

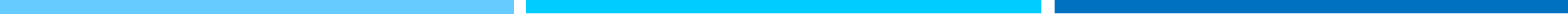
AI security Business

- 이 기 혁
- 중앙대학교 보안대학원 교수
- (사)한국디지털인증협회 회장
- 2024.06.13 포포인츠 바이 쉐라톤 구로



What cake do you call it?





Introduction

Security terminology summary

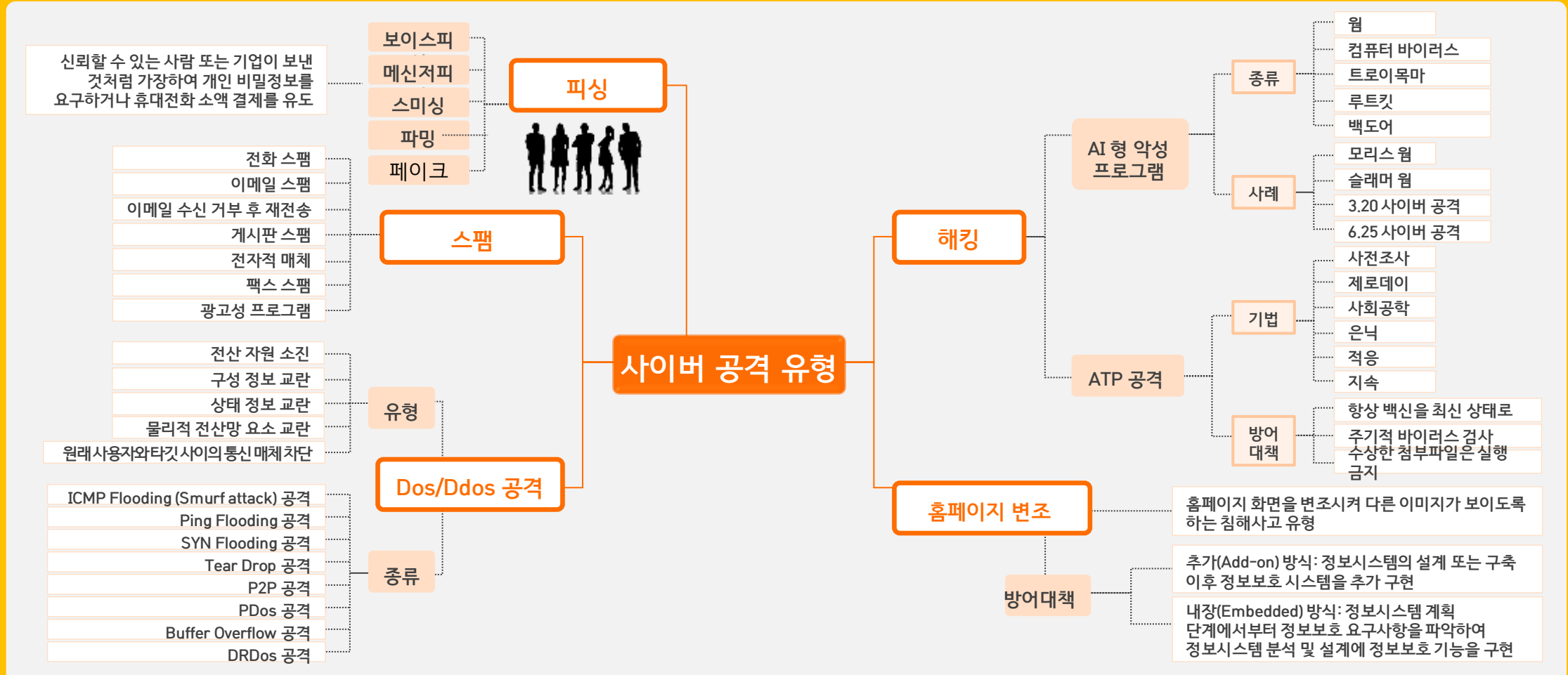
Terms	Concept
보안	환경(Environment)에 놓인 보호대상(Object)을 위험요소(Risk)로부터 보호하여 질서와 안녕을 유지하는 활동
정보보호	정보의 생애주기(생성~유통~파기)관점에서 정보를 가지고 있는 자산을 보호하는 활동
(AI)사이버 보안	사이버공간에서의 보호대상을 위협으로 부터 보호하는 활동
기업 보안	기업(조직)의 안정적인 비즈니스 활동을 위해 자산(보호대상)을 위협으로 부터 보호하는 활동
인적 보안	기업의 구성원과 퇴직 직원 및 비즈니스 파트너, 사람 관련 보안 활동 사람을 공격하는게 해커입장에서 가장 쉬운 공격 포인트
국가 보안	(국가 기관, 산하기관, 소속기관의) 문서보안, 인원보안, 시설보안을 총칭

