BUG BOUNTY

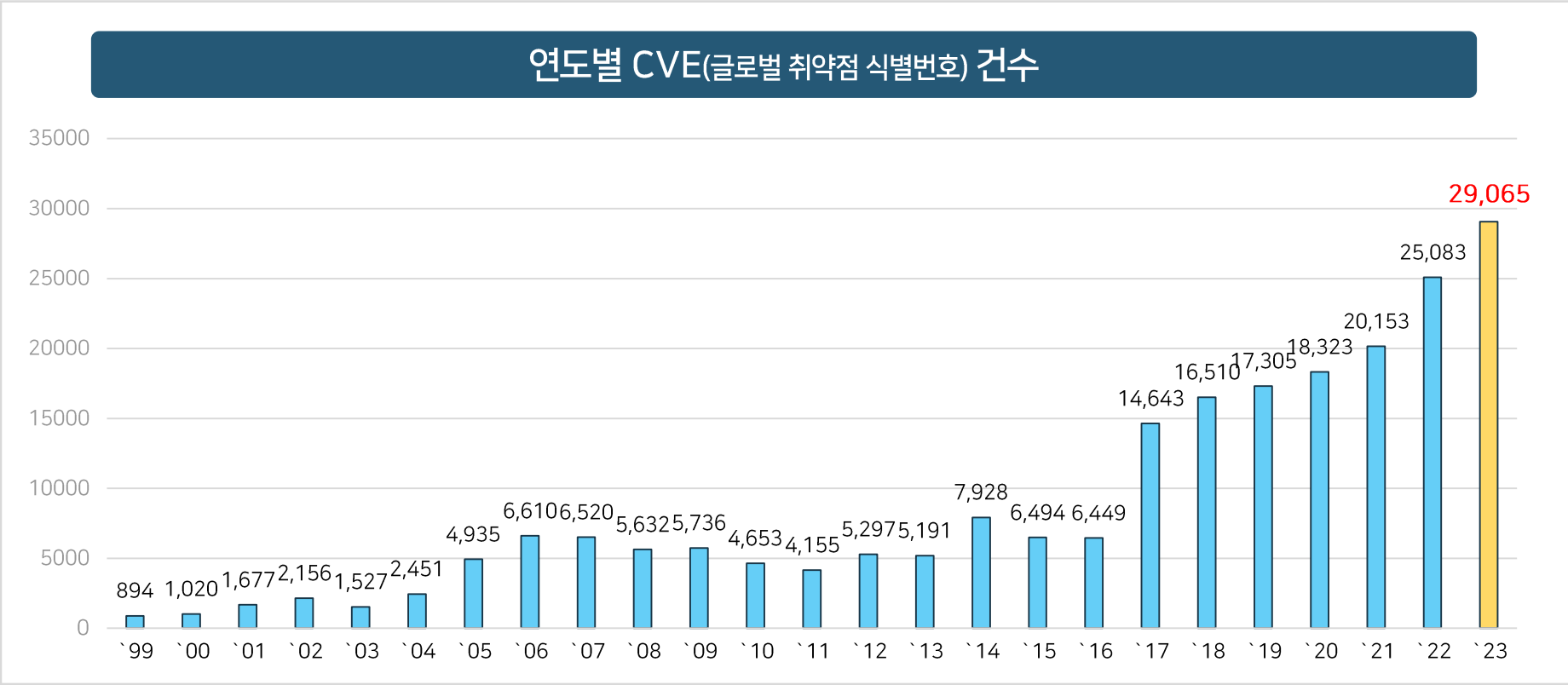
KISA 한국인터넷진흥원

보안 취약점 신고포상제(버그바운티)

& Hack the Challenge

급증하는 보안 취약점, 어떻게 대응할 것인가?

- ▶ 매년 신규 취약점 건수는 증가하고 있으며, 2023년은 총 29,065건으로 전년대비 약 15% 증가
- ➡ 이는 코로나19 사태로 급속화 된 디지털 대전환, 메타버스・NTF・AI 등 신기술 등의 영향



출처: CVE Details, https://www.cvedetails.com/browse-by-date.php

급증하는 보안 취약점, 어떻게 대응할 것인가?

