media
Public Disclosures

Training ML Models

Extract Tranform Load
Feature Selection
Generation

Target Acquisition

Prediction With ML

Initial Contact

Employ well-known
Social engineering
techniques

Attack

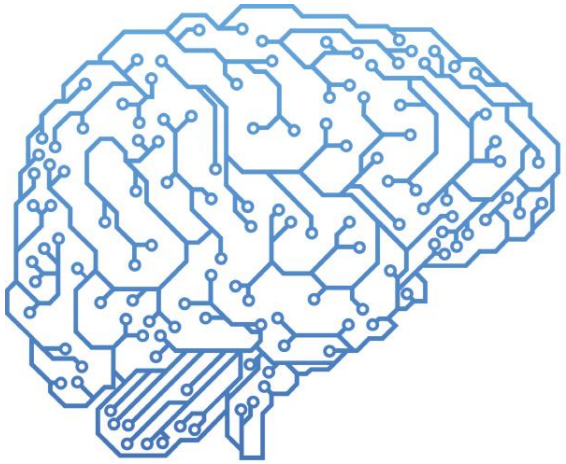
SET

Probability

30억

약 100개 국

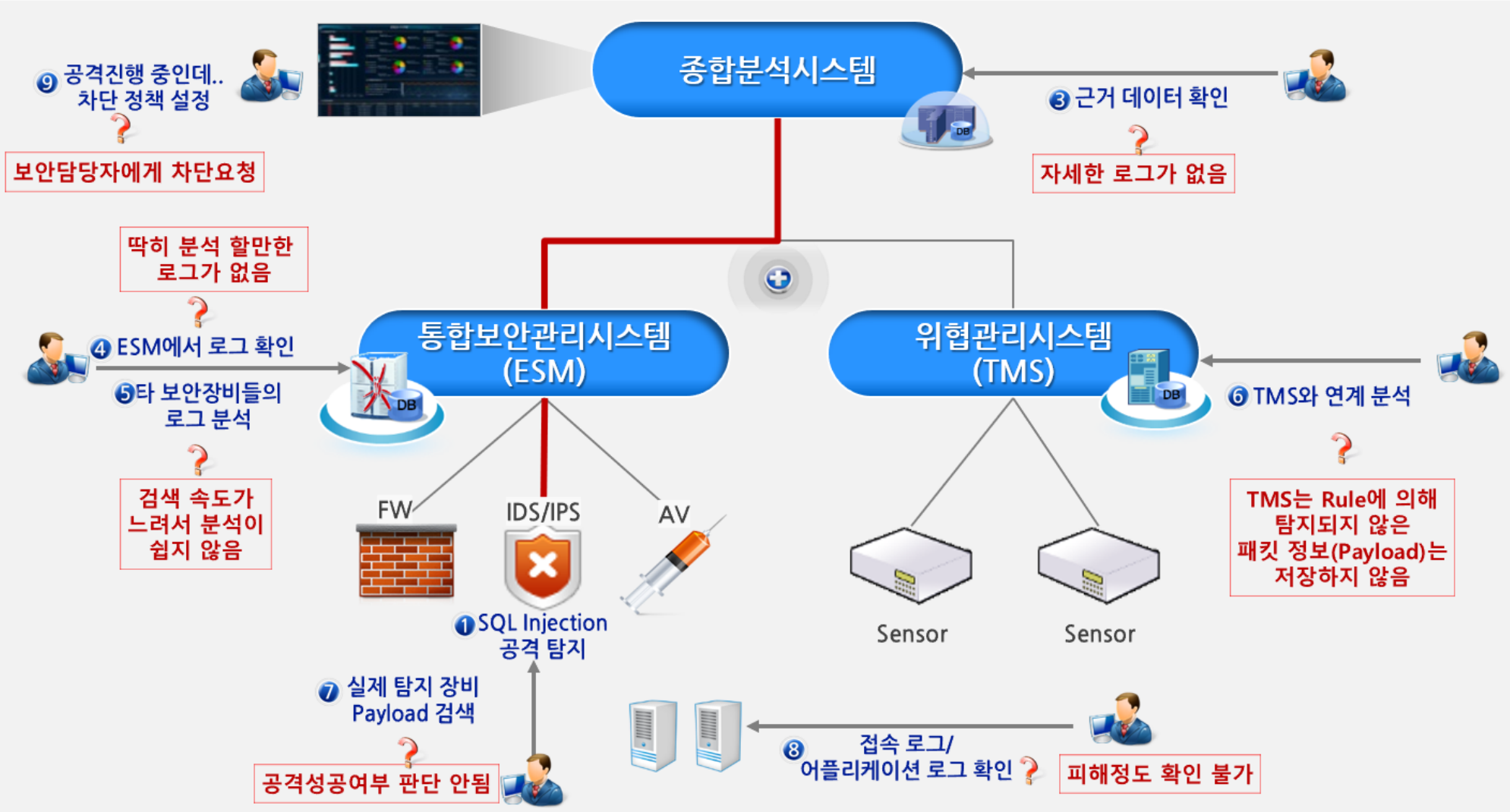
2.5 Future Task



03 Machine Learning Response

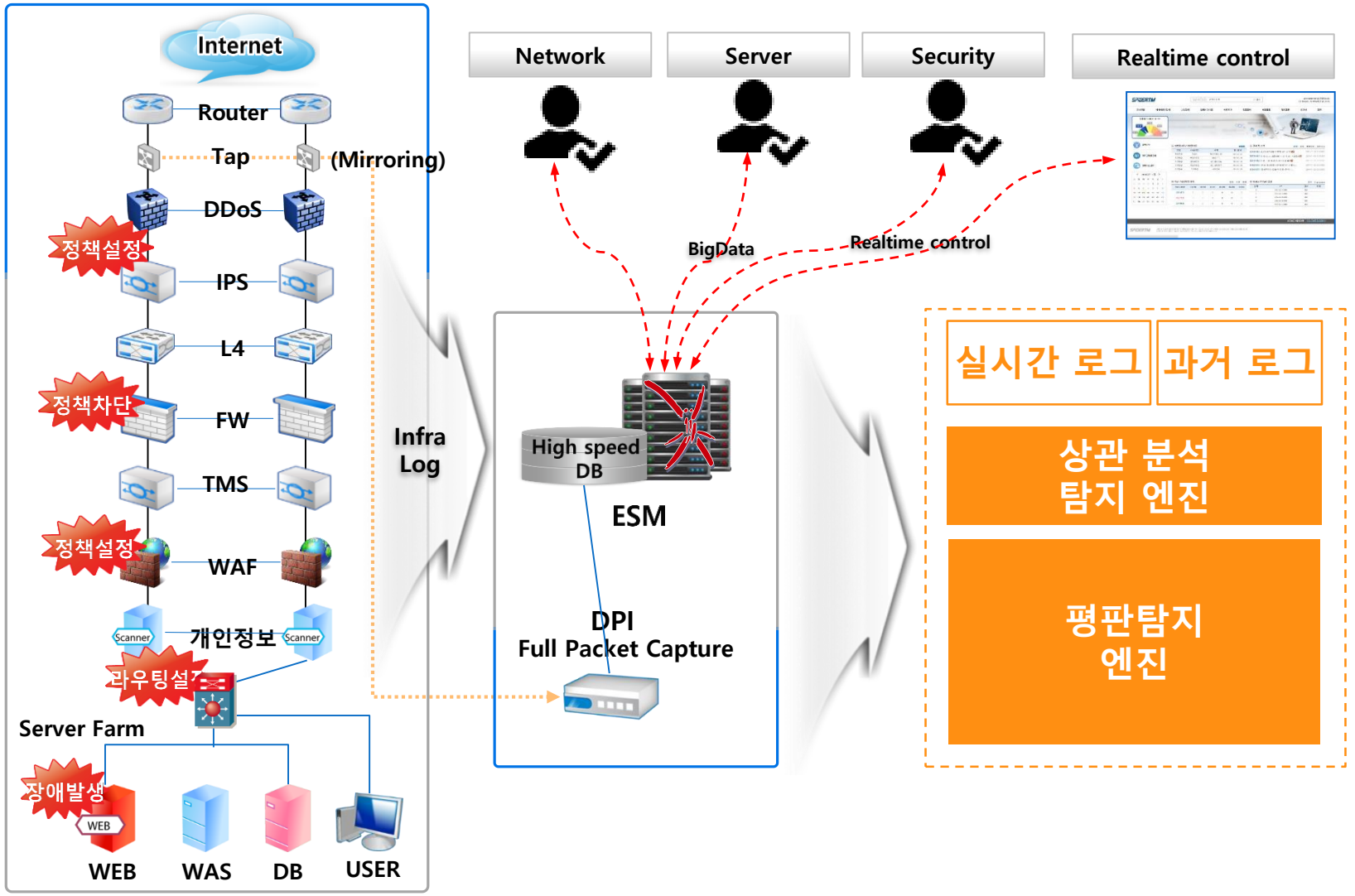
3.1 Response Status

Cyber Attack Response Status



3.2 Evolution of Response

Cyber Attack Evolution of response



IGLOOSECURITY

3.2 Evolution of Response

Cyber Attack Evolution of response

Issue sharing

SIEM

Knowledge Center

Weak point
Malignant code report

Harmful IP, Harmful URL
Automation acquisition

