Company Profile

WiKi Security Corporation

- ❖ DIFFERENTIATED STRENGTHS
- ❖ CORE BUSINESS AREAS
- ❖ CONSULTING SERVICE
- ❖ CYBERSECURITY SOLUTIONS
- ❖ CYBERSECURITY R&D SERVICE
- ❖ PATENTS, CERTIFICATIONS AND CONTRIBUTIONS
- ❖ OUR CUSTOMERS

DIFFERENTIATED STRENGTHS

A Quarter Century of Diverse Cybersecurity Expertise

For over 25 years, our company has been at the forefront of addressing a wide range of cybersecurity issues, adeptly navigating the ever-evolving landscape of emerging technologies such as AI and blockchain. Our expertise encompasses personal data protection, security architecture, and technological security solutions. Beyond serving corporations and institutions, we have played an instrumental role in formulating and implementing national cybersecurity strategies. Our distinguished expertise has garnered recognition and trust from both domestic and international entities, including governments and corporations.

Full-Spectrum Mastery Across the Cybersecurity Lifecycle

We are using an agile approach to cybersecurity with the Plan-Do-Check-Act lifecycle for continuous improvement and proactive responses to an ever-changing threat landscape. Our specialized cybersecurity consulting division and R&D center possess in-depth expertise, ensuring high-quality, comprehensive services and solutions at each stage of the cybersecurity lifecycle. Our adaptability and proficiency empower us to create and deliver bespoke, cybersecurity infrastructures and solutions for clients, setting new benchmarks globally based on their unique requirements.

A Cybersecurity Powerhouse with Global Leadership

Building on years of practical experience and profession, we are holding two technology patents and are committed to continuous innovation. Our company has earned certifications from various authorities, including the Ministry of SMEs and Startups, KOITA, KOTRA, MMA, MOEL, and KITA, which recognize our exceptional R&D capabilities, stable management, and position as the utmost in the cybersecurity industry. Moreover, we have established academic-industry collaborations with renowned entities such as KISA, KAIST, TTA, KCCI, Suwon University, and Seoul Women's University, and have also forged partnerships with overseas institutions and government agencies. Therefore, our company is a cybersecurity specialist dedicated to continuous research and development of high-technologies to ensure the provision of high-quality products and services.

- Website: EN) https://rura.wikisecurity.net KR) https://wiki.wikisecurity.net
- Youtube: https://youtu.be/XrpjJBbNigc
- Email: info@wikisecurity.net

CORE BUSINESS AREAS

At our company, we are committed to providing cybersecurity consulting, solutions, and research and development services to safeguard your organization against ever-evolving threats and ensure compliance with regulatory requirements. We combine deep profession, advanced methodologies, and innovative solutions to address your unique security challenges and support the achievement of your business objectives in the global market.

Cybersecurity Consulting Service

In the field of cybersecurity, professionalism and experience are paramount. Our company boasts a team of consultants who are equipped with years of experience and an in-depth understanding of various issues and solutions in cybersecurity. Our consulting services are essential throughout nearly all stages of the cybersecurity lifecycle, following the PDCA (Plan-Do-Check-Act) approach.

Over 90% of our consultants have specialized in ICT or information security at the bachelor's level, are registered with the National Research Information System (NRI), and possess an average of 15 years of hands-on experience. In addition, we employ over 10 distinct consulting methodologies to ensure the highest quality of service, and continuously develop new methodologies to tackle emerging challenges.

Our flagship cybersecurity consulting services include:

- Information Security Strategy Consulting Services
- ISO/IEC 27001 Certification Readiness Consulting Services
- Penetration Testing Service
- Vulnerability Testing Service
- Application Source Code Vulnerability Testing Service
- Open-Source License and Vulnerability Check Service
- And many more tailored to your specific needs

Cybersecurity Solutions & Products

Understanding the attacker's mindset and strategy is essential for effective cybersecurity. Our company utilizes our extensive experience in dealing with offensive cyber strategies to develop efficient and effective security solutions and products based on the patterns and characteristics of cyber attackers. As cyber threats continuously evolve, so must security solutions and products. Our WiKi Security R&D Center is dedicated to continuous research and development to evolve and adapt our offerings to meet emerging challenges.

