

# Self-Evolving 6G 네트워크에서의 AI for Security 기술 동향

한국전자통신연구원  
사이버보안연구본부  
인공지능데이터보안연구실  
선임연구원 박경민





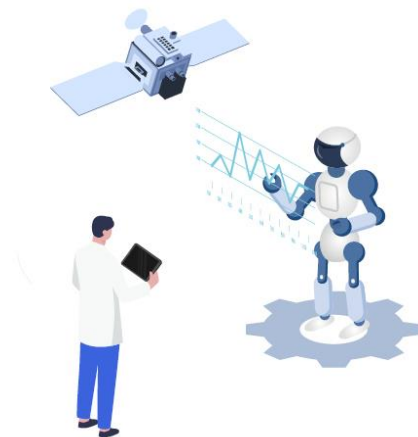
# Contents

PART **I** | AI 기반 NIDS 기술 (AI for Security)

PART **II** | 사이버 보안 관점에서의 6G 네트워크

PART **III** | AI for Security in 6G Networks

PART **IV** | 결 론



# 01

## AI 기반 NIDS 기술

### *Signature based NIDS (Network Intrusion Detection System)*



Electronics and Telecommunications  
Research Institute

03

보고된 네트워크 공격 (White Hackers)  
성공한 네트워크 공격 (Black Hackers)



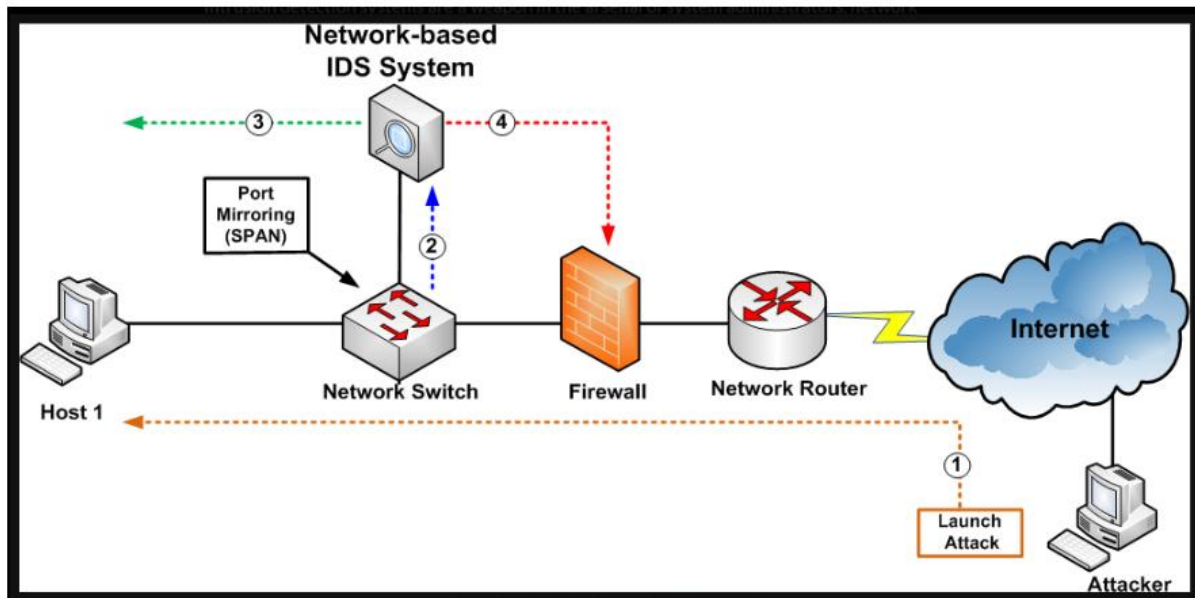
알려진 공격에 대한 패턴/시퀀스 배포



알려진 공격만들 대상으로 NIDS 운영



알려지지 않은 공격은 탐지 불가



R. Samrin and D. Vasumathi, "Review on anomaly based network intrusion detection system," 2017 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT)