Security trend

출처 : Igloo Security K-Center

3.3 Machine Learning Uses

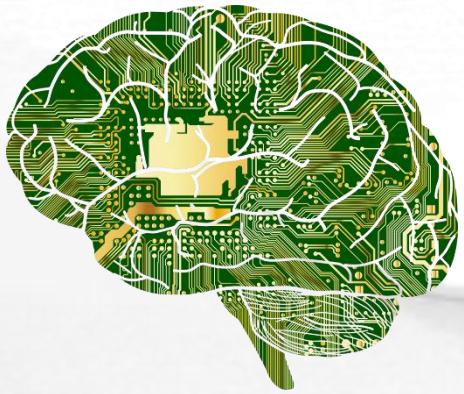
Learning Method

C-TAS

KISA 한국인터넷진흥원

OSINT

CYBER THREAT ALLIANCE



Internal Security Log

Information Flow

Scenario Rule

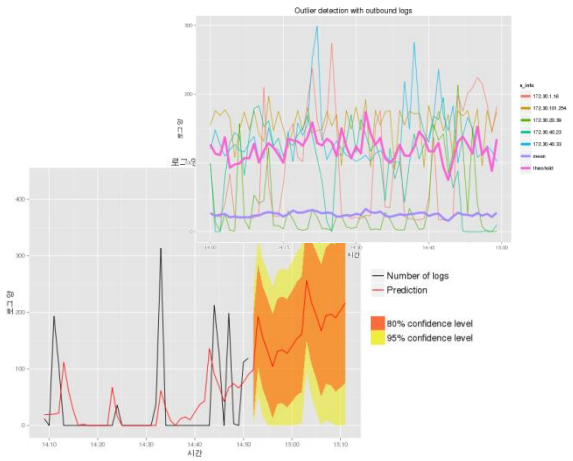
3.3 Machine Learning Uses

Machine-Learning Anomaly Detection

통계적 이상치 탐지 기법 연구

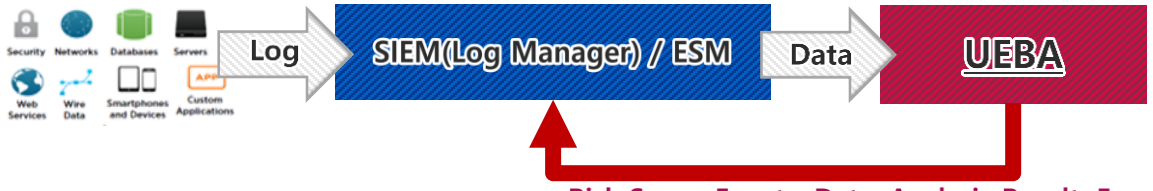
- Anomaly detection

- GARCH(Generalized ARCH) Model
  Holt-Winters
  알려지지 않은 비정상 트래픽 실시간 탐지 테스트



Gartner

User and Entity Behavior Analytics (UEBA)



- Risk Score, Events, Data, Analysis Result, Forensic

- Interrelationship of SIEM and UEBA
  Network, Malware Analysis, Endpoint, Identity and Access Management
- Machine Learning uses

