

hacking zone

버그바운티 플랫폼 : 집단지성을 활용한 보안취약점 대응

신봉건 프로 삼성SDS 해킹존소사장

버그바운티?

Bug Bounty

Bug: 프로그램 오류 + Bounty: 포상금


기업제품의 보안취약점 제보자에게 포상금을 지급하는 제도

기업이 허용하는 해킹범위 내에서
화이트해커가 해킹을 시도하여 보안취약점을 발견, 제보하면
기업은 제보된 취약점을 평가하고
그에 적합한 수준의 포상금을 지급한다.



Bug Bounty를 활용하는 글로벌 기업들





글로벌 기업들이 버그바운티를 하는 이유

모의해킹, 보안점검 등 기존의 방식과 버그바운티의 효과 비교 시 제보 취약점 건수 증가, 지출비용 감소 등 가성비가 뛰어나기 때문

구글 크롬



모의해킹 263건
버그바운티 371건

모질라 파이어폭스



모의해킹 48건
버그바운티 148건

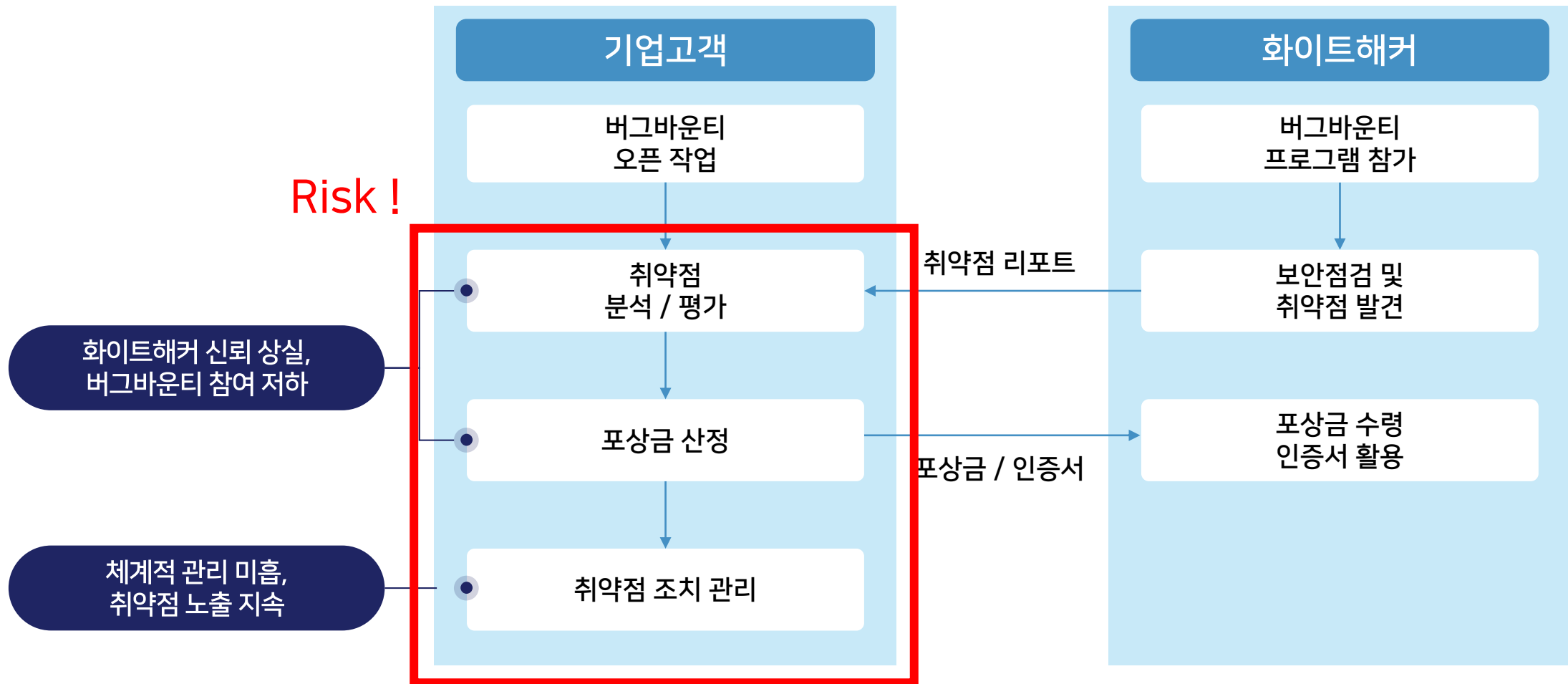
구글 크롬		(3년간)	모질라 파이어폭스	
모의해킹	버그바운티		모의해킹	버그바운티
263	371 (△41%)	취약점 건수	48	148 (△208%)
547,566	393,260 (▽28%)	지출비용(\$)	547,488	444,000 (▽20%)
2,082	1,060 (▽50%)	취약점 건당 지출비용(\$)	11,406	3,000 (▽74%)

