Making History

How to Raise the Next Generation of Whitehat Hackers

박세준 · Theori

Brian Pak
박세준

Theori
Empowering Innovation with Security

Carnegie Mellon University
Computer Science
B.S. (‘11), M.S. (‘12)

Lockheed Martin
Researcher (’10~’11)

Kaprica Security
Co-Founder (’12~’15)

Theori
Co-Founder & CEO (’16~present)

국내·외 해킹방어대회 70회+ 우승
DEFCON 6회 우승 (+ 5회 준우승)

프로그램 분석 자동화 연구 및 취약점 다수 제보
다양한 글로벌 벤더 및 오픈소스 프로젝트

대한민국 사이버사령부 자문위원
BoB, 고려대 융합보안사업, Web3@KAIST, 드림아카데미 등 멘토링

Overview

Hackers

1.1 대중에 알려진 해킹과 “진짜” 해킹

1.2 해킹 및 해커의 정의

1.3 해킹의 종류와 해커의 방법론

1.4 해킹 경제론

1.5 해킹의 범주

Growth

2.1 중·고등학생

2.2 대학생

2.3 대학원

Accelerate

3.1 협업

3.2 해킹 대회

3.3 포트폴리오

3.4 컨퍼런스 및 네트워킹

3.5 교육 프로그램 / 멘토링

Career

4.1 커리어, 그때와 지금

4.2 Academia (학계)

4.3 Industry (업계)

4.4 커리어 성장

Reaching to the Top

5.1 훌륭한 해커의 특징

5.2 최신 기술 동향 파악 및 연구

5.3 커뮤니티의 힘

5.4 윤리의식

5.5 Work-Life Balance (워라밸)

5.6 어려움 극복하기

Making History

6.1 역사를 만들어간다는 것

6.2 인재 양성의 중요성

6.3 역사의 다음 페이지

Hackers

해킹이란 무엇일까? 정체성을 찾아서

대중에 알려진 해킹

네이버 지식백과에 따르면...

“ 컴퓨터 네트워크의 취약한 보안망에 **불법적**으로
접근하거나 정보 시스템에 **유해한 영향**을 끼치는 행위 ”


가상화폐 거래소 지닥, 200억여원 해킹 피해…보관자산 23% 규모

입력 : 2023-04-10 19:44:04

성규환 부산닷컴 기자 bastion@busan.com


모바일 청첩장 눌렀는데 7000만원 대출 피해

입력 2023-04-23 19:00:27 수정 2023.04.23 19:00:27 김정욱 기자


‘30만 정보 유출’…LGU+는 왜 해킹과 디도스 공격에 취약했나

김수민 기자 | 입력 2023.04.27 14:39 | 수정 2023.04.27 18:16 | 댓글 3


사회

北 해킹조직 '필수 설치' 보안인증 해킹...61개 기관 피해

2023년 04월 18일 13시 03분 댓글

“진짜” 해킹

무언가를 **분석**하고 **이해**하는 과정 그 자체에서
즐거움과 **보람**을 느끼는 행위

호기심이 이끄는 **지식**의 목마름을 채우는 행동

왜 다를까?

