Security BugBounty
KOREA INTERNET & SECURITY AGENCY

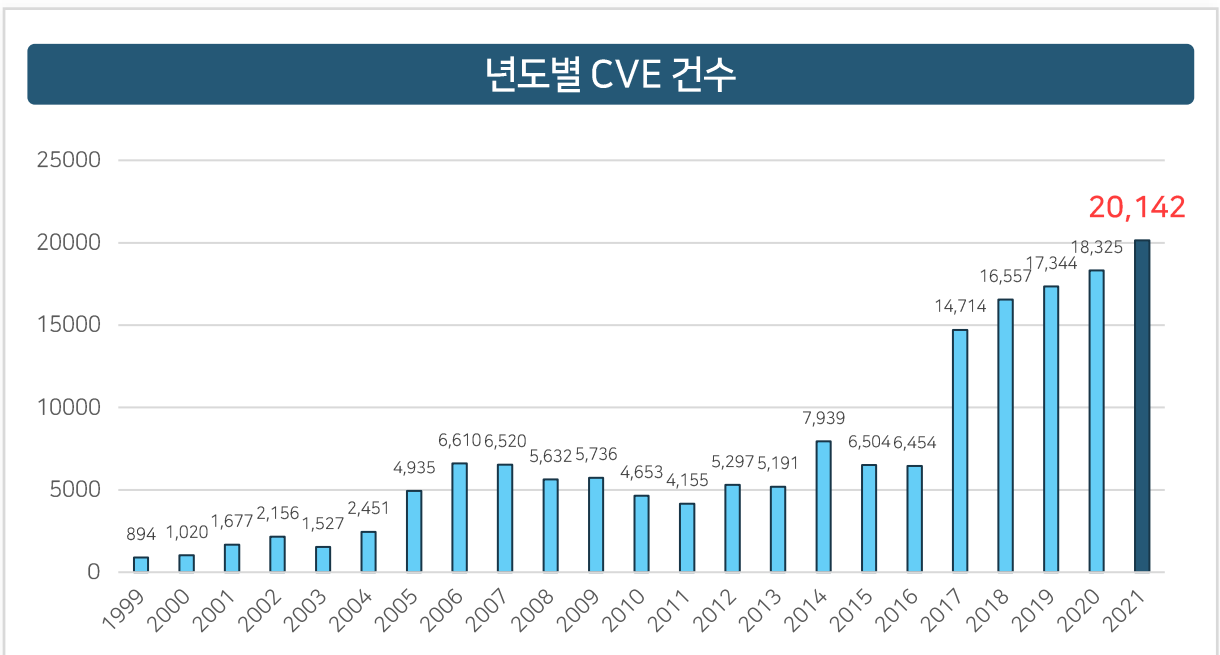
보안 취약점 신고포상제
&
Hack the Challenge

KISA 한국인터넷진흥원

급증하는 보안 취약점, 어떻게 대응할 것인가?