Our cybersecurity solutions and products include:0

- WiKi-RAV (Attack Surface Management System)
- WiKi-ARMA (Web Application Firewall)
- And the ability to develop custom solutions or products tailored to your requirements

Cybersecurity R&D Service

Organizations consider cybersecurity for various reasons, which can be categorized broadly into four drivers:

- Security Threat: Internal or external hacking threats, attacks
- Compliance: Legal and regulatory requirements an organization must comply with
- Business Requirements: Essential information security requirements for the organization's business
- Business Opportunities: Requirements necessary for enhancing competitiveness or expanding the business

These reasons each bring about different security requirements, and to address these requirements, an organization might need solutions that not only encompass technical elements but also management and operational aspects, or even solutions specifically customized to unique situations.

Our Cybersecurity R&D services aim to address these tailored issues within your organization. Depending on your organization’s requirements, this can take the form of technical security solutions or a combination of technology and management operations.

Our ongoing and available cybersecurity R&D services include:

- WiKi-Bug@ndAll (Bug Bounty Platform)
- A free website provided to security engineers around the world (for threat and vulnerability information)
- And options to collaborate on custom cybersecurity research and development initiatives that cater specifically to your needs.

CONSULTING SERVICE

Information Security Strategy Consulting Services

Many clients facing a variety of information security issues such as hacking, internal data breaches, personal data leaks, and compliance with regulations, often lack strategic planning and resort to ad hoc solutions for immediate issues. However, information security management is one of the critical functions that deserve recognition for its efforts and achievements. By accurately assessing the current state and establishing a strategic plan, which is to get approval via management, clients can systematically respond to the diversifying internal and external threats and maintain robust information security without faltering.

- **Objectives:**
  Analyze the current information security status of clients (national, corporate, institutional) to set cybersecurity goals, and establish short-term, mid-term, and long-term information security strategies and implementation plans to achieve these goals.

- **Scope:**
  According to the client's external compliance environment, information security is classified into managerial, technical, and physical domains, setting its scope accordingly.

- **Expected Outcomes:**
  - You can accurately understand the issues of information security risks they vaguely perceive from both quantitative and qualitative perspectives.
  - You can establish information security goals and models reflecting their organizational capabilities and environmental uniqueness.
  - You can obtain strategies and plans for short-term, mid-term, and long-term improvements, tasks, and budgets needed to achieve the targeted information security levels.

- **Distinctiveness:**
  - To understand the current status, our proprietary methodology allows not only the assessment of AS-IS but also AS-WAS, systematically grasping the clients' capabilities and conditions.
  - Utilizing our wide range of cases and know-how, we design an optimized TO-BE tailored to the client's environmental conditions and organizational capabilities.

CONSULTING SERVICE

ISO/IEC 27001 Certification Readiness Consulting Services

Government agencies and companies in need of external business credibility are increasingly requiring assurance of the reliability of their information security management. Especially for organizations that engage frequently with overseas partners, securing business credibility with partners by having the completeness of their information security management systems verified and certified by a third-party certification body is crucial. ISO/IEC 27001 is a prominent information security management system, and various ISO/IEC 27000 series standards exist, depending on the organization's objectives and scope.

- **Objectives:**
  Establish and operate your organization's Information Security Management System (ISMS) based on the ISO/IEC 27000 series as the primary target model, and secure certification by having its status verified by a certification audit body.

- **Scope:**
  Based on the core business provided by your organization, select the organizational, physical, technical, and managerial scope that needs to be protected and proceed accordingly.

- **Expected Outcomes:**
  - By securing the internationally recognized ISO/IEC 27000 certification, your organization can establish external business credibility.
  - By securing a management system that can flexibly respond to the information security risks that your organization faces or will face, you can operate and manage a robust level of organizational information security.
  - By undergoing risk management status audits annually from a certification audit body, continuous opportunities for security system management improvements can be secured.

- **Distinctiveness:**
  - Several employees hold the ISO/IEC 27001 Lead Auditor certification, enabling the accurate design of ISO/IEC 27001 requirements and implementation plans based on systematic consulting methodology.
  - Our company maintains a close network with ISO/IEC 27001 certification audit bodies and auditors, allowing for effective preparation for the certification audit.
  - Based on years of experience in certification preparation consulting services, we guarantee 100% success in obtaining certification for our clients, and in case of failure, we offer free consulting services until certification is achieved.

CONSULTING SERVICE

Penetration Testing Service

The causes of security vulnerabilities in systems or applications are generally categorized into three main areas: insecure system design, insecure program development, and operational errors. One of the effective methods for identifying these causes of security vulnerabilities in advance is through Penetration Testing, which is performed from an attacker's perspective (also known as "Ethical hacking"). Penetration Testing is particularly effective in uncovering security vulnerabilities that need urgent action and can also identify vulnerabilities arising from issues with business logic that are difficult to detect through White-box Testing. Our white-hat hackers, armed with years of Penetration Testing experience and numerous Bug Bounty achievements, provide Penetration Testing services to you.