# 01

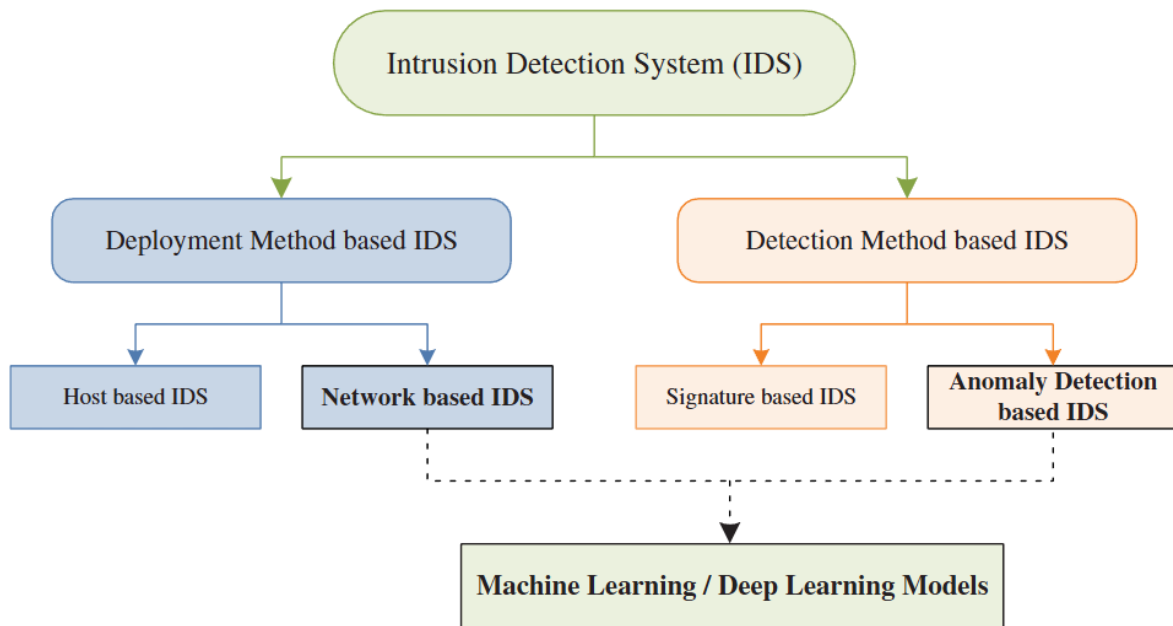
## AI 기반 NIDS 기술

### *Anomaly Detection based NIDS (AI Based NIDS)*



Electronics and Telecommunications  
Research Institute

05



방대한 네트워크 트래픽/플로우 학습

IDS의 지능화/자동화에 기여

데이터셋과의 싸움

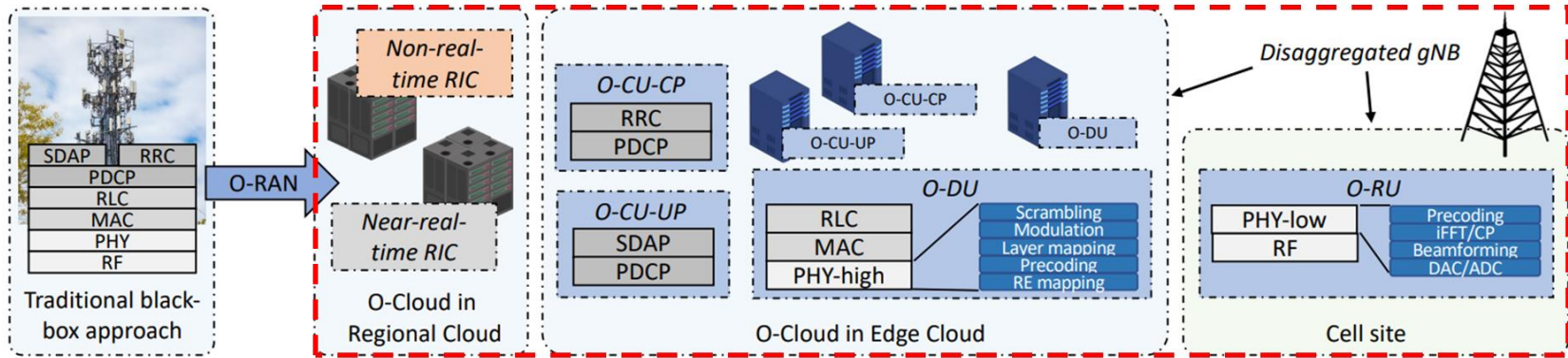
알려지지 않은 공격도 Detection  
(하고 싶음...)

