



CODE VECTOR

건강한 사이버 공간을 추구하는 세상





Welcome

우리는 고객의 **고민**을 함께 생각하고 함께 성장합니다.

안전한 사이버 공간을 만들고 있는 CodeVector를 소개 드립니다.

AGLIE

OUR CULTURE

빠른 의사 결정과 실행

코드백터는 완벽하진 않지만
애자일 문화를 가지고 있습니다.

우리는 완벽보단 완성에 집중하고
내부적으로 끊임 없이 실험하며
데이터를 반영하고 있습니다.



VISION

OUR CULTURE

깨끗한 인터넷 환경을 만드는 것

IT를 접하는 모든 사람들에게 편리하고,
안전하고, 깨끗하고, 신뢰 할 수 있는
공간으로 만드는 것 입니다.



우.리.는

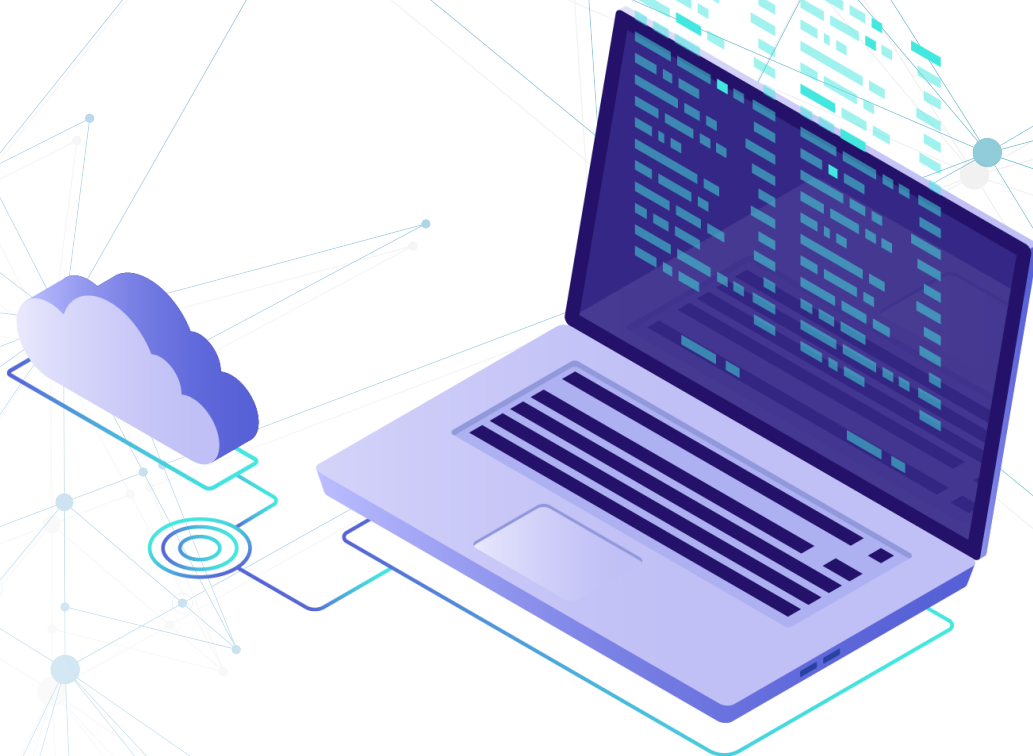
이런 문제점을 해결하고 있습니다.

우리는 클라이언트가 고민하고 있는 사이버 보안
이슈들을 끊임없이 해결하기 위해 연구하고 있습니다.

다양한 보안 기술 개발, 그리고 클라이언트 중심에
중/장기 서비스를 통해 차별화된 서비스 가치를
창출해 나가고 있습니다.

IT공간 안에서
잡못된 코드(CODE)

올바르게
바로 잡는 것(VECTOR)



빠른 속도와 집중력



완벽보단 완성



무한 확장성



데이터에 대한 신뢰

빠른 속도와 집중력

Our Value1

코드백터는 한 가지에 업무를 두고 장시간 또는 장기간 붙잡고 있는 것을 좋아하지 않습니다.

개인이 맡은 업무에 있어서 짧은 순간에 집중력을 발휘하고 빠른 속도로 업무를 진행하는 것을 선호합니다.



