회사 소개

주식회사 위키시큐리티

- ❖ 차별화된 강점
- ❖ 주요 비즈니스 영역
- ❖ 정보보안 컨설팅 서비스 영역
- ❖ 정보보안 솔루션 영역
- ❖ 정보보안 연구개발(R&D) 서비스
- ❖ 발명특허, 정부인증 및 사회공헌
- ❖ 주요 고객과 산업군

차별화된 강점

25년 이상 쌓아온 다양한 분야의 정보보안 전문성 보유

25년이 넘는 기간 동안 당사는 다양한 정보보안 문제를 해결하는데 노력해 왔으며, AI 및 블록체인과 같이 끊임없이 진화하는 신기술의 환경을 능숙하게 탐색해 왔습니다. 당사의 전문지식은 개인 데이터 보호, 보안 아키텍처, 기술 보안 솔루션을 포괄합니다. 기업 및 기관에 서비스를 제공하는 것을 넘어 국가 정보보안 전략을 수립하고 실행하는 데 중요한 역할을 해왔습니다. 당사의 차별화된 전문성은 정부와 기업을 포함한 국내외 기관으로부터 인정과 신뢰를 받고 있습니다.

정보보안 라이프사이클 전반에 걸친 전방위적 역량 확보

정보보안의 Plan-Do-Act-Check 라이프사이클을 통해 정보보안에 대한 민첩한 접근 방식을 채택하여 끊임없이 변화하는 위협 환경에 선제적으로 대응하고 지속적으로 개선해야 살아남습니다. 당사의 전문 사이버 보안 컨설팅 부서와 R&D 센터는 심층적인 경험과 지식을 보유하여 정보보안 라이프사이클의 각 단계에서 고품질의 종합적인 서비스와 솔루션을 보장합니다. 당사는 적응력과 숙련도를 바탕으로 고객을 위한 맞춤형 최첨단 사이버 보안 인프라와 솔루션을 제작하고 제공하며, 고객의 고유한 요구사항에 따라 전 세계적으로 새로운 벤치마크를 설정합니다.

글로벌 리더십을 갖춘 정보보안의 리더쉽 보유

다년간의 실무경험과 전문성을 바탕으로 두 개의 발명특허를 보유하고 있으며 지속적인 기술혁신을 위해 노력하고 있습니다. 중소벤처기업부, 코트라, 산업통상자원부, 고용노동부, 한국산업기술진흥원 등 다양한 기관으로부터 인증을 획득하여 탁월한 R&D 역량과 안정적인 경영, 정보보안 업계의 선구자로서의 입지를 인정받고 있습니다. 또한 한국인터넷진흥원, 카이스트, 한국정보통신기술협회(TTA), 대한상공회의소, 수원대학교, 서울여자대학교 등 대표적 기관 및 대학과 산학협력을 맺고 있으며, 해외 기관 및 정부 기관과도 파트너십을 구축하고 있습니다. 당사는 고품질의 제품과 서비스를 제공하기 위해 첨단 기술을 지속적으로 연구하고 개발하는 정보보안 전문 기업입니다.

- 웹사이트: 영문) https://rura.wikisecurity.net 한글) https://wiki.wikisecurity.net
- 유투브: https://youtu.be/XrpjJBbNigc
- 이메일: info@wikisecurity.net

주요 비즈니스 영역

당사는 끊임없이 진화하는 정보보안 위협으로 부터 고객사의 조직을 보호하고 규제 요건을 준수할 수 있도록 최첨단 사이버 보안 컨설팅, 솔루션, 연구 개발 서비스를 제공하기 위해 최선을 다하고 있습니다. 심층적인 전문지식, 고급 방법론, 혁신적인 솔루션을 결합하여 난해한 정보보안 이슈를 해결하고 글로벌 시장에서 비즈니스 목표를 달성할 수 있도록 지원합니다.

➢ 정보보안 컨설팅 서비스

정보보안 분야에서는 전문지식과 경험은 가장 중요한 요소입니다. 당사는 정보보안의 다양한 문제와 솔루션에 대한 심층적인 이해와 다년간의 경험을 갖춘 컨설턴트들을 보유하고 있습니다. 당사의 컨설팅 서비스는 정보보안 라이프사이클의 모든 단계인 PDCA(Plan-Do-Act-Check) 접근방식에 기초하여 서비스를 제공합니다.

우리 컨설턴트의 90% 이상이 대학 또는 대학원에서 ICT 또는 정보보안을 전공하고 국가연구정보시스템(NRI)에 등록되어 있는 전문인력들이며 평균 15년 이상의 실무 경력을 보유하고 있습니다. 또한 최고의 서비스 품질을 보장하기 위해 10여 가지 이상의 차별화된 컨설팅 방법론을 사용하고 있으며, 새로운 과제를 해결하기 위한 새로운 방법론들을 지속적으로 개발하고 있습니다.

당사 정보보안 컨설팅의 주요 서비스는 다음과 같습니다:

- 정보보안 전략 수립 컨설팅 서비스
- ISO/IEC 27001 인증 및 감사 컨설팅 서비스
- 모의해킹 진단, 침투테스트 서비스
- 보안 취약점 진단 서비스
- 애플리케이션 소스코드 취약점 진단 서비스
- 오픈소스 라이선스 및 보안 취약점 점검 서비스
- 그 외 고객의 특정 요구사항에 맞춘 다양한 서비스

➢ 정보보안 솔루션 및 제품

효과적인 사이버 보안을 위해서는 공격자의 사고방식과 전략을 이해하는 것이 필수적입니다. 당사는 다년간의 풍부한 경험을 바탕으로 공격자의 패턴과 특성을 파악하여 효율적이고 효과적인 보안 솔루션과 제품을 개발합니다. 사이버 위협이 지속적으로 진화함에 따라 보안 솔루션과 제품도 진화해야 합니다. 저희 WiKi Security R&D 센터는 새로운 도전 과제에 대응하기 위해 지속적인 연구와 개발을 통해 제품을 진화시키고 적용하는데 전념하고 있습니다.