▶ 매년 신규 취약점 건수는 증가하고 있으며,
2021년은 총 20,142건으로 전년대비 약 10% 증가

➡ 이는 코로나19 사태로 급속화 된 디지털 대전환, 메타버스·NTF·AI 등 신기술 등의 영향



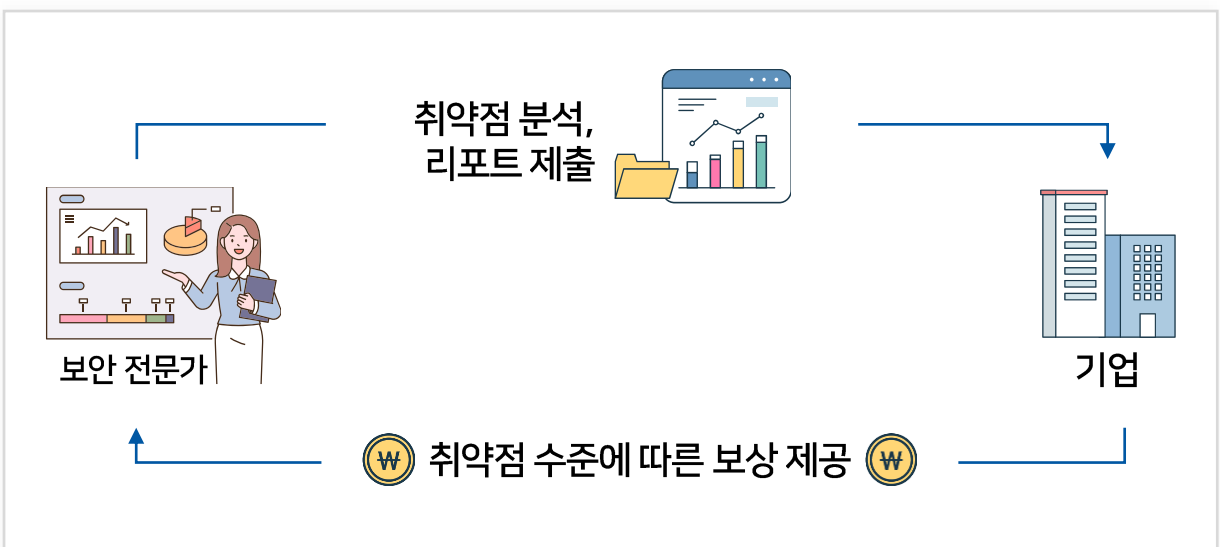
출처: CVE Details, https://www.cvedetails.com/browse-by-date.php

01 취약점에 대응하는 가장 좋은 수단,

버그바운티 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
- (보안 전문가) 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



Security BugBounty KOREA INTERNET & SECURITY AGENCY

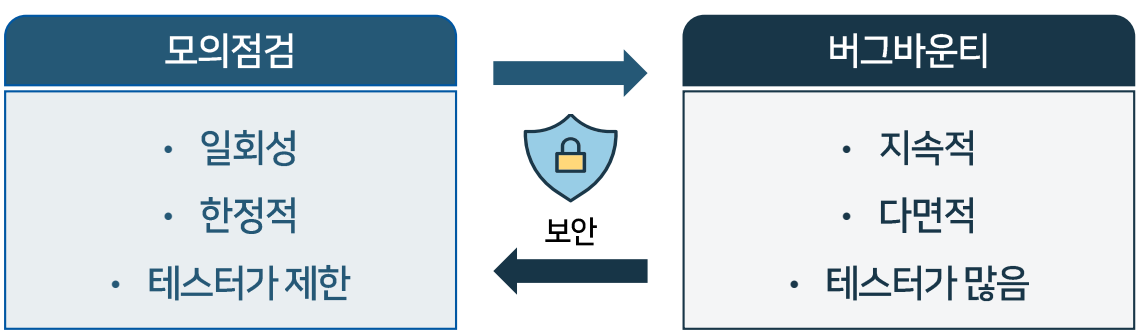
KISA 한국인터넷진흥원

01 취약점에 대응하는 가장 좋은 수단,

버그바운티 프로그램 (Bugbounty Program)

보안 취약점 신고포상제 & Hack the Challenge

▶ 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,

버그바운티 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

Security BugBounty KOREA INTERNET & SECURITY AGENCY

KISA 한국인터넷진흥원

02 KISA의 버그 바운티 프로그램,

보안 취약점 신고포상제

보안 취약점 신고포상제 &
Hack the Challenge

- 국내에서 사용중인 소프트웨어를 대상으로 분기별 우수 취약점을 선정하여 평가 결과에 따라최대 1,000만원의 포상금 지급

➡ 참가 대상 : 국내외 거주하는 한국인

➡ 신고 대상 취약점 : 국내에서 사용 중인 '소프트웨어' 대상 최신 버전에 영향을 줄 수 있는 보안 취약점

➡ 평가 및 포상 일정 : 분기별 평가를 실시하여 포상금 지급(3, 6, 9, 12월)