**Intrusion detection system classification taxonomy,**

Ahmad, Zeeshan, et al. "Network intrusion detection system: A systematic study of machine learning and deep learning approaches." Transactions on Emerging Telecommunications Technologies. 2021.

# 02 사이버 보안 관점에서의 6G 네트워크

## Open Architecture



특정 제조업체에 대한 종속이 줄어들

해커그룹의 취약점 분석이 상대적으로 수월

공급망 공격 (악성코드, 스파이칩) 가능성 증가

표준화된 인터페이스 기반의 상호 운용

벤더간 호환성 문제로 보안 이슈 발생 가능성

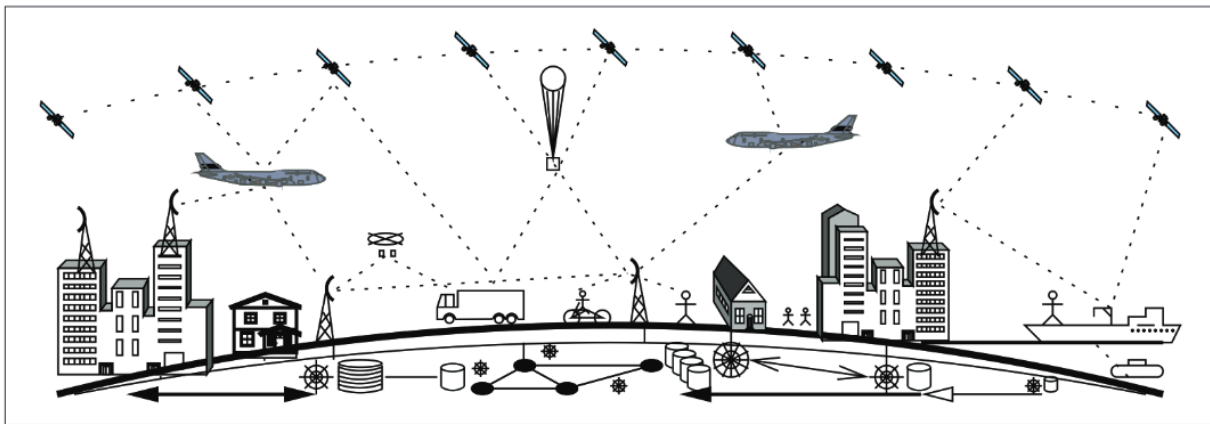
## 02

## 사이버 보안 관점에서의 6G 네트워크

## 3D Coverage and Open Space

Electronics and Telecommunications  
Research Institute

07



Cai, Lin, et al. "Self-evolving and transformative protocol architecture for 6g." IEEE Wireless Communications, 2022.