Security terminology summary

Terms	Concept
산업 보안	① 협의적 개념으로서 산업보안은 조직이 보유한 기술을 보호하는 것 ② 광의적 개념으로서 산업보안은 각 산업의 비즈니스 특징을 반영한 “산업의 보안”
연구 보안	국가연구개발사업의 전(全) 수행과정에서 발생하는 주요 연구 개발 성과를 유출 또는 침해 당하지 않도록 방지하기 위한 활동
(AI)산업융합 보안	① 보안수단의 통합(물리보안 + 정보보안) ② 보안기술과 타 산업과의 융합을 통한 새로운 가치 창출
(AI)물리/시설 보안	① 물리적 통제 장비를 통한 보안영역으로 일부 경호 경비 영역 포함 ② 전통적인 CCTV 출입 Gate등

Types of Cyber Attacks

공격형 인공지능 시스템



Cause of security incident



외부적 요인



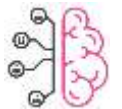
내부 직원



BP/CP등 협력사



복합적 요인

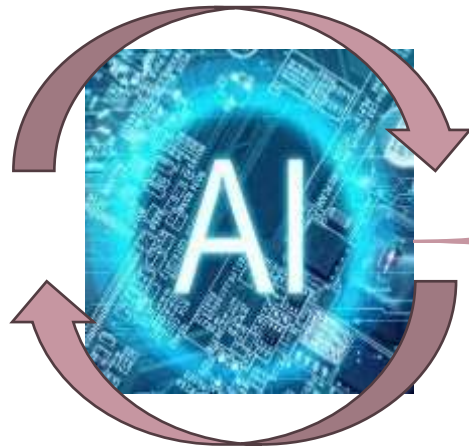


인공지능 공격

- 대부분 보안 침해사고는 외부적 요인에 의함
- OS보다는 Application 공격 시도가 많으며, 특히 취약점을 이용한 고의적 공격 양상
- 73%전후
- 내부 직원에 의한 보안 침해는 수치는 낮지만, 발생 할 경우 그 영향은 외부보다 큼
- 15%전후
- 협력사에 의한 보안 사고는 최근 급속히 증가하고 있음.. 앞으로도 지속적으로 증가하는 추세
- BP(비즈니스 파트너)가 연루된 사건이 전체의 1/3을 넘으며 최근 2~3년 동안 5배 이상 증가
- 39%전후
- 대부분 보안사고는 여러 계층간 연관된 경우로 보안 사고는 생태계 안에 포함되어 있는 모든 구성원을 대상으로 예방활동을 해야 함
- 알 수 없는 인공지능을 이용한 공격 방법의 대두
- AI학습 데이터 사용으로 공격을 더 정교하고, 탐지가 어렵게, 의심스럽지 않게, 대응은 어렵게

AI 지식체계에서 보안은 포괄적인 개념

환경구축 → 수집 → 가공 → 라벨링



기계학습

- 지도학습
- 비지도학습
- 강화학습

자연어처리

- 문장 분석
- 자동 번역
- 질의 응답
- 문장 생성

전문가시스템

- 지식 표현
- 논리 추론
- 불확실성 처리

컴퓨터 비전

- 이미지 인식
- 영상 인식
- 객체 추적

음성 인식

- STT
- TTS

플래팅

- 계획
- 스케줄링

로보틱스

- 자동화
- 이동과 위치

공격용
&
방어용

AI
데이터셋

AI 개발 가속화 및 고성능 IT 기반 인프라를 통한
대용량 데이터 학습으로
AI를 악용한 사이버 공격이나 AI 자체를 노린 새로운 공격시대 개막

AI 지식체계에서 **보안 위협**

AI 서비스 Life-Cycle 전체에서 다양하게 발생 가능

1

학습 단계

수집 데이터 전처리 후 AI가 알고리즘을 통해 학습하는 과정에서 adversarial machine learning을 통한 회피, 오염, 백도어 공격 등의
AI 모델 공격과 H/W와 S/W의 취약점 공격 등 보안위협 발생
(특히 개인정보 오남용)