➡ 웹 사이트 등 실제 운영 중인 서비스의 경우 사전에 대상과 시기를 정하여 한시적으로 취약점 발굴을 허용하는 "핵 더 챌린지"로 운영

※ 실제 운영 중인 서비스에서 동의 없이 취약점을 발굴하는 행위는 정보통망법에 의거하여 정보통신망 침입 행위로 간주될 수 있으므로 사전에 허가된 대상으로 한정

Security BugBounty
KOREA INTERNET & SECURITY AGENCY

KISA 한국인터넷진흥원

03

우리 기업에서 버그 바운티를 운영하려면?

보안 취약점 신고포상제 & Hack the Challenge

01	버그바운티를 허용하는 대상범위 또는 제품을 선정합니다. Ex) CCTV, 스마트 컨트롤러, 개발한 모든 소프트웨어, 개발한 서비스 (모바일 앱) 등	버그바운티 대상범위(제품) 지정
02	1년간 사용할 포상금을 계획합니다. 신고자에게 포상금수령 시 지급 프로세스를구축합니다.	예산 마련
03	취약점 별로 포상 기준을 마련합니다. Ex) XSS 취약점 : 5만원 버퍼오버플로우 취약점 : 50만원	포상 기준 마련
04	취약점 신고 받는 웹페이지를 제작합니다.	입수체계 구축
05	신고된 취약점 검증/평가/예산 지급을 진행할 역할 분담합니다.	운영 시작

" 버그 바운티를 운영하고 싶은데 어떻게 해야 할 지 모르겠어요 "
" 예산을 1년에 얼마나 잡아야 할 지 감이 안 잡혀요 "
" 신고자와의 의사 소통이나 취약점 평가 기준을 수립하는 게 어려워요 "
" 갖춰야 할 게 많아 단계적으로 지원 받으며 버그 바운티를 구축하고 싶어요 "

04 KISA의 보안 취약점 대응 지원책 (1)
신고포상제 공동 운영 제도

보안 취약점 신고포상제 &
Hack the Challenge

▶ 신고 포상제 공동 운영사란?

➡ 자사 SW 또는 서비스를 취약점 발굴 대상으로 제공하거나, 포상금을 신고자에게 직접 지급함으로써 취약점에 대한 책임있는 역할을 수행하는 기업

KISA 한국인터넷진흥원

1. 민간 주도의 자발적 버그바운티 문화 도입을 위한 공동 운영사 참여 확대
2. 다년간 신고 포상제를 운영해온 평가체계 등을 민간기업에 지원

공동운영사

1. 자체 버그바운티 단계적 도입을 위한 지원활용(평가체계 등)
2. 국제표준식별체계 CVE 발급이 필요한 경우 MITRE 연계 서비스 KISA(CVE 발급 가능한 CNA 기관)를 통해 CVE 발급 가능
3. 보안취약점을 빨리 알아내고 신속히 조치하여 사고예방

공동운영사 협약 + 신고포상제 노하우 및 기반 역량 마련 + 버그바운티 자체 운영을 통한 민간 보안 선순환

Security BugBounty
KOREA INTERNET & SECURITY AGENCY

KISA 한국인터넷진흥원

04 KISA의 보안 취약점 대응 지원책 (1)

신고포상제 공동 운영 제도

보안 취약점 신고포상제 &
Hack the Challenge

- 공동운영사 21개 운영('21년 삼성SDS, 현대, 기아 협약)
- 네이버社 공동 운영사 독립 자체 운영('19년 3분기)
- 카카오社 독립 운영 준비중

