# Attack the risk!

지피지기면 사이버 전쟁도 전승이라

목차



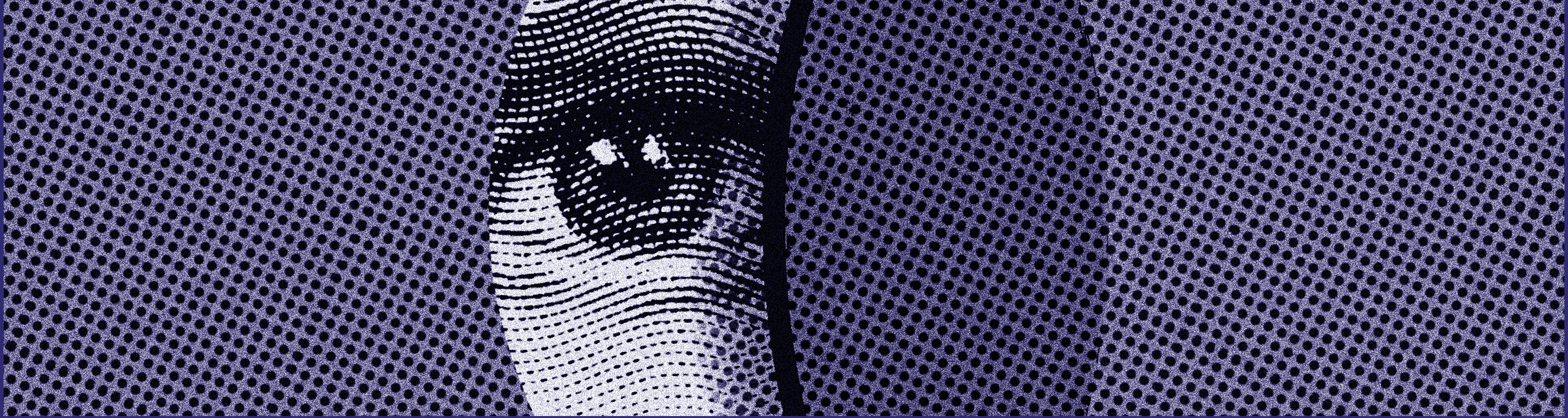
Security Office

2026-02-25

# 01 What we offer

## Offensive security,
## executed the attacker’s way.

공격자와 같은 방식으로 시스템에 침투합니다.
시간 낭비 없이 진짜 위협만 찾아냅니다.



# Vulnerability assessment and penetration testing

저희가 제공하는 VAPT 서비스는
모의해킹·모의침투 기반 보안 진단뿐만 아니라
확립된 베스트 프랙티스에 기반한
코드, 인프라, 설계 리뷰를 진행합니다.

견고한 보안은 단순 수정이 아니라 이해에서 출발합니다.
저희가 습득한 지식을 고객에게 전달하여
더욱 단단한 보안 태세를 함께 구축하고자 합니다.

# How we work

표면적인 체크리스트가 아닌
의미 있는 결과에 집중

보안 진단이 진행되는 동안
명확하고 지속적인 소통

고객의 팀이 참여하는
라이브 해킹 시연과 연속적인 협업

자동 스캐너나 “바이브” 테스트에
의존하지 않는 전문가 분석

정확성을 유지하면서
시간과 비용을 줄일 수 있는
화이트박스 테스트 옵션

# Methodology

### 진단 준비

- 진단 범위 특정
- 명세 문서 준비
- 소통 채널 확립

### 보안 진단 수행

- 보안 취약점 발견
- 고객의 버그 추적 도구에 직접 보고

### 지속적인 소통

- 지식 전달을 위해 고객의 팀과 연속적인 협업
- 대응된 취약점 검증과 후속 진단

### 결과 리뷰

- 담당 팀과 결과 보고 미팅
- 보안 성명서와 보고서 전달

# Target

공격자의 관점에서
직접, 정확하게, 의도를 가지고
애플리케이션과 인프라를 테스트합니다.