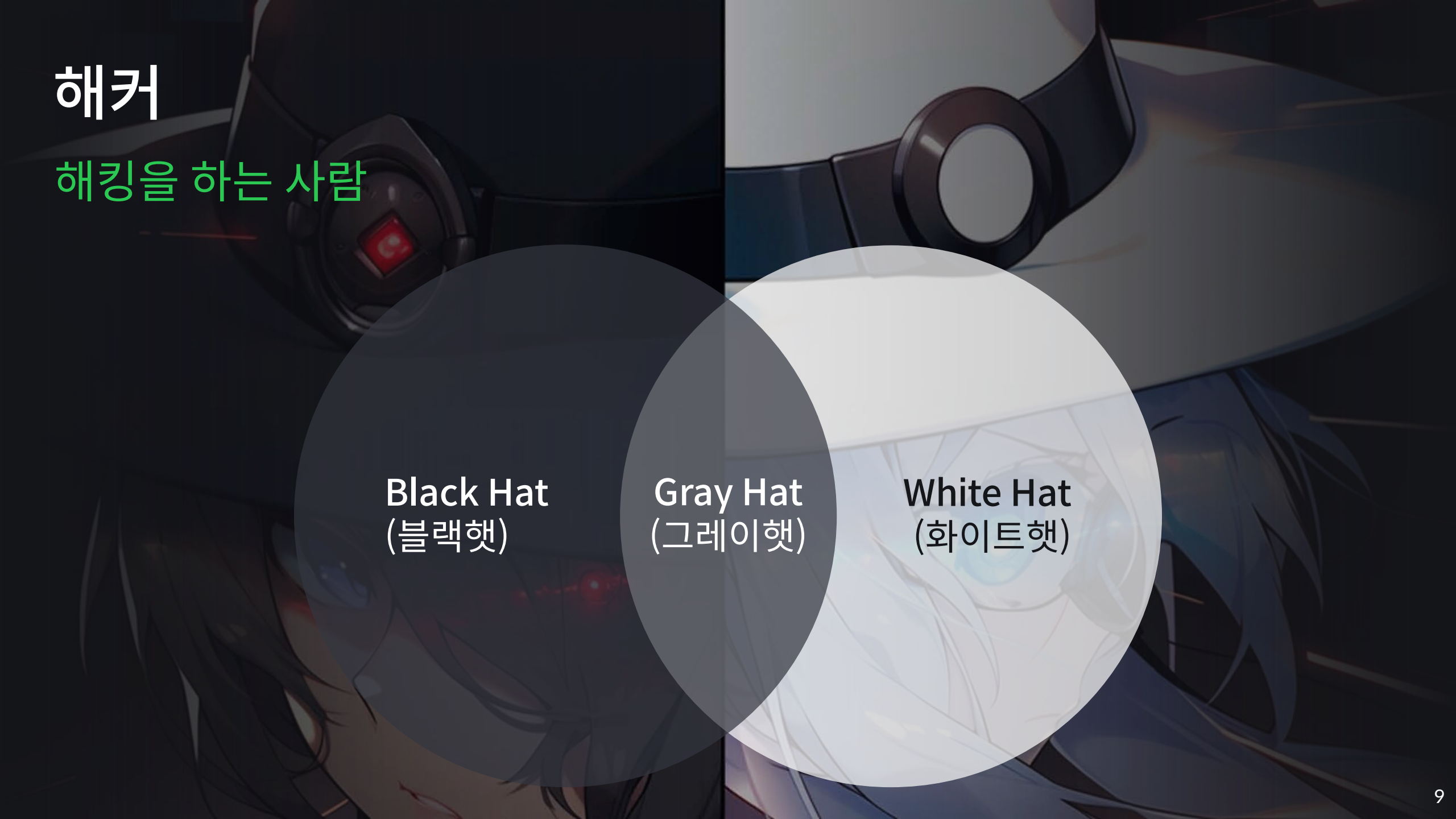
특별한 기술이나 지식을 남용하는 사건 발생

대중 매체에서 부정적인 이미지의 뜻으로 사용

하지만, 착한 해커는 억울하다! 😢

해커

해킹을 하는 사람



해킹의 종류

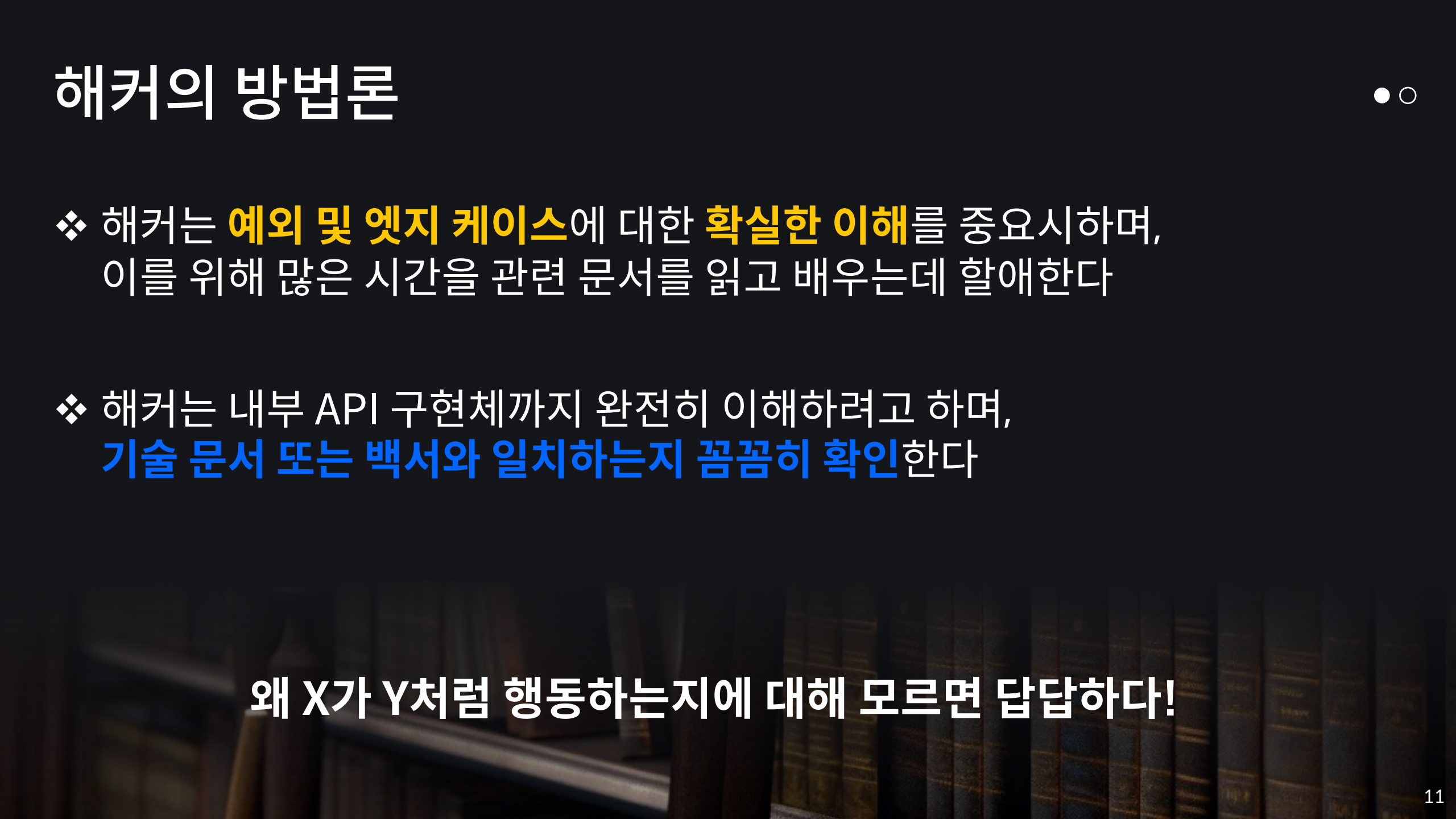
- 기술 중심 해킹
  - 타겟 시스템에 대한 매우 깊은 이해
  - 고난이도 기술에 대한 연구 및 구현
  - High Cost, More Predictable; Stealthy

- 소셜엔지니어링 해킹
  - 사람에 대한 이해 (심리학..?)
  - “The weakest link in security chain is PEOPLE”
  - Lower Cost, High Return; Visible

해커의 방법론

❖ 해커는 **예외 및 엣지 케이스**에 대한 **확실한 이해**를 중요시하며,
이를 위해 많은 시간을 관련 문서를 읽고 배우는데 할애한다

❖ 해커는 내부 API 구현체까지 완전히 이해하려고 하며,
기술 문서 또는 백서와 일치하는지 꼼꼼히 확인한다



왜 X가 Y처럼 행동하는지에 대해 모르면 답답하다!