당사의 정보보안 솔루션 및 제품은 다음과 같습니다:

- WiKi-RAV (Attack Surface Management System)
- WiKi-ARMA (Web Application Firewall)
- 그리고 고객의 요구사항에 맞춘 맞춤형 솔루션 또는 제품을 개발함

➢ 정보보안 연구개발(R&D) 서비스

조직이 정보보안을 고려하는 배경은 크게 4가지로 분류할 수 있습니다.:

- 보안위협(Security Threat): 내부의 비인가자 또는 외부 비인가자의 해킹 위협 또는 공격
- 규정준수(Compliance): 조직이 준수해야 하는 법률 및 규제상의 요건
- 비즈니스 요구사항(Business Requirements): 조직의 비즈니스에 필수적인 정보보안에 대한 요
- 비즈니스 기회(Business Opportunities):비즈니스 경쟁력 강화 또는 사업확장을 위한 정보보안 요구

이러한 배경은 각각 다른 형태의 정보보안 요구사항을 발생시키며, 조직은 이러한 요구사항들을 해결하기 위해 기술적 요소뿐만 아니라 관리 및 운영 측면을 포괄하는 솔루션 또는 고유한 상황에 맞게 특별히 맞춤화된 솔루션이 필요하게 됩니다.

당사의 WiKi Security R&D 센터는 고객사의 이러한 다양한 형태의 문제를 해결하기 위한 맞춤형 서비스 제공을 목표로 합니다. 고객사의 최종 목표 요구사항에 따라 기술적 보안 솔루션 또는 기술 및 관리 운영의 조합의 형태가 될 수도 있습니다.

당사가 현재 진행중이거나 이용가능한 WiKi Security R&D센터의 서비스는 다음과 같습니다:

- WiKi-Bug@ndAll (Bug Bounty Platform)
- 전 세계 보안엔지니어에게 무료로 제공되는 웹사이트(위협 및 취약점 정보)

그리고 고객의 특정 요구사항에 맞는 맞춤형 사이버 보안 연구 및 개발 이니셔티브에 협력할 수 있는 사항도 있습니다.

정보보안 컨설팅 서비스 영역

Information Security Strategy Consulting Services

해킹, 내부 데이터 유출, 개인 데이터 유출, 규정 준수 등 다양한 정보보안 문제에 직면하는 대부분의 고객사는 전략적 계획이 부족하거나 즉각적인 문제를 해결하기 위해 임시방편적인 솔루션에 의존하는 경우가 많습니다. 하지만 정보보안 관리는 그 노력과 성과를 인정받아야 하는 중요한 기능 중 하나입니다. 현재 상태를 정확하게 평가하고 최고 경영진의 승인을 받아 전사적 차원의 전략적 계획을 수립함으로써 고객은 다양하게 변화하는 내부 및 외부의 위협에 대하여 체계적이고 조직적으로 대응하고 흔들림 없는 강력한 정보보안을 유지할 수 있습니다.

- **목표:**
  고객사(국가, 기업, 기관)의 정보보안 현황을 분석하여 정보보안의 목표를 설정하고, 목표 달성을 위한 단기, 중기, 장기 정보보안 전략과 실행 계획을 수립합니다.

- **범위:**
  고객의 외부 컴플라이언스 환경과 여건에 따라 정보보안을 관리적, 기술적, 물리적 영역으로 분류하여 그에 따른 범위를 설정합니다.

- **기대 효과:**
  - 막연하게 인식하고 있는 정보보안 위험을 정량적, 정성적 관점에서 정확하게 파악할 수 있습니다.
  - 조직의 역량과 환경적 특수성을 반영한 정보보안 목표와 모델을 수립할 수 있습니다.
  - 목표한 정보보안 수준을 달성하기 위해 필요한 단기, 중기, 장기 개선 전략과 계획, 과제, 예산을 확보할 수 있습니다.

- **차별성:**
  - 고객사의 역량과 현황을 체계적으로 파악할 수 있는 독자적인 방법론을 이용하여 AS-IS 평가뿐만 아니라 AS-WAS 평가를 통해 고객사의 위치와 여건을 정확하게 분석합니다.
  - 다양한 선진사례 경험과 노하우를 바탕으로 고객의 환경과 조직 역량에 맞는 최적화된 TO-BE를 설계합니다.

정보보안 컨설팅 서비스 영역

ISO/IEC 27001 인증준비 컨설팅 및 심사

대외적인 비즈니스 신뢰도가 필요한 정부기관과 기업들은 정보보안 관리의 신뢰성을 보장받기 위해 점점 더 많은 노력을 기울이고 있습니다. 특히 해외 파트너와 교류가 잦은 기업의 경우 제3자 인증기관으로부터 정보보안 관리체계의 완성도를 검증받고 인증받음으로써 비즈니스 파트너와의 신뢰성을 확보하는 것이 매우 중요합니다. 대표적인 정보보안 경영시스템의 표준 및 인증체계는 ISO/IEC 27001이 있으며, 조직의 목적과 범위에 따라 다양한 ISO/IEC 27000 시리즈 표준이 존재합니다.

- **목표:**
  ISO/IEC 27000 시리즈를 목표 모델로 하여 조직의 정보보호 관리체계(ISMS)를 수립 및 운영하고, 인증 심사 기관으로부터 그 상태를 검증 받아 인증을 획득합니다.

- **범위:**
  조직에서 제공하는 핵심 비즈니스를 기반으로 보호가 필요한 조직적, 물리적, 기술적, 관리적 범위를 선정하고 정보보안 경영을 위한 관리체계를 수립 및 운영하고 이를 제3기관에게 심사받아 인증서를 획득하는 전체 공정을 제공합니다.

- **기대 효과:**
  - 국제적으로 인정받는 ISO/IEC 27000 인증을 확보함으로써 대외적인 비즈니스 신뢰성을 확보할 수 있습니다.
  - 조직이 직면하고 있거나 직면하게 될 정보보안 위험에 유연하게 대응할 수 있는 관리 체계를 확보함으로써 견고한 수준의 조직 정보보안을 운영 및 관리할 수 있습니다.
  - 매년 인증 심사기관으로부터 위험 관리 실태 심사를 받음으로써 지속적인 정보보안체계의 관리 개선 기회를 확보할 수 있습니다.

- **차별성:**
  - 당사의 여러 임직원이 ISO/IEC 27001 선임심사원 자격증을 보유하고 있으며 체계적인 컨설팅 방법론을 바탕으로 ISO/IEC 27001 요구사항과 이행계획을 정확하게 설계할 수 있습니다.
  - 또한 ISO/IEC 27001 인증 심사기관 및 심사원과 긴밀한 네트워크를 유지하여 인증 심사를 효과적으로 준비할 수 있습니다.
  - 다년간의 인증 준비 컨설팅 서비스를 제공한 경험을 바탕으로 고객의 인증 획득 성공을 100% 보장하며, 실패 시에는 인증 획득 시까지 무료 컨설팅 서비스를 제공합니다.

