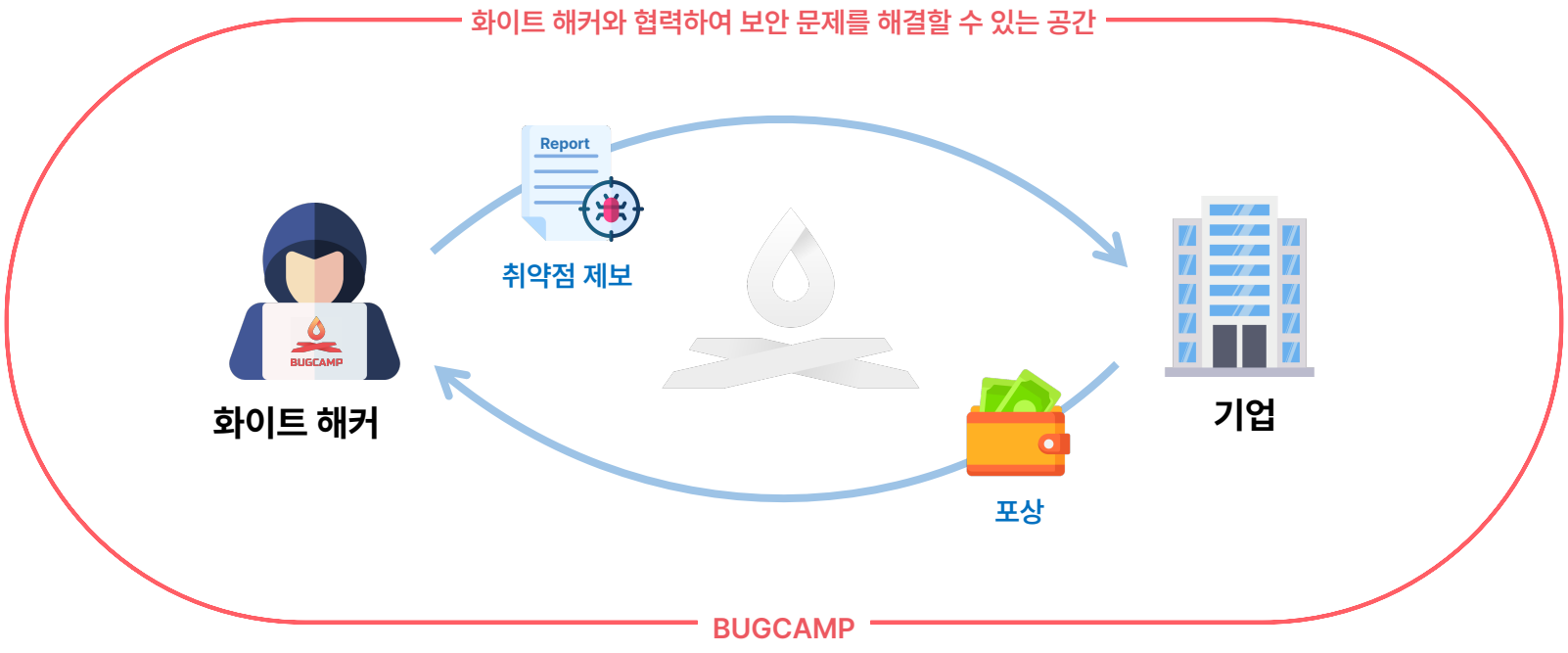
BUGCAMP

Service Information

버그바운티 플랫폼, 버그캠프

버그캠프는 해킹 기술을 이롭게 활용하는 화이트 해커와 기업이 협력하여 보안 문제를 해결하는 플랫폼입니다. 보안 취약점이라는 작은 빈틈은 우리 기업에 경제적 손실을 주는 보안 사고로 번질 수 있으므로 보안 취약점 관리는 필수적이며, 보안 취약점을 제거하는 노력을 통해 기업은 잠재적 보안 사고를 제거할 수 있습니다.

버그바운티는 보안 취약점에 현상금을 걸어 화이트 해커들의 적극적인 참여를 유발해 오랜 기간 동안 기업의 작은 빈틈까지 발견할 수 있는 효과적인 정보 보안 방법입니다.



버그바운티 특징

기업들은 사이버 공격에 사전 대응하기 위해 보안 장비/솔루션 도입, 모의해킹, 보안 교육 등 많은 보안 방법이 있습니다. 특히 구글, 마이크로소프트, 애플, 삼성 등 기업 보안 역량 강화를 위해 오랜 시간과 많은 비용을 투자한 기업은 자사 보안 체계의 안전성을 지속적이고 장기적으로 관리하기 위해 버그바운티라는 보안 방법을 선택했고, 화이트 해커와 협력하여 효과적으로 보안성을 향상시키고 있습니다.