DARKTRACE LIGHTCYBER VECTRA™ niara RSA CONFERENCE

IGLOOSECURITY

Network / Malware

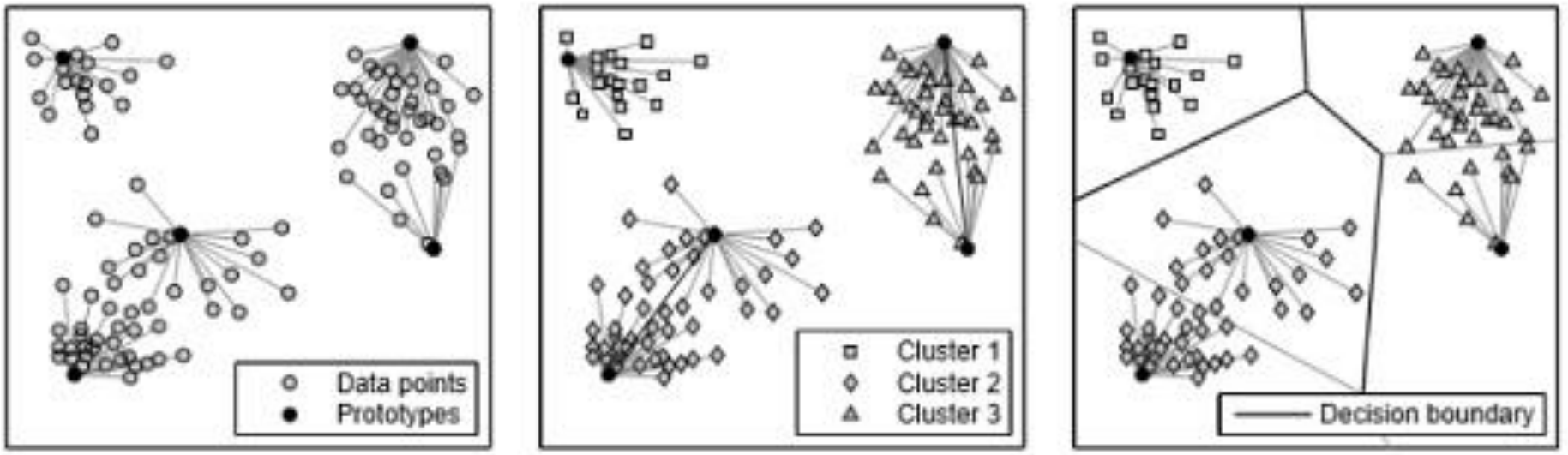
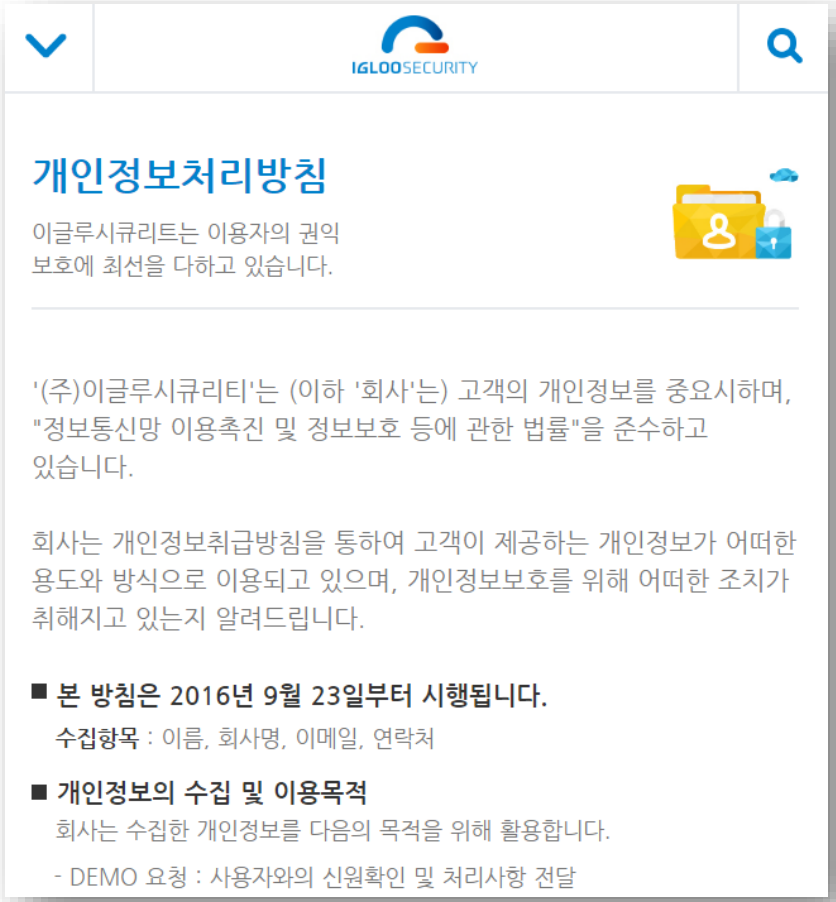


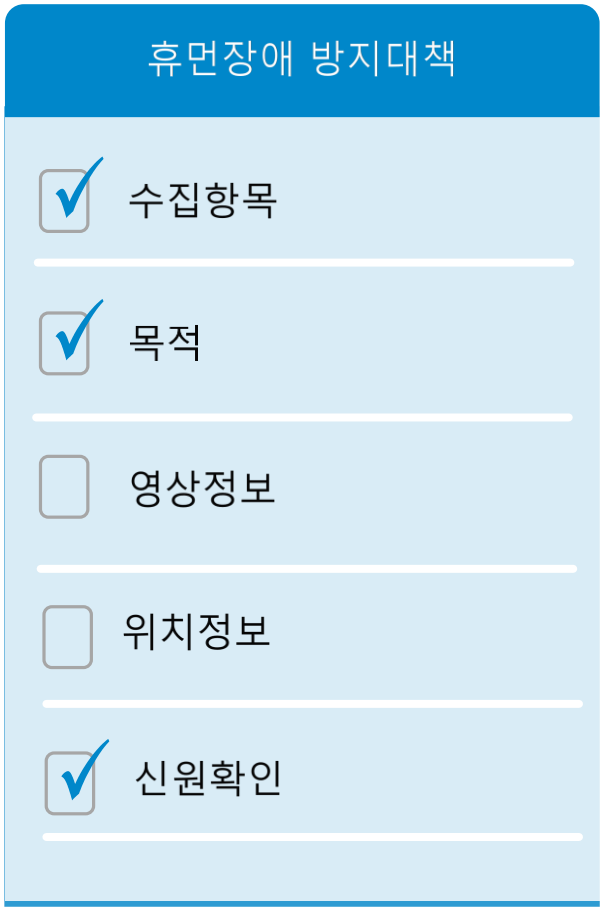
Figure 4: Behavior analysis using prototypes: (a) prototypes of data, (b) clustering using prototypes, and (c) classification using prototypes. Black lines in Figure 4(b) indicate prototypes joined by linkage clustering. Black lines in Figure 4(c) represent the class decision boundary.

• 악성코드 행위 분석 예시 (출처: Automatic Analysis of Malware Behavior using Machine Learning)

3.3 Machine Learning Uses

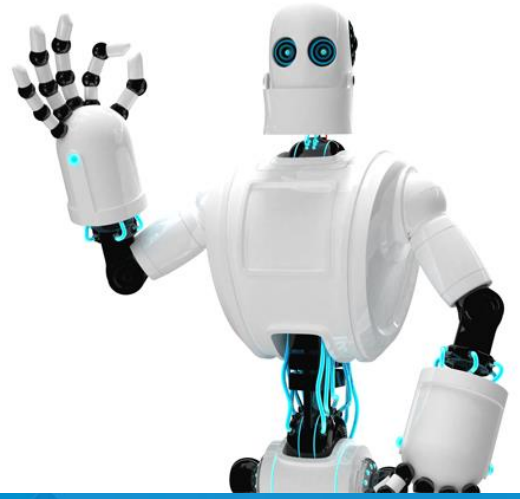
Information protection policy / Weak point





3.4 Future Task

Effective Method



04 Security Artificial Intelligence

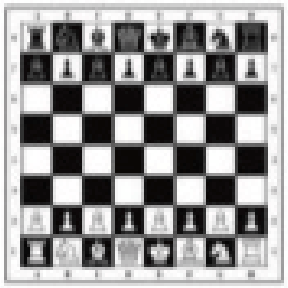
4.1 Artificial Intelligence Concept

AI

AI

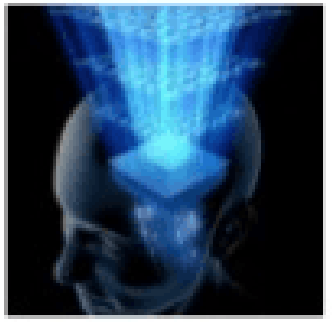
Three types or calibers of AI:

- Artificial Narrow Intelligence (ANI)
- Artificial General Intelligence (AGI)
- Artificial Superintelligence (ASI)



ANI: Chess Program

AGI: Human Level Intelligence



ASI: Superintelligence

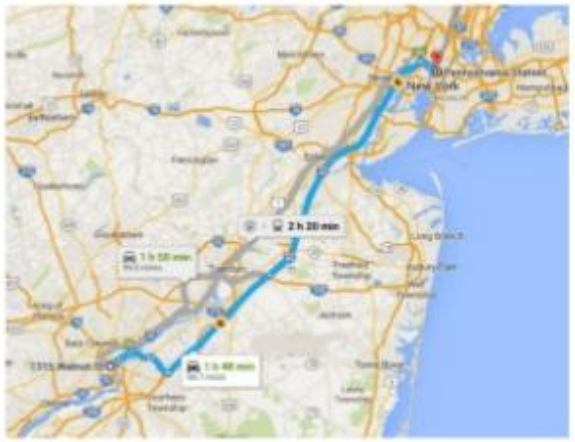
• 이미지 출처: MIS2101 Superintelligence ALALOUF