▶ 증가하는 대학교 보안위협

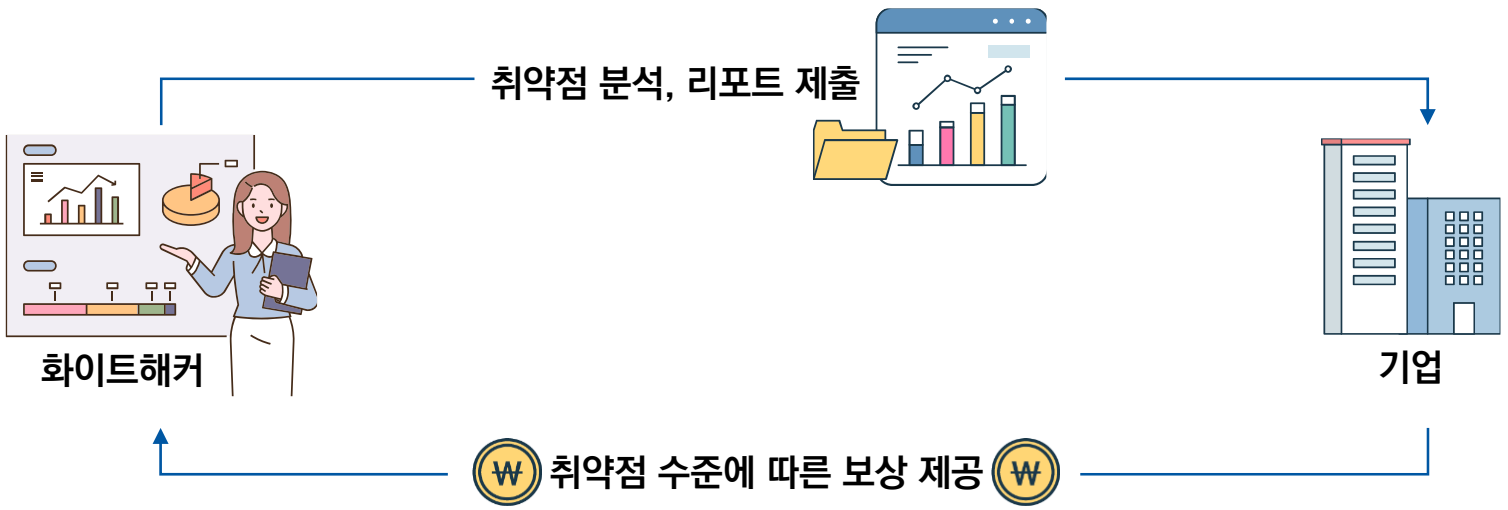
취약점을 악용한 해킹공격(정보유출 등) 발생 증가

01 취약점에 대응하는 가장 좋은 수단,

버그 바운티 프로그램(Bugbounty Program)

보안 취약점 신고포상제 &
Hack the Challenge

- 하드웨어, 소프트웨어, 웹 서비스 등 지정된 프로그램의 보안 취약점을 찾아낸 사람에게 취약점의 파급도에 따라 포상금을 지급하는 제도
- (화이트해커) 개인 역량 및 인지도 상승, 포상금으로 인한 금전적 이득
- (기업) 보안 취약점 패치, 보안 위협 대응, 정보보호 비용 예산 절감, 소프트웨어 및 서비스 품질 향상