- **Objectives:**
  - To test the possibility of internal and external attacker penetration into the target system or service, identify security vulnerabilities that need urgent action, and strengthen security by taking appropriate measures.
  - In some cases, it is used to test the defense system against internal and external penetration into the system or service you provide.

- **Target and Scope:**
  The targets for Penetration Testing such as Wired or Wireless Networks, Servers, Web/WAS, Middleware, Applications, Mobile Apps, SCADA, ICS, PLC, etc., are determined in consultation and agreement with you, and the scope is determined through prior consultation.

- **Expected Outcomes:**
  - Gain insights into security vulnerabilities from an attacker's perspective in the target system or service, and identify vulnerabilities that need urgent action.
  - Receive comprehensive technical recommendations for effectively addressing identified security vulnerabilities based on various best practices and solution.
  - Depending on the objective, you can also identify issues with your organization's defense system against attacks from unauthorized internal and external parties.

- **Distinctiveness:**
  Penetration Testing is divided into Internal, External and Privileged Internal Penetration Testing depending on its purpose, and can be negotiated in various ways depending on the target, including:
  - Network Penetration Testing
  - Application, Mobile App Penetration Testing
  - SCADA, ICS Penetration Testing
  - Social Engineering Penetration Testing
  - Penetration Testing for Specific Topics

CONSULTING SERVICE

Vulnerability Testing Service

Security testing is typically classified into Black-box Testing, Gray-box Testing, and White-box Testing based on the approach. While Penetration Testing falls under Black-box Testing, Vulnerability Testing is aligned with the Gray-box Testing approach. This means that the testing is performed with a certain level of access or authorization, such as a logged-in user account or network access, to the target system or service. Vulnerability Testing utilizes standardized security inspection items according to the type of target system for in-depth diagnosis of vulnerabilities. For instance, if the target system is an Application or Mobile App, OWASP Top 10 and Mobile Top 10 are applied. Server OS, Web, WAS, DBMS, API, Container (Docker), Kubernetes, etc., are also tested for configuration vulnerabilities, security patch statuses, etc., using globally recognized inspection items.

- **Objectives:**
  The purpose of Vulnerability Testing is to identify and address detailed security vulnerabilities in the target system or service to enhance security.

- **Target and Scope:**
  The testing targets are diverse and include the following:
  - OS: Unix, Linux, Windows, AIX, HP-UX, Solaris, FreeBSD, etc.
  - Web/WAS Server: Apache, Tomcat, Nginx, IIS, WebLogic, WebSphere, Lighttpd, Jigsaw, etc.
  - DBMS: Oracle, SQL Server, DB2, PostgreSQL, MariaDB, MySQL, etc.
  - Network Device: Switch, Router, etc.
  - Security System: Network Firewall, WAF, VPN, etc.
  - Others: Container (Docker), Kubernetes, TP-Monitor, etc.

- **Expected Outcomes:**
  You will be able to identify all security vulnerabilities that exist in the target system and receive guidance on how to address these vulnerabilities.

- **Distinctiveness:**
  - Our service is performed systematically using methodologies and automation tools that our company possesses, making it possible to discover security vulnerabilities in a large number of systems or services in a short period.
  - Addressing security vulnerabilities can vary depending on the system's functionality and environment; our service provides various solutions based on years of experience and case information.

Application Source Code Vulnerability Testing Service

Typically, security vulnerability diagnosis in applications is divided into dynamic diagnosis and static diagnosis according to the method. Dynamic diagnosis involves inspecting an application while it is running, which falls under the previously mentioned Vulnerability Testing Service. Static diagnosis involves inspecting the source code of an application line by line to check for security vulnerabilities. For this reason, it is necessary to provide the source code of the target application to perform the inspection. As the size of the application's source code is generally large, automated tools are used for the inspection. The reliability of these tools and the engineer's ability to interpret the results to identify false positives are critical.

- **Objectives:**
  The goal is to conduct a detailed security inspection down to the line level of the Application's Source Code, to find all security vulnerabilities within the application, and to take measures against the discovered vulnerabilities.

- **Target and Scope:**
  Depending on the form of the application, it can be divided into Web Application, Mobile Application, and Client/Server Application. To perform an inspection, the source code of the target application must be provided.