해커의 방법론

❖ 해커는 대상 구현체 로직의 **정확성을 항상 의심**하며 분석한다

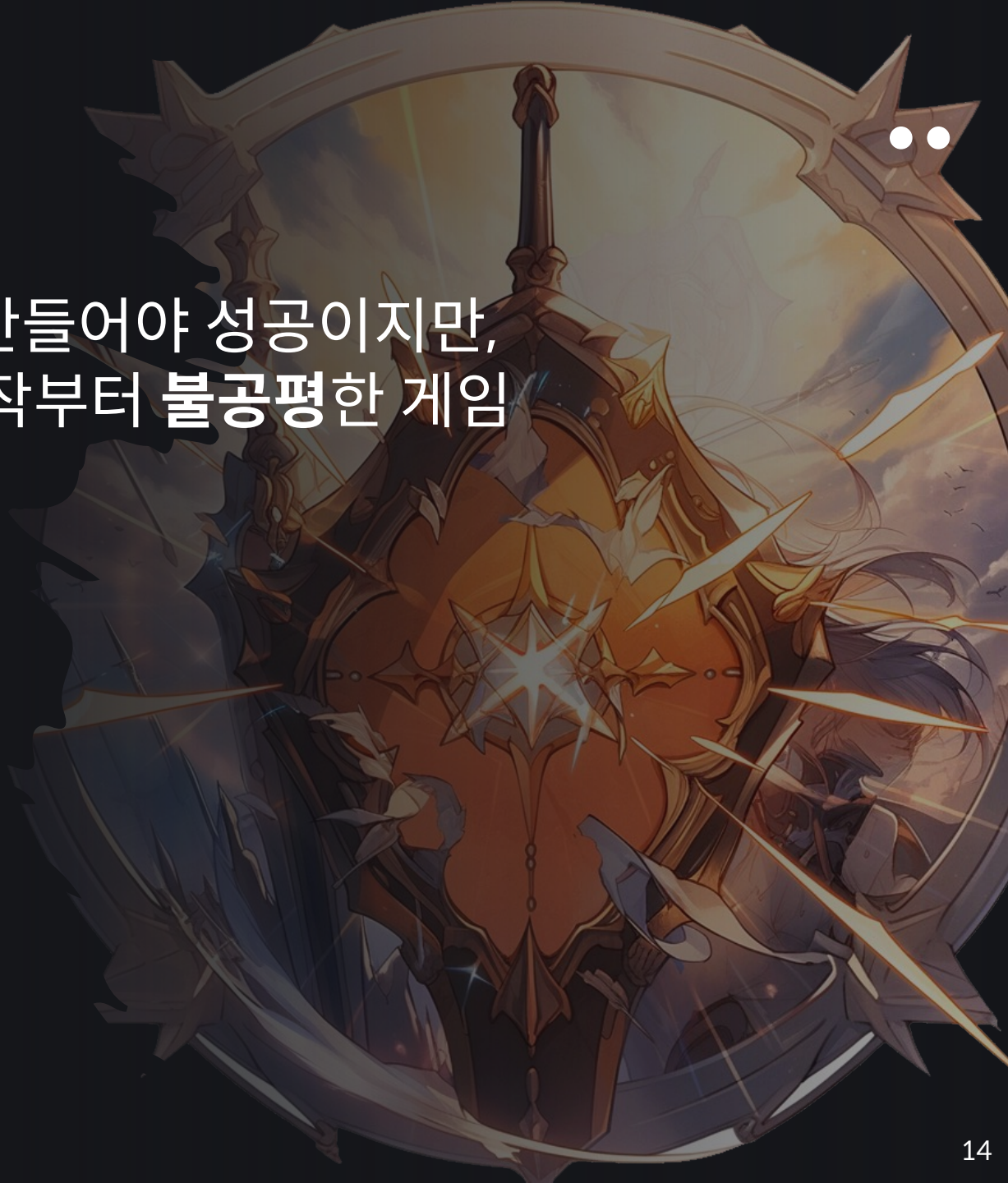
❖ 해커는 대중적으로 잘 **알려진 방법 이외의 길**을 선택했을 시 나타나는 **side effect를 유심히 관찰**한다

❖ 해커는 본인이 원하는 작업을 해주는 방법이나 툴이 없을 경우, 그것을 기어코 **우회 또는 직접 구현해서라도 실험**한다

개발 vs. 해킹 경제론

- 개발자는 서비스 또는 제품 완성의 **데드라인**에 독촉 받는다
  - 저항이 가장 적은 방법으로, 최대한 빠르게, 일단 **작동만 되면 OK**
- 개발자는 자신이 개발하지 않은 부분은 **블랙박스**로 생각한다
  - API 규격만 맞춰서 작동하면 내부 구현체는 들여다 볼 필요 X
- 개발자는 모든 **예외 및 엣지 케이스**를 신경 쓸 수 없다
  - Unit test 등이 도움 되지만 **시간 비용과 trade-off**

개발 vs. 해킹 경제론



❖ 개발자는 열을 만들면 열을 안전하게 만들어야 성공이지만,
해커는 보통 **하나만 뚫어도 성공**인, 시작부터 **불공평**한 게임

❖ 단, 각 진영 모두 가진 리소스는 한정적

보안을 **효율적**으로,
자동화하는 것이 중요한 이유

해킹의 범주

- **State-sponsored Attacks**
  - 새로운 국가간 전쟁 형태
  - 매우 정교하고 수 년의 연구 개발 과정을 거침
  - 다수의 0-day 익스플로잇 사용
  - 배후를 알 수 없도록 최대한 노력하지만 대부분은 추측 가능

Nitro Zeus
7.7 DDoS Attack
Operation Aurora
Sony Pictures Hacking

해킹의 범주

- **Money & Fame**
  - 취약점 및 익스플로잇 판매 (Gray & Black hat)
  - 취약점 찾기 대회 참여
  - 버그바운티 참여 (White hat)
  - Responsible disclosure

hackerone

patchday

해킹의 범주

●●●○

- ❖ **Work**
  - ❖ 모의해킹, 취약점 점검
  - ❖ 보안 컨설팅
  - ❖ 연구 개발 프로젝트

- ❖ 자율주행차 모듈 제작 (?!)