정보보안 컨설팅 서비스 영역

모의해킹 진단, 침투테스트 서비스

시스템이나 애플리케이션의 보안 취약점의 원인은 일반적으로 안전하지 않은 시스템 설계, 안전하지 않은 프로그램 개발, 운영 오류의 세 가지 주요 영역으로 분류됩니다. 이러한 보안 취약점의 원인을 사전에 파악하는 효과적인 방법 중 하나는 공격자의 관점에서 수행되는 침투 테스트(일명 '윤리적 해킹')입니다.
침투 테스트는 긴급 조치가 필요한 보안 취약점을 발견하는 데 특히 효과적이며, 화이트박스 테스트를 통해 탐지하기 어려운 비즈니스 로직 문제로 인해 발생하는 취약점도 식별할 수 있습니다.
수년간의 침투 테스트 경험과 수많은 버그 바운티 성과로 무장한 당사의 화이트 해커가 귀사에게 침투 테스트 서비스를 제공합니다.

- **목표:**
  - 시스템 또는 애플리케이션의 보안 취약점의 원인은 일반적으로, 안전하지 않은 시스템 설계, 안전하지 않은 프로그램 개발, 운영상의 오류 등 세 가지 주요 영역으로 분류됩니다.
  - 이러한 보안 취약점의 원인을 사전에 파악하는 효과적인 방법 중 하나는 공격자의 관점에서 수행되는 모의 침투 테스트('윤리적 해킹'이라고도 함)입니다.
  - 모의 침투 테스트는 긴급한 조치가 필요한 보안 취약점을 발견하는 데 특히 효과적이며, 화이트박스 테스트로는 탐지하기 어려운 비즈니스 로직의 문제로 인해 발생하는 취약점도 식별할 수 있습니다.
  - 다년간의 모의 침투 테스트 경험과 수많은 Bug Bounty 성과로 무장한 화이트햇 해커가 모의 침투 테스트 서비스를 제공합니다.

- **대상 및 범위:**
  유무선 네트워크, 서버, 웹/WAS, 미들웨어, 애플리케이션, 모바일 앱, SCADA, ICS, PLC 등 침투 테스트 대상은 고객사와 협의 및 합의를 통해 결정되며, 범위는 사전 협의를 통해 결정됩니다.

- **기대 효과:**
  - 공격자 관점에서 대상 시스템 또는 서비스의 보안 취약점을 찾아내고, 긴급 조치가 필요한 심각한 보안취약점을 식별할 수 있습니다.
  - 당사의 다양한 모범사례와 노하우를 바탕으로 식별된 보안 취약점을 효과적으로 해결하기 위한 체계적인 보안 개선방안을 확보할 수 있습니다.
  - 또한, 고객사의 요청에 따라 인가되지 않은 내부 및 외부의 공격에 대한 현재 조직의 방어체계의 문제를 식별하는데 도움이 될 수 있습니다.

- **차별성:**
  모의해킹 진단은 목적에 따라 Internal, External, Privileged Internal 모의해킹 진단으로 구분되며, 대상에 따라 다음과 같이 다양한 방식으로 협의를 진행할 수 있습니다:
  - 네트워크 모의해킹 진단
  - 애플리케이션, 모바일 앱 모의해킹 진단
  - SCADA, ICS 모의해킹 진단
  - 사회공학적 모의해킹 진단
  - 고객사의 요구사항에 따른 특정주제의 모의해킹 진단

정보보안 컨설팅 서비스 영역

보안 취약점 진단 서비스

보안 취약점 진단은 접근방식에 따라 Black-Box Test, Gray-Box Test, White-Box Test로 분류됩니다. 모의해킹 진단 (또는 침투테스트)가 Black-Box Test에 속한다면, 보안 취약점 진단은 Gray-Box Test방식에 해당합니다. 즉, 대상 시스템 또는 서비스에 대해 로그인한 사용자 계정 또는 네트워크 액세스 권한과 같은 일정수준의 액세스 또는 권한이 있는 상태에서 테스트를 수행합니다.
취약점 진단은 대상 시스템의 유형에 따라 표준화된 보안 점검 항목을 활용하여 취약점을 심층적으로 진단합니다. 예를 들어, 대상 시스템이 애플리케이션 또는 모바일 앱인 경우 OWASP Top 10과 Mobile Top 10을 적용합니다. 서버 OS, 웹, WAS, DBMS, API, Container(Docker), Kubernetes 등도 글로벌 공인 점검 항목을 활용해 구성 취약점, 보안 패치 상태 등을 검사합니다.

- **목적:**
  보안 취약점 진단의 목적은 대상 시스템 또는 서비스의 세부적인 보안 취약점을 식별하고 해결하여 대상의 보안을 강화하는 것입니다.

- **대상 및 범위:**
  보안 취약점 진단의 대상은 다음과 같습니다:
  - OS: Unix, Linux, Windows, AIX, HP-UX, Solaris, FreeBSD 등
  - Web/WAS Server: Apache, Tomcat, Nginx, IIS, WebLogic, WebSphere, Lighttpd, Jigsaw 등
  - DBMS: Oracle, SQL Server, DB2, PostgreSQL, MariaDB, MySQL 등
  - Network Device: Switch, Router 등
  - Security System: Network Firewall, WAF, VPN 등
  - Others: Container (Docker), Kubernetes, TP-Monitor 등

- **기대 효과:**
  대상 시스템 또는 서비스에 현재 존재하는 모든 보안 취약점을 식별하고 이러한 취약점을 해결하는 방법에 대한 해결방안을 확보할 수 있습니다.

- **차별성:**
  - 당사에서 보유하고 있는 방법론과 자동화 도구를 활용하여 체계적으로 서비스를 수행하므로 단기간에 다수의 시스템 또는 서비스의 보안 취약점을 발굴할 수 있습니다.
  - 시스템의 기능과 환경에 따라 보안 취약점 해결 방법은 달라질 수 있지만, 당사 서비스는 다년간의 경험과 사례 정보를 바탕으로 다양한 솔루션을 제공합니다.

정보보안 컨설팅 서비스 영역

애플리케이션 소스코드 보안취약점 진단

일반적으로 애플리케이션의 보안 취약점 진단방법은 동적진단과 정적진단으로 나뉩니다. 동적 진단은 애플리케이션이 실행 중인 상태에서 검사하는 것으로, 앞서 언급한 보안취약점 진단 서비스에 해당합니다. 정적진단은 애플리케이션의 소스코드를 한 줄 한 줄 검사하여 보안상의 취약점을 검사하는 방식입니다. 따라서 검사를 수행하기 위해서는 대상 애플리케이션의 소스코드를 받아야 합니다. 일반적으로 애플리케이션의 소스코드 용량이 크기 때문에 검사에는 자동화된 도구가 사용되며 이러한 도구의 신뢰성과 결과를 해석하여 오탐 또는 과탐들을 잘 식별하는 엔지니어의 역량이 매우 중요합니다.