- **Expected Outcomes:**
  - Identifies detailed security vulnerabilities in the Application Source Code.
  - Provides effective methods tailored to the application's functions and environment to address the discovered security vulnerabilities.

- **Distinctiveness:**
  - As automated tools are used to identify security vulnerabilities in application source code, it is essential to use tools that have been verified in the market. Our inspection tools are globally recognized for their reliability.
  - Despite using verified tools, false positives can occur due to the limitations of static analysis of source code. Therefore, we provide high-level engineers capable of efficiently identifying false positives from the results produced by automated tools.
  - Addressing security vulnerabilities can vary depending on the application's functionality and environment. Our specialized engineers, with years of experience, guide clients in implementing effective solutions.

Open-Source License and Vulnerability Check Service

The widespread damage caused by the Log4j vulnerability in Apache has been a shocking event for IT professionals worldwide, highlighting that many products use open-source software without adequately managing or understanding the open-source components they rely on. Consequently, the US federal government, among others, is mandating the submission of Software Bills of Materials (SBOM) for software deliveries and calling for systematic management of widely used open-source components. Organizations need to check and continuously manage open-source licenses for compliance and known security vulnerabilities (CVEs) in the software they are operating or developing. Through our service, you can identify which open-source components are being used and verify the existence of associated security vulnerabilities.

- **Objectives:**
  Identify licenses and known security vulnerabilities (CVEs) of open-source components used in your organization's software, and create an SBOM to comply with legal requirements and prevent attacks exploiting these vulnerabilities.

- **Target and Scope:**
  - Investigate open-source packages used in the software to be checked and identify their licenses and known security vulnerabilities (CVEs).
  - Generate SBOMs for software based on open-source usage in formats such as SPDX, CycloneDX, Xlsx, or JSON, according to organizational policy.

- **Expected Outcomes:**
  - Gain detailed insights into the version, license, dependencies, copyright, and known security vulnerabilities (CVEs) of open-source packages used in your organization's software.
  - Secure the necessary documentation to comply with open-source related compliance requirements.

- **Distinctiveness:**
  - Utilize globally verified automation tools to provide detailed information about open-source components.
  - Offer flexibility by generating SBOMs in various formats based on your organization's policy through a single process.
  - Upon request, we can provide validation services for the SBOMs that you already have.

WiKi-RAV (Attack Surface Management System)

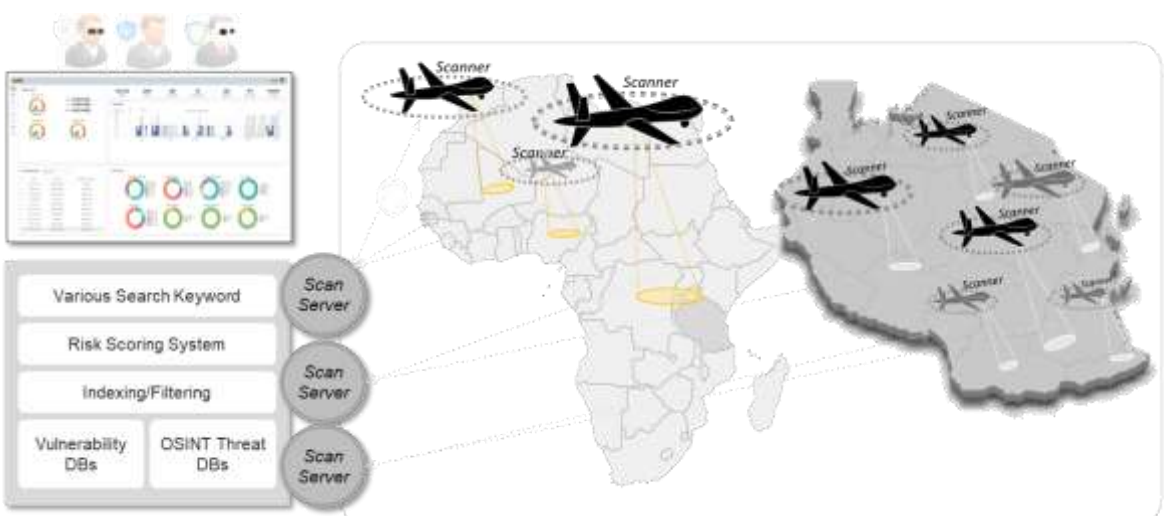
If you work in an organization like CSIRT, ISP/IXP, SOC, NOC which manages extensive networks and services, it is a daunting task to proactively prevent security vulnerabilities that occur from a multitude of IP devices. Especially when security vulnerabilities that have a widespread impact, such as the recently disclosed multiple vulnerabilities in Apache Web Server, are revealed, it's vital to quickly identify how severe the vulnerabilities are on which IP devices and deploy countermeasures. In addition, the frequent creation, deletion, and alteration of systems due to the increased use of cloud networks add to the burden of security professionals.
In the fast-changing ICT environment with various types of threats, externally exposed information systems are highly attractive targets for attackers. Monitoring these exposed systems for vulnerabilities and taking pre-emptive measures before they can be exploited by attackers is an essential part of Threat Hunting and a necessary task for security professionals.
WiKi-RAV, like a reconnaissance drone on a battlefield, uses the latest security vulnerability database and OSINT Threat Database to constantly scan an extensive range of network bands, and provides security professionals with various features such as over 60 keyword-based search functions to understand detailed situations for specific types of equipment or bands.