Microsoft Google SAMSUNG

LG Electronics NAVER B

toss banksalad

ethereum klaytn NEXON

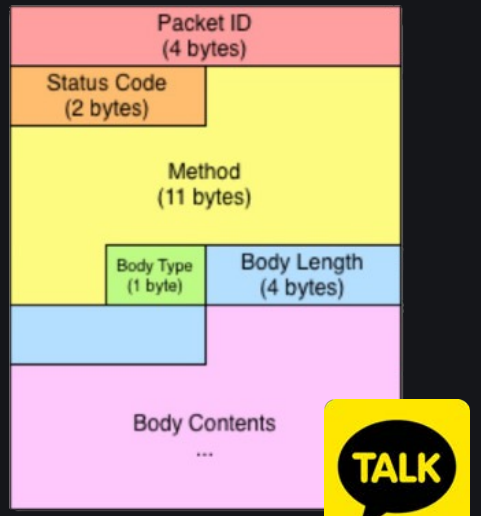
두나무 coinone KRAFTON

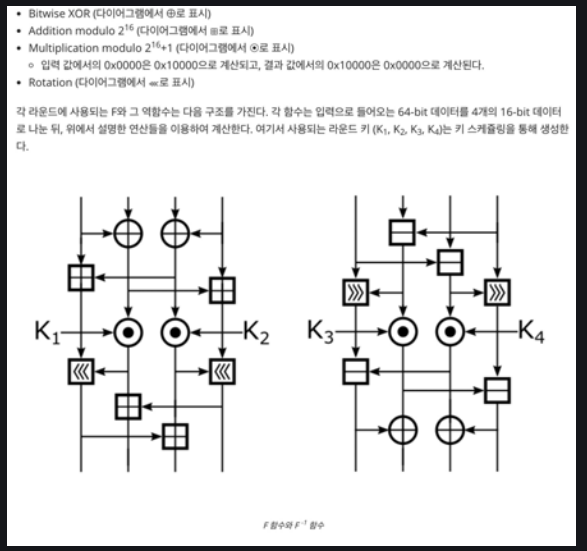
NSR 국가보안기술연구소 대한민국 국방부 Ministry of National Defense 대한민국 대통령실 DARPA

. . .

해킹의 범주

- **Hobby**
  - 메신저 프로토콜 분석하기
  - 게임 애드온 만들기
  - 암호 알고리즘 분석하기
  - . . .





Growth

“라떼” 성장 연대기로 살펴보는 바람직한 성장 방법

라떼는 말이야~

⚠ 주의 및 참고 ⚠

- 발표자는 Offensive Security를 전문으로 함
- 발표자의 나이가 생각보다 많음 (aka. 고인물)
- 발표자의 지극히 개인적인 의견임
- 본 발표는 인생 가이드가 절대 아님

  (본인 인생은 온전히 본인 선택임)

중·고등학생 (그때)

cyworld

2005년 전후

인터넷 속도 100Mbps..
(미국에서 케이블 모뎀으로 10Mbps)

사파(?)로 보안 공부 시작

게임 / 소셜네트워크 / 웹하드 등
마땅치 않은 공부 자료..

제한적인 커뮤니티

매우 폐쇄적이고, 전반적으로 높은 연령층

중·고등학생 (지금)

집중해야 할 것

비판적·논리적·창의적 사고력 기르기
공부하는 습관 / 배움의 즐거움 느끼기

충분한 공부 자료 존재

컴퓨터 및 정보보안 특성화고 / 교육 플랫폼
오히려 (깊이가 얕은) 자료가 너무 많아서 문제

다양한 동아리·커뮤니티

오픈 커뮤니티, 학교/외부 동아리
온라인 및 오프라인 교류

대학생 (그때)

정보보안 **전공 · 학과** 없음

Computer Science / Computer Engineering
이산수학 · 운영체제 · 네트워크 · 컴파일러 등

동아리 활동

대학교 2학년 여름방학, PPP 설립
학교에서 인정해주는데 까지 DEFCON 우승 3회..

교육 프로그램 부재

자체적으로 공부 및 논문 읽기
대학교 리서치 랩 연구원 · 기업 인턴십 지원

대학생 (지금)

특기자 전형 존재

특성화고 출신 및 검정고시 졸업자 기회 ⬆
수능 최저 없는 경우 대다수, 실력·실적 위주

사이버보안 학과 등장

하지만, CS Fundamental (기본기) 정말 중요함
정보보안은 응용 학문임을 잊지 말기!

다양한 교육 프로그램

BoB / K-Shield Jr.
Dreamhack / Google Course

대학원 (그때)

이론 중심 연구

좋은 결과를 위해 환경을 조율
다만, 새로운 아이디어와 시도는 좋은 이론에서 시작!

학회 발표

주로 Top-Tier 아카데믹 학회 중심적
Industry 컨퍼런스가 그리 많지 않음

해외 대학원 위주

국내 대학의 연구 깊이 부족 현상
대부분의 좋은 연구들은 해외 대학원 랩에서 진행

대학원 (지금)

실용성 고려한 연구

이상적인 환경에서만 가능한 실험 결과가 아닌,
실무 환경에서 “Practical” 하게 활용 가능한 연구

산학연계 협업

학계와 업계가 함께 어려운 문제를 해결
Industry 컨퍼런스에도 좋은 연구 결과가 많이 나옴

훌륭한 국내 대학 교수진

다만, 더 넓고 다양한 경험을 위해
해외 대학원은 여전히 추천함!