NTN으로 대표되는 입체통신 지원

극한의 Open Space, 해커의 물리적 접근 용이

3D Coverage 제공을 위한 새로운 체계 등장

신규 프로토콜 취약점(잠재적) 사전 분석 가능성

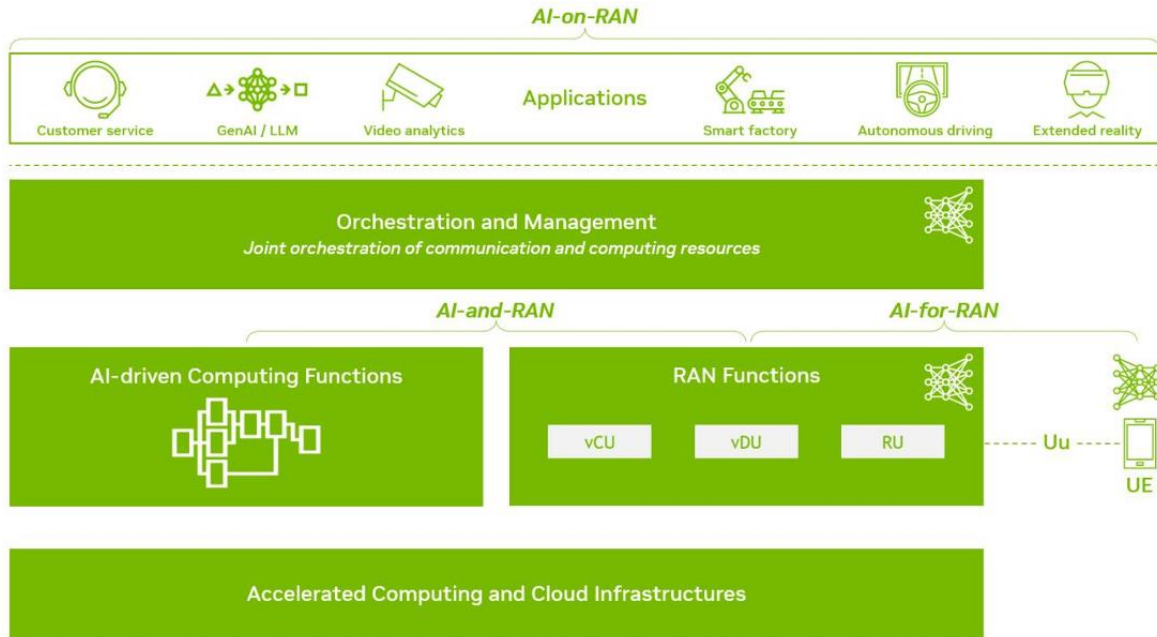
# 02 사이버 보안 관점에서의 6G 네트워크

## AI-RAN



Electronics and Telecommunications  
Research Institute

08



RAN에서의 AI 서비스 제공

AI를 이용한 RAN 성능 향상

AI for RAN

AI for Secure RAN

A high-level overview of AI-RAN,

Kundu, Lopamudra, et al. "AI-RAN: Transforming RAN with AI-driven Computing Infrastructure."  
arXiv preprint arXiv:2501.09007 (2025).