- **목표:**
  애플리케이션의 소스코드 라인 수준까지 상세하게 보안 점검을 실시하여 애플리케이션 내의 모든 보안 취약점을 찾아내고 발견된 취약점에 대한 조치를 취하는 것이 목표입니다.

- **대상 및 범위:**
  애플리케이션의 형태에 따라 웹 애플리케이션, 모바일 애플리케이션, 클라이언트/서버 애플리케이션으로 구분할 수 있습니다. 점검을 수행하려면 대상 애플리케이션의 소스코드를 제공받아야 합니다.

- **기대 효과:**
  - 애플리케이션 소스 코드의 세부적인 보안 취약점을 식별합니다.
  - 발견된 보안 취약점을 해결하기 위해 애플리케이션의 기능 및 환경에 적합한 효과적인 방법을 제공합니다.

- **차별성:**
  - 애플리케이션 소스 코드의 보안 취약점을 식별하기 위해 자동화된 도구를 사용하기 때문에 시장에서 검증된 도구를 사용하는 것이 필수적입니다.
  - 당사는 전 세계적으로 신뢰성이 확보되고 검증된 전용 진단 도구를 사용합니다.
  - 검증된 도구를 사용하더라도 소스코드 정적 분석의 한계로 인해 오탐이 발생할 수 있습니다. 따라서 저희는 자동화된 도구가 생성한 결과에서 오탐 또는 과탐을 효율적으로 식별할 수 있는 고급 엔지니어를 제공합니다.
  - 발견된 보안 취약점을 해결하는 방법은 애플리케이션의 기능과 환경에 따라 달라질 수 있습니다. 다년간의 경험을 갖춘 전문 엔지니어가 고객이 효과적으로 문제점을 해결할 수 있는 방안을 제공합니다.

정보보안 컨설팅 서비스 영역

오픈소스 라이선스 및 보안취약점 점검 서비스

최근 Apache의 Log4j 취약점으로 인한 광범위한 피해는 전 세계 IT 전문가들에게 충격을 주었으며, 많은 제품이 오픈소스 소프트웨어를 사용하면서 이에 의존하는 오픈소스 컴포넌트를 적절히 관리하거나 이해하지 못하고 있다는 점을 부각시켰습니다. 이에 따라 미국 연방 정부는 소프트웨어 납품 시 소프트웨어 자재 명세서(SBOM) 제출을 의무화하고, 널리 사용되는 오픈소스 구성 요소에 대한 체계적인 관리를 촉구하고 있으며 국내 금융감독기관을 이를 의무화하려는 추세에 있습니다. 기업은 운영 또는 개발 중인 소프트웨어의 오픈소스 라이선스 규정 준수 여부와 알려진 보안 취약점(CVE)을 확인하고 지속적으로 관리해야 합니다. 당사의 서비스를 통해 사용 중인 오픈소스 컴포넌트를 파악하고 관련 보안 취약점의 존재 여부를 확인할 수 있습니다.

- **목표:**
  조직의 소프트웨어에 사용되는 오픈 소스 구성 요소의 라이선스 및 알려진 보안 취약점(CVE)을 파악하고, 법적 요구 사항을 준수하고 이러한 취약점을 악용하는 공격을 방지하기 위해 SBOM을 작성하는 것입니다.

- **대상 및 범위:**
  - 점검할 소프트웨어에 사용되는 오픈 소스 패키지를 조사하고 라이선스와 알려진 보안 취약점(CVE)을 식별합니다.
  - 조직 정책에 따라 오픈소스 사용량을 기반으로 소프트웨어에 대한 SBOM을 SPDX, CycloneDX, Excel 또는 JSON과 같은 형식으로 생성합니다.

- **기대효과:**
  - 조직의 소프트웨어에 사용되는 오픈 소스 패키지의 버전, 라이선스, 종속성, 저작권, 알려진 보안 취약점(CVE)에 대한 자세한 인사이트를 얻을 수 있습니다.
  - 오픈소스 관련 규정 준수 요건을 준수하는 데 필요한 문서를 확보할 수 있습니다.

- **차별성:**
  - 전 세계적으로 검증된 자동화 도구를 활용하여 오픈소스 구성 요소에 대한 자세한 정보를 제공합니다.
  - 고객사의 관련 정책에 따라 다양한 형식의 SBOM을 생성하여 제공함으로써 유연한 서비스를 제공합니다.
  - 고객사의 요청이 있는 경우 이미 고객사가 보유하고 있는 SBOM에 대한 검증 서비스를 제공합니다.

정보보안 솔루션 영역

WiKi-RAV (Attack Surface Management System)