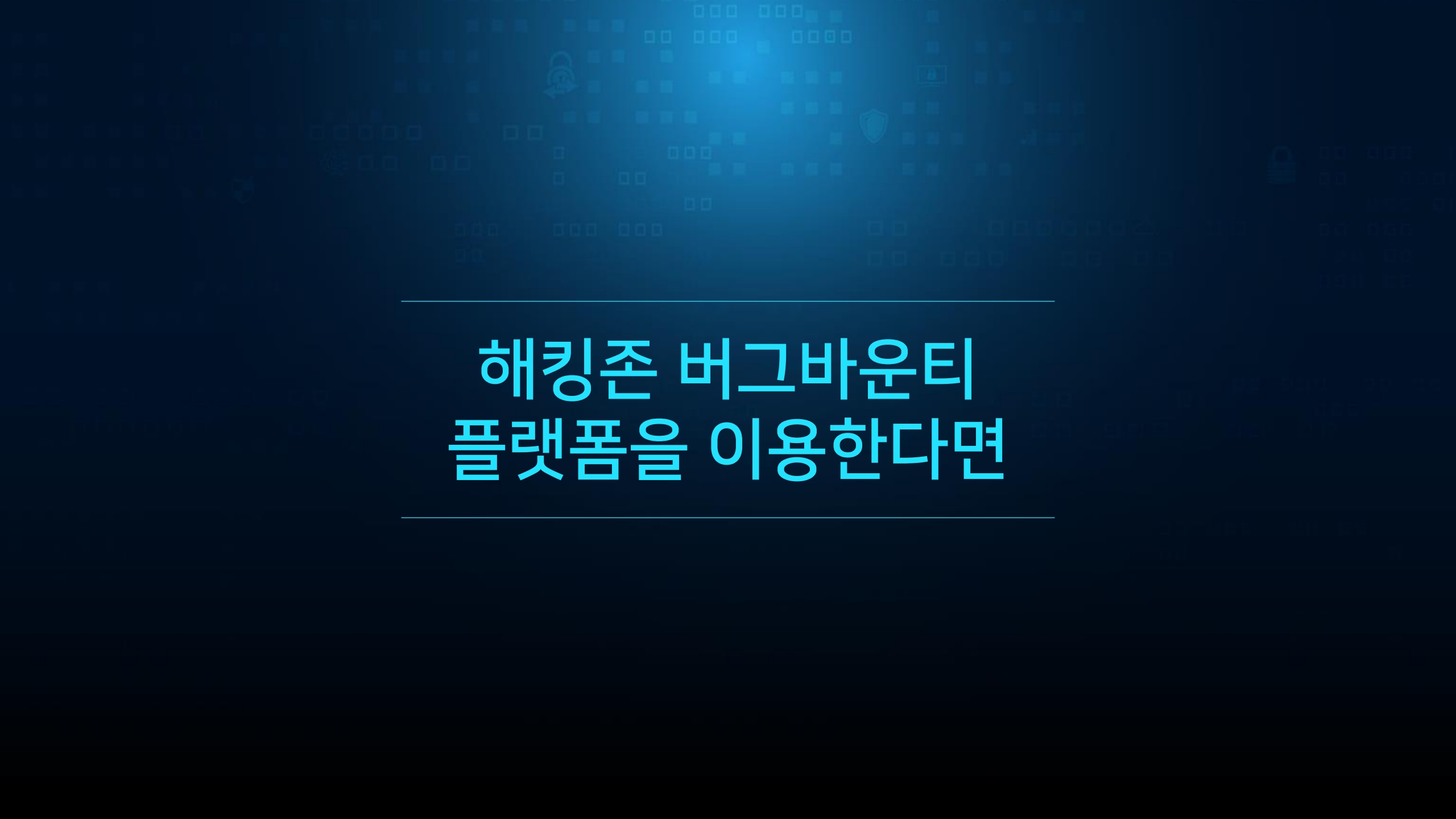
* 2020년 KISA 취약점 분석팀 제공자료

하지만,
버그바운티 자체 운영은
필요한 것들이 많다!

버그바운티 운영에 필요한 프로세스

버그바운티 자체 운영 기업들의 최소 운영 인력 평균 5~10명.(글로벌 기업의 경우 수십명 이상인 경우도 다수). 제대로 된 프로세스가 없다면 오히려 역효과가 날 수 있다.