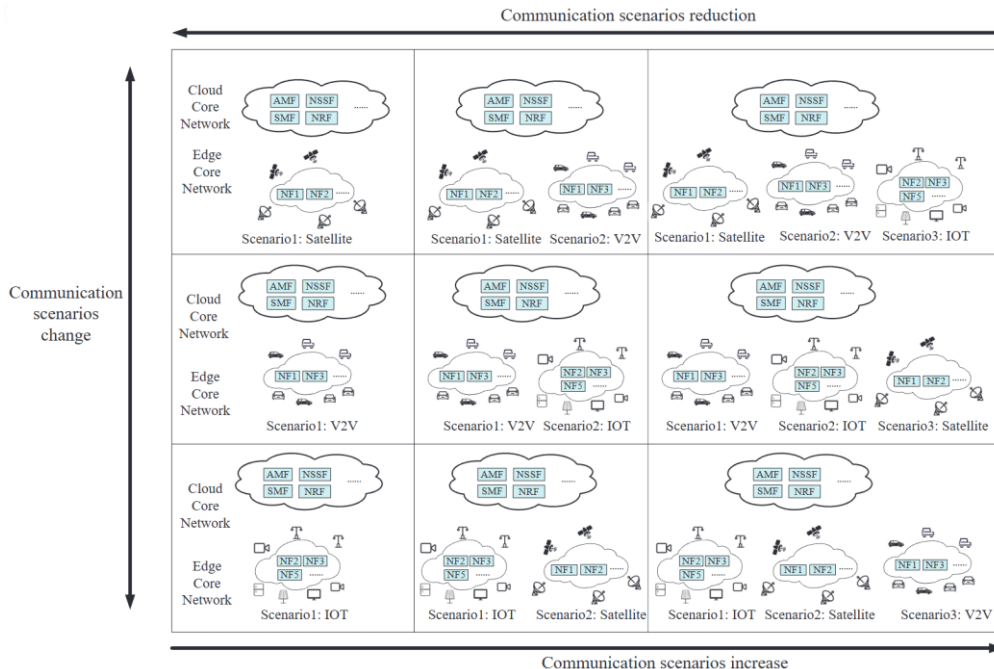
# 02 사이버 보안 관점에서의 6G 네트워크

## Self-Evolving Network



Electronics and Telecommunications  
Research Institute

09



유즈케이스에 따른 코어 NF들의 유기적 변화

네트워크 형상이 시나리오에 따라 바뀜

6G AI 네이티브의 서포트를 기반으로 스스로 진화하고 최적화 형상이 구축될 수 있음

보호해야할 네트워크의 경계가 모호해짐,  
수동적 방어 기술의 한계가 드러날 것

AI based IDS 보다 혁신적인 기술 필요

The Self-evolution mechanism under environment change,

Liu, Zihao, et al. "6G network self-evolution: Generating core networks." 2023 IEEE International Conference on Communications Workshops (ICC Workshops), 2023.