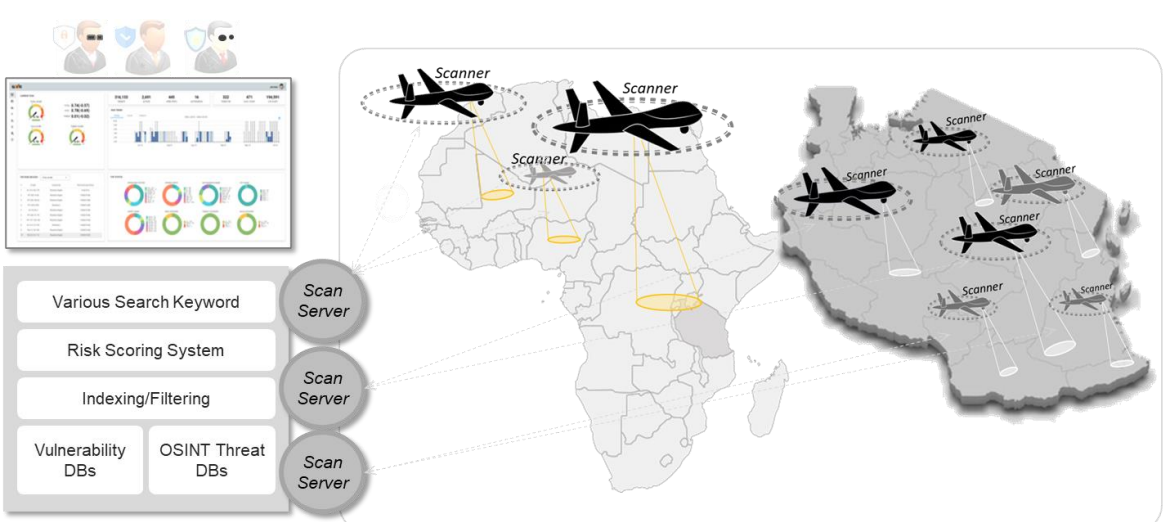
당신이 광범위한 네트워크와 서비스를 관리하는 CSIRT, ISP/IXP, SOC, NOC와 같은 조직에서 근무한다면, 수많은 IP 디바이스에서 발생하는 보안 취약점을 선제적으로 예방하는 것은 쉽지 않은 일입니다. 특히 최근 공개된 아파치 웹 서버의 다중 보안 취약점과 같이 광범위한 영향을 미치는 보안 취약점이 알려지는 경우, 해당 취약점이 어떤 IP 디바이스에서 존재하며 얼마나 심각한 상태인지를 신속하게 파악하고 대응책을 구축하는 것은 중요한 업무 중에 하나입니다. 또한 증가하는 클라우드 컴퓨팅 환경은 잦은 시스템 생성, 삭제, 변경이 발생하기 때문에 이러한 IT환경은 조직의 보안담당자에게 큰 부담을 가중시키고 있습니다.
또한, 다양한 유형의 보안위협이 발생하는 급변하는 ICT 환경에서 외부에 노출된 정보 시스템은 공격자 입장에서는 매우 매력적인 공격 대상입니다. 이렇게 노출된 시스템의 취약점을 모니터링하고 공격자가 악용하기 전에 선제적인 조치를 취하는 것은 조직의 보안위협 헌팅의 필수적인 부분이자 보안 전문가에게 필수적인 업무입니다. WiKi-RAV는 전쟁터에서의 정찰드론처럼 최신 보안 취약점 데이터베이스와 OSINT 위협 데이터베이스를 활용해 광범위한 네트워크 대역을 지속적으로 스캔하고, 60개 이상의 키워드 기반 검색 기능 등 다양한 기능을 통해 조직의 보안담당자가 특정 장비나 대역에 대한 세부 상황을 파악할 수 있도록 지원합니다.

- 솔루션 소개자료: https://youtu.be/MTuOaj8gIaY
- 데모용 시스템: https://rav.wikisecurity.net
- 사용자 메뉴얼: https://www.youtube.com/playlist?list=PLm3FFkiZ2YJ4iEBbCi-Xu7dHWgv10n6PE

- **주요 기능:**
  - **Large Scale Network에서 보안 취약점 및 위협을 상시스캔:**
    여러 곳에 위치한 스캔 클라이언트가 고객이 관리하는 Large Scale Network의 모든 IP 장치에서 보안 취약점과 OSINT 위협을 자동으로 상시적으로 검사합니다.
  - **최신 취약성 및 OSINT 위협 데이터베이스를 매일 업데이트:**
    WiKi-RAV는 알려진 보안 취약점(CVE) 및 OSINT 위협 데이터베이스를 매일 업데이트하여 최신 정보를 활용합니다.
  - **정량적 Risk Scoring 체계:**
    CVSS(공통 취약점 점수 체계) 기반의 위험 점수 시스템을 적용하여 사용자가 Large Scale Network의 보안 취약점 및 위협 수준을 한눈에 파악할 수 있도록 지원합니다.
  - **향상된 사용자 인증 및 액세스 제어:**
    WiKi-RAV는 웹 인터페이스를 통해 언제 어디서나 접속이 가능하지만, OTP를 이용한 강화된 인증으로 권한이 부여된 사용자만 접속할 수 있습니다. 사용자 접근 권한은 시스템 관리자가 메뉴별로 설정할 수 있습니다..

- **대상 고객:**
- Large Scale Network을 담당하는 CSIRT (Computer Security Incident Response Team)
- 광범위한 네트워크 대역에 IT서비스를 제공하는 기업 SOC(보안 운영 센터).
- 수많은 네트워크 대역에 대한 ISP/IXP 서비스를 제공하는 기업의 정보 보안 전담 조직.
- Smart City와 같이 다수의 IoT 디바이스를 운영하는 NOC(네트워크 운영 센터).

- **차별성:**
- 클라우드 또는 온프레미스 형태의 맞춤형 서비스 제공.
- 취약점 수준을 정량적으로 알 수 있는 Risk scoring System.
- 고객의 요구사항에 따른 맞춤형 서비스 제공시스템 운영에 필요한 기본 교육 프로그램 제공.



정보보안 솔루션 영역

WiKi-ARMA (Web Application Firewall)

사이버 위협이 증가하는 시대에 기업은 웹 애플리케이션을 악의적인 공격으로부터 보호하기 위한 적극적인 조치를 취해야 합니다. 기존의 네트워크 방화벽은 네트워크 수준의 공격을 탐지하고 차단하는 데는 능숙하지만, 웹에 특화된 공격에는 효과적으로 대응하지 못하는 경우가 많습니다. 이러한 중요한 격차를 이해한 WiKi-ARMA는 봇 공격, 인젝션, 애플리케이션 수준 DoS 공격 등 다양한 악성 활동으로부터 웹 서비스를 보호하는 데 필수적인 방어선 역할을 하는 고급 웹 애플리케이션 방화벽(WAF) 솔루션입니다. 악성 및 의심스러운 웹 트래픽에 대한 포괄적인 보호 기능을 제공하는 WiKi-ARMA WAF는 IP 차단, HTTP 헤더 검사, URI 문자열 필터링 등의 보안 규칙을 구현하고 모니터링하여 OWASP 상위 10대 보안 취약점에 효율적으로 대응할 수 있도록 지원합니다.

- **주요 기능:**

- 현황을 요약하는 Dashboard:
  WiKi-ARMA는 상위 10개 공격자의 IP 주소, URL, 이벤트와 같은 중요한 데이터를 효율적으로 통합하여 표시하는 직관적인 대시보드를 제공합니다. 요약된 정보를 한 눈에 볼 수 있어 사용자는 세심한 주의가 필요한 데이터를 손쉽게 모니터링하고 분석할 수 있습니다.

- 직관적인 Ruleset 관리:
  끊임없이 진화하는 웹 애플리케이션 공격의 특성을 해결하기 위해 WiKi-ARMA는 Ruleset 관리 기능을 통합했습니다. 이 직관적인 인터페이스를 통해 사용자는 탐지 및 차단 Ruleset을 손쉽게 구성하고 수정할 수 있어 유연하고 적응력 있는 보안 태세를 제공합니다.