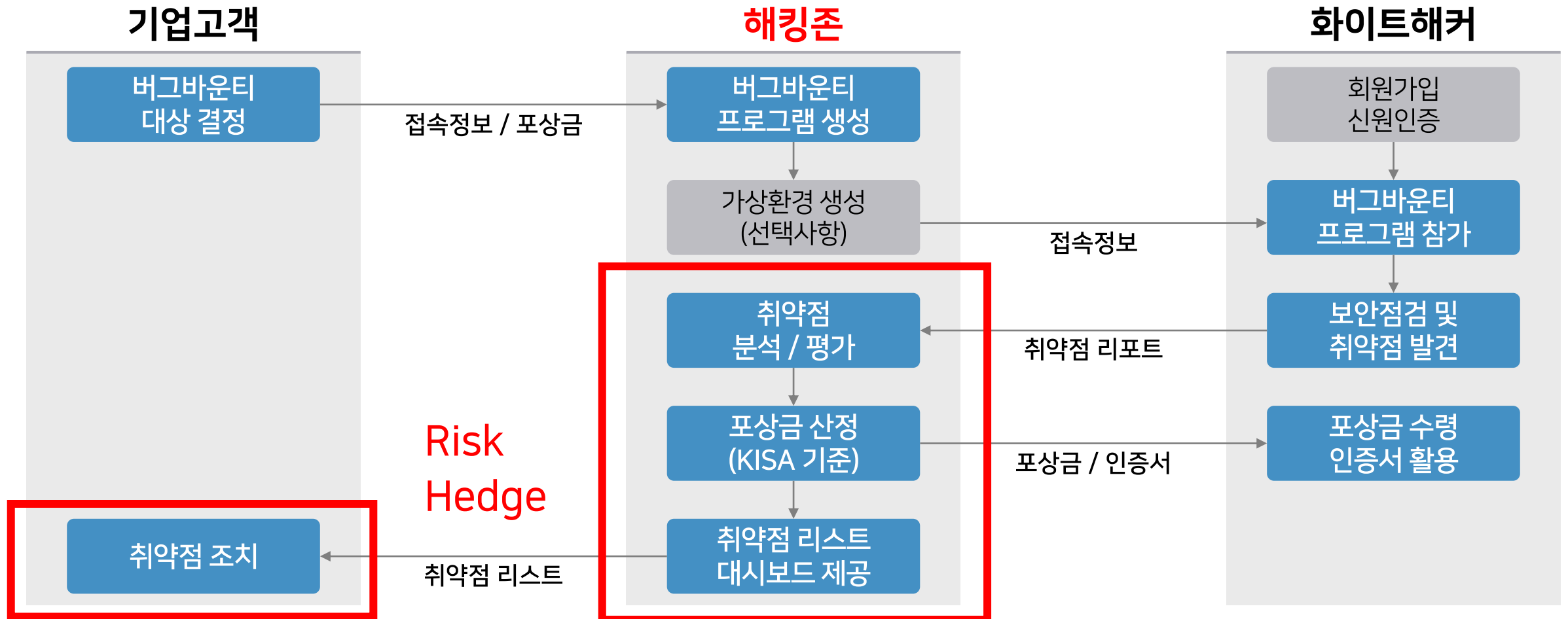




해킹존 버그바운티 플랫폼을 이용한다면

버그바운티 플랫폼 서비스

플랫폼은 취약점 접수, 평가, 포상 등 버그바운티에 필요한 전문성 제공 및 소요공수, 비용 최소화 등의 서비스 제공한다.