- Introduction: https://www.youtube.com/watch?v=kE94jeUKbJs
- User Manual: https://www.youtube.com/playlist?list=PLm3FFkiZ2YJ4iEBbCi-Xu7dHWgv10n6PE

- **Key Features:**
  - Continuous scanning of security vulnerabilities and threats across wide-band networks:
    Scan clients located in multiple places will automatically and continuously scan for security vulnerabilities and OSINT threats on all IP devices in the wide network bands you manage.
  - Daily updates of the latest vulnerability and OSINT threat databases:
    WiKi-RAV updates known security vulnerabilities(CVE) and OSINT Threat Databases daily to utilize the latest information.
  - Quantitative Risk Score System:
    The system applies a CVSS (Common Vulnerability Scoring System)-based risk scoring system to help users understand the level of security vulnerabilities and threats across wide network bands at a glance.
  - Enhanced user authentication and access control:
    WiKi-RAV provides accessibility from anywhere at any time through a web interface, but access is restricted to authorized users with strengthened authentication using OTP. User access permissions can be set by the system administrator on a menu-by-menu basis.

- **Target Customers:**
- CSIRT (Computer Security Incident Response Team) is responsible for the information security of extensive networks.
- Corporate SOC (Security Operations Center) serving a large range of network bands.
- Information security-dedicated organizations of companies providing ISP/IXP services for numerous network bands.
- NOC (Network Operations Center) operating a large number of IoT devices, such as Smart City.

- **Distinctiveness:**
- Customized service provision in cloud form or On-Premise form.
- Simplified Scoring System providing quantitative levels of vulnerability.
- Customization services available according to your requirements.
- Provision of basic training programs necessary for system operation.



WiKi-ARMA (Web Application Firewall)

In the age of escalating cyber threats, organizations must take active measures to protect their web applications from malicious attacks. While traditional network firewalls have been adept at detecting and thwarting network-level attacks, they often fall short of countering web-specific assaults effectively. Understanding this critical gap, WiKi-ARMA introduces an advanced Web Application Firewall (WAF) solution that stands as an indispensable line of defense for securing web services against an array of malicious activities including Bot attacks, Injections, and Application Level DoS attacks. By providing comprehensive protection from malicious and suspicious web traffic, WiKi-ARMA WAF enables the implementation and monitoring of security rules such as IP blocking, HTTP Header checks, URI string filtering, and more, to combat the OWASP Top 10 security vulnerabilities efficiently.

- **Key Features:**

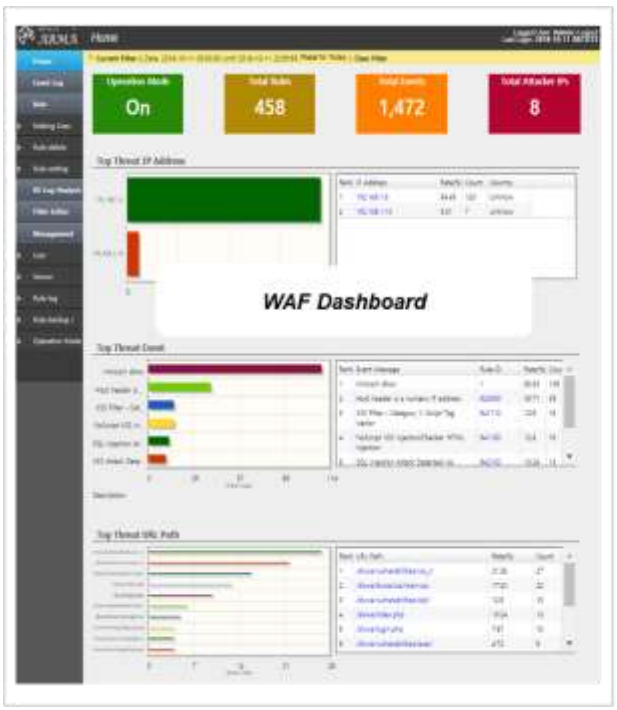
- Informative Dashboard:
  WiKi-ARMA offers an intuitive dashboard that efficiently consolidates and presents crucial data such as the Top 10 Attacker's IP addresses, URLs, and Events. This at-a-glance view of summarized information empowers users to effortlessly monitor and analyze data that requires meticulous attention.
- Intuitive Ruleset Management:
  To address the ever-evolving nature of web application attacks, WiKi-ARMA incorporates a Ruleset Management feature. Through this intuitive interface, users can effortlessly configure and modify detection and blocking rulesets, providing a flexible and adaptive security posture.