1

2

완벽보단 완성

Our Value2

모든 일에는 완벽 할 수 없다는 전제를 두고 완성에 더 집중하여 부족한 점에 대한 빠른 피드백으로, 코드백터는 완벽에 가깝도록 일하는 방식을 채택하고 있습니다.





데이터에 대한 신뢰

Our Value3

전자 기계에서 발생 되는 데이터는 인간이 생각하는 데이터보다 정확하다고 판단하고 있습니다.

우리는 개인 또는 조직의 의견보다 우리가 쌓아 온 데이터에 더 많은 신뢰를 가지고 있습니다.



무한 확장성

Our Value4

코드백터는 정보보안 분야 뿐만 아니라 다양한 IT분야를 연구하고 있습니다.

인간의 인생에 접목 할 수 있는 IT기술 이라면 무엇이든지 연구하고 실행하는 습관을 가지고 있습니다.



4



Company Overview

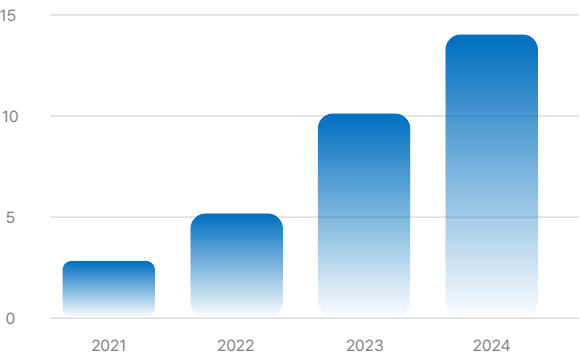


Finance

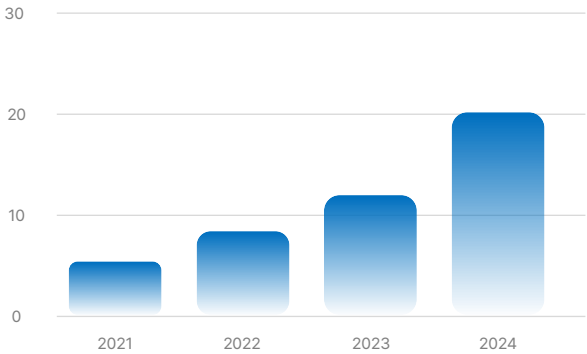
2024년 매출액 17% 상승

전년 동기 대비 매출 상승 | 프로젝트 가동률 평균 92% | 연가매출 추이 지속 상승

단위 : 억원



단위 : 명



HR+

전년 대비 인재인력 2배 증가

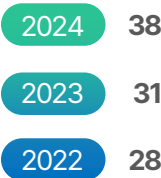
연간 임직원 채용률 15% 지속 상승 | IT 연구 전담 부서 지속 채용 | BugBouny 전담 전문 인력 가동

BUSINESS PROJECT

연간 신규 프로젝트 25% 이상 확대

미주 실리콘 벨리 사업 진출 | 연간 신규 고객사 창출 | 사업 다각화 신규 프로젝트 수주

프로젝트 (수주)



2019 스타트업 코드벡터 시작

코드벡터는 2019년 IT보안 환경을 정화시키고자 전문가들과 모여 회사를 설립하게 되었습니다.

History



2020

- 국내 대기업 및 정보보안 업체 협력사 등록
- +10개의 정보보안 사업 수주 및 참여
- 사이버대학 산학 협력 계약



2021

- 사업 초기 대비 연간 매출 3배 이상 증가
- 연구 전담 부서 설립
- +25개의 정보보안 사업 수주
- B2C 사업 플랫폼 개발 착수
- 벤처기업 인증 및 협회등록



2022

- 세종 사이버대학 산업체 위탁 협약
- 한국 무역협회 회원 등록 및 수축 인증
- TCB우수기술기업 인증
- 10개 이상의 버그바운티 제보



2023

- 성과 공유제 기업 인증
- B2C 플랫폼 개발
- 경기도 유망 중소기업 선정(경기도지사 표창)
- 10개 이상의 버그바운티 제보



2024

- 벤처기업인증 연장 심사 통과
- 2024 경기 우수 벤처기업 경기지방 중소기업청장 표창
- 2024 경기 벤처기업 협회 우수 근로자 표창
- 사이버보안 모의해킹 컨설팅 용역수출 10만불 달성
- 10개 이상의 버그바운티 제보