4.2 Artificial Intelligence Uses Case

AI Service Case

ANI is **everywhere**:

- Google maps
- Autonomous cars
- Spam filters
- Google translate
- Travel bookings
- Manufacturing
- Facebook suggestions



IBM Watson

- Analyzes unstructured data
- Understands complex questions
- Learns human constructs like language, culture, and context

IBM Watson

• 이미지 출처: MIS2101 Superintelligence ALALOUF

4.2 Artificial Intelligence Uses Case

AI Service Case

프로 9단 이세돌

인간 대 인공지능의 대결

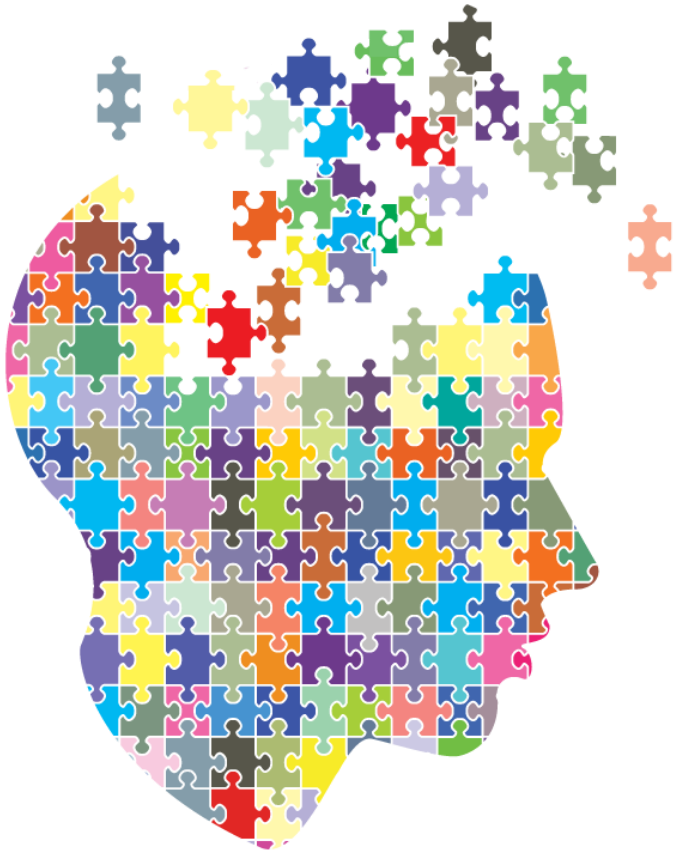
1967년	체스	체스 프로그램 '맥핵' vs 철학자 후버트 드레퓌스	맥핵 승
1996년	체스	IBM 수퍼컴퓨터 '딥블루' vs 체스 세계챔피언 개리 카스파로프	카스파로프 승 (3승 2무 1패)
1997년	체스	IBM 수퍼컴 '디퍼블루' vs 카스파로프	디퍼블루 승 (2승 3무 1패)
2011년	퀴즈	IBM 수퍼컴 '왓슨' vs 퀴즈 챔피언 제닝스·루터	왓슨 우승
2013년	장기	장기 프로그램 '어웨이크' vs 일본 프로기사 연합	어웨이크 승 (3승 1무 1패)
2015년	포커	포커 프로그램 '클라우디코' vs 프로 포커선수 4명	프로 선수 승리
2015년	바둑	구글 '알파고' vs 프로 바둑기사 판후이(2단)	알파고 승 (5승 무패)
2016년 3월	바둑	알파고 vs 프로 9단 이세돌	?

AlphaGo

그래픽=양인성

4.3 Future Task

Security AI



Google 정보보안 ai

전체 이미지 뉴스 동영상 지도 더보기 설정 도구

검색결과 약 210,000개 (0.53초)

인공지능(AI)과 정보보안 - One Step Ahead 이글루시큐리티
www.igloosec.co.kr/BLOG_인공지능(AI)과%20정보보안?searchItem...1...1
2016. 10. 5. - 시기. 주요 내용. 1940년. 뉴런의 기능 및 작용과 명제 논리에 대한 연구로부터 인공지능의 개념 등장. 1950년. Dartmouth Conference를 통해 인공 ...

[칼럼] 인공지능(AI)과 정보보안 - 키뉴스
www.kinews.net/news/articleView.html?idxno=72554
2016. 9. 6. - 복합적인 지능과 판단력이 요구되는 바둑 영역까지 정복한 인공지능에 대한 관심은 점점 더 커져가고 있으며, **정보보안** 분야 역시 예외는 아니다.

인공지능(AI)과 정보보안, 어디까지 왔나? : 네이버 블로그
blog.naver.com/PostView.nhn?blogId=skinfosec2000&logNo...12...
2016. 4. 3. - 여전히'딥러닝' 중이라는 알파고, 그리고 **AI**로 통칭되는 인공지능의 현재를 알아보고 우리가 속한 **정보보안** 분야가 나가야 할 방향에 대해 생각해 ...

AI는 사이버 보안을 승리로 이끌 것인가 - 지디넷코리아
www.zdnet.co.kr/news/news_view.asp?artice_id=20160718145352
2016. 7. 18. - **보안** 위협 급증 속 **AI** 활용해 인력부담 해소 기대 ... 것은 사기든 이례적이든 의심되는 것만 보여주므로 더 정확한 **정보**를 받게 해준다"고 밝혔다. .

"AI 보안, 지능형 공격 막기는 아직 무리" - 지디넷코리아
www.zdnet.co.kr/news/news_view.asp?artice_id=20160421173433
2016. 4. 21. - "**AI 보안**, 지능형 공격 막기는 아직 무리". MIT, AI2 프로젝트 가동...일반적인 방어엔 효과. 손경호 기자; 입력 : 2016.04.21.18:03; 수정 ...

'인공지능(AI)' 기술, 보안 분야 활용 본격화되나 - 디지털데일리
www.ddaily.co.kr/news/article.html?no=139884
2016. 1. 31. - [디지털데일리 이유지기자] "인공지능(**AI**) 기술이 **보안** 분야에 활용하는 ... 분야에서 발생한 사이버 위협 **정보**를 서로 공유하는데 활용할 수 있다.