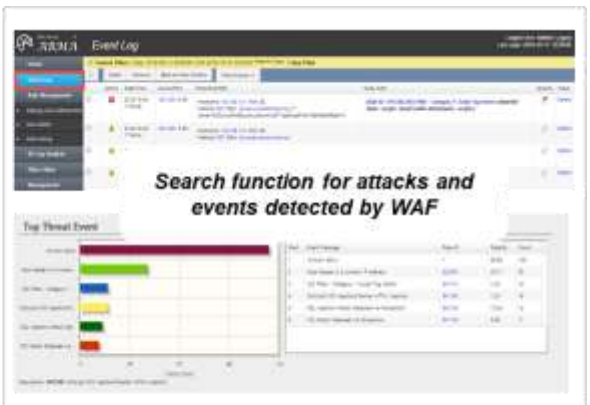
- **Target Customers:**

- Web Application Security Personnel
- Information Security Officers

- **Distinctiveness:**

- Pre-emptive Web Application Vulnerability Testing
  Unlike conventional WAF solutions, WiKi-ARMA takes a proactive stance by conducting Web Application Vulnerability Testing before the WAF installation. This preemptive measure ensures that the target application is free of known security vulnerabilities before deploying the WAF, thus, enhancing the security stance.
- Optimized Ruleset Configuration
  WiKi-ARMA leverages the data obtained through pre-emptive vulnerability testing to identify any peculiarities that should be applied as WAF rulesets. Consequently, this information is used to define and implement a set of rules that are specifically optimized for the target application's functionality and security vulnerabilities.





CYBERSECURITY R&D SERVICE

WiKi-Bug@ndAll (Bug Bounty Platform)

In the digital age, cybersecurity is paramount. Major global entities, such as Google, Meta, Microsoft, and Apple, have long acknowledged the importance of proactive measures in protecting their assets. WiKi-Bug@ndAll, our Bug Bounty Platform, is an integral part of our R&D services aimed at bolstering cybersecurity worldwide. Bug Bounty, also known as the Vulnerability Reward Program (VRP), is a crowdsourced security initiative that rewards security researchers for discovering and reporting vulnerabilities in services, IT infrastructures, and software. It's a win-win situation; companies safeguard their products, while security engineers earn rewards and recognition, honing their skills. The U.S. Department of Defense, among other organizations, adopted Bug Bounty Programs, reaping economic and technological benefits by uncovering critical security vulnerabilities. Following suit, the U.S. federal government mandates a Vulnerability Disclosure Policy (VDP) across all government agencies. Many developed countries, including Republic of Korea, operate governmental Bug Bounty Programs, embracing strategies that protect national software and services while nurturing cybersecurity talent.
Our Bug Bounty Platform, WiKi-Bug@ndAll, is currently being developed in collaboration with UAUR University in Rwanda. It is tailored to Rwanda's cybersecurity environment, designed to cultivate white-hat hackers and discover and protect national security vulnerabilities. Notably, the platform can operate multiple Bug Bounty Programs concurrently and serves as an intermediary, providing a community channel for security engineers and companies or organizations, enabling swift security measures.

- **Key Features:**

1. Security Engineer Web Interface:
- OTP authentication for participating security engineers.
- Guidelines and rules for each Bug Bounty Program.
- Hall of Fame to encourage participation.

2. Administrator Dashboard:
- Chatting Channel to quickly analyze the authenticity of reported vulnerabilities and provide feedback
- Overview of participating security engineers, reported vulnerability types, and more.
- Store and manage vulnerability information and security engineer data.