2026

- 메인비즈 인증 / 이노비즈 인증
- 일&생활 균형 캠페인 참여(고용노동부)
- 사이버 보안 모의해킹 컨설팅 용역 수출 15만불 달성
- 사이버 보안 관련 AI솔루션 Core 개발 완료
- 과기부 [혁신 프리미어 1000] 기업 선정

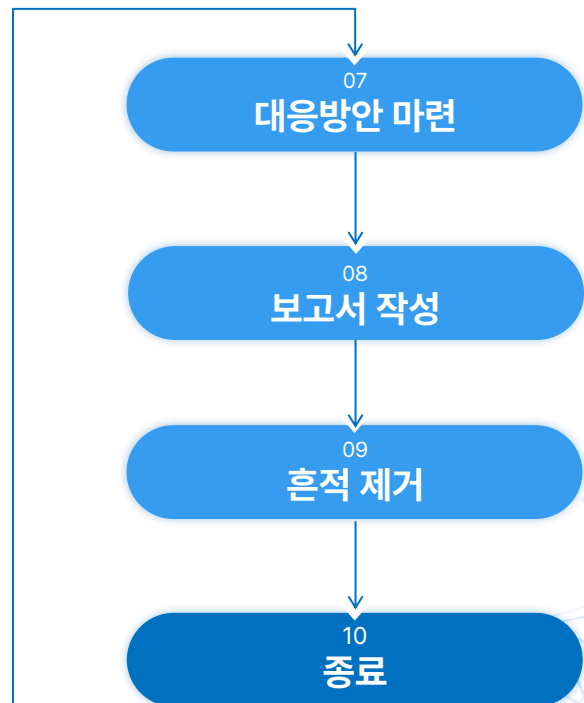
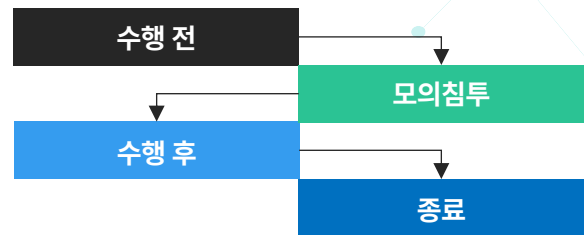
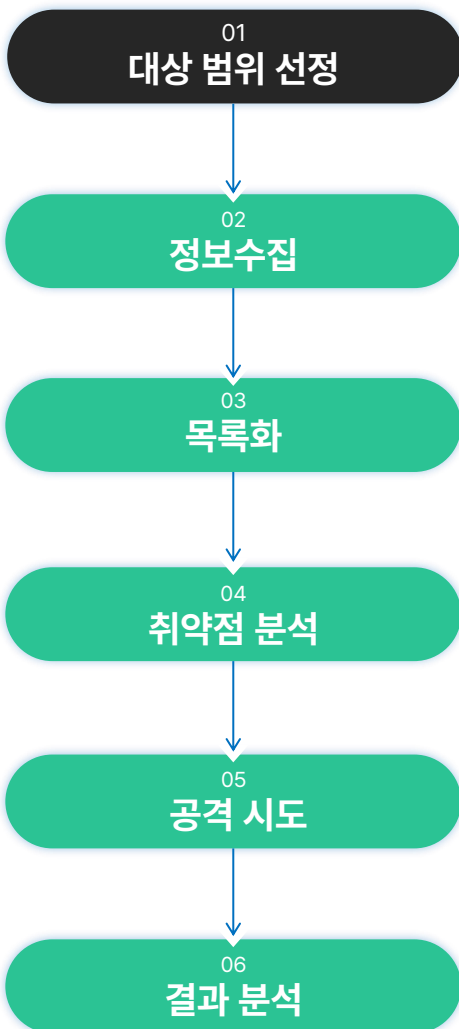
Service

고객의 미래가 곧 코드벡터의 미래다.