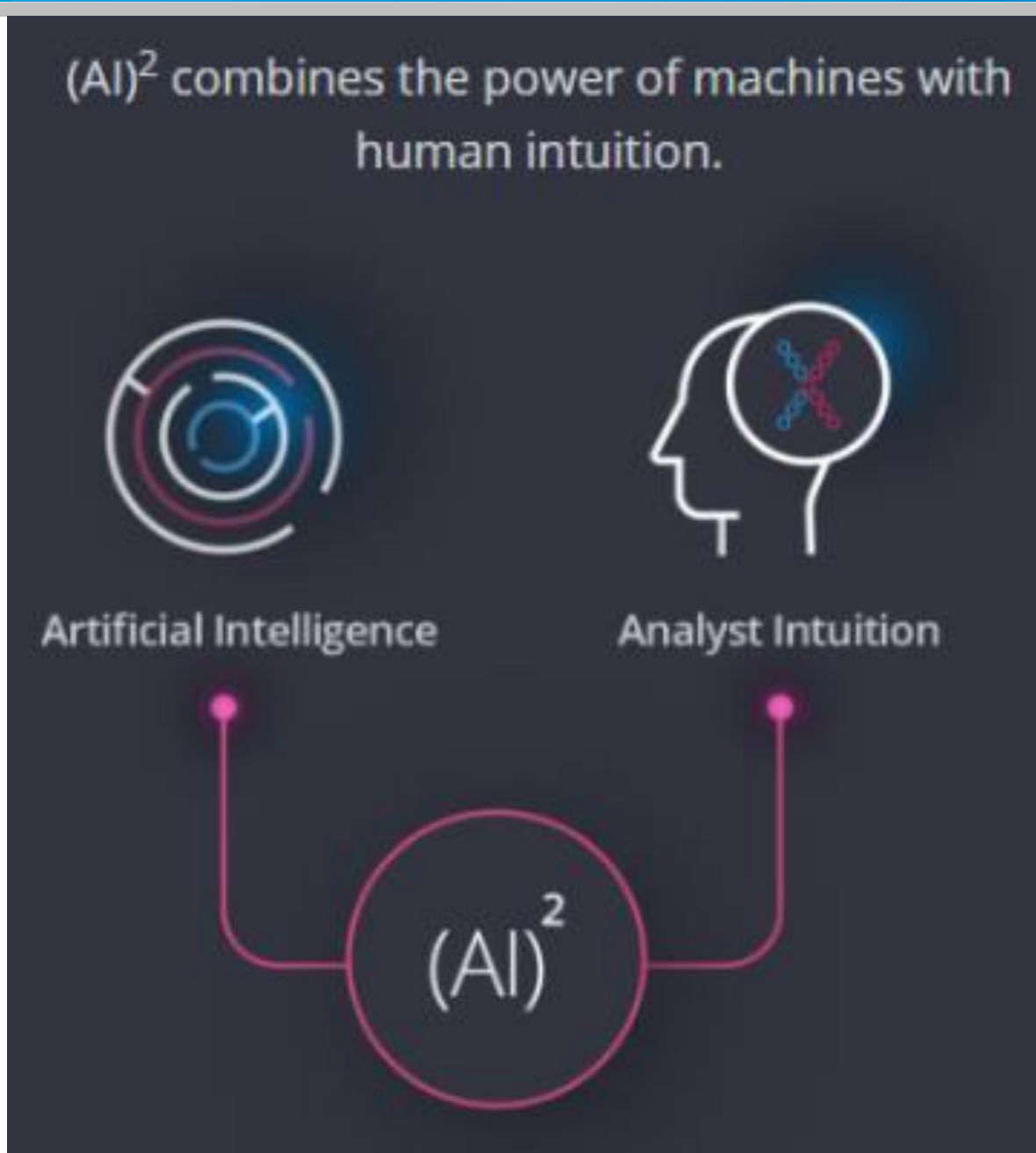
IT 보안도 이젠 AI가 맡는다 - 검색 - 소비자금융 - 메트로신문
m.metroseoul.co.kr/news/newsview?newscd=2016053100125
2016. 5. 31. - [메트로신문 오세성 기자] 알파고로 시작된 인공지능(**AI**) 열풍이 IT**보안** ... 서울고검에서 북한 해킹조직이 국내 금융**정보 보안**업체 I사의 '코드서명'을 ...

인공지능이 정보보안과 물리보안에 미치는 영향 - SECON 2016 ...
www.seconexpo.com/2016/kor/press/view.asp?idx=920&page=1&search...
그럼에도 불구하고 올해 물리**보안** 분야에서도 인공지능 기술 활용을 통한 **보안** 강화와 효율성 제고가 주

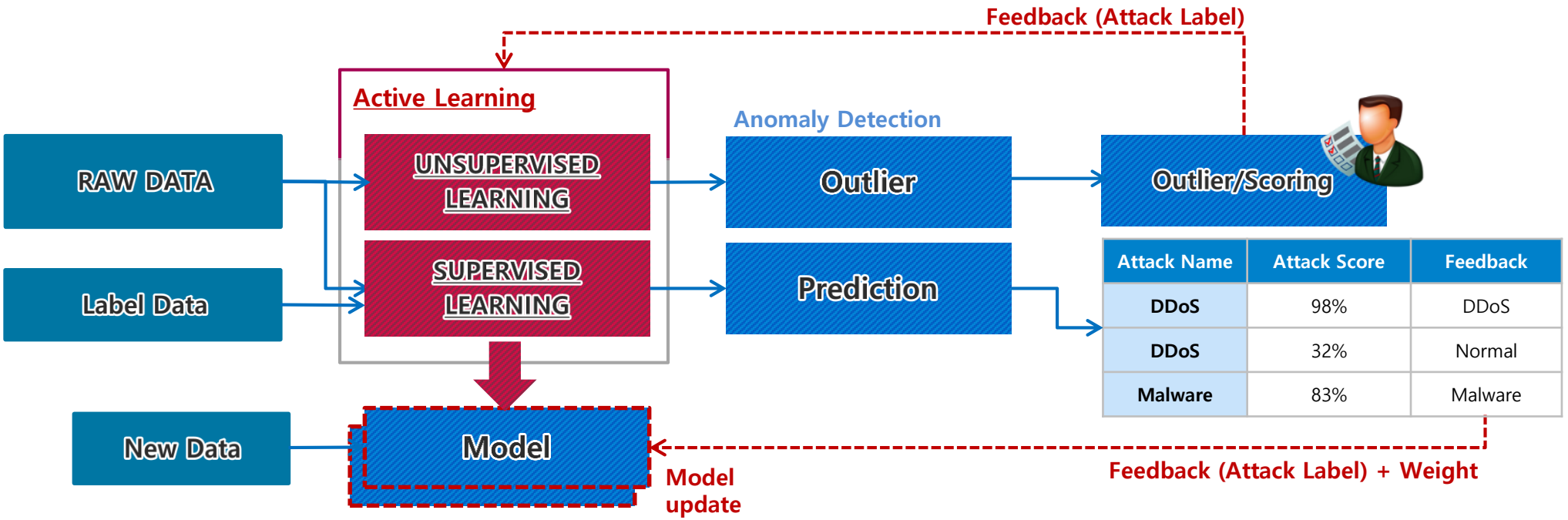
4.3 Future Task

ACTIVE LEARNING - DYNAMIC LABELS

- The Human Is the Key Ingredient(중요한 요소) for AI
- 사람과 기계의 결합 $(AI)^2$ =
  분석가의 직관력(Analyst Intuition, AI)
  +
  인공지능 (Artificial Intelligence)
- 보안 전문가의 피드백에 기반 학습



