ENKI

회사 소개서

CONTENTS

01 회사 소개

- 일반현황
- 사업 수행 실적
- 엔키의 강점

02 서비스 소개

- 화이트햇 컨설팅
- 사이버 위협 대응
- 사이버 훈련 및 교육
- 버그캠프
- VATE, 사이버 훈련장

01 회사 소개

일반현황

사업 수행 실적

엔키의 강점

ENKI

01 일반 현황

엔키는 업력 7년차 보안 전문 기업으로 **침투테스트 컨설팅, 악성코드 분석, 보안기술 연구**를 주로 수행하고 있습니다.
엔키는 **해커의 관점**으로 보안 문제를 해결하는 전문가 조직으로 수행인력 모두가 **뛰어난 기술력을 보유**하고 있습니다.

1 일반 현황

회 사 명	주식회사 엔키
대 표 자	이 성 권
소 재 지	경기도 성님시 수정구 고등로 3, 현대지식산업센터 412호
전화/팩스	031-722-1337 / 031-722-1338
설 립 일	2016년 09월 09일
사업분야	• 화이트햇 컨설팅(침투테스트) • 악성코드 분석 및 사이버 위협 인텔리전스 • 사이버 공격 방어 대회 운영 및 문제 출제 • 사이버 기술 교육 및 실습 • 버그바운티 플랫폼 서비스 운영 (버그캠프)

2 조직 현황

임원진	연구소	보안 사업부	서비스 사업부	솔루션 사업부	경영 기획부	총 인원
5	1	19	7	1	4	37

02 사업 수행 실적

엔키는 공공기관, 금융사, 대형병원, 대기업 등 **다양한 업종의 기업 기관에 보안 컨설팅 서비스를 제공**하여 고객사의 서비스 및 플랫폼에 대한 **잠재적 보안 위협에 선제 대응**할 수 있도록 지원 하였습니다.

금융기관 | 공공기관 | 대기업 | 병원 | OTT플랫폼

kakaobank, 키움저축은행, 한전KDN, NC WINDOW TO THE FUTURE, SAMSUNG 삼성전자, 서울아산병원 Asan Medical Center, CJ ENM, WATCHA

신한은행, 키움YES저축은행, KORES, LS, 대우건설, 건국대학교병원 KONKUK UNIVERSITY MEDICAL CENTER, SBS 아이앤엠, TVING

키움증권, KAI 한국항공우주산업㈜, (주)정우비나, KIA Movement that inspires, HYUNDAI, Cigna 라이나생명 다이렉트, Volkswagen Financial Services, 우아한형제들

ENKI

03 엔키의 강점

엔키는 다양한 서비스, 환경을 대상으로 침투테스트 수행 결과 **위험도 높은 취약점 발견 100% 실적을 보유**하고 있습니다.

1 침투테스트 성과 이력

취약점 발견 및 악성 행위 증명 100%

자료유출

- 고객 개인정보, 내부 문건 등 **중요정보 유출 성공**
- 임의 명령 실행으로 중요 정보 **외부 유출 성공**
- 관리자 권한 획득 후 고객 **개인정보 유출 성공**
- 보안솔루션 우회하여 **자료 유출 성공**
- SSH 터널링으로 **외부 인터넷으로 자료 유출 성공**

서버장악 및 권한 획득

- 원격지에서 **서버 최상위 권한 획득 성공**
- 미사용 포트, 취약 버전의 서비스 취약점 식별 및 공격을 통한 **서버 장악 성공**
- 서비스 취약점 식별 및 공격을 통한 **내부 서버 접근 성공**

악성행위

- **전자화폐(포인트) 복제, 부정결제 성공**
- **악성 앱 제작 및 유포가능성 증명**
- 취약점 공격(XSS, Info Leak)으로 **상위 권한 획득 성공**
- 외주직원/임직원 사용 단말 **보안솔루션 우회 성공**

ENKI

03 엔키의 강점

엔키의 기술인력은 해킹방어대회 수상 경력 및 운영 경험을 보유하고 있으며, 국내·외 유수 벤더의 신규 취약점을 제보한 **화이트 해커들을 다수 보유하고 있습니다.**

2 글로벌 수준의 전문가 그룹

"최신 보안 기술과 높은 전문성을 갖춘 화이트해커 다수 보유"