'14년 HANCOM GROUP

'15년 NAVER

'16년 kakao NEOWIZ GAMES

'17년 ESTsecurity INITECH LG전자 Genians kakaobank AhnLab INCA

'18년 HAURI XBLOCK SYSTEMS BOScoin GLOSFER

'19년 sga 에스지에이솔루션즈(주) SOTERIA CYBER SECURITY HUNESION

'20년 zigzag K VISION 지란지교시큐리티

'21년 삼성SDS HYUNDAI KIA

Security BugBounty KOREA INTERNET & SECURITY AGENCY

KISA 한국인터넷진흥원

신고포상제 공동 운영 제도

▶ 단계별로 운영하는 공동 운영 제도

1단계(포상)		2단계(평가)		3단계(분석)		4단계(독립)	
내용	주체	내용	주체	내용	주체	내용	주체
1. 입수	KISA	1. 입수	KISA	1. 입수	KISA	1. 입수	공동 운영사
2. 취약점 검증 및 분석	KISA	2. 취약점 검증 및 분석	KISA	2. 취약점 검증 및 분석	공동 운영사	2. 취약점 검증 및 분석	공동 운영사
3. 취약점 평가	KISA	3. 취약점 평가	공동 운영사	3. 취약점 평가	공동 운영사	3. 취약점 평가	공동 운영사
4. 취약점 포상	공동 운영사	4. 취약점 포상	공동 운영사	4. 취약점 포상	공동 운영사	4. 취약점 포상	공동 운영사

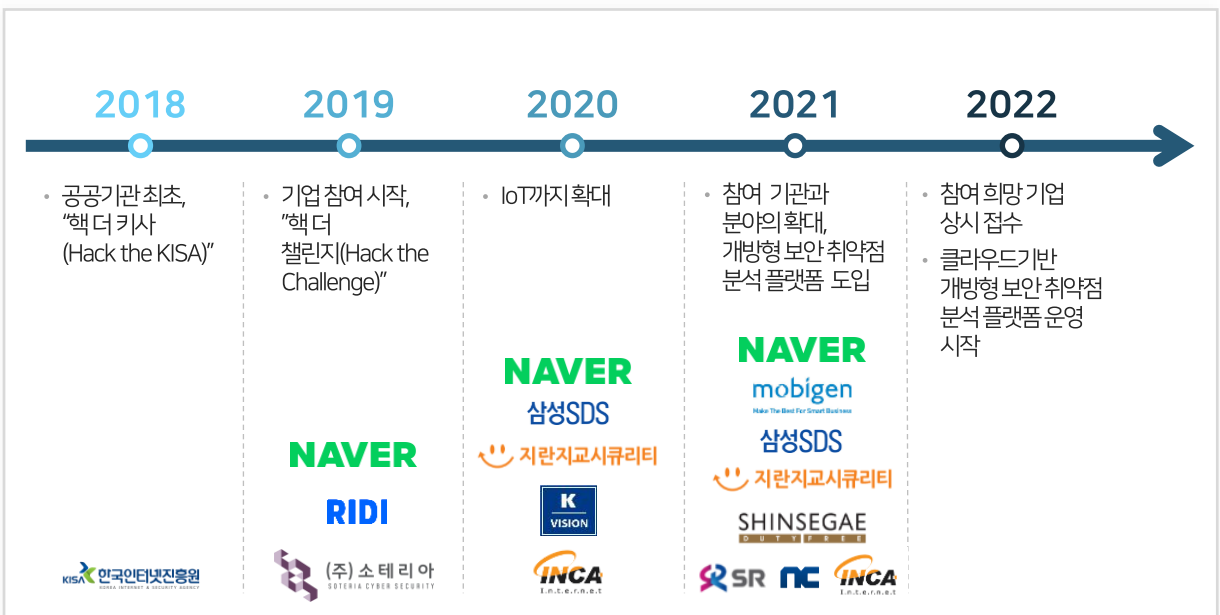
핵 더 챌린지 (Hack the Challenge)

" 버그바운티를 운영하고는 싶은데 계속하기에는 부담스러워요 " –

보안 취약점 신고포상제 & Hack the Challenge

▶ 핵 더 챌린지란?