SIEM + AI System Interoperability

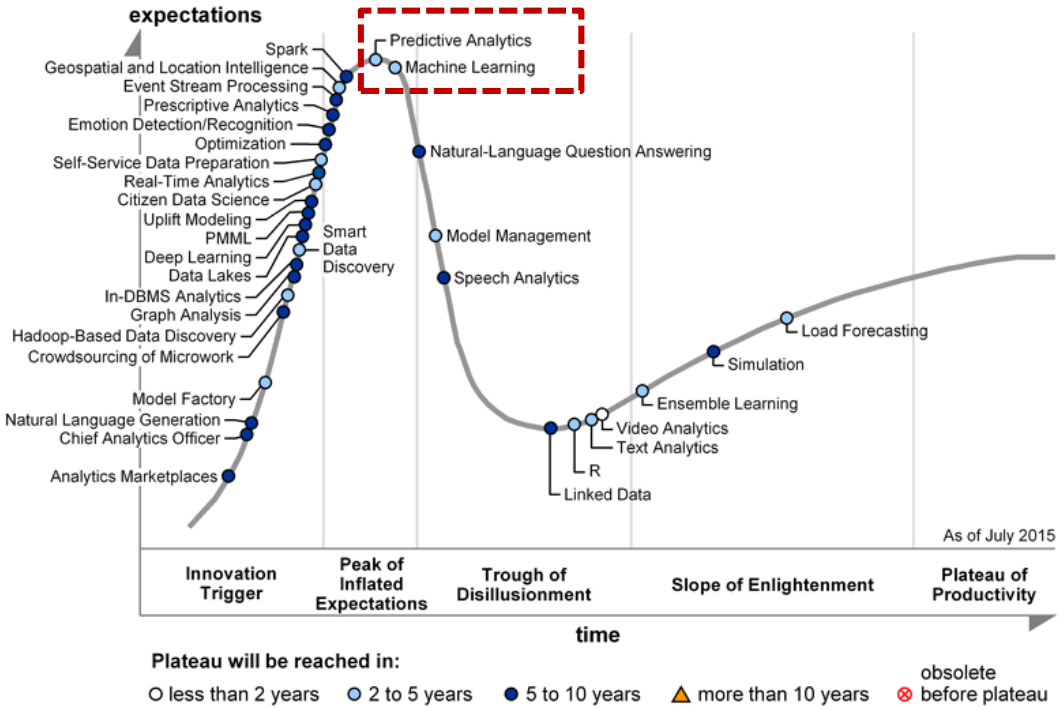


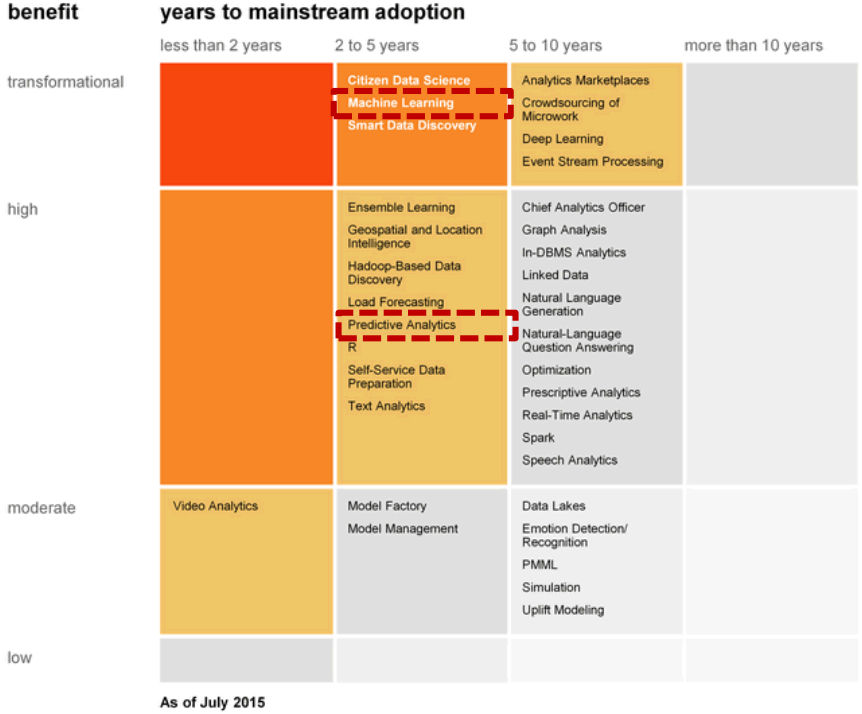
- 보안 전문가와 인공지능의 결합을 통한 선순환 구조를 가진 Active Learning 아키텍처를 통하여 오탐(False Positives)을 줄이고 정확도를 향상시키도록 연구 개발

Hype Cycle for Advanced Analytics and Data Science, 2015

Gartner

- **Priority Matrix for Advanced Analytics and Data Science, 2015**





IGLOOSECURITY

Strategic Planning Assumptions

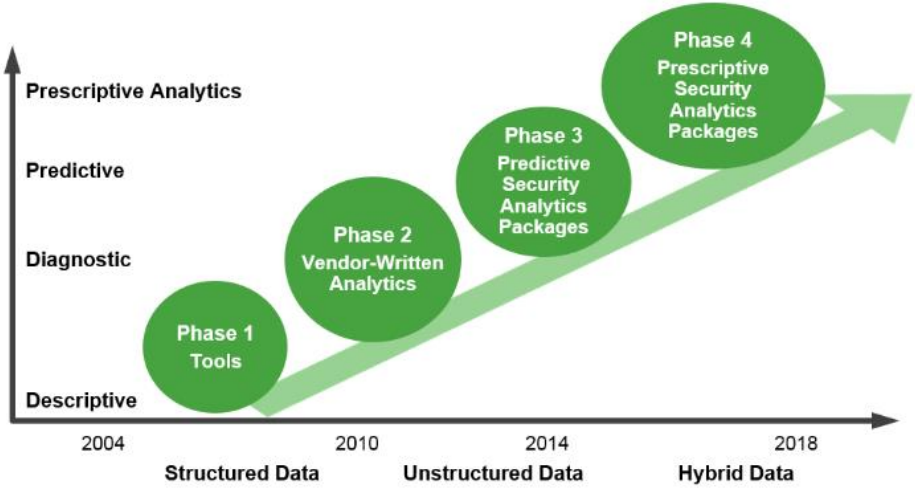
Gartner

- By 2018, at least 50% of major SIEM vendors will incorporate UEBA functionality into their products.
- By 2018, 25% of security products used for detection will have some form of machine learning built into them.

  50% SIEM UEBA 포함, 25% 보안제품 머신러닝 사용
- By 2018, prescriptive analytics will be deployed in at least 10% of UEBA products to automate response to incidents, up from zero today.

  사건의 자동화 대응을 위해 UEBA 10% 적용

- Emergence of Advanced Security Analytics



IGLOOSECURITY

05 AI vs Human

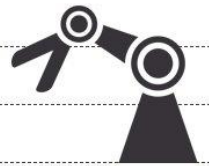
AI Job

인공지능시대, 살아남을 확률 낮은 직업은?

1위 콘크리트공
2위 정육원 및 도축원
3위 고무 및 플라스틱 제품조립원
79위 보안 관제사

4위 청원경찰
5위 조세행정사무원
6위 물품이동장비조작원
7위 경리사무원
8위 환경미화원 및 재활용품수거원
9위 세탁 관련 기계조작원
10위 택배원
11위 과수작물재배원
12위 행정 및 경영지원 관련 서비스 관리자
13위 주유원
14위 부동산 컨설턴트 및 중개인
15위 건축도장공

특징 tong+
- 단순 반복적인 업무
- 정교함이 떨어지는 동작
- 사람들과 소통하는 직업

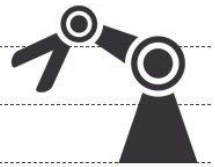


그래픽 tong+ 자료 한국고용정보원 대상 우리나라 주요 직업 400여개

인공지능시대, 살아남을 확률 높은 직업은?