3. Vulnerability Reporting & Artifacts Storage:
- Systematic and secure storage management of structured and unstructured data in reports.
- Safe processing and indexed storage of video files submitted by security engineers, including virus scanning.
- Fast search functionality for stored files.

4. Verification of Reported Vulnerabilities:
- Automatic handling of irrelevant reports, violating program rules, or duplicates.

5. Evaluation & Reward System:
- An evaluation system to assess the severity of new vulnerabilities using international standards such as CVSS and decide appropriate rewards.

- **Target Customers:**
- Organizations planning to operate Bug Bounty Programs at a national level (e.g., National CSIRT).
- Companies or institutions looking to operate their Bug Bounty Programs.

- **Our Edge:**

1. ML and DL-Based Automation:
- Minimizing human errors by automating operations using Machine Learning and Deep Learning technologies.

2. Technology Transfer:
- Leverage our years of experience and expertise, having technically supported the South Korean government's Bug Bounty Program through KISA (Korea Internet & Security Agency).

3. Dedicated Technical Support:
- Our technical support ensures seamless communication among stakeholders and effective operation of the Bug Bounty Platform, including the evaluation system.

WiKi-Bug@ndAll is at the forefront of cybersecurity solutions. With our Bug Bounty Platform, organizations can proactively protect their assets and foster a culture of cybersecurity. Partner with us for an impenetrable and secure digital future.

CYBERSECURITY R&D SERVICE

Miscellaneous R&D

WiKi Security R&D Center is thrilled to introduce our web services for security engineers across the globe. Through our free services, we aim to fortify the cybersecurity landscape by leveraging our Research and Development experience. Our web services are designed to address the blind spots in global cybersecurity and are made accessible to everyone without any restrictions.

1. Black IP Address Search (https://threat.wikisecurity.net)
In the era of heightened cybersecurity threats, staying vigilant of your organization's IP Address status is paramount. Our Black IP Address Search is the perfect tool for those responsible for information security within an organization.

- **Key Features:**
- Comprehensive Database Search:
  Simply enter an IP address and our web service will scour through over 6 million global Blacklist Databases to check whether the entered IP Address is blacklisted.
- Daily Updates:
  Our service utilizes the extensive FireHOL Database, which is constantly updated to maintain accuracy and timeliness.
- Multi-Categorized Database:
  The Blacklist Database is categorized into 7 types (abuse, malware, anonymizers, spam, organizations, attacks and reputation) and is contributed to by around 300 providers daily.

2. Known Security Vulnerability Search (https://vul.wikisecurity.net)
Whether you are a security engineer participating in a Bug Bounty Program or managing security vulnerabilities within an organization, our Known Security Vulnerability Search service is indispensable.

- **Key Features:**
- Instantaneous Vulnerability Information:
  Input the name of a specific package or application, and our web service will retrieve security vulnerability information related to your query from a database of over 2 million known vulnerabilities.
- Reliable Sources:
  Our database integrates information from MITRE's CVE vulnerability database, Exploit-DB, and Packet Storm, providing you with credible and up-to-date data.

3. Contributions to Bug Bounty
As a dedicated information security organization in Republic of Korea, KISA (Korea Internet & Security Agency) operates a Bug Bounty Platform targeting private companies. Since 2019, our company has been annually contracted to provide technical support for this platform. We analyze and evaluate newly reported security vulnerabilities, contributing significantly to cyber security.

In addition, we actively participate in enhancing cyber security by reporting new security vulnerabilities to KISA, such as:

- 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)

Our commitment to these efforts reflects our dedication to social responsibility in strengthening cybersecurity.

PATENTS, CERTIFICATIONS AND CONTRIBUTIONS

The field of cybersecurity demands relentless technological development and a spirit of challenge to provide the best service to customers. WIiKi Security Corporation is dedicated to illuminating the blind spots of global cybersecurity through continuous research, development, and exploration.

Ongoing Research, Development, and Patenting

Our company holds the following patents in the cybersecurity sector and is constantly enhancing our technological competitiveness and barriers through ongoing research and development. We are actively identifying and pursuing new patent opportunities to maintain our edge in the industry.

- No. 10-1259897: Apparatus for Efficient Remote Security Threat Diagnosis and Its Method
- No. 10-0628296: Method for Analyzing Network Attack Situation

Government Recognition for Technological Innovation and Venture Spirit

We have received several certifications from the Korean government, acknowledging our expertise and technology in cybersecurity. These include the INNO-Biz Certificate for technological innovation, the Certificate of Venture Business, and the Certificate of WiKi Security R&D Center, along with recognition as a Hidden Champion SME.