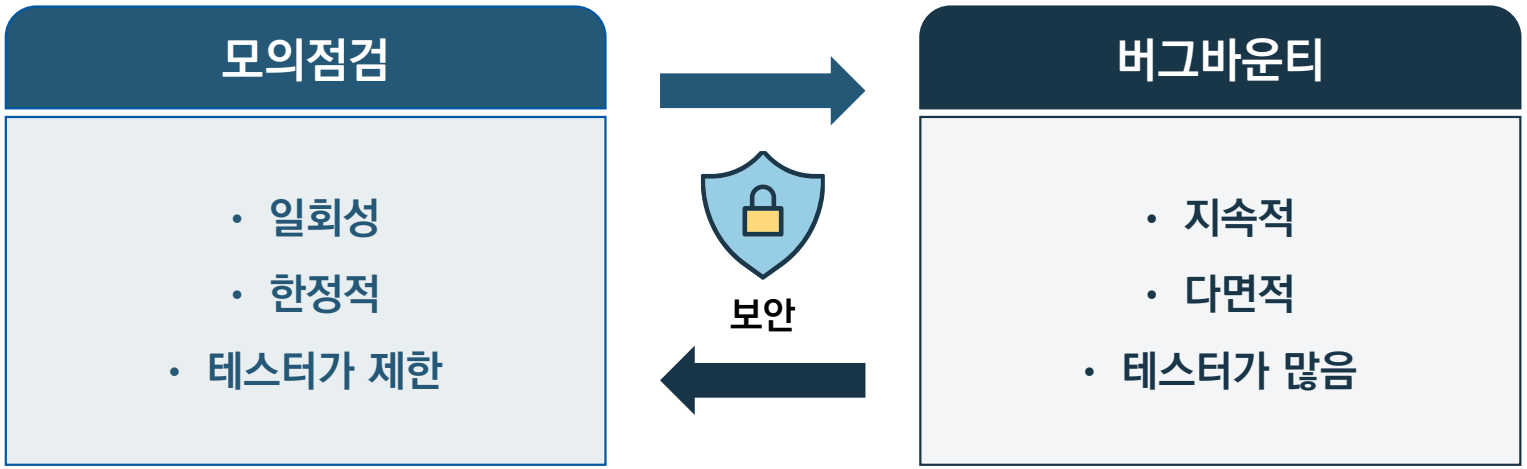


BUG BOUNTY
Korea Internet & Security Agency

KISA 한국인터넷진흥원

버그 바운티 프로그램(Bugbounty Program)

▶ 버그 바운티 프로그램을 운영하면 조직 내부적으로 보안 인력을 통해 점검을 하는 것 대비 심각도가 높은 취약점을 발견하는데 7배 이상 도움이 됨



출처 : BugCrowd, 7 Bug Bounty Myths

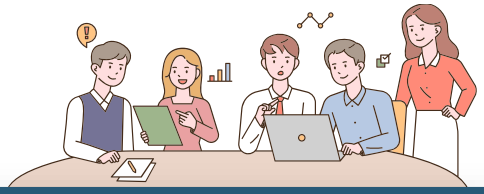
01 취약점에 대응하는 가장 좋은 수단,

버그 바운티 프로그램(Bugbounty Program)

보안 취약점 신고포상제 &
Hack the Challenge

버그바운티	
장점	• 다양한 예산에 맞게 범위 대상을 바로 조정할 수 있음 • 24시간 지속적으로 운영되므로 더 많은 취약점을 찾을 수 있음 • 초기 비용을 지불할 필요가 없이 기술적 증적자료가 있는 보고만을 대상으로 보상 • 다양한 관점의 시작으로 보안취약점을 찾을 수 있음
단점	• 취약점을 보고한 뒤 패치 등의 과정은 책임지지 않음 • 노출에 따른 저품질 보고서 등의 잠재적 유입에 따른 취약점 검증 과정 등이 필요

모의점검	
장점	• 체계적으로 다양한 테스트 옵션을 사용하여 진행 • 취약점 보고 그 이후 작업 및 관리까지 가능 • 팀 워크별 전담 들을 통해 효율적으로 취약점을 찾을 수 있음
단점	• 정형화된 체크리스트 등을 통한 점검 • 팀워크별 전담 등을 통해 효율적으로 취약점을 찾을 수 있음