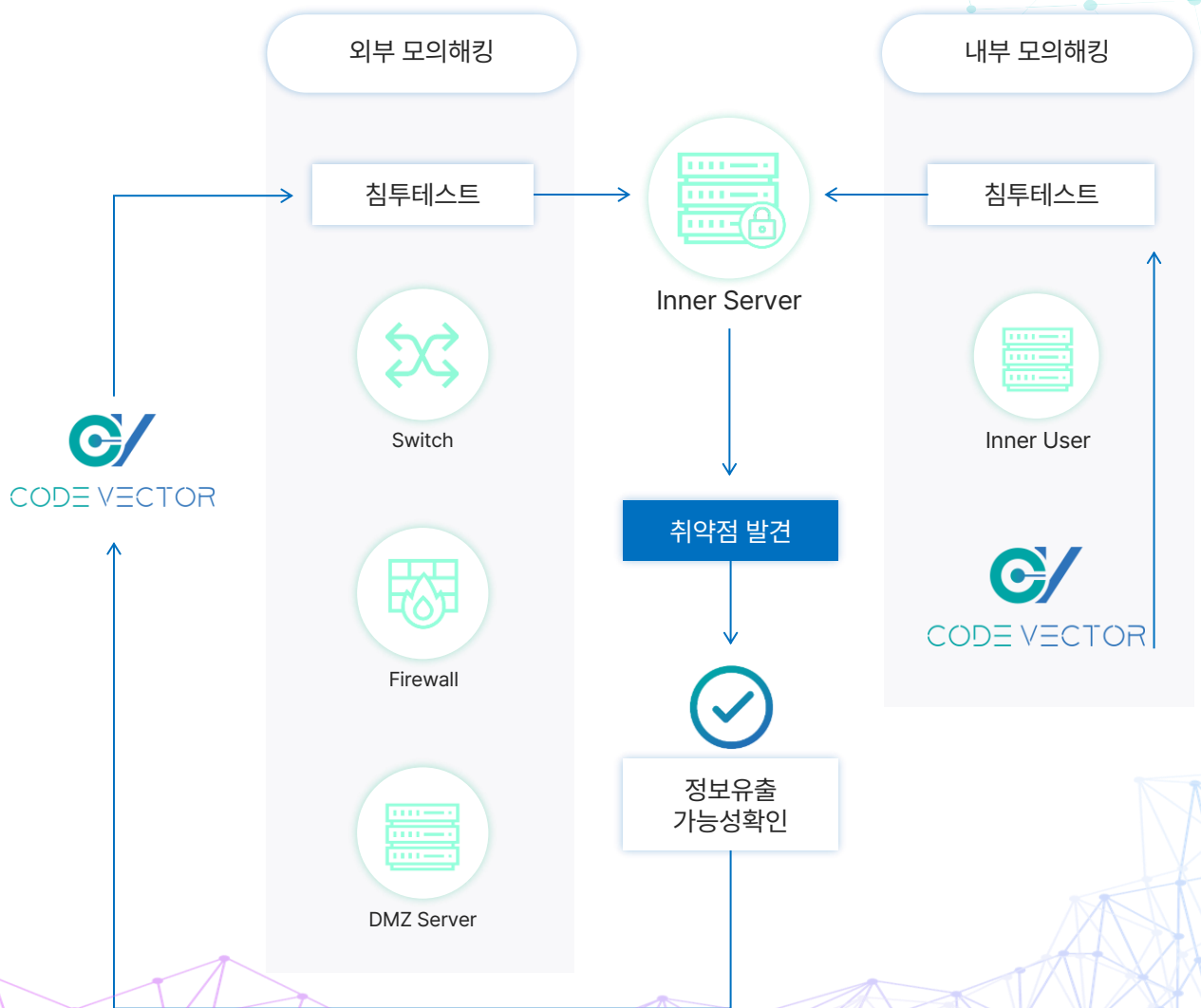
코드벡터에서 제공하고 있는 서비스입니다.