- INNO-Biz Certificate (No. 230102-01078): Technology Innovation-Oriented SME (Ministry of SMEs and Startups Republic of Korea)
- Certificate of Venture Business (No. 20230517020007): KIBO Technology Fund Republic of Korea
- Certificate of Industrial R&D Center (No. 2011112773): Ministry of Science and ICT of the Republic of Korea

Social Contributions for Vulnerable Groups and the Next Generation

We are registered supporters of the global NGO World Vision, participating in child sponsorship for over a decade. We have also established academic-industry collaborations with institutions like Seoul Women's University, Suwon University, and Polytechnic High School, contributing to the training of the next generation of professionals.

- Over 10 years of sponsorship as a World Vision child support company
- Academic-industry Collaborations for next-generation talent development with domestic high schools and universities: Seoul Women's University, Suwon University, Daeduk College, Hanyang Women's University, Incheon Information Industry High School, Incheon Meister High School
- International Academic-industry Collaborations: UARA(United Africa University of Rwanda) in African Rwanda, Gloders College in the Philippines

OUR CUSTOMERS

Over the years, our company has built a rich heritage in the cybersecurity arena by acting as a steadfast partner to a broad spectrum of industries. We pride ourselves on navigating through their challenges and architecting tailored solutions.

A Special Focus on High-Stakes Industries

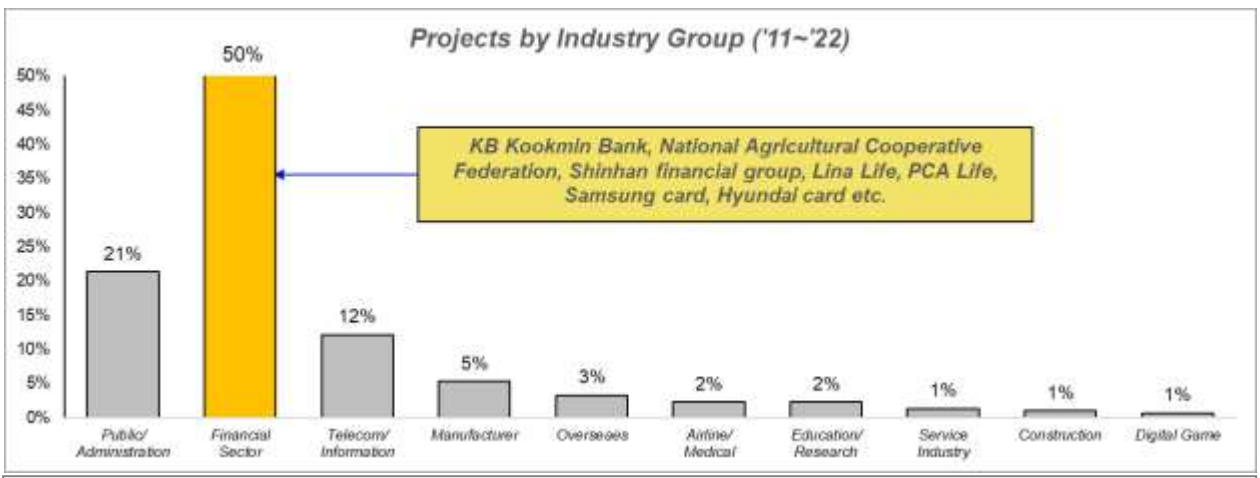
Our clientele is especially prevalent among sectors where the bar for cybersecurity is set exceedingly high, such as financial institutions and public/government entities. These discerning clients are not just any organizations; they are pacesetters within their respective domains.

Trusted by Industry Leaders

Our patrons include illustrious companies and agencies that wield significant influence and lead by example in their industries. The continuous stream of business inquiries and engagements from these clients is a testament to the unwavering confidence they place in our expertise and integrity.

Commitment Meets Excellence

Our customer portfolio serves as a badge of honor that inspires us to relentlessly pursue excellence. Our commitment is our currency, and it's the reason industry vanguards do not merely make our acquaintance – they build lasting alliances with us.



In this rapidly evolving digital landscape, align your organization with a partner that's been tried and tested by the best in the business. Trust us, as they do, to fortify your cybersecurity infrastructure and safeguard your digital assets.

Join the leaders. Secure your future with us.

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