버그바운티는

모의점검과 함께 시행되는 것이 가장 효율적인 방법

BUG BOUNTY
Korea Internet & Security Agency

KISA 한국인터넷진흥원

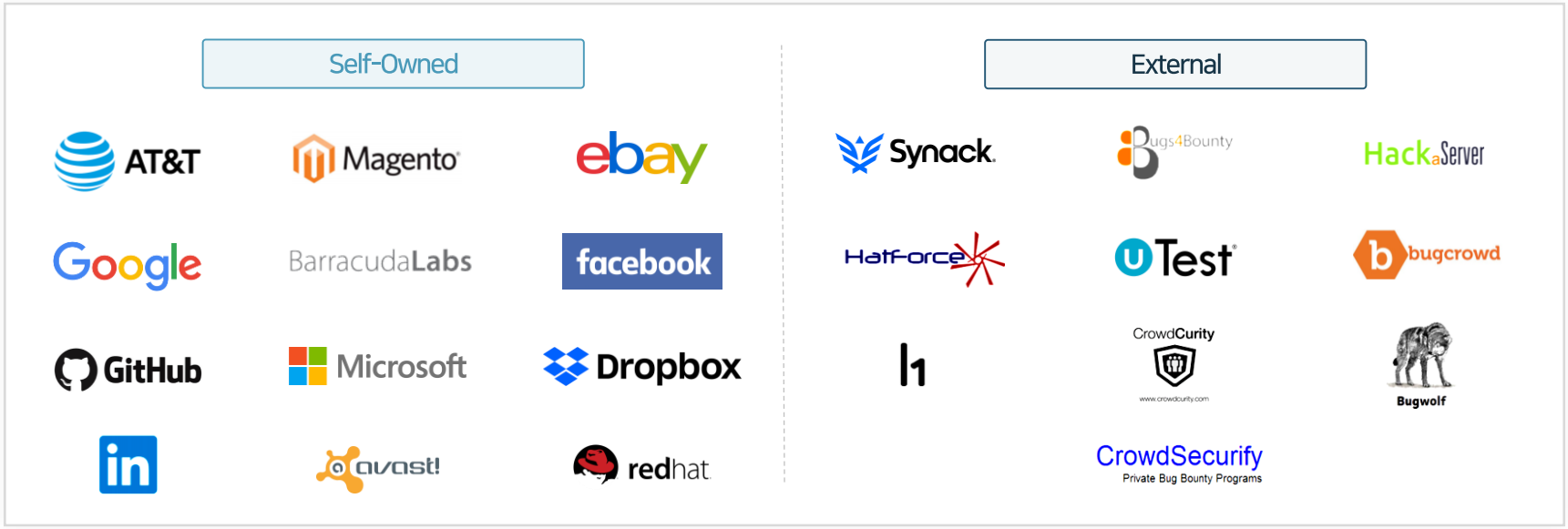
버그 바운티 프로그램(Bugbounty Program)

▶ 해외 사례

➡ 소프트웨어 취약점 : 구글('13.10 ~), Microsoft('13.11 ~), 애플('16.9)

➡ 온라인 서비스 취약점 : 페이스북('11 ~), 깃허브('13.6 ~), 야후('13.10 ~), Hack the Pentagon('16.4)

➡ 자체 도입이 어려운 경우, Hackerone, Bugcrowd 등 버그 바운티 플랫폼 서비스를 통하여 위임/운영하기도 함



버그 바운티 프로그램(Bugbounty Program)

▶ 국내 사례

네이버	• KISA의 신고포상제 공동 운영사로 참여 후 2019년부터 독립하여 별도 버그바운티 운영 시작 • 네이버 페이, 블로그, 웹툰 등 서비스 뿐만 아니라 MYBOX 탐색기, 클로바 등 다양한 대상으로 점차 확대 중 • 취약점의 파급도에 따라 최대 2,000만원까지 포상금 지급 https://bugbounty.naver.com/ko • 웨일 브라우저의 경우, 별도 버그바운티 페이지를 통해 운영 중이며 최대 7,500만원의 포상금 지급 https://bugbounty.whale.naver.com/ko
삼성전자	• TV 하드웨어/소프트웨어, 모바일 기기 등을 대상으로 버그바운티 실시 • 포상금액의 범위는 USD $200 ~ $200,000 https://samsungtvbounty.com/certificatesPost https://security.samsungmobile.com/rewardsProgram.smsb
리디북스	• 2019년부터 리디북스 서점 웹 사이트, iOS/Android용 리디북스 앱 등을 대상으로 진행 https://ridi.dev/bounty.html