Accelerate

성장의 가속화

협업

백지장도 맞들면 낫다

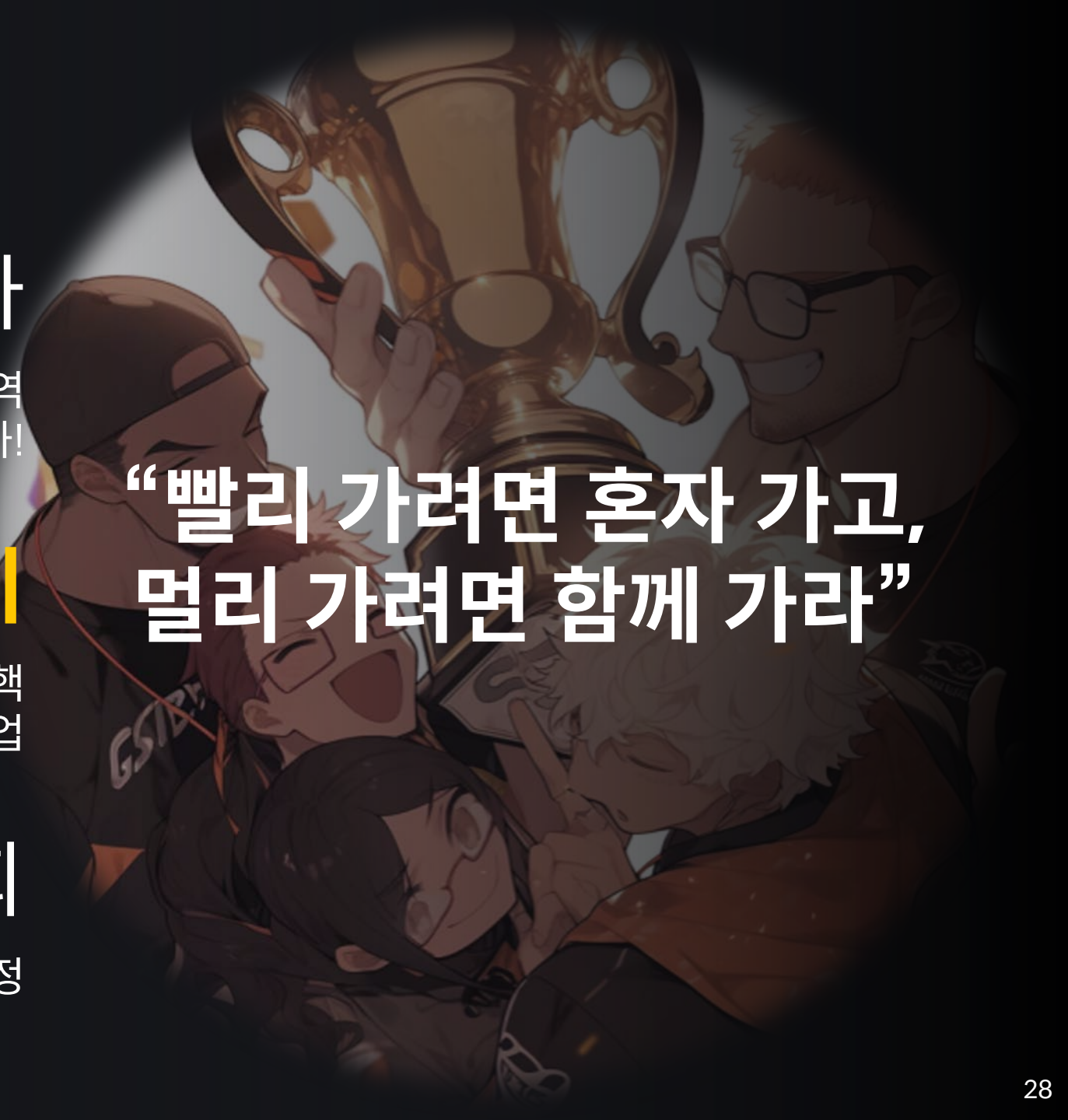
물론, 혼자서도 충분히 성장할 수 있는 영역
하지만, 외롭고 힘드니까!

온·오프라인 커뮤니티

동아리 / 연합 / 디스코드 / 드림핵
컨퍼런스 / 세미나 / 밋업

해커톤 / 해킹대회

함께 머리 맞대고 고민하고 성장하는 과정



**“빨리 가려면 혼자 가고,
멀리 가려면 함께 가라”**

해킹 대회

Wargame / CTF

예전에는 “닥치는대로 다 해라” 조언 했지만..
평판 좋은 것으로, 본인 수준에 맞는 대회 선정

순위는 중요하지 않음

이전에 풀지 못했던 문제를 풀었는지,
이전보다 빠르게 풀었는지가 중요 (성장 진척도 확인)

팀워크 훈련

처음에는 혼자 참여해보고, 어느정도 감이 생기면
팀을 만들거나 조인해서 참여하는 것을 추천

포트폴리오

꾸준한 포트폴리오 관리

GitHub 프로젝트 · 오픈소스 활동 등
CV · Resume 관리

활발한 대외 활동

취약점 제보 및 CVE/KVE 발급 이력
블로그 활동 · 외부 발표 경험

자격증 획득

대부분의 업무에는 필수적이지는 않지만,
특정 커리어에는 필수일 수 있음

컨퍼런스 및 네트워킹

각종 **컨퍼런스** 참여

해외 – DEFCON, BlackHat, RSAC, CCC, HitB, OffensiveCon, HITCON, INFILTRATE, ...

국내 – CODEGATE, CCE, POC, Zer0Con, ...

다양한 **Meetup** 참여

지역별 모임, 동아리 활동 등 적극적 참여
세미나, 교육/트레이닝, 발표, 해커톤, ...
컨퍼런스 after-party!

교육 프로그램 / 멘토링

인재양성 · 교육 프로그램

예전에 비해 훨씬 다양한 수준별 기회 존재
본인 상황에 맞춰 잘 활용하는 것이 좋음

준비된 만큼 얻어가는 구조

준비되지 않은 채로 무작정 프로그램에 참여하는 것은
오히려 시간낭비 및 자존감 하락으로 이어질 수 있음!

멘토 활동의 장점

성장한 이후에는 본인이 직접 멘토링을 하거나 주변에
도움을 주는 것도 본인의 성장에 큰 도움이 됨

Career

직업과 적성, 그리고 그 이상

커리어 (그때)

부족한 기술 역량

소프트웨어 엔지니어링 지식 없는 “해커”들도 많았음
(사실 지금도 그런 사람들은 많이 존재함..)

사이버보안 전문 직무 부족

사이버보안에 대한 인식의 성숙도 결여
전담 팀이 존재하는 것보다는 담당자 1-2명 정도 규모

소극적인 투자

모두가 보안이 중요하다고 입 모으지만,
실제로 리소스를 투자하는 곳은 적음

커리어 (지금)

체계화 된 채용과정

채용 면접 프로세스, 인턴십 제도, 수습기간 등
OJT (트레이닝) 통한 실무 센스 준비

보안 인력 부족 현상

보안 “인원”이 아닌 보안 “팀” 존재
훨씬 복잡해진 인프라 및 코드 구성

제도적 강화

비교적 약했던 제도 강화 / 징벌적 손해배상 등
(여전히 해외에 비하면 상대적으로 약함..)