# 03

## AI for Security in 6G Networks

### *Gen AI based Proactive Defense*



Electronics and Telecommunications  
Research Institute

010



***Network Deception***

기존 AI for Security 에서의 Gen AI는  
데이터 불균형을 해소하는 목적으로만 사용됨

Gen AI를 직접적으로 보안에 활용하기 위한 기술로서  
Network Deception(공격자 기만) 이 주목됨

Deception은 신기술은 아니지만 Gen AI를 통해 완전히  
새롭게 태어날 수 있을 것으로 기대됨

# 03 AI for Security in 6G Networks

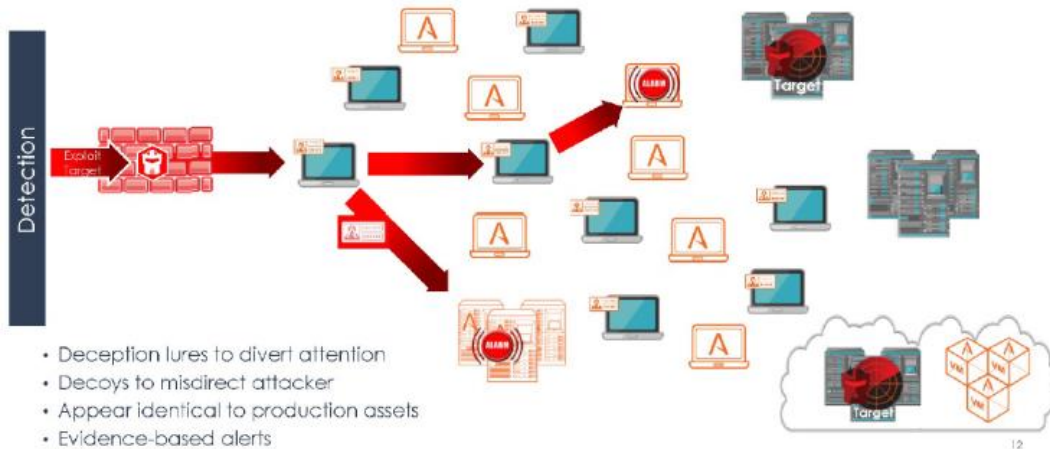
## Gen AI based Proactive Defense



Electronics and Telecommunications  
Research Institute

011

### Deception Obscures the Attack Surface and Disrupts Attacks



네트워크 상에 다양한 가짜(Decoy)를 만드는 것

공격자가 Decoy를 건들도록 유도하는 것

Decoy에서 공격자의 정보를 알아내는 것

자동화된 악성 스크립트에는 어느정도 효과 있음

숙련된 공격자는 Decoy를 금방 인식

## 03

## AI for Security in 6G Networks

## Gen AI based Proactive Defense

Electronics and Telecommunications  
Research Institute

012

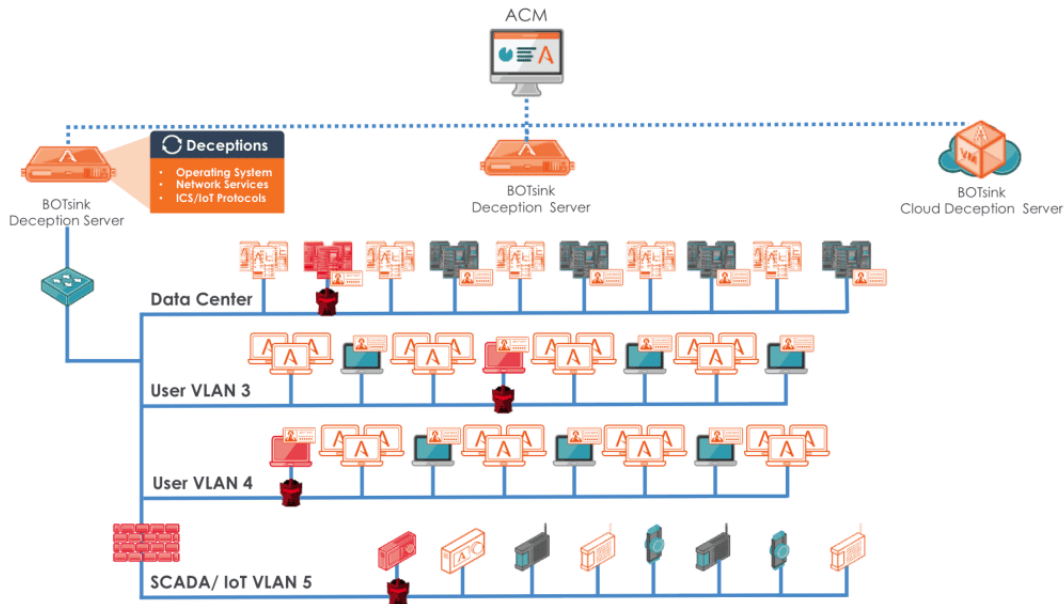
Gen AI로 Decoy를 생성

공격자도 속을 정도로 실제 시스템과 유사하게

공격자가 실제 타겟으로 인식하게끔 유도

Self-Evolving Network에 적응할 수 있는  
지능형 Decoy 플랫폼 개발 가능

최소한의 컴퓨팅 자원으로 극대화된 방어 효과



## 03

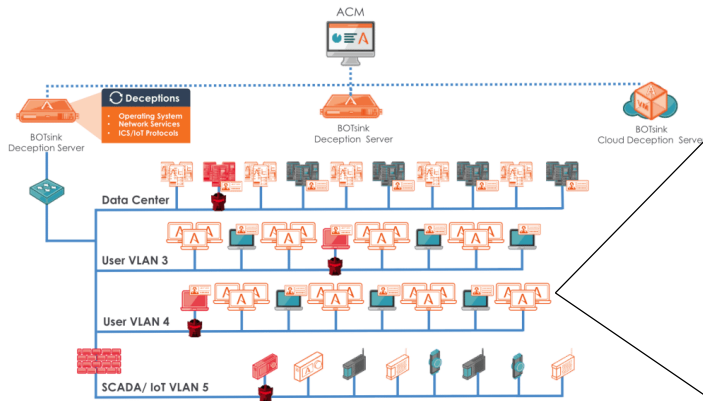
## AI for Security in 6G Networks

## Gen AI based Proactive Defense - Use case



Electronics and Telecommunications  
Research Institute

013



```

acme-api-dev-us-west

9 additional security updates can be applied with
ESM Apps.
Learn more about enabling ESM Apps service at
https://ubuntu.com/esm

*** System restart required ***
Last login: Mon Aug 5 03:45:03 2024 from
203.97.21.86
stan@acme-prod:~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
tmpfs            96M   1.1M  95M   2% /run
/dev/vda1        25G   13G   12G  54% /
tmpfs            479M   0   479M   0% /dev/shm
tmpfs            5.0M   0   5.0M   0% /run/lock
/dev/vda15       105M   6.1M   99M   6% /boot/efi
tmpfs            96M   4.0K   96M   1% /run/user/0
user/1002        96M   4.0K   96M   1% /run/

stan@acme-prod:~$
  