파인더갭	• 파인더갭에서 운영하는 버그바운티 플랫폼 • 가상환경(VDI)에 기업에 운영하는 솔루션 등을 설치하여 위험을 줄이고 취약점을 찾을 수 있는 환경 제공 https://findthegap.co.kr/
zerowhale (파스텔 플래닛)	• 국내 스타트업에서 운영하는 신생 버그바운티 플랫폼 • 중소기업 및 스타트업 기업을 주요 대상으로 운영 중 https://zerowhale.io/
BugCamp (엔키)	• 플랫폼 시스템을 통해 기업과 화이트해커 간에 포상금 지급 등을 원활하게 할 수 있도록 지원 https://bugcamp.io/
PatchDay (Theori)	• 뱃지, 평균 포상금 및 응답률 등 화이트해커가 검증하기 용이하도록 UI 구성 및 위험도 지정을 통해 직관적인 평가체계 제공 http://patchday.io/

01 취약점에 대응하는 가장 좋은 수단,

버그 바운티 프로그램(Bugbounty Program)

보안 취약점 신고포상제 &
Hack the Challenge

▶ 버그바운티 사례

[G-PRIVACY 2022] 최병훈 신세계디에프 CISO "버그바운티, 집단지성 이용한 보안 강화…결과 만족"(영상)

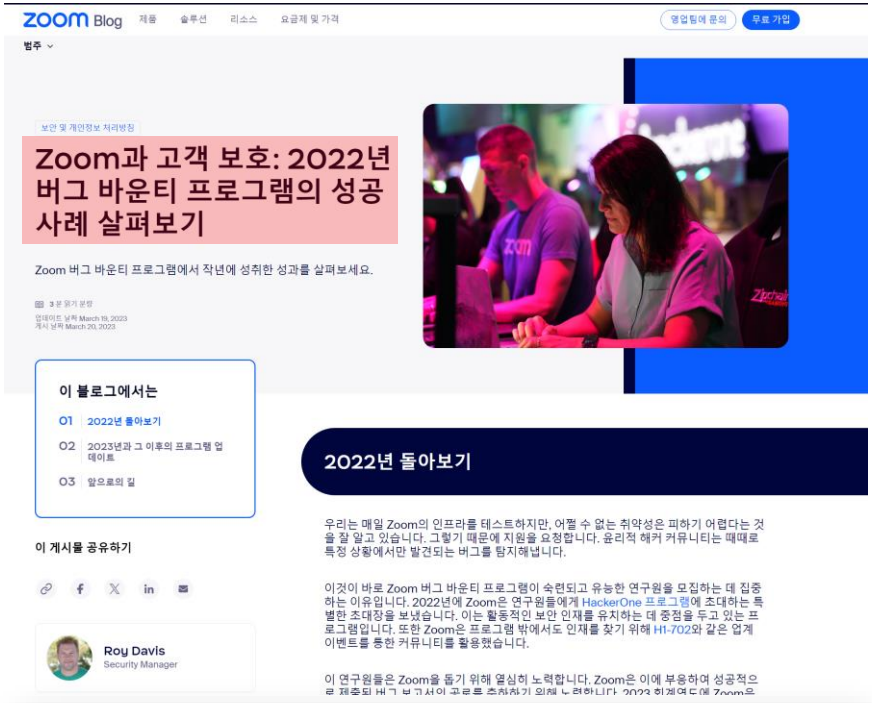
김민권 기자 | 승인 2022.04.03 2021

"기존 모의해킹이나 취약점 점검 대비 50% 이상 많은 취약점 결과물 발견"

G-PRIVACY 2022. 최병훈 신세계디에프 CISO 강연

데일리시큐가 주최하고 개인정보보호위원회, 한국인터넷진흥원, 한국정보보호산업협회가 후원하는 G-PRIVACY 2022가 3월 29일 더케이호텔서울 아야금홀에서 공공, 금융, 기업 개인정보보호 및 정보보안 실무자 700여 명이 참석한 가운데 성황리에 개최됐다.