1위 화가 및 조각가
2위 사진작가 및 사진사
3위 작가 및 관련 전문가

4위 지휘자·작곡가 및 연주가
5위 애니메이터 및 만화가
6위 무용가 및 안무가
7위 가수 및 성악가
8위 메이크업아티스트 및 분장사
9위 공예원
10위 예능 강사
11위 패션디자이너
12위 국악 및 전통 예능인
13위 감독 및 기술감독
14위 배우 및 모델
15위 제품디자이너



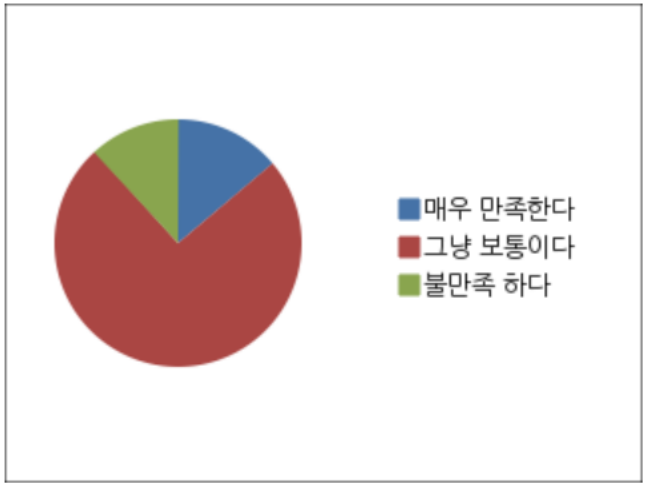
특징 tong+
- 감성에 기초한 예술 관련 직종
- 창의적 지능 이용
- 손을 이용한 정교한 작업
- 협상 및 설득 요구하는 직업

그래픽 tong+ 자료 한국고용정보원 대상 우리나라 주요 직업 400여개

5.2 Security Expert Job Satisfaction

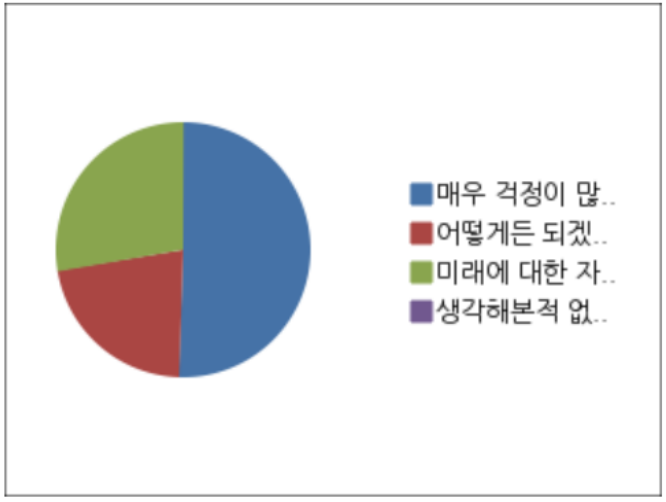
Question Investigation

1. 보안전문가로서 근무함에 있어서 만족 하십니까?



매우 만족한다	14	13%
그냥 보통이다	75	74%
불만족 하다	12	11%

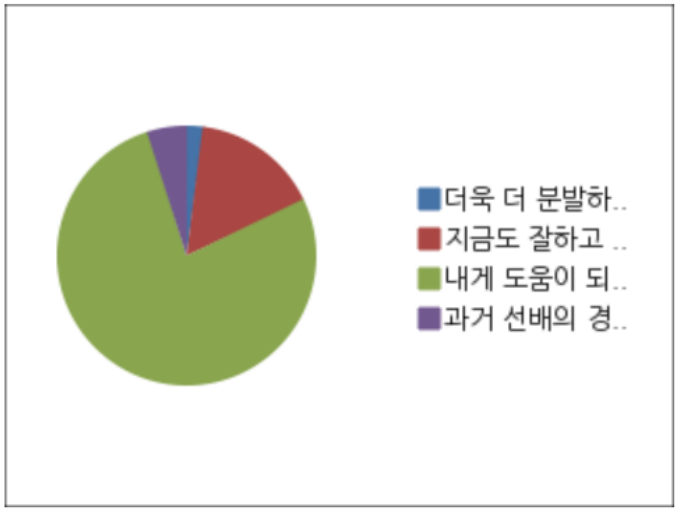
2. 지금 하는일로 근무하면서 미래에 대한 걱정이 있는가?



매우 걱정이 많이된다	51	50%
어떻게든 되겠지라고 낙천적이다	22	21%
미래에 대한 자신감과 비전을 가지고 있다	28	27%
생각해본적 없다	0	0%

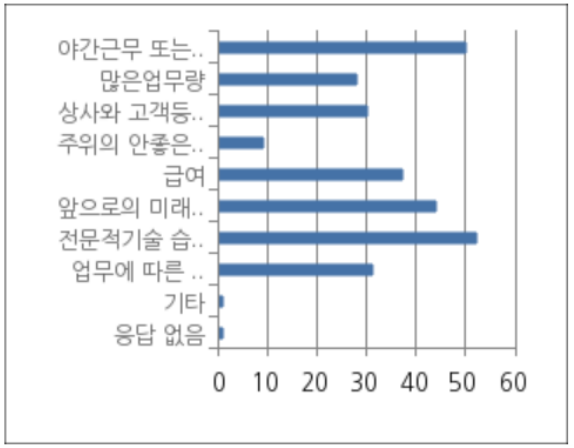
Question Investigation

3. 직장 상사나 선배 보안전문가가 내게 해주었으면 하는 조언이 있다면 무엇일까요?



더욱 더 분발하라는 충고와 채찍질	2	1%
지금도 잘하고 있다는 칭찬	16	15%
내게 도움이 되는 자세한 방향성에 대한 설명	78	77%
과거 선배의 경험담	5	4%

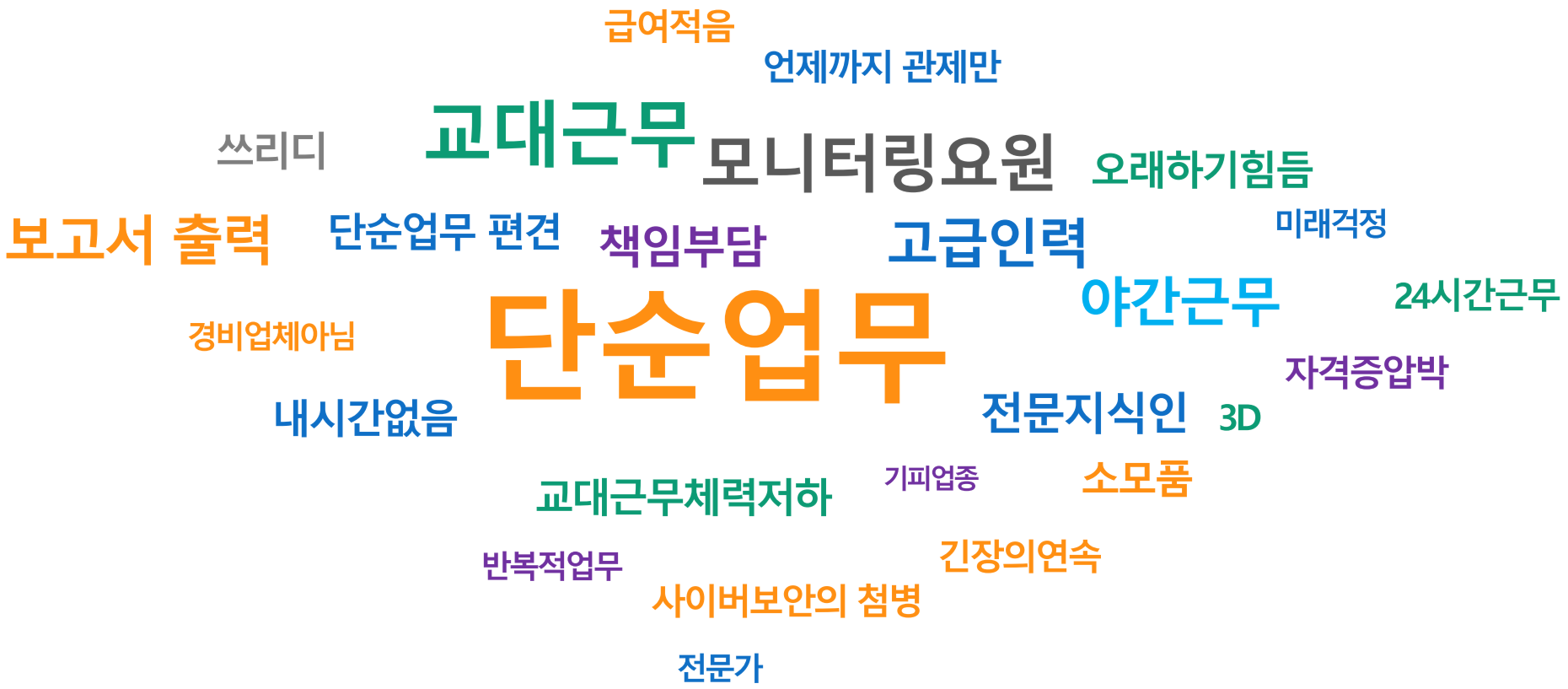
4. 현재 근무하면서 가장 어려운점은 무었입니까?