2

저장 단계

AI가 학습을 위한 수집데이터와 AI 제품 · 서비스 제공을 위한 학습 후 데이터를 저장하는 데이터베이스에서 DB 내 데이터 위변조, 랜섬웨어, 악성코드등 보안위협 발생

3

활용 단계

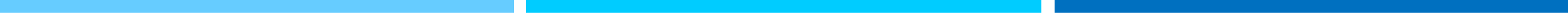
AI 제품·서비스가 제공되고 활용되는 과정에서 기기 오작동으로 인한 이용자의 생명위협, 개인 사생활침해, 스마트도시·공장시스템 마비등 발생

중요하지 않은 데이터에서 개인 정보 추론과 예측 가능

(사례) 초거대 AI 적용

구분	주요 내용
의료	의료영상 판독을 통한 질환 진단 보조 고도화, 임상·질환 합성 데이터 생성, 신약후보 물질 발굴, 약물 디자인 등 활용 확대 전망 ('23, 미래에셋보고서)
마케팅	'25년까지 생성형 AI가 대기업 마케팅 메시지의 30%를 만들 전망(가트너), 美 1,000대 기업은 콘텐츠 생성(58%), 고객지원(57%) 등에 ChatGPT 활용('23)
금융	고객상담, 금융상품 추천, 신용평가, 금융사고 감지 등 금융 전반에 활용 확대 전망, 글로벌 금융회사의 20%가 대화형 AI 도입 중(엔비디아, '23)
미디어	ChatGPT를 활용한 사용자 맞춤형 콘텐츠, 퀴즈 제작을 발표(美 버즈피드), AI가 90%를 만든 블록버스터 영화가 '30년 1편 이상 개봉될 것('23년 가트너)
법률	초거대 AI가 법률대리인의 서류 작업 등을 지원하고, 판사 업무를 보조하는 등 리걸테크 서비스 고도화 전망

출처: 인공지능 안전 및 보안규범 분석 및 시사점(KIS 2023년)



Main subject

1 특정 시장 또는 특정 산업 맞춤형에 초점

AI 보안 기술을
특정 시장이나 산업에 맞추어 개발
(가능하면 소싱)
초기에는 해당 시장의 Bedrock업체
로 자리매김.

예) 금융, 의료, 제조 등 특정 산업군
의 보안 요구 사항을 충족하는 솔루션
을 개발이나 인수, 소싱 등

2 파트너십 형성

기술 Technology Partnership 을
형성하여 초기에는 시장 진입 장벽
을 낮추고 효율성 높임.

주요 보안 업체나 기술 제공 업체와
의 파트너십 협력하여 종합적인 보
안 솔루션을 제공.

가능하면 초기 투자 없이 위 1번에
맞추어 시범적으로 사업을 추진함을
권장

3 맞춤형 솔루션 제공

작은 규모의 고객에게 맞춤형 솔루션
을 제공하여 시장에서의 입지를
확보.

이를 통해 고객의 Needs를 이해하
고 솔루션을 최적화.

인공지능이 필요한 산업群 영역을
발굴하여 추진

기존 보안제품영역을 인공지능영역
으로 바꿀 수 있는지?

4

마케팅 및 브랜딩

적극적인 마케팅과 브랜딩 전략을 채택하여 시장에서 **인식도를 높임**. 효과적인 디지털 마케팅, 컨퍼런스 및 이벤트 참가 등을 통해 **목표 고객층에 대한 인식 높임**.

인공지능 보안의 대표주자로 선점이나 이미지 마케팅을 1개 추진.

(특정제품을 부각하는 Decoration 전략)

5

가격 경쟁력

시장에서 경쟁력을 확보할 수 있는 **고품질의 저가격 전략**.

6

AI보안제품 및 서비스 확산사업 등 정부 지원 과제 추진

AI보안 시장 규모가 확대 됨에 따라 **경쟁력 있는 AI 보안 제품과 서비스 개발**
정부지원사업 참여를 통한 예산 확보
및 시장 확보 추진

AI security application examples

AI기술을 활용한 Security Tool은 패치 적용이 필요하게 되는 종래의 Security Tool 보다도 정확성이 뛰어남.

1 . 인적 실수 방지

Security Risk의 대부분을 차지하는 것이 인적 실수.