기업은 자체 운영하는 경우보다 훨씬 적은 프로세스만 관리하면 된다.



해킹존 플랫폼의 차별점 가상환경 버그바운티

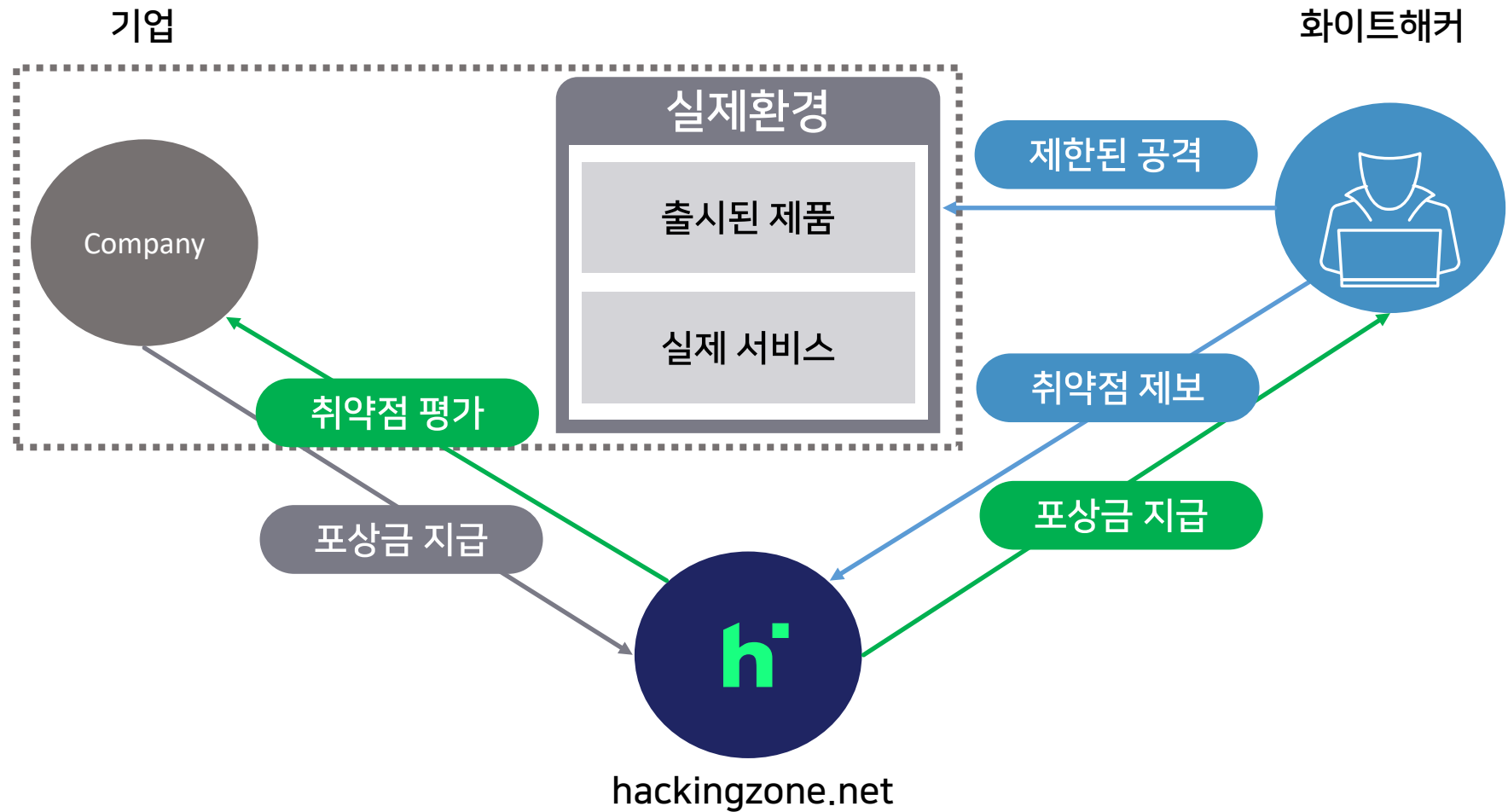
기업고객과 화이트해커를 연결해주는 플랫폼으로서 버그바운티 운영 서비스와 함께 가상환경 버그바운티를 제공합니다