체계적이고 객관적인 모의해킹을 위하여 모의침투테스트 방법론에 따라 9단계의 절차로 수행



고객사의 보안담당자와 사전협의 후 코드벡터의 모의해킹 전담 컨설턴트에 의해 수행
정보시스템 외부에서 해커를 가장하여 침투테스트를 수행, 내부의 악의적인 사용자를 가장한
정보유출 및 시스템 파괴 등의 시나리오를 이용하여 점검 실시



Blind Penetration Testing

외부 공격자의 관점에서 DMZ 공간에 노출 되어있는 서비스 및 인프라 자산에 대한 보안성을 검증하는 서비스입니다.

외부 DMZ 영역에 노출 되어있는 웹 서비스 및 모바일 서비스 자산에 대한 취약성 검증 테스트

DMZ 공간에 노출 되어있는 중요 서비스에 대하여 공격을 수행합니다.

공격자는 별도의 제공되는 정보 없이, 외부에서 획득 가능한 정보를 수집하고, 수집된 정보를 통하여 공격을 진행합니다.

서비스에 장애가 발생되지 않는 범위 내에서 서비스 가용성에 대한 영향도를 파악하고, 수행자는 공격을 진행합니다.

악의적인 외부의 공격자로 인하여 발생될 수 있는 고객사의 위험을 미리 예방하고, 방어 할 수 있는 가이드를 제시합니다.

Alliance Penetration Testing

장기적인 관점에서 고객사 자산을 보안 검수하고 정기적인 취약점 및 보안 관리를 진행하는 서비스입니다.

중/장기 계약을 진행하고 고객의 웹 서비스 및 인프라 자산에 대한 취약성 분석

고객의 전체 서비스에 대하여 장기적인 관점으로 비즈니스를 분석하여 우선순위를 정하고 보안 진단을 수행합니다.

고객 서비스에 대한 정기 진단 정보가 쌓일 수록, CODEVECTOR는 고객의 서비스 이해도가 높아질 것이며, 최초 서비스 이후 기능 업데이트 내역에 대하여 추가 취약점을 발견하기 유리해집니다.

또한 새로운 CVE 취약점이 존재할 수 있는 서비스의 공통 모듈에 대하여 긴급테마진단을 실시하고, 정기 진단 사이에 취약점이 방치될 수 있는 '진단 공백'이 최소화 되도록 진단을 수행하는 것이 가능합니다.

장기적인 관점에서 고객과 서비스를 함께 제공한다는 파트너십을 가지고,

고객이 제공하는 서비스의 충분한 이해와 서비스 코드에 대한 향상된 이해를 바탕으로 된 취약점 진단은 고객의 상황에 최적화 될 것이며, 발견된 취약점에 대하여 고객과의 충분한 협의를 거쳐 비즈니스에 미치는 영향도가 최소화 되도록, 그리고 서비스의 보안성이 최대한 향상될 수 있는 최적의 대응책이 제공됩니다.

Mobile Penetration Testing

모바일 환경에서 다양한 형태로 나타날 수 있는 위협으로부터
사용자를 보호하는 서비스입니다.

대국민 모바일 서비스 및 내부 임직원 업무용 모바일 서비스에 대한 취약점 진단

모바일 보안 진단은 모바일 환경에서 다양한 형태로 나타날 수 있는 위협으로부터 사용자를 보호하는 서비스입니다.

대국민 고객 서비스로 제공되는 모바일 앱이 악의적인 사용자에게 의하여 분석이 어렵도록, 그리고 분석이 되더라도 변조하여 악의적으로 이용 하는 것이 어렵도록, 마지막으로 악용될 리스크를 사전에 정의하여 빠르게 조치 될 수 있도록 악용 가능성에 대한 시나리오를 제공 합니다.

내부 임직원이 사용 가능한 모바일 앱에 대한 허가되지 않은 앱 사용을 통하여 발생가능한 위협, 변조된 악성 앱을 통하여 발생 가능한 다양한 시나리오 등 예측하고 여러 관점에서의 모바일 진단 테스트를 수행하는 것이 가능합니다.

테스트를 통하여 확인된 위험 내역은 코드백터 모바일 보안 취약점 가이드를 통하여 고객의 상황에 최적화된 해결 방안을 제시하며 안정된 서비스를 제공 합니다.