최병훈 신세계디에프 CISO는 'KISA 버그바운티를 통한 개인정보보호'를 주제로 키노트 발표를 진행했다.



신세계디에프 CISO

버그바운티는 집단지성을 이용해 기존 모의해킹과 취약점점검에서는 찾을수 없는 새로운 문제점을 발견하였음

조직의 정보보호 수준이 업그레이드 될수 있다는 것을 경험

Zoom

자체적인 보안점검을 진행하지만 발견하지 못하는 취약점이 있음

보안부서의 업무량을 대폭 감소시켰으며, 취약점을 통해 문제가 발생하기 전 해결하였음

핵더챌린지 분석 플랫폼(Hack the Challenge)

▶ 핵더챌린지 분석 플랫폼이란?

➡ 클라우드 형태의 서버를 제공하여 분석 대상 소프트웨어/서비스를 사전 설치 후 화이트해커에게 개방

➡ 화이트해커는 취약점 분석 환경이 구성된 가상 환경(VDI)에 접근하여 취약점 분석 진행

SW 개발기업

· 취약점 발굴환경 설치
· 보안취약점 신속 패치 제공

매칭

화이트해커

· 신규 보안취약점 발굴·신고
· 최신 취약점 정보공유

핵더챌린지 분석 플랫폼

민간기업

· 신규 보안취약점 보안패치 개발지원
· 백신업데이트 등 피해확산방지

일반국민

·보안취약점 동향, 예방·조치방안 등
각종 취약점 정보 온라인 제공

핵더챌린지 분석 플랫폼(Hack the Challenge)