취약점 제보 102건

2021 Apple LPE 취약점 1건
2021 Parallels LPE 취약점 1건
2021 NAVER CAFE XSS 1건
2021 Parallels Desktop VM 이스케이프 취약점 1건
2021 Pwn2Own Austin CISCO 라우터 RCE 취약점 및 WD NAS RCE 취약점
2021 KISA 취약점 제보 30건
2020 국내・외 IP Camera, Router 취약점 9건
2020 Parallels Desktop 권한상승 및 VM 이스케이프 취약점 8개
2020 Samsung Email XSS 취약점 1건
2019 NAVER RCE, SESSION STEAL with SSRF
2019 NAVER Path Traversal
2019 Riot Games XSS 2건

대회 수상 19건

2023 DEFCON 31 Final Round 진출
2022 Digital Forensics Challenge 3위
2022 DEFCON 30 Final Round 3위
2021 DEFCON 29 Final Round 진출
2021 Pwn2Own 2021 winner(Paralles Desktop)
2021 Real word CTF 1위
2020 DEFCON 28 CTF Final Round 진출
2020 Tencent CTF Quals 1위 (중국)
2019 CODEGATE 국제해킹방어대회 Final Round
2019 PCTF 국제해킹대회 3위 (미국)
2019 DEFCON 27 CTF Final Round 진출 (예선 국내 1위, 세계 3위)
2018 RCTF online 1위
2018 0ctf/Tctf 본선 2위 (중국)
2018 CODEBLUE CTF 1위

대회 운영 19건

2023 사이버 공격 방어대회(CCE) 운영
2023 금융보안원 FIESTA 운영
2023 CODEGATE 국제해킹방어대회 운영
2022 IITP 사이버 보안 챌린지 운영
2022 사이버 공격 방어대회(CCE) 운영
2022 금융보안원 FIESTA 운영
2022 CODEGATE 국제해킹방어대회 운영
2021 사이버 공격 방어대회(CCE) 운영
2021 금융보안원 FIESTA 운영
2020 사이버공격방어대회(CCE) 운영
2020 금융보안원 FIESTA 운영
2020 시큐인사이드 문제 출제
2019 사이버공격방어대회(CCE) 운영
2019 CODEGATE 국제해킹방어대회 문제 출제
2019 LINE-Codeblue CTF 문제 출제 및 운영
2019 Christmas CTF 문제 출제
2018 CODEGATE 국제해킹방어대회 문제 출제

02 서비스 소개

화이트햇 컨설팅

사이버 위협 대응

사이버 훈련 및 교육

버그캠프

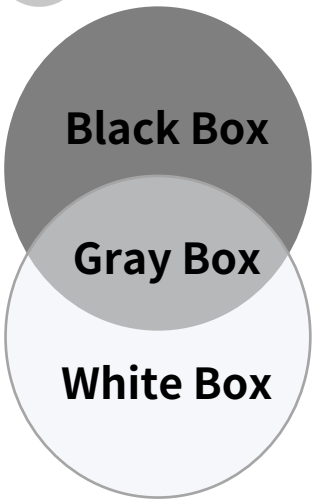
VATE, 사이버 훈련장

ENKI

01 화이트햇 컨설팅

공격자의 관점으로 실제 기업에게 경제 피해, 정보 유출, 서비스 장애 등으로 이어질 수 있는 보안문제를 미리 찾아 해결하는 서비스로, **높은 기술력을 보유한 화이트 해커**가 수행합니다.

1 화이트햇 컨설팅 개요



고객의 내부의 네트워크/보안 설계를 전혀 모르는 **외부 공격자의 관점**으로 외부 서비스를 취약점 점검 하고 내부 침투, 악용 가능성 등을 점검 합니다.

고객의 임직원, 외주 인력 등 낮은 권한의 계정 및 내부 환경 정보를 입수하여 **악의적인 내부 임직원 관점**으로 공격 가능성과 잠재적 위협을 점검합니다.

네트워크/프로그램 설계도 및 소스코드 등을 입수하여 **공격자의 관점**으로 전문 화이트 해커가 직접 정적·동적 취약점 진단을 수행합니다.