해킹존 플랫폼 이용방법 1

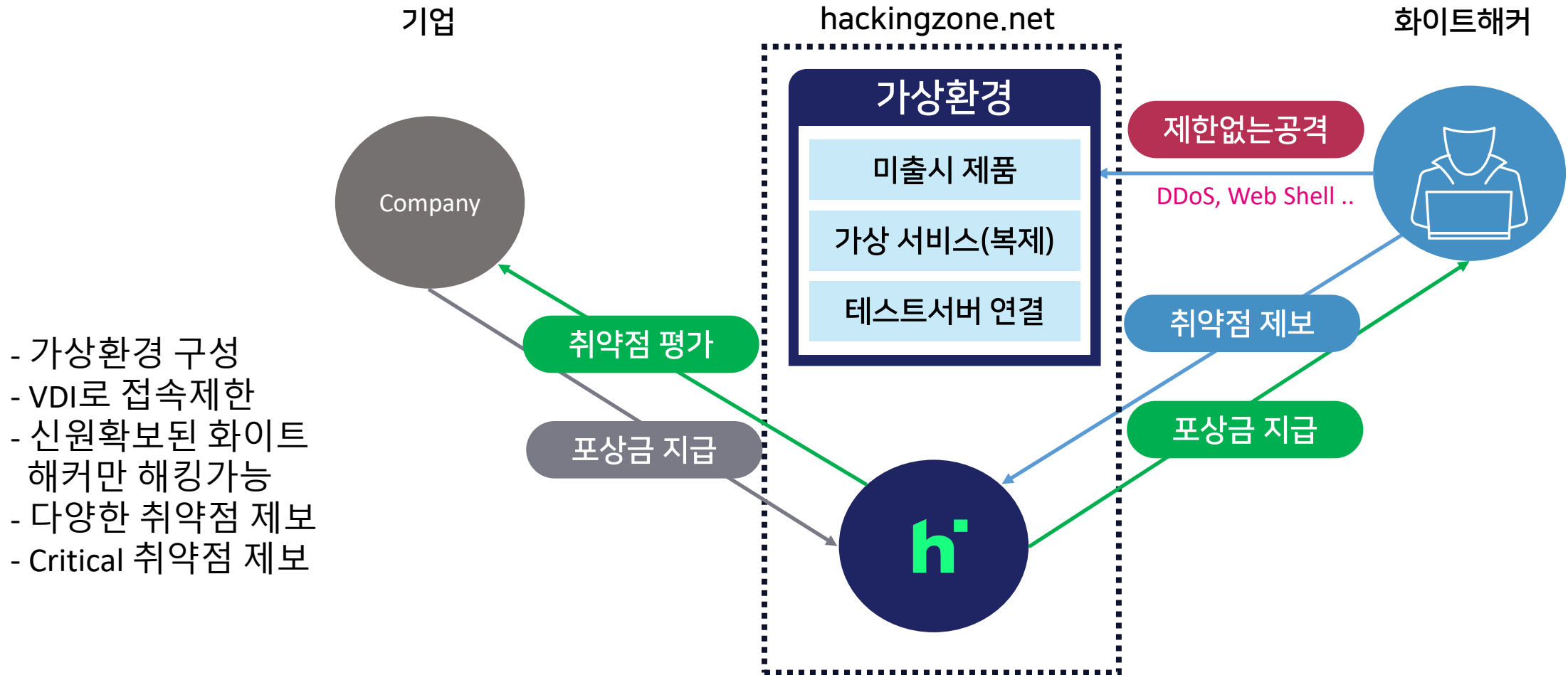
- 실제환경에서 운영하는 버그바운티

- 실제 환경 수행
- 공격방법 제한
- 취약점 중요도가 상대적으로 낮음




해킹존 플랫폼 이용방법 2

- 가상환경에서 운영하는 가상환경 버그바운티



- 가상환경 구성
- VDI로 접속제한
- 신원확보된 화이트 해커만 해킹가능
- 다양한 취약점 제보
- Critical 취약점 제보



가상환경 버그바운티의 효과

(2020년 7월 베타 버그바운티)

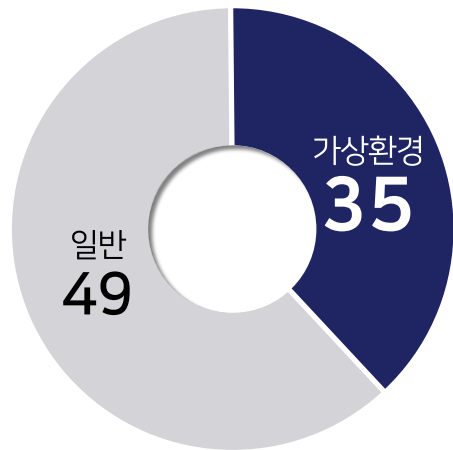
5개 일반 서비스와 5개 가상환경 서비스에 버그바운티를 진행



* 2020년 해킹존 베타 버그바운티 결과 (KISA 취약점 평가)

발견 취약점의 수는 일반 서비스에서 더 많았으나
중요 취약점은 가상환경에서 월등히 많이 발견.
해킹 공격에 대한 제약사항이 적었기 때문

발견취약점 **84**



유효취약점 **57**



중요취약점 **14**



시스템 장악

서비스 마비

결재금액 조작

개인정보 유출

⋮

* 2020년 해킹존 베타 버그바운티 결과 (KISA 취약점 평가)



해킹존 진행상황 및 현황



해킹존 진행상황

10여개 기업 제품 및 서비스
버그바운티 진행,

400여개의 유효한
취약점 리포트 접수

버그바운티 플랫폼 오픈

- 2020. 2Q** 비공개 버그바운티 진행 (10개 기업 제품 및 서비스 대상) - 총 84건 취약점 리포트 접수
- 2020. 4Q** KISA 주관 Hack the Challenge 버그바운티 진행 - 총 259건 취약점 리포트 접수
- 2021. 1Q** 신고포상제 공동운영사 협약 후 상시 버그바운티 진행 - 총 110건 취약점 리포트 접수
- 2021. 2Q** 해킹존 시범서비스 오픈 (예정)
- 2021. 3Q** 해킹존 정식서비스 오픈 (예정)

버그바운티 경험 인터뷰

(참여한 기업, 해커, KISA)