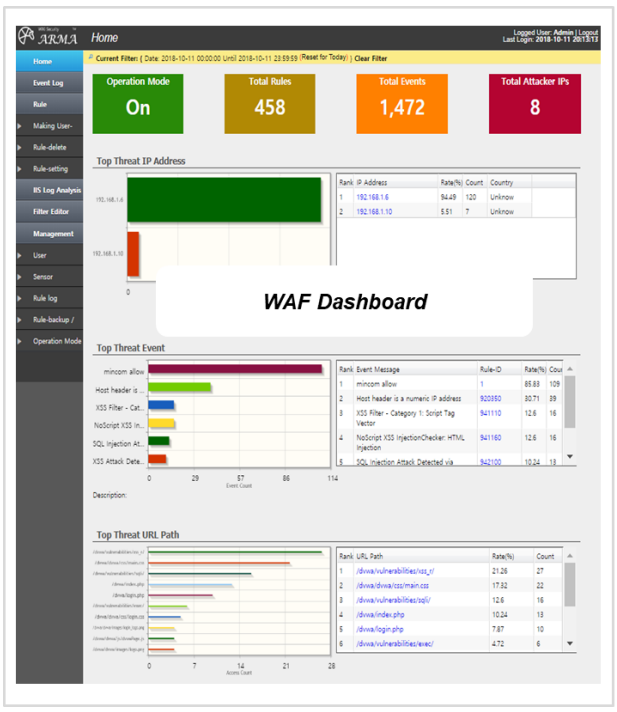
- **대상 고객:**

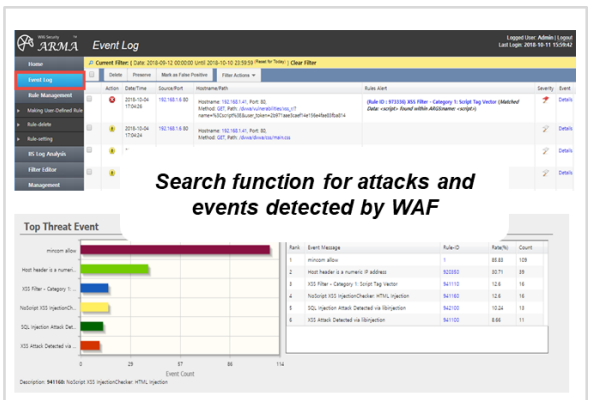
- 웹 애플리케이션 담당자
- 정보보안 담당자

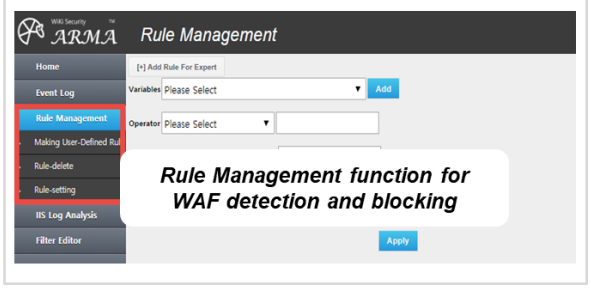
- **차별점:**

- 선제적 웹 애플리케이션 취약점 테스트:
  기존 WAF 솔루션과 달리 WiKi-ARMA는 WAF 설치 전에 웹 애플리케이션 취약점 테스트를 수행하여 사전 예방을 합니다. 이러한 선제적 조치를 통해 WAF를 배포하기 전에 대상 애플리케이션에 알려진 보안 취약점이 없는지 확인하여 보안 상태를 강화할 수 있습니다.

- 최적화된 룰셋 구성:
  WiKi-ARMA는 선제적 취약성 테스트를 통해 얻은 데이터를 활용하여 WAF 룰셋으로 적용해야 하는 특이점을 식별합니다. 결과적으로 이 정보는 대상 애플리케이션의 기능 및 보안 취약성에 맞게 특별히 최적화된 규칙 집합을 정의하고 구현하는 데 사용됩니다.







정보보안 연구개발(R&D) 서비스

WiKi-Bug@ndAll (Bug Bounty Platform)

디지털 시대에서 조직의 정보보안은 기본적인 정책이며 필수 요소입니다. 구글, 메타, 마이크로소프트, 애플과 같은 주요 글로벌 기업들은 자체 자산을 보호하기 위한 사전 예방적 조치의 중요성을 오래전부터 인식해 왔습니다. 최첨단 버그 바운티 플랫폼인 WiKi-Bug@ndAll은 전 세계 사이버 보안 강화를 목표로 하는 당사의 대표적 R&D 서비스입니다.
취약점 보상 프로그램(VRP)이라고도 하는 버그 바운티는 서비스, IT 인프라, 소프트웨어의 취약점을 발견하고 신고하는 보안 연구자에게 보상을 제공하는 크라우드소싱 보안 이니셔티브이며, 기업은 자체 서비스 또는 제품의 보안을 강화하고 보안 취약점을 발굴하는 보안 엔지니어는 보상과 인정을 받으며 기술을 연마하는 등의 효과가 있기 때문에 기업이나 기관과 보안엔지니어가 상생할 수 있는 전략입니다. 미국 국방부를 비롯한 여러 기관에서 버그 바운티 프로그램을 도입하여 중요한 보안 취약점을 발견함으로써 경제적, 기술적 이점을 누리고 있습니다. 이에 따라 미국 연방 정부는 모든 정부 기관에 취약점 공개 정책(VDP)을 의무화했으며 우리나라를 포함한 많은 선진국에서는 정부 차원의 버그 바운티 프로그램을 운영하며 국가 소프트웨어와 서비스를 보호하는 동시에 사이버 보안 인재를 양성하는 전략을 채택하고 있습니다.

당사의 WiKi Security R&D Center는 르완다의 UAUR 대학과 협력하여 버그 바운티 플랫폼인 WiKi-Bug@ndAll을 개발 중입니다. 이 플랫폼은 르완다의 사이버 보안 환경에 맞게 설계되어 화이트 해커를 양성하고 국가 보안 취약점을 발견 및 보호할 수 있도록 설계되었습니다. 특히, 이 플랫폼은 여러 버그 바운티 프로그램을 동시에 운영할 수 있으며, 보안 엔지니어와 기업 또는 단체를 위한 커뮤니티 채널을 제공하여 신속한 보안 조치를 가능하게 하는 중개자 역할을 합니다.