학계 커리어

연구원 / 과학자

대학이나 연구기관에서 연구를 수행하는 역할
새로운 보안 기술 및 전략 개발

교수

학생들에게 강의하고, 대학원생들 지도하며 연구 수행
새로운 학술 연구 및 학회 발표

학과장

담당 학과나 교내 프로그램의 관리와 운영 담당
교육 커리큘럼 기획, 교직원 관리 등

업계 커리어

기업 보안 엔지니어

사내 보안 정책 설정 및 구현
시스템 보안 강화, 공격 탐지 및 방어

보안 컨설턴트

고객사 서비스/시스템 취약점 점검
보안 위협 시나리오 도출 및 감사

사이버 범죄 수사관

사이버 범죄 조사, 악성해커 추적 등
사법 집행 기관과 협력하여 범죄자 검거

TI / 악성코드 분석가

위협 정보 수집 및 범죄 조직 동향 파악
악성코드 분석을 통해 방어책 및 해결책 도출

취약점 분석가

최신 소프트웨어 및 하드웨어 취약점 발굴
새로운 공격 기술 도출 및 방어 기법 설계

...

업계 커리어 단계

인턴 / 신입

- 첫 실무 경험
- 사회 생활의 시작
- 본인에게 맞는 팀 문화와 기업 찾기

Mid-level

- 전문성 개발 및 역량 증진
- 약간의 리더십 경험

Senior & C-level

- 경험과 통찰력을 바탕으로 방향성 제시
- 팀 / 프로젝트 관리

다양한 산업군

꼭 회사에 취직할 필요는 없다: 프리랜서

장점

- 유연한 일정
- 다양한 경험
- 본인 능력과 경험에 비례하는 수입

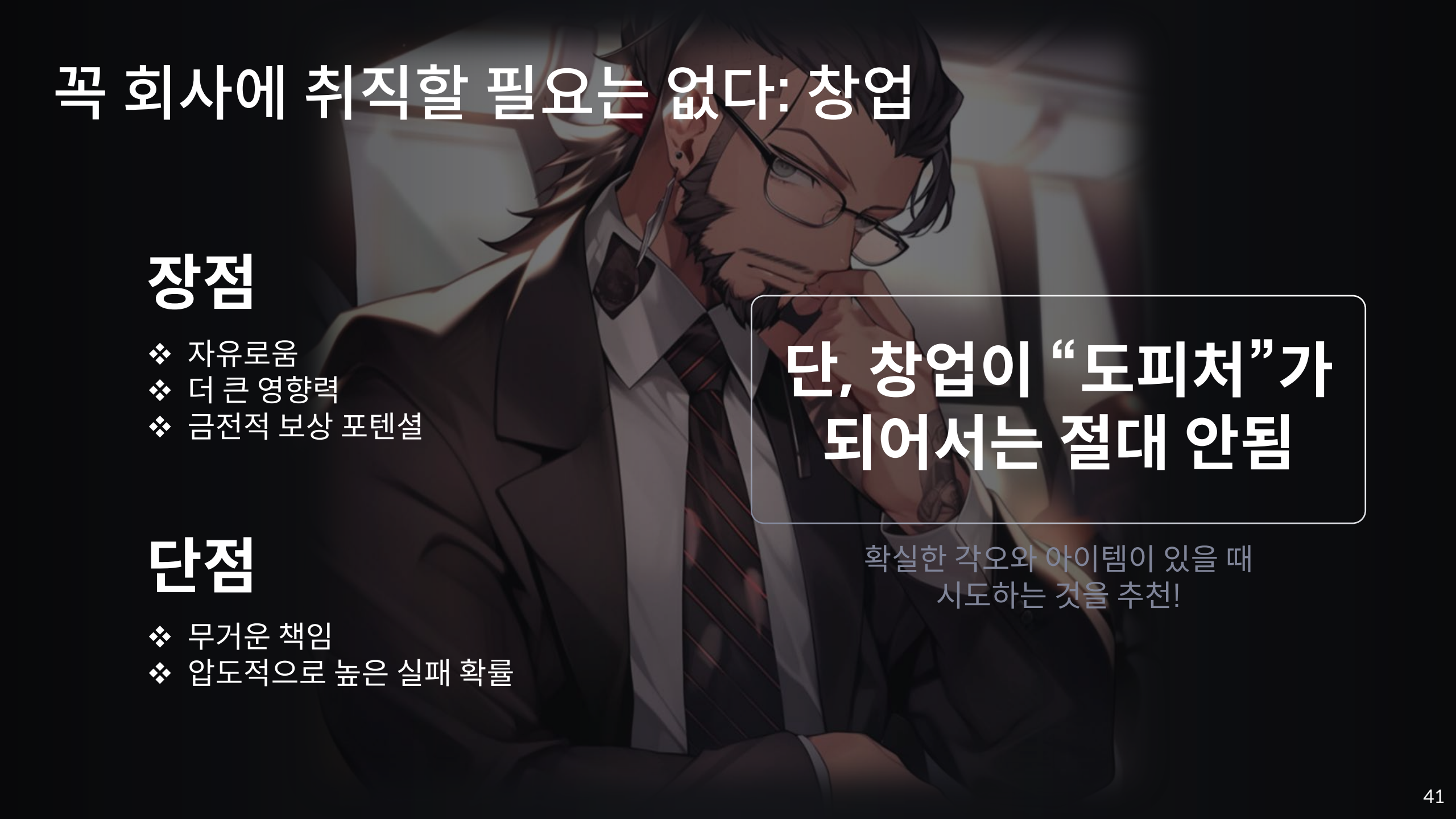
단점

- 불안정한 수입
- 자체적인 리소스 관리
- 복지 혜택 부족 (좋은 팀원도 복지)
- 큰 프로젝트 기회는 얻기 어려움

독립적으로 업무를 맡아 수행하는 전문가

특정 기업이나 조직에 소속되지 않고
자유롭게 활동 가능

꼭 회사에 취직할 필요는 없다: 창업



장점

- ❖ 자유로움
- ❖ 더 큰 영향력
- ❖ 금전적 보상 포텐셜

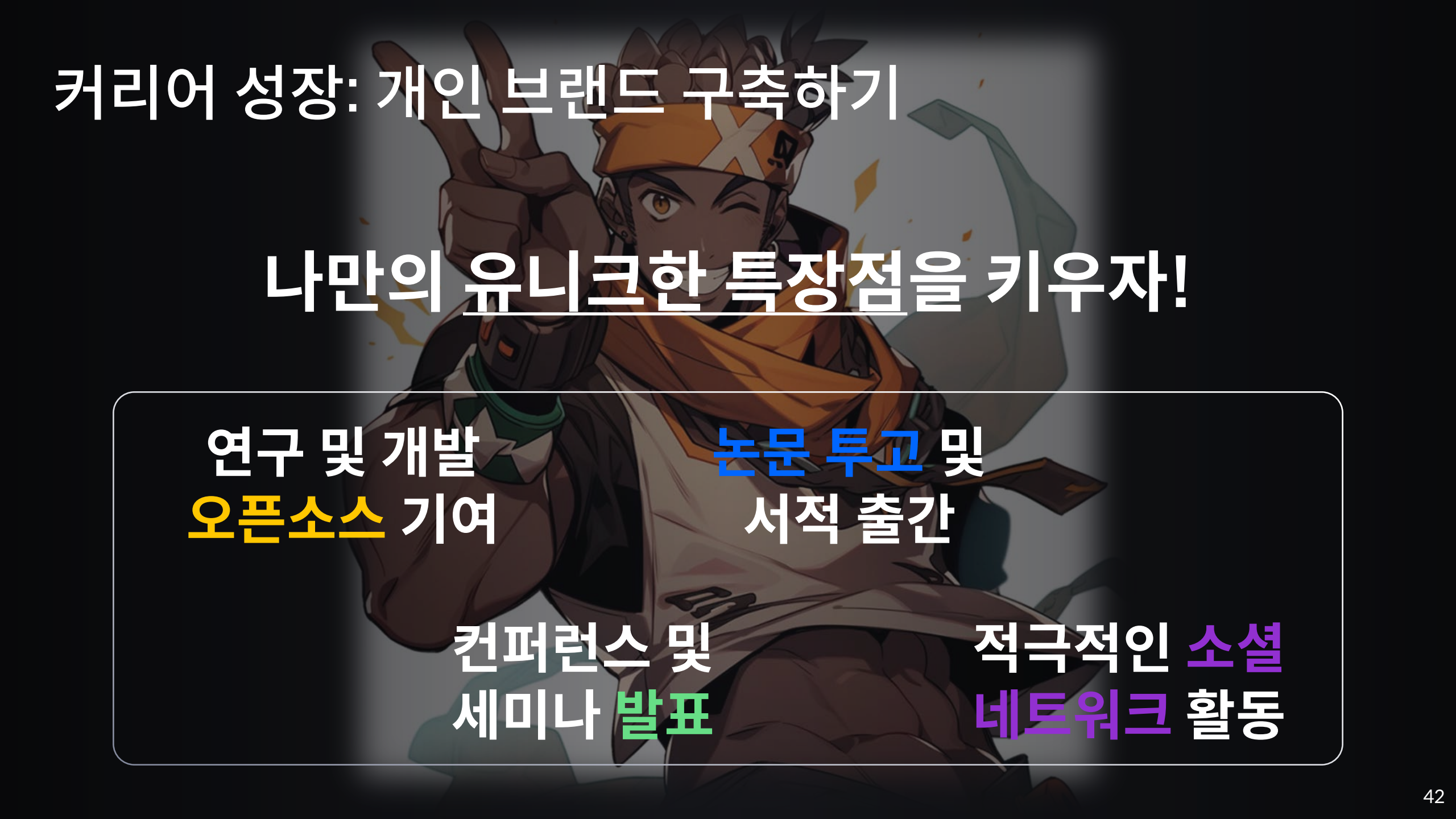
단점

- ❖ 무거운 책임
- ❖ 압도적으로 높은 실패 확률

단, 창업이 “도피처”가 되어서는 절대 안됨

확실한 각오와 아이템이 있을 때
시도하는 것을 추천!

커리어 성장: 개인 브랜드 구축하기



나만의 유니크한 특장점을 키우자!

연구 및 개발
오픈소스 기여

논문 투고 및
서적 출간

컨퍼런스 및
세미나 발표

적극적인 소셜
네트워크 활동

커리어 성장: 개인 역량 강화하기

지속적인 공부 및 연구

빠른 속도로 변하는 트렌드 분석

컨퍼런스 및 트레이닝 참석

Reaching to the Top

최고의 경지에 오르는 방법