집단 지성

다수의 화이트 해커들이 **각자 다른 기술과 경험을 활용하여 다양한 관점의 취약점을 발견**할 수 있습니다. 또한, 외부에 공개된 서비스를 대상으로 블랙 박스 형태의 취약점 발굴에 탁월합니다.

비용 절감

취약점 진단 인력의 시간, 기술료 등을 포함하는 모의해킹과 달리 버그바운티는 **발견된 취약점에 대해서만 비용을 지불하면 되므로 비용이 절감되는 효과**가 있습니다. 또한, 기업의 보안 예산과 취약점의 심각도, 개수 등에 따라 유동적으로 비용을 책정할 수 있습니다.

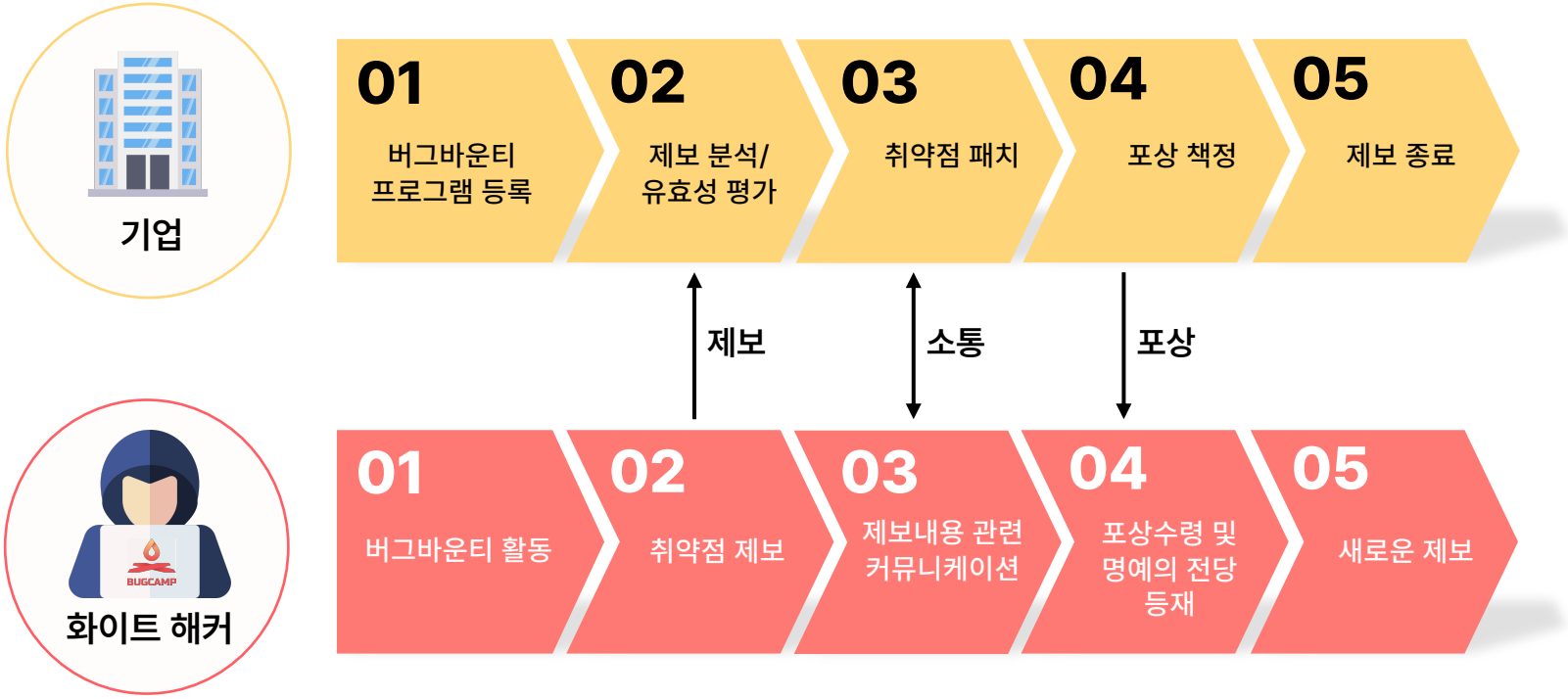
지속성

기간 제한 없이 반복하여 지속적으로 보안 테스트를 진행할 수 있습니다. 발견된 취약점만 포상하므로 장기간 동안 운영하여 보안 관리를 진행할 수 있습니다.

BUGCAMP

버그바운티 프로세스

버그캠프는 버그바운티 프로그램에 필요한 환경을 제공하고 중개하는 버그바운티 플랫폼으로, 버그바운티 프로그램 운영부터 포상까지 관리를 대행하는 서비스를 제공합니다. 버그캠프안에서 기업과 화이트 해커는 5단계에 따라 버그바운티를 진행하고 있습니다.