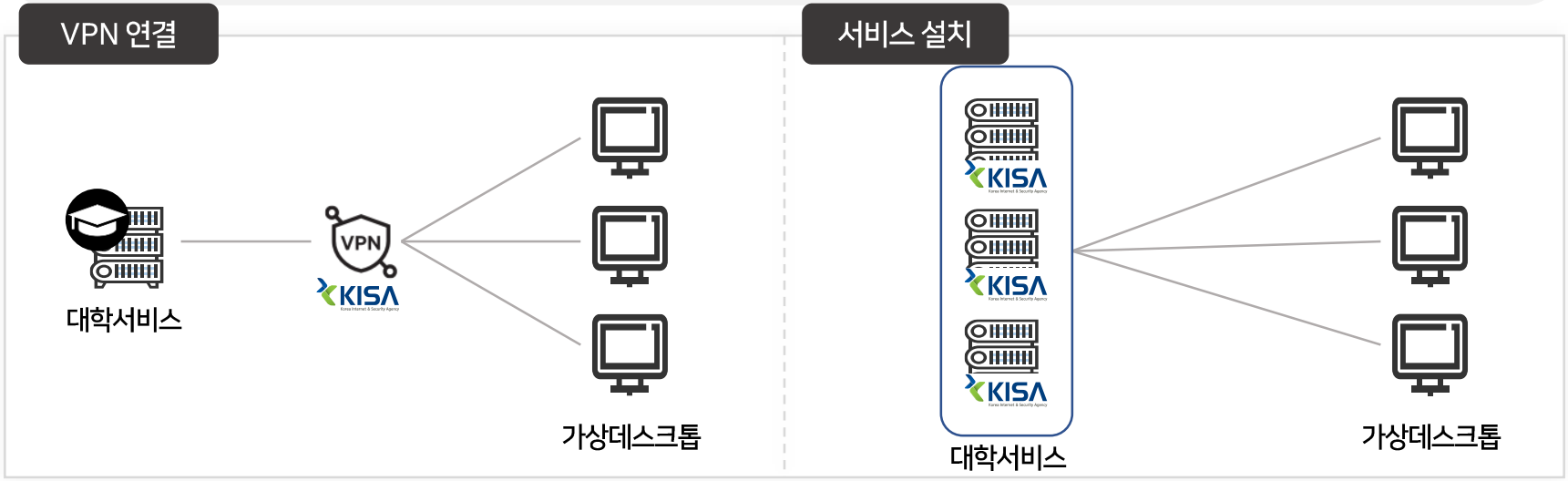
▶ 핵더챌린지 분석 플랫폼 이용시 장점

① (안전한 환경) KISA에서 제공하는 서버에 취약점 발굴대상 설치 후 버그바운티를 운영

➡실제 운영중인 서비스 장애 우려 해소, 소스코드 등 정보 유출 차단

② (안전한 분석) 가상데스크톱(VDI)를 통해 취약점을 발굴 및 신고

➡신청된 인원만 참가가능, VDI 내부 자료 외부 반출 차단, KISA로 취약점 신고 가능



핵더챌린지 분석 플랫폼(Hack the Challenge)

▶ 핵더챌린지 분석 플랫폼 이용사례

KISA 버그바운티(21년)

참가기업	신세계디에프, 엔씨소프트 등 9개 기업
화이트해커	595명 참가
취약점	신규취약점 689건 발굴

대기업(CJ올리브네트웍스) 연계(22년~23년)

참가기업	크린랩, 글로벌브릿지 등 13개 기업
화이트해커	200명 참가
취약점	신규취약점 977건 발굴

참가기업	한국디지털거래소, 링글 등 15개 기업
화이트해커	600명 참가
취약점	신규취약점 786건 발굴

보안사고 발생율 ZERO!!

BUG BOUNTY
Korea Internet & Security Agency

KISA 한국인터넷진흥원

03 대학교 보안강화를 위한 제안

대학교 서비스 대상 버그바운티 추진

보안 취약점 신고포상제 &
Hack the Challenge

▶ 버그바운티, 이렇게 운영합니다!

➡ 대학교에서 원하는 서비스와 운영 방식 등 선정

➡ 취약점 발굴 과정 : (방법1) 참여 기업에서 대상 서비스 또는 솔루션 제공 VPN을 통해 VDI와 연결

(방법2) KISA가 제공하는 핵더챌린지 분석 플랫폼을 이용하여
실제 환경과 동일한 환경 구성

➡ KISA의 다년간 신고포상제 운영 노하우를 바탕으로 버그 바운티 프로그램 운영 기반 제공

취약점 입수, 취약점 평가 체계 기반 검토, 신고자와의 의사소통, 포상금 지원

추진 일정(안)

4월~5월 : 버그바운티 운영을 위한 사전준비(클라우드 내 서비스 설치, VPN 연결 등)
6월~7월 : 버그바운티 대회 개최(화이트해커 참여)
8월~9월 : 취약점 평가
10월~11월 : 포상금 지급 및 결과 공유회

취약점이 있는 것은 당연, 신속하게 인지하여 조치하는 것이 중요!

버그바운티! 지금 바로 신청하세요

BUG BOUNTY
Korea Internet & Security Agency

KISA 한국인터넷진흥원

대학교 서비스 대상 버그바운티 추진

▶ 버그바운티 운영 R&R

TASK	KISA	KERIS	대학교
대학생 홍보 및 모집	■	■	■
대학생 선발 및 교육	■		
대학교 협조 요청		■	■
버그바운티 환경 제공	■		
버그바운티 환경 구축			■
버그바운티 운영	■		
취약점 검증 및 평가	■		
취약점 전달 및 지원	■	■	
취약점 조치		■	■
포상금 산정	■		
수상자 선정	■	■	
포상금 지급	■		
결과공유회 준비	■	■	
결과공유회 참석	■	■	■

Thanks!

보안 취약점 신고포상제 & Hack the Challenge

KISA 한국인터넷진흥원