➡ 한시적으로 참여 기업이 필요한 제품 또는 서비스를 선정하여 취약점 발굴을 허용하고 포상금을 지급



05 KISA의 보안 취약점 대응 지원책 (2)

핵 더 챌린지 (Hack the Challenge)

" 버그바운티를 운영하고는 싶은데 계속하기에는 부담스러워요 " -

보안 취약점 신고포상제 & Hack the Challenge

▶ 핵 더 챌린지 대회, 이렇게 운영합니다!

➡ 참여 기업이 원하는 일정과 운영 기간, 대상 제품 선정

➡ **취약점 발굴 과정 :** (방법1) 참여 기업에서 대상 서비스 또는 솔루션 제공

(방법2) KISA가 제공하는 개방형 보안 취약점 분석 플랫폼을 이용하여 실제 환경과 동일한 환경 구성

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

취약점 입수, 1차 검토, 취약점 평가 체계, 신고자와의 의사소통, 포상금 지원(일부)

이럴 때 추천해요!

① 기업 내부에서만 사용하는 프로그램을 대상으로 취약점 발굴을 원할 때
② 실제 운영 중인 서비스에 존재하는 취약점을 주치하고 싶은데 서비스 영향에 우려가 될 때
③ 제품 출시 전 사전 취약점 점검을 원할 때

취약점이 있는 것은 당연, 신속하게 인지하여 조치하는 것이 중요!

핵 더 챌린지! 지금 바로 신청하세요

관련 문의 및 참여 신청 : htc@krcert.or.kr

Security BugBounty KOREA INTERNET & SECURITY AGENCY

KISA 한국인터넷진흥원

06 KISA의 보안 취약점 대응 지원책 (3)

개방형 보안 취약점 분석 플랫폼

보안 취약점 신고포상제 & Hack the Challenge

▶ 개방형 보안 취약점 분석 플랫폼이란?