취약점 발견 100% 실적 보유

공공/금융/대기업 등을 대상으로 웹,앱 애플리케이션 (iOS/Android), 소스코드 취약점 진단, APT 공격 등 **다양한 화이트햇 컨설팅 수행 경험多**

2 화이트햇 컨설팅 프로세스

수행준비	침투 수행	위협 증명	보안대책 제시
• 진단 범위 및 일정 협의 • 분석 환경 구축 • 점검 방안 상세화	• 정보 수집 • 기능 및 공격 백터 식별 • 공격 시나리오 설계 • 취약점 분석	• 내부 침투 시도 • 공격 증명 • 악의적인 행위 증명	• 취약점 별 개선방안 제시 • 이행 점검 지원

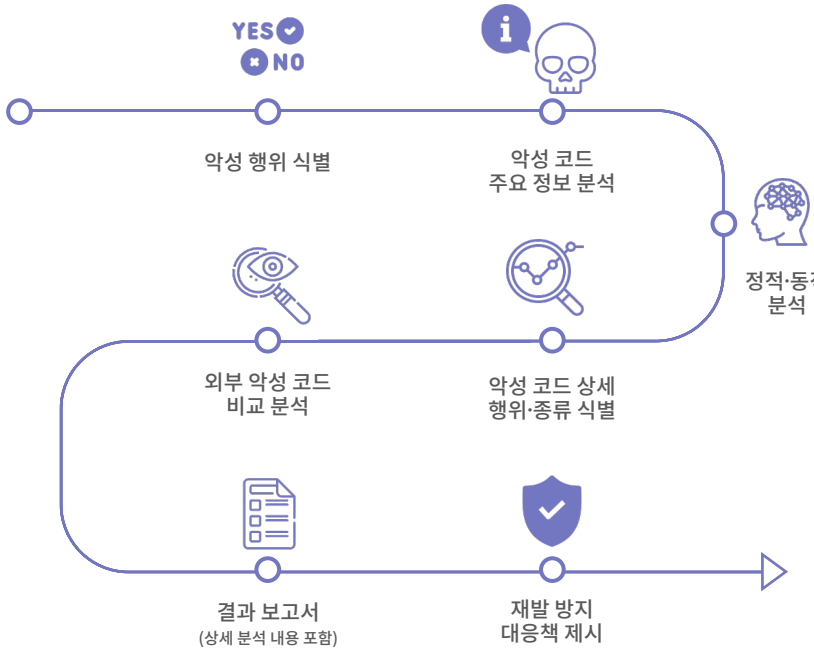
ENKI

02 사이버 위협 대응

약 6년간 북한, 중국, 러시아 등 2만여 건 이상의 악성코드를 분석하며 쌓은 경험과 기술을 활용한 **위협 인텔리전스를** 제공합니다.
악성 파일의 상세 분석 정보, 탐지 룰, 연관 위협 정보, 기술 등을 **전문 분석가가 직접** 분석하여 정제된 상세 보고서를 제공합니다.

1 악성코드 분석

프로세스



탐지된 악성 행위를 정적·동적 분석하여 정밀 분석 정보가 포함된 결과 보고서를 제시하고, 악성코드 탐지 대응을 위해 Rule을 직접 제작하여 대응 방안을 제시합니다.

산출물

02 사이버 위협 대응

침해 사고 발생시 위협을 완전히 제거하기 위해 **기업의 특성에 맞춰 조사하고 근본적인 위험을 제거**합니다.
분석 전문가가 직접 감염 의심 대상을 분석하여 내부에 침투한 공격자의 행위, 피해 범위, 침투 경로 등을 조사 후에 대응방안을 제시합니다.

2 침해흔적 조사




의심 대상 정보 수집	사고 범위 조사	침투 경로 분석	대응 방안 제시
진단 범위 및 일정 협의	의심 데이터 분석	탈취 정보 및 피해 범위 산정	취약점 패치 신속 지원
침해 의심 대상 정보 수집	악성파일 채증	유출 경로 및 시간 분석	탐지 Rule 제작 및 제공
맞춤형 정보 수집 도구 제작	로그 분석 및 범위 파악	침투 경로 정적 • 동적 분석	조사 결과 상세 보고
진단 결과 기반 수동 점검	난독화 해제 및 악성코드 분석		

악성코드 분석 상세 제공

ENKI

03 사이버 훈련 및 교육

국내 1위 기업의 노하우로 사이버 해킹방어대회에서 참가자들이 참여중에 **유의미한 기술을 얻어가는 문제 출제, 성공적인 대회 운영**을 지원합니다.
실제 보안 사고를 모사한 콘텐츠를 제공하여 필요 기술을 강화하는 목적으로 실전에서 적용 가능하도록 문제를 구현합니다.