- **주요 기능:**

1. 보안담당자 웹 인터페이스:
- 프로그램 참여자의 인증을 강화하기 위한 OTP인증
- 각 프로그램별 가이드라인 및 정책을 제공
- 프로그램 참여를 독려하기 위한 명예의 전당

2. 관리자 대시보드:
- 보고된 취약점의 진위 여부를 신속하게 분석하고 피드백을 제공하는 채팅 채널
- 참여 보안 엔지니어 개요, 보고된 취약점 유형 등을 확인
- 취약점 정보 및 보안 엔지니어 데이터를 저장하고 관리

3. 보안취약점 보고 및 결과물 저장:
- 보고서의 정형 및 비정형 데이터를 체계적이고 안전하게 저장 관리
- 바이러스 검사 등 보안 엔지니어가 제출한 영상 파일의 안전한 처리 및 인덱싱 저장
- 저장된 파일에 대한 빠른 검색 기능

4. 제출된 취약점 보고서의 사전 검증:
- 관련 없는 보고서, 프로그램 규칙을 위반하거나 중복된 보고서를 딥러닝 기술기반으로 자동처리
- 평가우위를 위해 동일인이 작성하여 타인의 이름으로 제출되는 보고서를 딥러닝 기술기반으로 자동식별

5. 평가 및 보상기능:
- CVSS와 같은 국제 표준을 사용하여 신규 취약점의 심각도를 평가하고 적절한 보상을 결정하기 위한 평가기능

- **대상 고객:**
- 국가 차원에서 버그 바운티 프로그램을 운영할 계획이 있는 조직(예: 국가 CSIRT).
- 버그 바운티 프로그램을 운영하고자 하는 기업 또는 기관.

- **Our Edge:**

1. 머신러닝 및 DL 기반 자동화:
   머신러닝 및 딥러닝 기술을 사용하여 운영을 자동화함으로써 인적 오류를 최소화합니다.
2. 기술 이전:
   KISA(한국인터넷진흥원)를 통해 한국 정부의 버그 바운티 프로그램을 기술적으로 지원하며 쌓아온 경험과 전문성을 활용합니다.
3. 전담 기술 지원:
   기술 지원을 통해 이해관계자 간의 원활한 커뮤니케이션과 평가 시스템을 포함한 버그바운티 플랫폼의 효과적인 운영을 보장합니다.

WiKi-Bug@ndAll은 사이버 보안 솔루션의 최전선에 서 있습니다. 버그바운티 플랫폼을 통해 조직은 선제적으로 정보자산을 보호하고 사이버 보안 문화를 조성할 수 있습니다. 철통같이 안전한 디지털 미래를 위해 당사와 협력하세요.

정보보안 연구개발(R&D) 서비스

기타 R&D 서비스

WiKi Security R&D 센터는 전 세계 보안 엔지니어를 위한 최첨단 웹 서비스를 소개하게 되어 기쁘게 생각합니다. 당사는 연구 개발 경험을 활용하여 사이버 보안 환경을 강화하는 것을 목표로 합니다. 당사의 무료 웹 서비스는 글로벌 사이버 보안의 사각지대를 해소하기 위해 설계되었으며, 누구나 제한 없이 이용할 수 있습니다.

1. Blacklist IP Address 검색 웹사이트 (https://threat.wikisecurity.net)
사이버 보안 위협이 강화되는 시대에는 조직의 IP 주소 상태를 항상 경계하는 것이 무엇보다 중요합니다. 당사의 Blacklist IP 주소 검색은 조직 내 정보 보안 담당자를 위한 완벽한 도구입니다.

- **주요 기능:**
- 포괄적인 데이터베이스 검색:
  간단히 IP 주소를 입력하면 당사의 웹 서비스가 600만 개 이상의 글로벌 블랙리스트 데이터베이스를 검색하여 입력된 IP 주소가 블랙리스트에 있는지 확인합니다.
- 일일 업데이트:
  당사 서비스는 정확성과 적시성을 유지하기 위해 지속적으로 업데이트되는 광범위한 FireHOL 데이터베이스를 활용합니다.
- 다중 분류 데이터베이스:
  블랙리스트 데이터베이스는 7가지 유형(악용, 맬웨어, 익명화 프로그램, 스팸, 조직, 공격 및 평판)으로 분류되며 매일 약 300개의 공급자가 제공합니다.

2. 알려진 보안 취약점 정보 검색 웹사이트 (https://vul.wikisecurity.net)
버그 바운티 프로그램에 참여하는 보안 엔지니어 또는 기업이나 기관의 조직 내에서 보안 취약점을 관리하는 담당자는 당사의 알려진 보안 취약점 검색 서비스는 반드시 필요합니다.

- **Key Features:**
- 즉각적인 취약점 정보:
  특정 패키지 또는 애플리케이션의 이름을 입력하면 당사의 웹 서비스가 200만 개 이상의 알려진 취약점이 포함된 데이터베이스에서 귀하의 쿼리와 관련된 보안 취약점 정보를 검색합니다.
- 신뢰할 수 있는 소스:
  당사의 데이터베이스는 MITRE의 CVE 취약성 데이터베이스, Exploit-DB 및 Packet Storm의 정보를 통합하여 신뢰할 수 있는 최신 데이터를 제공합니다.

3. 버그 바운티 기여
KISA(한국인터넷진흥원)는 우리나라의 정보보호 전담기관으로 민간기업을 대상으로 버그바운티 플랫폼을 운영하고 있으며, 당사는 2019년부터 이 플랫폼에 대한 기술 지원을 제공하기로 매년 계약을 맺고 새롭게 보고된 보안 취약점을 분석, 평가하여 사이버 보안에 크게 기여하고 있습니다.

또한, 다음과 같은 새로운 보안취약점을 KISA에 제보하는 등 사이버 보안 강화에 적극 참여하고 있습니다.

- KVE-2022-0695: Multiple vulnerabilities in SIHAS (Sihas) IoT Web Server
- KVE-2022-0696: Reflected XSS vulnerabilities in SIHAS IoT and Sixshop
- KVE-2022-0697: Stored XSS vulnerabilities in SIHAS IoT and Sixshop
- KVE-2022-0698: Authentication flaws and parameter tampering vulnerabilities in SIHAS IoT
- KVE-2022-2187: Reflected XSS vulnerability on the imweb website
- KVE-2022-2188: Stored XSS vulnerability on the imweb website
- KVE-2021-2038: Parameter vulnerability in SONO Resort Hotel (SONO Hotel & Resort Mobile App)
- KVE-2021-1825: Parameter vulnerability in BMW (BMW Mobile App)
- KVE-2021-0153: Exposure of personal and internal information (AMANO Parking Management System)

이러한 노력에 대한 우리의 헌신은 사이버 보안 강화에 대한 사회적 책임에 대한 우리의 헌신을 반영합니다.

발명특허, 정부인증 및 사회공헌

정보보안 분야는 고객에게 최고의 서비스를 제공하기 위해 끊임없는 기술개발과 도전정신이 요구되는 분야입니다. ㈜위키시큐리티는 지속적인 연구, 개발 및 탐구를 통해 글로벌 사이버 보안의 사각지대를 제거하는 데 전념하고 있습니다.