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

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

Security BugBounty KOREA INTERNET & SECURITY AGENCY

KISA 한국인터넷진흥원

붙임 1

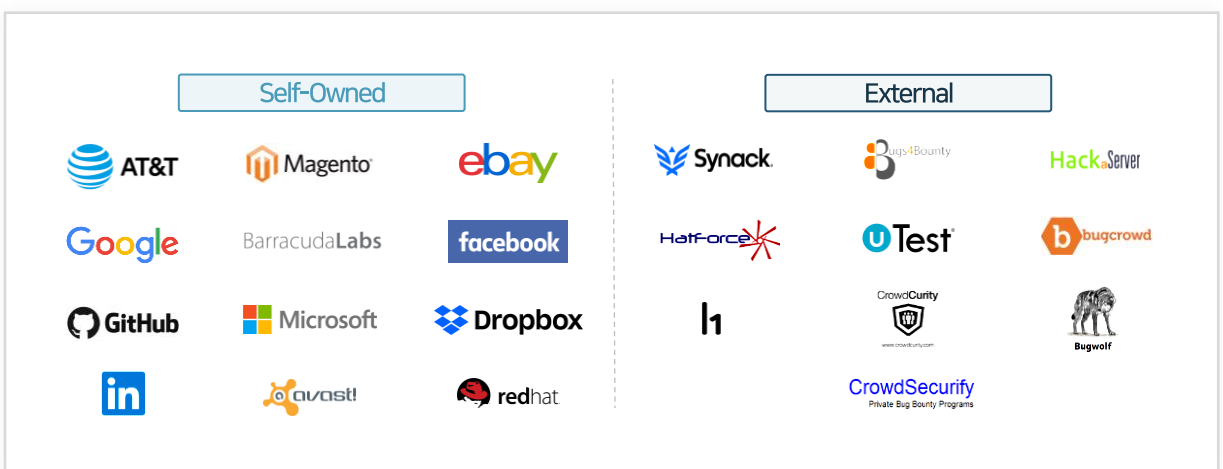
버그 바운티 프로그램 사례

▶ 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



붙임 1

버그 바운티 프로그램 사례

▶ 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

붙임 1

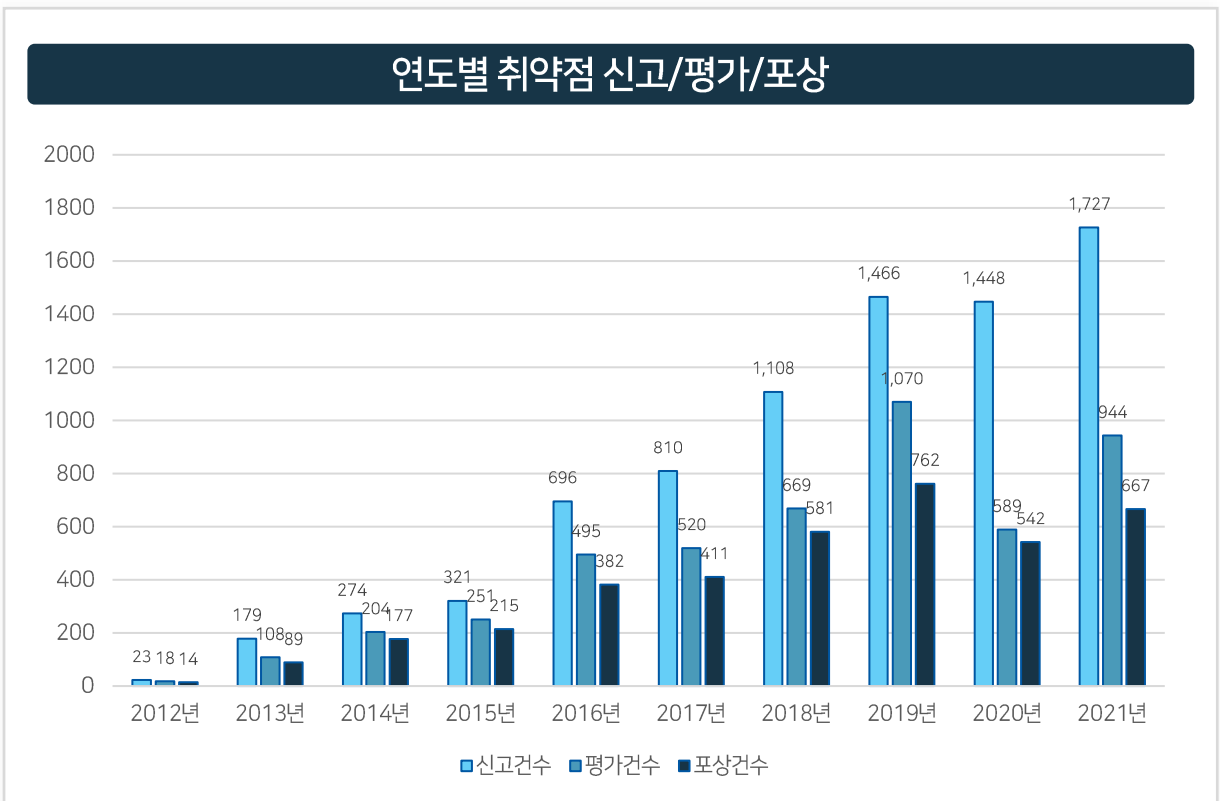
버그 바운티 프로그램 사례

▶ 국내 사례

Hacking Zone (삼성SDS)	• 삼성SDS에서 운영하는 버그바운티 플랫폼 • 가상환경(VDI)에 기업에 운영하는 솔루션 등을 설치하여 위험을 줄이고 취약점을 찾을 수 있는 환경 제공 https://hackingzone.net/
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/

보안 취약점 신고포상제 운영 현황

▶ 신고포상제 운영 현황



핵 더 챌린지 운영 현황

▶ 핵 더 챌린지 운영 현황