개발 과정에서 아무도 모르게 추가된
보안 취약점을 발견하세요.

통제된 환경에서 선제적으로 모의해킹을 수행하여
공격자가 보안 취약점을 어떻게
악용할 수 있는지 확인하세요.

| Application |
| --- |
| Web |
| Android |
| iOS |
| Windows |
| macOS |
| Linux |

| Infrastructure |
| --- |
| Microsoft Active Directory + LDAP |
| Amazon Web Services |
| Microsoft Azure + Entra ID |
| OpenShift + OKD + Kubernetes |
| Google Cloud |
| Red Hat IdM |
| IBM AS/400 + Mambu |
| 상용 IT 시스템 |

# Deliverable

직접 버그 추적 도구에, 또는 일반적인 보고서 형태로,
필요한 곳에 진단 결과를 전달해 드립니다.

## Integrated

발견된 취약점을 고객의 버그 추적 도구에
직접 추가하여 즉각적인 대응을 도모합니다.

## Traditional

체계적인 보고서나 보안 성명서 형태로도
전달해 드릴 수 있습니다.

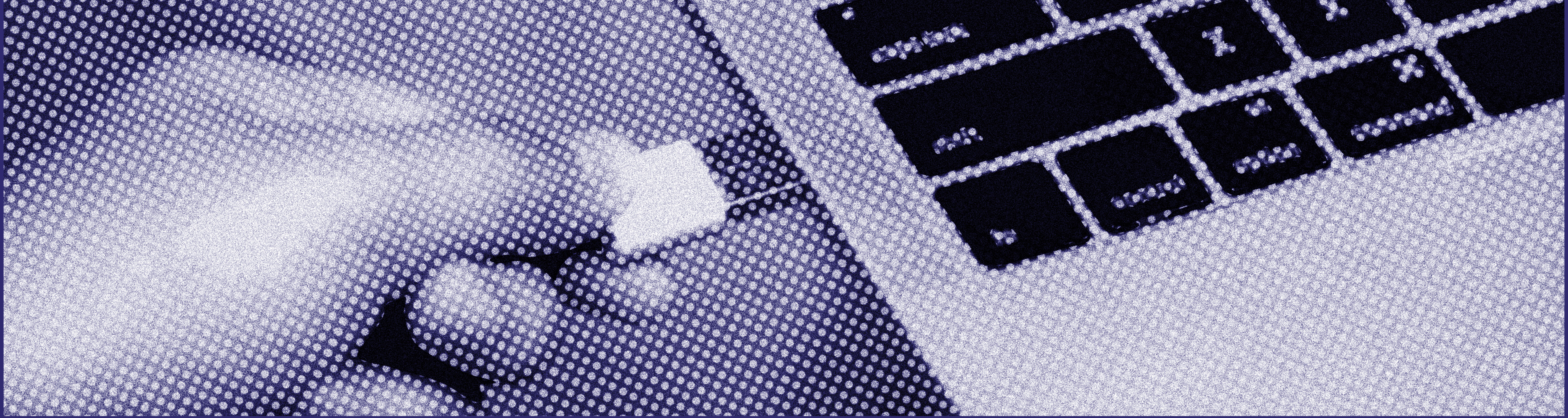
# Systematic assessment

진단 범위의 우선순위를 결정하고 주기적인 테스트를 수행하여
지속적으로 보안성을 강화할 수 있는 시스템 보안 진단 옵션을 제공해 드립니다.

이 옵션은 LIS/ISMS 요건에 부합하며
NIS2 가이드라인을 충족시킬 수 있습니다.

진단 범위에 대한 명확한 우선순위 결정과
주기적이고 장기적인 테스트

LIS/ISMS 요건과 호환되며
NIS2 가이드라인에 부합



# Social engineering

현실적인 공격 시나리오에 기반하여
악의적인 USB 메모리/케이블을 이용하거나 피싱 등
통제된 환경에서의 소셜 엔지니어링 테스트를 수행합니다.