```

Gen AI로 ssh terminal text만 생성

오로지 Text만 생성하여 네트워크 전체가  
실제로 존재하는 것처럼 공격자를 속일 수 있음

최소한의 비용, 극대화된 방어 효과



# 03 AI for Security in 6G Networks


## AI Agent based CISO




Electronics and Telecommunications  
Research Institute

014


**H** 헬로티  
보안 사고는 왜 반복되는가...쿠팡 해킹으로 본 국내 보안 한계  
최근 발생한 쿠팡 해킹 사태는 단순한 보안 사고를 넘어 국내 기업 보안 구조 전반의 취약성을 다시 한 번 드러낸 사건으로 평가된다.  
8시간 전




**BN** 바이라인네트웍스  
3370만건 고객정보 털린 쿠팡, 뭐가 문제였을까?  
국내 최대 이커머스 플랫폼 쿠팡에서 약 3370만건의 고객 개인정보가 무단 유출된 사실이 확인되면서 정부가 민·관합동조사단(이하 조사단)을 꾸려...  
2주 전



**매일경제**  
“해킹 시대” 기업 사이버 침해 건수 급증...전방위 대응체계 마련 시급  
우리 기업들을 대상으로 한 사이버 침해건수가 해마다 급증하고 있지만 이에 대한 대응책은 미흡하다는 지적이 나왔다. 대한상공회의소는 15일 서울...  
8시간 전



**M** 매일경제  
“또 털렸습니다”...폭발적으로 늘어나는 중소기업 해킹, 관련 예산은 ‘썩둑’  
중소기업중앙회 관계자는 “중소기업은 제품 개발·생산·마케팅 같은 기본 업무만 하기도 벅찬 경우가 대부분이라 사이버 보안에 투입할 자금이나 인력이...  
2025. 6. 26



뛰어난 해커보다 더 무서운 것은 내부의...부주의, 체계, 인식 등등

AI based IDS 기술은 보안위협을 탐지만 할 수 있음

Gen AI based Deception 기술은 공격을 지연만 시킬 수 있음

AI for Security의 또다른 혁신은 AI가 CISO 역할을 해주는 것

AI Agent를 이용한 입체적인 보안 체계 모니터링 및 대응 가능

# 03 AI for Security in 6G Networks

## AI Agent based CISO – Use case

Agent는 타 AI for Security와는 달리 조직  
내의 다양한 보안 관련 시스템에 접근할 수 있음

IDS와 방화벽에 접근 가능한 Agent들이  
상호작용하여 탐지와 대응을 실시간으로 연동

### The role of the CISO



- Be an internal and external security expert
- Embed security information
- Stay informed
- Hire solid security staff
- Become a trusted business advisor
- Identify C-level team members
- Create monthly reports
- Follow the three C's

Agent가 IDS 시그니처 배포 사이트에 접근, 새로운 IDS 룰셋을 조직 내의 IDS에 접근하여 자동으로 갱신

**Virtual CISO** is a flexible approach to cybersecurity where businesses outsource the role of Chief Information Security Officer (CISO) to a third-party provider.



이와 유사한 Virtual CISO 상용제품이 있으며,  
AI Agent를 통해 더욱 고도화 시킬 수 있음

# 04 결론



현재의 AI for Security 기술은 NIDS로 대표되는 침해위협 "탐지"에 치중하고 있음

6G 네트워크는 Self-Evolving, AI-RAN 등을 포함하여 다양한 변화를 예고함

보안 관점에서 Self-Evolving은 기존 경계기반 "탐지" 기술의 한계를 드러나게 할 수 있음

보안 관점에서 AI-RAN은 AI for Security 기술을 RAN에 적용하기에 좋은 동력이 됨

Self-Evolving에 의한 네트워크의 다형성/무경계에 대응하기 위한 AI for Security 기술로서  
Gen AI 기반의 Deception 기술에 대한 가능성 확인

최근 가장 주목받는 AI 트렌드인 AI Agent를 이용하여 AI CISO를 개발할 수 있을 것으로 예상됨

6G, 그리고 AI 네트워크의 신뢰성 보장을 위한 AI for Security 기술의 발전 가능성이 매우 높음





---

Electronics and Telecommunications Research Institute

---

# THANK YOU