BUGCAMP

효과적인 버그바운티 운영 공간

버그캠프는 420명 이상의 화이트 해커와 함께하고 있으며, 각기 다른 경험과 기술을 통해 유의미한 취약점 제보 활동이 이루어지고 있습니다. 버그캠프의 화이트 해커와 협력하여 기업의 보안 문제를 효과적으로 해결할 수 있습니다.

https://bugcamp.io

화이트 해커

420명+

취약점 제보율

100%

첫 취약점 제보

28h

총 취약점 제보

250건+

BUGCAMP

편리한 버그바운티 운영

담당자가 직접 처리하던 업무들을 버그캠프에 구현된 기능을 활용하여 높은 비용 없이 효율적인 버그바운티 프로그램 운영이 가능합니다.

1 편리한 운영

프로그램 등록

간편하게 버그바운티 프로그램 오픈을 시작으로 **필요시 즉각적인 정책 수정**과 해커들에게 공유

매니저 초대

프로그램을 **같이 운영할 내부 직원을 초대**하여 업무를 실시간으로 분담, 공유, 확인할 수 있으며 무제한 초대 가능

매니지드 서비스

취약점에 이해가 높은 화이트 해커가 직접 프로그램 운영, 티켓 평가, 소통, 보상 금액 책정 등 **모든 일을 대행하고 가공된 결과보고서 제공**

2 실시간 소통

알림

취약점 제보, 코멘트, 평가 내역 등 모든 업데이트를 알림 및 이메일을 통해 매니저와 화이트 해커에게 알려 **실시간 대응 가능**

취약점 평가

취약점 제보와 관련해 **유연한 평가, 보상 책정**이 가능하며 평가 내역을 실시간으로 화이트 해커가 조회할 수 있어 불만 해소

코멘트 소통

취약점 제보 내용을 펼쳐 놓고 소통하여 관련한 내용의 **보충 설명, 문의 대응**이 가능하며 알림 기능을 통해 빠른 대응 가능

3 간편해진 포상

포상금 지급 대행

반복적이고 불편한 서류 처리 없이 **클릭 한 번으로** 화이트 해커에게 포상금 송금부터 세금 처리까지

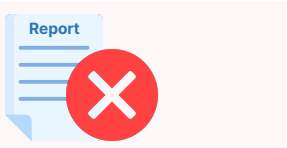
명예의 전당 등재

복잡한 과정 없이 **클릭 한 번으로** 우리 프로그램의 전용 명예의 전당에 우수한 화이트 해커 등재

Q&A

여러분의 걱정과 궁금증을 해결해 드립니다.

1



프로그램을 오픈했지만, 해커가 관심이 없거나 취약점 제보가 없으면 어떻게 하죠?

화이트 해커들이 버그를 제보하는 목적 중 1위는 포상입니다. 금전 이득을 위해 **화이트 해커는 등록된 자산을 끊임없이 테스트하고 취약점 발굴을 시도**합니다. 버그바운티 프로그램을 통해 보안 체계 유효성을 평가할 수 있으며, 공격자 관점의 취약점 점검 효과를 얻을 수 있습니다.

2

취약점이 너무 많이 제보되면 어떻게 하죠?

취약점이 많이 나온다는건 **보안 사고로 이어질 수 있는 위협을 그만큼 제거했다는 의미**입니다. 한 가지 테스트 대상에 대해서 대개는 포물선 형태로 취약점이 제보됩니다. 이벤트처럼 기간을 정해 운영하여 컨트롤할 수 있으니 크게 걱정하지 않으셔도 됩니다.

3

버그바운티를 진행함으로써 실제 서비스 가용성에 문제는 없을까요?

실제로 사이버 위협 그룹은 외부에 공개된 상용 서비스를 대상으로 공격합니다. 버그바운티를 통해 **침해 사고 대응 훈련/서비스 복원력 평가가 가능하며 실제 위협 그룹이 악용할 수 있는 보안 취약점을 제거**할 수 있습니다. 그럼에도 가용성 저해가 걱정되거나 저장된 데이터가 민감하여 고민이 되는 경우, 버그바운티를 위한 별도의 서버를 분리하고 임의의 데이터를 저장하여 진행할 수 있습니다.

4

버그캠프를 통해서 어떤 효과를 볼 수 있을까요?

체계적인 프로그램 운영, 많은 화이트 해커들의 참여를 위해서는 높은 비용과 화이트 해커 네트워크를 필요로 합니다. **모든 것이 갖춰진 버그캠프에서는 낮은 비용으로 체계적인 버그바운티 프로그램을 바로 시작하고 취약점 제보를 받을 수 있습니다.** 또한 **화이트 해커에게 프로그램 관리를 위임할 수 있어 내부에 보안팀이 없더라도 보안 관리가 가능합니다.**

https://bugcamp.io

버그캠프와 함께 숨겨진 보안 문제를 찾고 해결해 보세요. 우리는 당신의 보안 팀처럼 모든 과정에 함께합니다.

Tel. 031-722-1337
URL. www.bugcamp.io
E-mail. contact@bugcamp.io