hacking zone

참여기업 인터뷰 주목할만한 점



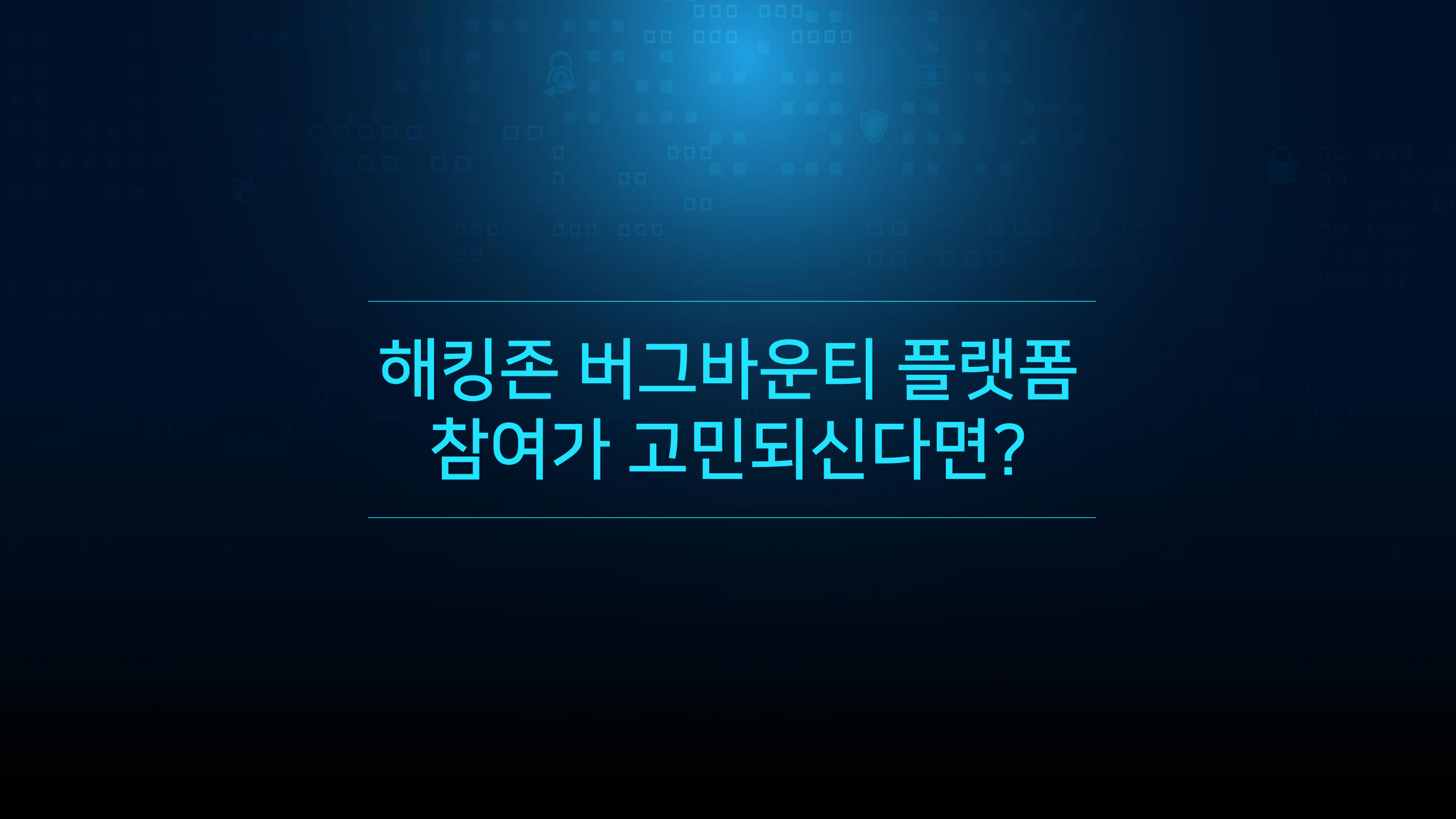
버그바운티에 대한 인식변화

1회성으로 참여하기로 했던 기업이 지속적으로 참여하기로 검토, 진행중



보안 고도화의 필요성 인식

자사에 적합한 보안 컨설팅, 서비스, 솔루션에 대한 정보 요청.
지속적인 보안 강화 필요성 또한 인식



해킹존 버그바운티 플랫폼
참여가 고민되신다면?



아래에 해당된다면, 해킹존 버그바운티 플랫폼에 참여하세요!

- 1 내부 보안점검만 하는 기업
- 2 비용절감과 보안강화가 동시에 필요한 기업
- 3 체계적인 취약점 관리가 필요한 기업
- 4 자사의 제품에 애정과 책임감이 있는 임직원
- 5 운영시스템에 영향이 없고 신원인증된 해커가 참여하여 중요취약점이 제보되는 버그바운티 운영이 필요한 기업



Thank you