IOT Penetration Testing

IoT제품군 또는 제조 서비스의 다양한 형태로 발생 가능한 위험에 대하여 사전 진단을 수행하는 서비스입니다.

IoT 제품 보안성 검토 및 제조 서비스에 대한 취약성 분석

홈 IoT 서비스, 헬스케어 IoT 장비, 스마트 IoT 모빌리티 시스템, 스마트팜 IoT 장비, 제조 설비 등 IoT가 접목된 다양한 산업 제품군에 대한 진단 서비스입니다.

각 제품군에 맞추어 발생 가능한 취약점을 발견하고 IoT 장비가 적용된 네트워크 환경과 장비 내부 보안 로직 분석, 장비에 입력되는 데이터의 무결성 및 변조테스트 등의 다각적인 분석을 통하여 IoT 장비 보안성을 테스트 하고 있으며, 이를 통하여 발생 가능한 공격 시나리오가 제공되는 서비스입니다.

CodeVector에서는 자체 진단 체크리스트 및 기술을 활용하여 고객의 제품 또는 요구사항에 맞추어 최고의 수준진단을 제공하고 있습니다.

Firmware Penetration Testing

IoT 장비에 적용되는 Firmware에 존재하는 취약점을 진단하여
위험을 사전 예방하는 서비스입니다.

펌웨어 내부 코드에 대한 역분석 및 취약점 진단

제조 공정 시스템, 스마트 단말기 등 전방위 산업에서
활용되고 있는 C/S를 대상으로 펌웨어 모의해킹 서비스를
제공하고 있습니다.

해당 펌웨어에서 제공되는 기능에 대한 리스트업 부터
진행되며, 각 기능별 바이너리에 대한 리버싱 작업을 통하여
취약점을 도출하고 연관 시스템에 대한 위협요소를 확인 및
예방하는 서비스 입니다.

단순히 IoT 기기 취약점이 아닌 펌웨어가 적용된 시스템군에
대한 영향도 평가를 통하여 네트워크 환경과 시스템 적인
가이드를 제공하는 것이 가능합니다.

RedTeam Penetration Testing

프로젝트 목표를 위하여 실전과 동일한 공격을 수행하는
최고수준의 공격 서비스입니다.

제한없는 차별화된 공격 서비스

CodeVector에서 운영중인 레드팀팀은 일반적인 취약점 진단 또는 시나리오 기반의 취약점 진단과는 다른 한 단계 더 강도 높은 취약점 진단을 진행하게 됩니다.

프로젝트 목표(고객정보, 계약정보, 회사기밀, 설계공정 도면, 비공개 특허정보 등)를 탈취하기 위하여 고객사의 전 방위적인 인프라 및 내부침투 시나리오를 프로젝트 진행 중 작성 및 테스트하며, 이는 단순한 웹, 모바일 서비스 뿐 아니라 서비스 운영에 필요한 서드파티 장비 및 어플리케이션에 대한 공격 등, 모든 가능성을 염두에 둔 공격이 진행됩니다.

따라서, 여러 이유에 의하여 발생한 취약점에 대한 즉각적인 가이드가 어려운 경우가 발생할 수 있으나, 도출된 시나리오에 따른 리스크를 최소화 할 수 있는 고객사의 현황에 맞는 단계별 가이드 제공을 통하여, 고객의 안정적인, 안전한, 그리고 지속가능한 서비스가 될 수 있도록 하는 최선의 공격 서비스입니다.

Reference



코드벡터는 50개 이상의 기업과 함께하였으며, 앞으로 더 많은
고객과 함께 고민하고 해결해 나갈 것 입니다.

 **KCP**

 Hanwha Systems

 **신한생명**

 **SK hynix**

 **SK shieldus America**

 **MG 새마을금고**

 **toss payments**

 **SAMSUNG**
삼성전자

 **DAESANG**
대상주식회사



코드벡터는 다양한 기술력으로
경쟁력 있는 높은 서비스를
제공해 드릴 것을 약속 합니다.

<http://codevector.kr/>

<https://techlabcv.oopy.io/>

<https://www.youtube.com/@codevector./>

031)286-5949

biz@codevector.kr

경기도 용인시 기흥구 기흥로58 기흥ICT벨리 SK V1 B동 405호(16976)