1 해킹 방어 대회 문제 출제 및 운영

"국내 해킹 방어 대회 운영 시장 점유율 1위"

문제기획

시나리오 대비
배점, 난이도 제시
문제 검토

문제출제

기획된 문제 기반 개발
부정행위 방지 기능 개발

문제검토

기획 대비 적절성 확인
구현상 문제점 확인
난이도 적절성 확인
운영 문제점 사전 검토

사전점검

홈페이지 점검
탑재된 문제 풀이
점수 반영 확인
구동상 문제점 확인

대회운영

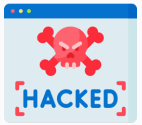
운영채널 관리
부정행위 확인
문제 풀이 데이터 모니터링
시스템 모니터링

03 사이버 훈련 및 교육

다수의 침투테스트, 글로벌 해킹 방어 대회 수상 경험을 토대로 현업에서 필요한 기술을 **알기 쉽게 난이도별 강의를 제공**합니다.
이론을 배우기 위한 단발 실습이 아닌 업무에 적용 가능한 유사 실습 환경을 직접 제작하여 **최신 보안 기술 교육 및 실전형 실습 환경을 제공**합니다.

2 기술강의커리큘럼

웹 해킹



- 웹 해킹의 이해
- 웹 해킹 도구
- 정보 수집 방법
- SQL Injection
- Server Side 취약점
- 웹 취약점 분석 및 공격 실습
- CTF 실습

리버싱 엔지니어링

- 리버싱 기초
- 리버싱 분석 방법
- 리버싱 이론(실습형)
- 안티 리버싱 기술/ 우회 실습
- 악성코드 분석
- 에뮬레이터 활용
- 코드 가상화 기술 및 문제풀이

시스템 해킹

- 스택 오버플로우 공격 유형 이론 학습 및 실습
- 힙 오버플로우 공격 유형 이론 학습 및 실습
- 워게임 문제 풀이 및 실습
- 대회 문제 풀이 및 실습
- 보안 사고 케이스 스터디

웹 브라우저 해킹

- 브라우저 기본의 이해
- Javascript Engine 이해
- JIT 컴파일러 이해
- 브라우저 버그 케이스 스터디 (실습형)
- Javascript Runtime 1-day 취약점 분석 및 실습
- Javascript JIT Compiler 1-day 취약점 분석 및 실습

만들면서 배우는 악성코드

- 악성코드 제작 개요
- 악성코드 개발 환경 구축
- APT 악성코드 제작 실습
- APT 악성코드 AV/EDR 탐지 우회
- APT 악성코드 지속 실행 구현
- APT 악성코드 제작 응용

악성코드 분석

- 악성코드 유형 및 그룹별 특징
- 정적/동적 분석 도구 실습
- 침해사고 악성코드 특징과 분석 방법
- 실제 침해사고 악성코드 분석
- 악성코드 모의 헌팅

ENKI

03 사이버 훈련 및 교육

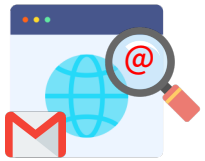
악성코드 분석 전문가들이 이메일 보안 사고, 악성 이메일 정보 등을 수집 및 분석하여 실제와 유사한 **이메일 APT 훈련을 제공**합니다.
직접 제작한 악성 이메일을 발송하여 이메일 열람 등의 결과를 보고하고, 훈련을 통해 **내부 임직원의 보안 인식을 제고**합니다.

3 이메일 APT 모의 훈련

악성 이메일 제작

악성코드 분석 전문가들이 수집한 정보를 바탕으로 APT 이메일 보안 사고를 모사한 악성 이메일을 직접 제작합니다.

01 step



훈련 대상 정보 수집

외부의 공개된 임직원 이메일을 엔키의 기술력을 활용하여 직접 수집하거나 협의하에 훈련 대상의 이메일 정보를 입수합니다.