# CTF & workshop

고객의 팀이 서로 협력하여 현실적인 환경의 보안 취약점을 발견하는 챌린지를 개최합니다.

저희의 경험은 물론 고객의 시스템에서 이전에 발견된 실제 보안 취약점을 기반으로 맞춤 CTF 문제와 워크숍을 제작해 드립니다.

# 02 Who we are

## Built by intelligence experts. Proven in real life.

스웨덴 정보기관 출신 전문가가 설립하고,
진짜 결과와 연구로 증명합니다.

Security Office

# Qualification

여러 업계의 기업이 끊임없는 사이버 위협에 대항하기 위해 저희를 신뢰하고 있습니다.
지속적인 연구 활동을 통해 다양한 기술과 플랫폼에서 45개가 넘는 CVE를 발견하였습니다.

**Trusted by organizations across industries**

**Recognized by leading vendors and platforms**

**Public research and industry engagement**

# Trusted by organizations across industries

고위험 고복잡 환경에서 운영하는
다수의 기업으로부터 신뢰받고 있습니다.

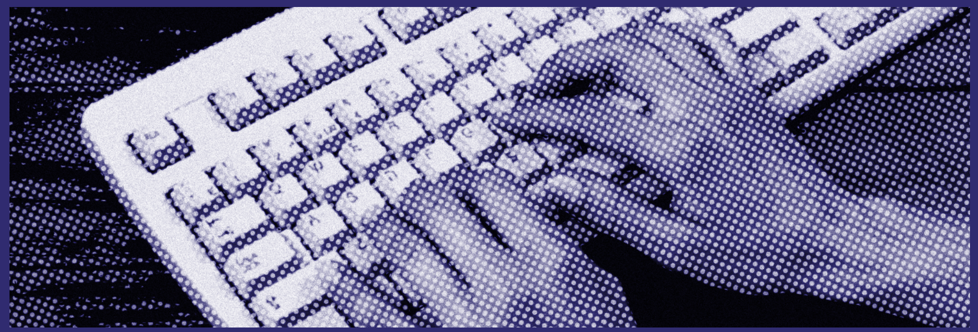
**금융 기관**

은행, 투자사, 핀테크

**본인 확인 기관**

**정부 기관**

**클라우드 플랫폼**



**IT 서비스 업체**

**비디오 게임 스튜디오**

**테크 스타트업**

# Recognized by leading vendors and platforms

연구 활동과 책임 있는 공개를 통해
45개 이상의 CVE를 발표하며
폭넓은 분야의 기술 리더와 기관으로부터
정식으로 인정받았습니다.

**Red Hat**
Keycloak, RHACS

**Apache Foundation**
Superset

**PHP**

**Apple**
Safari

**Google**
Chrome, Android

**Samsung**

**네이버**
Hall of Fame

**VLC**

**Rubrik**

외 다수

# Public talks and industry engagement

컨퍼런스 발표, 전문가 패널, 산업 행사에 참여하며
전세계 보안 커뮤니티에 기여합니다.

**DEF CON 26, 30, 31**

**Øredev 2024**

**한국–유럽연합 고위급 사이버안보 컨퍼런스 2023**

**주한스웨덴상공회의소**

**법무법인 디엘지–인베스트서울**
2024 넥스트 호라이즌: 서울시 외국인직접투자와 스타트업

**Dentons Lee**
Data Security & Privacy Law Seminar

**CyberSecure**

# 진심으로,
# 도와드리겠습니다.

contact@securityoffice.io

Security Office APAC AB
No. 559454-2234
Makrillvägen 10 B
181 30 Stockholm
Sweden

시큐리티오피스에이팩 주식회사
등록번호: 765-84-00048
04534 서울특별시 중구
을지로 50 2008호
대한민국



Security Office