지속적인 연구개발로 인한 발명특허

당사는 정보보안 분야에서 다음과 같은 발명특허를 보유하고 있으며 지속적인 연구개발을 통해 기술경쟁력과 장벽을 지속적으로 높여가고 있습니다. 우리는 업계 우위를 유지하기 위해 새로운 특허 기회를 적극적으로 식별하고 추구하고 있습니다.

- No. 10-1259897: 원격 보안취약성 진단장치 및 그 방법
- No. 10-0628296: 네트워크 공격상황 분석방법

기술혁신 및 벤처정신에 대한 정부의 관련인증

당사는 주요 정부기관으로부터 여러 가지 인증을 통해 정보보안 분야의 전문성과 기술을 인정받았고 있습니다. 기술혁신형 INNO-Biz 인증, 벤처기업 인증, WiKi 보안R&D센터 인증과 강소기업 인증 등이 있습니다.

- INNO-Biz 인증(No. 230102-01078): 기술혁신형 중소기업(중소기업청)
- 벤처기업 인증 (No. 20230517020007): KIBO 기술보증기금
- 기업부설연구소 인증 (No. 2011112773): 과학기술정보통신부

취약계층과 차세대를 위한 사회공헌

당사는 글로벌 NGO 월드비전의 후원자로 등록되어 있으며, 10년 넘게 전세계 취약 계층 아동 후원에 참여하고 있습니다. 또한, 서울여자대학교, 수원대학교, 산업기술고등학교 등의 기관과 산학협력을 구축하여 차세대 전문인력 양성에 기여하고 있습니다.

- 월드비전 아동후원기업으로 10년 이상 후원
- 국내 고·대학과 차세대 인재양성을 위한 산학협력:
  서울여자대학교, 수원대학교, 대덕대학, 한양여자대학교, 인천정보산업고, 인천마이스터고
- 국제 산학협력:
  아프리카 르완다 UARA(United Africa University of Rwanda), 필리핀 Gloders College

주요 고객과 산업군

수년에 걸쳐 우리 회사는 광범위한 산업 분야의 확고한 파트너 역할을 함으로써 사이버 보안 분야에서 풍부한 유산을 구축해 왔습니다. 우리는 그들의 과제를 헤쳐나가고 맞춤형 솔루션을 설계하는 것에 자부심을 느낍니다.

보안 목표수준이 높은 산업군의 고객사

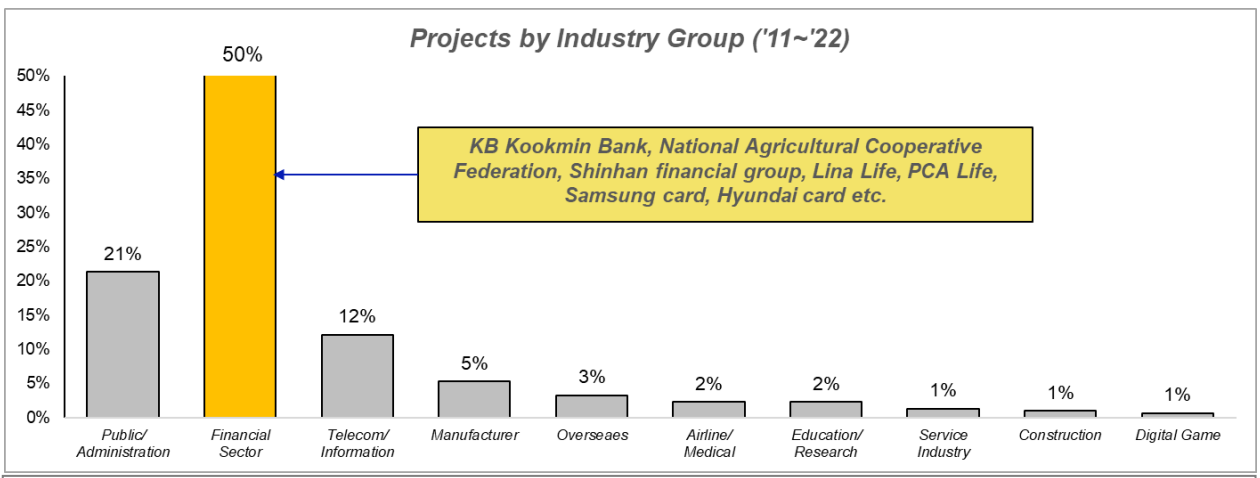
우리의 고객은 특히 금융 기관, 공공/정부 기관 등 사이버 보안에 대한 목표수준이 매우 높은 산업군에 높은 비중을 차지하고 있습니다. 또한 당사의 고객사들은 각 산업군에서 대표성을 갖고 있는 기업 또는 기관이므로 우리는 사명감을 갖고 업무에 임하고 있습니다.

그 산업계에서 신뢰받고 있는 고객사

당사의 고객 중에는 그 산업군에서 큰 영향력을 행사하고 모범을 보이는 저명한 기업 또는 기관들이 포함되어 있습니다. 이러한 고객들의 지속적인 비즈니스 문의 및 참여는 그들이 우리의 전문성과 진실성에 대해 확고한 신뢰를 갖고 있다는 증거입니다.

진정성과 우수성으로 맺어진 관계

우리의 고객 포트폴리오는 우리가 끊임없이 우수성을 추구하도록 영감을 주는 명예의 휘장 역할을 합니다. 우리의 약속은 우리의 진정성이며 업계 선두주자가 단순히 우리와 친분을 나누는 것이 아니라 우리와 지속적인 동맹을 구축하는 이유입니다.



당사는 다년간의 경험과 전문성을 갖고 있으며 귀사는 당사이 서비스와 솔루션으로 갈증을 해소할 수 있습니다.

우리와 함께 귀사의 미래를 확보하세요.

End of Document

WiKi Security Corporation
Information Security Solution Provider

Contact Us

South Korea – Head Office

#1910, Ace Gasan Tower, 121, Digital-ro, Geumcheon-gu, Seoul
T) +82-2-322-4688 F) +82-2-322-4646
E) info@wikisecurity.net

WiKi Security India – Office

Lane No 5 , Sushanti Vihar, Tankapani Road, Bhubaneswar, Odisha 751018
T) +91-99-3754-7700
E) india@wikisecurity.net

WiKi Security Rwanda – Office

2, KG28AV., Kimihurura, Gasabo, Kigali PO BOX 5561
T) +250-788- 557-782
P) Eng. Peterson T Mutabazi +250-738-528-594
E) africa@wikisecurity.net