02 step

훈련 수행 및 결과보고

악성 이메일 발송 후 이메일 열람 및 악성코드 실행 내역 등의 정보를 포함한 수행 결과를 보고서의 형태로 보고합니다.

03 step

04 버그캠프

버그캠프는 화이트 해커와 함께 보안 문제를 찾아내고 해결하는 **버그바운티 플랫폼 서비스**입니다.
버그바운티란, 취약점 신고 포상제로 보안 취약점을 제보한 화이트 해커에게 포상을 지급하는 제도입니다.

BUGCAMP

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

https://bugcamp.io

01
Public/Private
맞춤형 프로그램 운영 지원

02
VPN을 통해
안전한 점검 및 통제

03
고객사의 보안팀처럼
전반적인 업무 대행

04
증빙 자료로 쓰일 수 있는
상세한 결과 보고서 제공

취약점 제보율

100%

취약점 제보

350건+

포상 금액

1,500만+

ENKI

05 VATE, 사이버 훈련장

VATE(**V**ersatile **A**utomatic **T**est **E**quipment)는 엔키가 직접 연구하고 경험한 기술들을 적용하여 개발한 **실전형 사이버 공방 훈련장 서비스**입니다.
실제 보안 사고를 시나리오로 재현하여 **공격팀/방어팀 관점에서 체험할 수 있는 환경을 제공**합니다.

다양한 환경 모의 훈련 시나리오

VATE는 다양한 인프라 환경, 산업군에 대해 공격/방어 모의 훈련을 제공합니다. 훈련생은 다양한 산업군 환경을 이해하고 상황에 필요한 기술을 강화할 수 있습니다.

실시간 공격/방어 모드 기술 훈련

VATE는 다양한 사이버 사고를 공격팀/방어팀 관점에서 실시간으로 훈련할 수 있습니다. 훈련생은 실제 공격과 위협을 대응하는 기술을 동시에 훈련할 수 있습니다.

게임처럼 즐기는 사이버 훈련

VATE는 시나리오속 개별 미션을 수행하고 점수를 획득하며 클리어하는 게임형입니다. 단발성 교육이 아닌 연속적 훈련과 기술 습득을 게임처럼 즐길 수 있습니다.

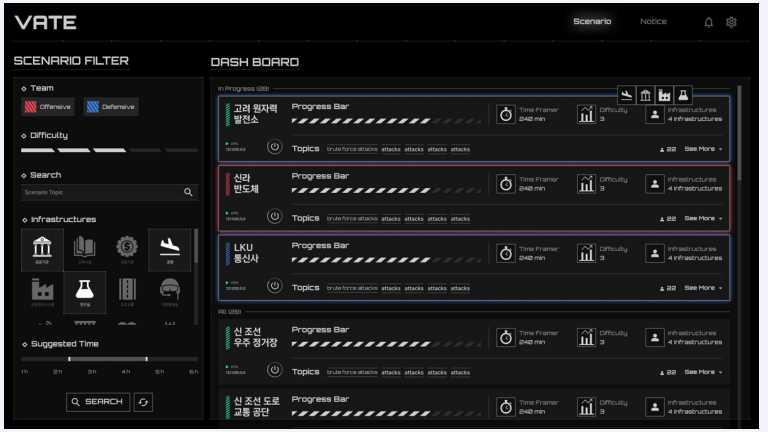
공격팀(RED)

실제 침해사고에서 공격자가 수행하는 공격이 미션으로 제공되며, 정보 유출, 서버 장악 등을 목표로 타겟을 공격합니다.

방어팀(BLUE)

공격팀이 기업을 침해할 수 없게 하는 것을 목표로 공격 벡터를 제거하고 실시간 공격에 대응하는 미션을 클리어하며, 기업 보안 체계를 향상시킬 수 있는 기술을 강화합니다.

훈련 시나리오 목록



훈련 수행 메인 페이지

ENKI

ENKI

모든 보안 문제는 서로 다르며, 그 해답 역시 달라야 합니다.

주식회사 엔키 (Enki Co., Ltd)
Tel. 031-722-1337
Fax. 031-722-1338
E-mail. info@enki.co.kr