야간근무 또는 야근	50	49%
많은업무량	28	27%
상사와 고객등의 인간관계	30	29%
주위의 안좋은편견	9	8%
급여	37	36%
앞으로의 미래 또는 비젼	44	43%
전문적기술 습득	52	51%
업무에 따른 책임소지	31	30%
기타	1	0%
응답 없음	1	0%

5.2 Security Expert Job Satisfaction

Question Investigation



Question Investigation

- 관제란 업무가 단순 모니터링만 하는것으로 인식되는 것 같고,보안관련 이슈와 중요도가 증가되고 있는 추세이며 업무량및 근무시간도 증가되지만 급여 및 인력충원이 증가되지 못하는 듯하다
- 유의미한 정보(공격시도, 취약사항)를 알려줘도 운영자들에게 귀찮은 존재 [illegible] 하지 않는다면 할만하다
- 전망은 밝지만 낙오되면 실업자가 된다
- 자부심을 가져야하지만 현실은 좀 다르다
- 보안 [illegible] 근무하는 직원들의 지위 [illegible] 업무/자부심 [illegible] 높이기 [illegible] 됩니다.
- 서로 많이 공유하고 배워나갔으면 좋겠습니다
- 실무자들끼리 정보공유의 장이 있었으면 좋겠습니다
- 현실에 [illegible] 된다 [illegible]
- 자기 하는 일에 대한 자부심을 느꼈으면 합니다
- 보안전문가로 성장할수 있게 회사 내부에서 [illegible] 교육과정을 만들었으면 좋겠습니다
- 보안일을하면서 어느누구보다도 자부심을갖고 일을했지만 보안이라는일자체가 주가아닌 부라는 갑이아닌 을로 일을해야하는 매번 반복되는상황에서 항상 갑이라는 곳에서 알아봐주지않음. 어떠한일을하는지 어떻게일을하는지
- 맡은 업무에 비해 부담감이나 인정받는 부분이 현실적으로 다른 직업군보다 [illegible] 이런 부분을 국가기관이나 기업에서 나서서 앞으로의 사이버 피해로 지적재산 등에 따른 큰 피해 후 늦장조치보다 인력양성 등을 통한 지원으로 손실을 예방하여 피해를 최소화하는 잇점과 보안인의 가치를 높일수 있는 계기를 만들어 줬으면 합니다.
- 관제업무를 하면서 장비의 능력도 중요하지만 그걸 운영하고 정책룰을 생성하는것은 관제및분석요원입니다. 선배님들의 노하우를 많이 전수해줬으면 좋겠습니다

✓ 실무자들끼리 정보공유의 장이 있었으면 좋겠습니다

✓ 자기 하는 일에 대한 자부심을 느꼈으면 합니다

✓ 내가 어떻게 업무에 관련된 실무능력을 배워나갈지 방향성을 제시 받고싶습니다.

✓ 좀더 IT가 대우받는세상이 왔으면 좋겠다.

Question Investigation

- 진정한 보안전문가가 되겠다는 꿈을 가지고 입사한 각오가 있었으나 단순 반복 업무만 진행이되서 성장이 정체 되었고 회사에 기댈수 없고 스스로 알아서 성장해야 하는 분야, 정보보안에 대한 성장의 길을 확실히 알기가 어렵고 스스로 찾아야하고 하루 시간의 대부분을 회사에서 지내다보니 자연스럽게 잊혀진 초기의 목표.. 어느순간 나는 모든 선배들과 똑같이 무난하게 일[illegible] 있었다.

✓ 힘들어도 같이일하는사람과 으쌰~하면 될거같습니다

- 내가 어떻게 업무에 관련된 실무능력을 배워나갈지 방향성을 제시 받고싶습니다.
- 보안분야는 [illegible] 그렇지만, 반드시 누군가는 이 일을 해야만하는 분야
- 관제[illegible] 더 발전적인 업무를 하고 싶다는 [illegible]를 해야한다.

✓ 선배근무자들에게 진로를 물어보며 앞으로의 계획을 가지는게 좋을거 같습니다.

- 지[illegible]
- 힘들어도 같이일하는사람과 으쌰하면 될거같습니다 무사고율 0%를 위해 고생하십니다 파이팅!
- 일할만하니깐어렵게생각하지말아요

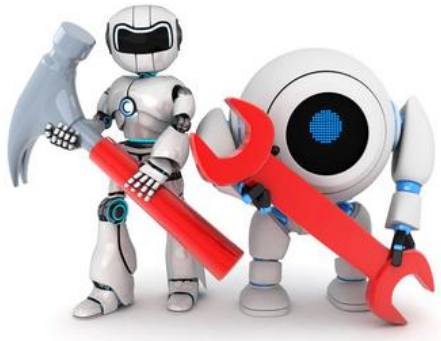
✓ 지속적인 공부와 불투명한 미래에 대해 불안합니다.

- 보안[illegible] 선배근무자들에게 진로를 물어보며 앞으로의 계획을 가지는게 좋을거 같습니다. 보안전문가가 되기 위한 좋은 밑거름이 되는건 확실하다고 생각하지만 신기술 해킹기술과 신규 취약점, 기타 보안동향이 너무 많아 따라가기 위해서는 많은 노력과 지식을 꾸준히 쌓아야 할 [illegible]

✓ 앞으로 나아가야 할 가이드라인이나 방향성 혹은 공부 방향제시가 필요해보임

- 여러[illegible]
- 전문기술을 사용할 수 있는 업무환경이 구축되었으면 함 실제 보안관제 업무를 수행시 전문기술을 적용할 환경이 되지않음 대부분 단순업무 콜대응, ip또는 룰차단. 보안장비 운영이 대부분.
- 앞으로 나아가야 할 가이드라인이나 방향성 혹은 공부 방향제시가 필요해보임

IGLOOSECURITY



감사합니다.