훌륭한 해커의 특징

최신 기술 동향 파악 및 연구

끊임 없이 **엄청난 속도**로
새로운 기술이 나오는 중

Artificial Intelligence
Quantum Computing
Blockchain
Robots

모든 분야에
보안은 필수적!

직접적으로 보안에 관련이 없어도
접목 가능성 여부 파악 필요

커뮤니티의 힘

혼자서 할 수 있는 것에는 분명한 한계가 있음

커뮤니티 파워,
함께 도전하고 개척하는 힘

스타트업, 동아리, 연합, 팀, ...
다만, too much 친목화는 조심해야 함
(우리가 왜, 무엇을 하기 위해 모였지?)
확실한 목표와 아젠다를 가지고 운영 필요

다양한 커뮤니티의 종류 존재

컨퍼런스, 세미나
드림핵 (포럼, 디스코드)
오픈채팅방, 카페

윤리의식

사이버보안을 커리어로 꿈꾼다면 가장 중요한 요소

해커는..

현대 사회에서 **마법사** 같은 존재

- **아무나 되기 어려움**
  많은 지식, 연습이 필요함
- 막강한 힘/능력을 가짐
  불가능하다고 여겨지는 영역의 것들을 할 수 있음
- 엄중한 책임이 따름
  어떻게 그 힘을 사용하느냐에 따라 **백마법사**.. 혹은 흑마법사

굳건한 마음

수 많은 **유혹**에도 흔들리지 않아야 함

실력이 아무리 좋아도 윤리의식이 결여된
해커는 **범죄자**일 뿐!

Work-Life Balance (워라밸)

안그래도 짧은 직업수명,
최대한 오래 하려면?

신체건강 + 정신건강 챙기기

효율적인 시간 관리

습관화 및 계획화 중요

일단 본인이 즐거워야 함

만약 그렇지 않다면, 다른 업무나 커리어를
고민해보는 것도 괜찮음

어려움 극복하기

●○

열심히 해킹을 하다보면...🧠

💩**슬럼프**💩

🤯**번아웃**🤯

무조건 옵니다

어떻게 **극복**하느냐가 중요함

어려움 극복하기

사이버보안 문제는 하루 아침에 해결되지 않는 것이 **정상**

😌 마음을 **여유롭게** 가지고,
💪 **끈기** 있게,
🔬 **과학적**으로,
문제 해결에 접근해야 함

💡 **bpak의 Tip!**

- ✓ 더 쉽고, 더 작은 단위의 무언가를 해결함으로써 성취감 획득
- ✓ 든든한 팀원들에게 도움 요청

즐거움과 FOMO 사이 어디에서인가 오랜 시간 붙잡히면 👉 번아웃

💁‍♂️ 잊지 말아야 할 것: 우리는 **인간**이다
🏝️ **휴식**이 필요함!
(단, 사람마다 휴식의 방법/방식은 다름)

Making History

역사에 한 획을 긋는다는 것

역사를 만들어 간다는 것 (bpak edition)

해킹대회를 더 **경쟁적**으로!