AI기술을 활용하여 End User의 행동 패턴을 분석을 통한 대처

AI기술에 의해서 시스템이나 End Point (단말) 、 네트워크 등을 계속 감시로 사람 행동패턴 특정 가능
내부 위협이나 부정 액세스의 시도 등、 Security Risk 내포하는 이상한 행동을 검출

2 . 메일 웨어의 검출

AI기술을 이용, 메일이나 트래픽을 분석, 피싱 공격이나 사기를 검출하고, 공격 Risk 를 저감 가능

AI기술의 하나인 기계 학습을 이용하면, 기지의 위협만이 아니라 관측되고 있지 않은 위협 대처 가능
메일 웨어의 효과적 검출 가능

AI security application examples

3 . 공격의 초기 대처

AI기술은 위협의 특징에 요하는 시간을 단축하는 것만이 아리나, 초기 대처에도 도움이 될 가능성이 있다. 예를 들면 자동 수정 프로그램의 기동, 영향을 받은 서버의 격리, 특정 사용자 계정에 의한 시스템에 대한 액세스 방지 등이다.

4 . Insight (통찰력) 의 제공

보안팀은 AI기술을 사용함으로써, 공격에 대한 신속하며 정확한 대처를 가능하게 하는 통찰력을 얻을 수 있다. 예를 들면 Microsoft는 보안과 생산성의 문제를 해결하기 위해、Security 업무용 AI 챗 bot「Microsoft Security Copilot」를 제공하고 있다.

Microsoft Security Copilot: 기업이 사전에 정의한 보안 절차나 정책에 근거하여、보안 관련된 다양한 사건을 조사하여 분석한다. 기업의 보안 리스크를 경감하기 위해、보안 관련의 문제를 요약하거나, 근본적인 원인을 설명하거나 하는 것 외、해결책을 제안하는 것도 가능하다. (TechTarget0919)

(예) AI Security Product

① AI 기반 침입 탐지 시스템

실시간 Network(시스템 트래픽)을 Monitoring, AI 알고리즘을 사용하여 침입 및 악성 행위 감지

② AI 기반 취약점 분석 및 보완

Software 및 시스템의 취약점을 찾아내고 보완하는 AI를 활용하는 서비스 제공

③ AI를 활용한 행동 기반 보안

사용자 및 기업의 행동 패턴을 분석하여 이상 징후를 탐지하고 보안 위협 대응

④ AI 기반 악성 코드 탐지 및 분류

AI를 사용하여 악성 코드를 탐지하고 분류하여 시스템에 대한 보안 강화 솔루션

(예) AI Security Product

⑤ AI 활용한 자동 보안 감사 및 준수(거버넌스 제품)

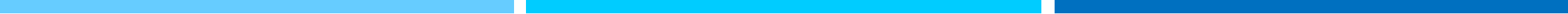
기업 보안 정책 및 규정을 준수하도록 지원하는데 AI를 활용하여 보안 감사 및 준수 프로세스를 자동화

⑥ AI 기반 위협 Intelligence

다양한 소스에서 데이터를 수집하여 AI를 사용하여 보안 위협을 예측하고 대응 방안을 제시하는 서비스

⑦ AI 기반 사이버 보안 교육 및 훈련

구성원들에게 사이버 보안 교육을 제공하고 AI를 사용하여 실제 사이버 공격을 시뮬레이션하고 훈련하는 서비스를 제공



conclusion

How should companies face AI tools?

- AI보안 솔루션은 일부 벤더가 선전과 마케팅을 위한 과장 된 것으로 판단.
- AI 툴 확산은 아직 시기 상조다. 그러나 시장에는 AI기술을 활용한 효과적인 보안 솔루션이 출시됨

→ 그 이유는

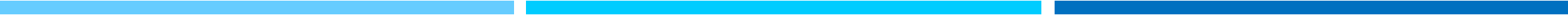
① AI Tool은 방대한 데이터를 신속하게 분석하고 복잡한 패턴이나 이상 검출로 보안관련

② 다양한 프로세스를 자동화로 많은 이득이 있기 때문이고 휴먼 에러 방어에 효율적이다

(단, AI기술은 사람의 전문지식을 대체하는 것이 아니라 보완하는 기능 임)

(보안담당자는 각 영역에서 최신AI기술을 search하고 입수하여, 자사의 수요나 근거에 활용해야 함)

→ AI 보안은 점진적으로 서서히 제품 Base로 진화 발전할 것이다



Thank you