국내·외 해킹대회 70회 이상 우승
DEFCON CTF 6회 우승 (+5회 준우승)
CODEGATE CTF 5회 우승
SECUINSIDE CTF 3회 연속 우승

커뮤니티를 위한 기여

Plaid CTF 운영 (12년째)
사이버보안 스타트업 설립 및 운영 (8년째)
Dreamhack 교육플랫폼 운영 (5년째)
보안 인재 양성 프로그램 멘토링 / 운영 (11년째)
각종 연구 결과 발표 및 논문 게재 (14년째)

전세계 **사용자 보안성** 및 **국가안보** 향상

소프트웨어 및 하드웨어 취약점 다수 제보
사이버무기 연구 및 개발 🤐

역사를 만들어가는 인재 양성의 중요성

사이버 위협 대응

급격한 사이버 공격 발전 (규모, 속도)
기업·정부·개인 등 모든 부문에 영향

경제적 이익

기업 보안 사고로 인한 금전적 손실 축소
산업 발전으로 일자리 창출 및 기술 수출

보안 기술 발전

보안 기술의 연구·개발 활성화
기술 고도화 및 혁신적인 해결책 제시

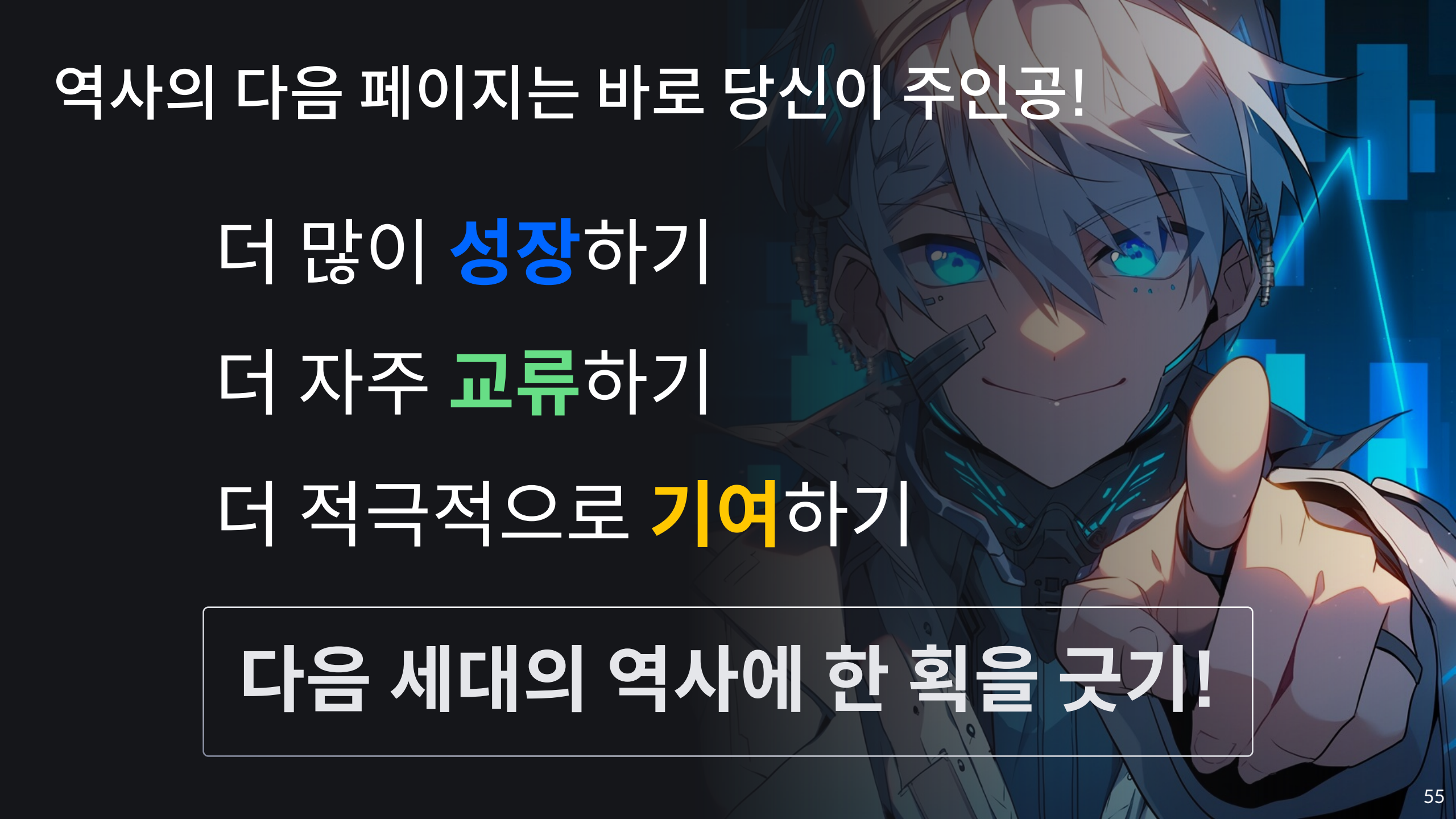
국가 안보 강화

현재진행형인 사이버전 및 공격에서
국가와 국민의 사이버영토를 보호

인공지능 및 기술융합

최신 기술을 접목·활용한 보안 솔루션
다양한 분야의 보안 문제 효율적 해결

역사의 다음 페이지는 바로 당신이 주인공!



더 많이 **성장**하기

더 자주 **교류**하기

더 적극적으로 **기여**하기

다음 세대의 역사에 한 획을 긋기!

Thank You

Making History
How to Raise the Next Generation of Whitehat Hackers

Brian Pak, CEO, Theori

brian@theori.io / @brian_pak

fb.com/theori.io

linkedin.com/company/theori

@theori_io

Theori