RSAConference 2022

KORRA PAVILION

San Francisco, Moscone center

Jun. 6–9, 2022

About Korea Trade-Investment Promotion Agency (KOTRA)

Agency established to contribute to the development of the national economy by performing work such as trade promotion, investment between domestic and foreign companies and support of industrial technology cooperation etc.

Main functions and roles

- Expanding medium and small-size enterprises' business in overseas markets
- Supporting small-sized enterprises (SME) to extend their business abroad
- Overseas market information production, spread and consulting
- Attract foreign investment
- SME Global Business Training and attracting foreign professionals
- Improving national brand, supporting international development cooperation, supporting munitions trade

Organization

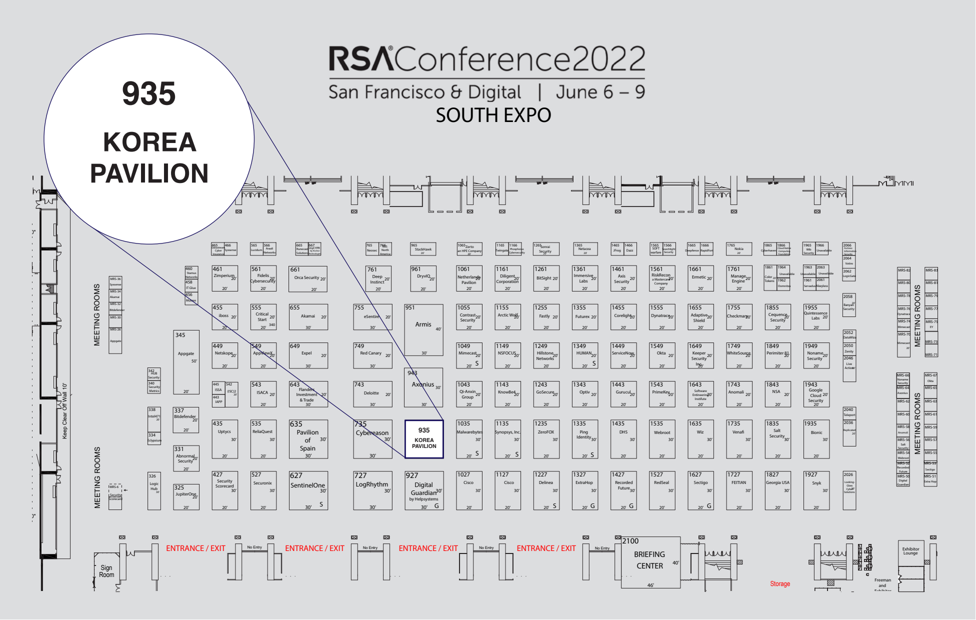
- Performing projects accepted by the government
- Headquarters: 6 headquarters 33 departments 3 centers
- Overseas: 10 regional headquarters, 127 Overseas Trade Centers (84 countries)
- Korea: 12 KOTRA support Center, 1 Airport office

KOTRA History

1962	KOTRA Established in accordance with Korea Trade Promotion Agency Act
1995	Changed its name into Korea Trade-Investment Promotion Agency
1998	Newly established Support Center for Foreign Investment
2004	Awarded WTO/ITC World's Best Trade-Investment Promotion Agency Award
2006	Constructed IKP(Invest Korea Plaza) building
2012	the 50th anniversary of KOTRA
2016	Global Business Research Center(GBRC) Opening Ceremony
2020	Online Business Matchmaking
2022	the 60th anniversary of KOTRA

About Korea Information Security Industry Association (KISIA)

KISIA, founded in 1998, is a nonprofit organization designed to foster the Korean cyber and physical security industry. We represent Korean security companies and maintain a close relationship with them.
With over 250 member companies, KISIA is aimed at the growth of the infrastructure of the security industry in Korea. As a specialized and professional body in the private sector, we listen attentively to the voice of the industry and create the optimized ecosystem for the businesses.
Besides, we provide the Korean information security industry with support for global market entry. Organizing overseas business meetings and exhibitions, we encourage domestic companies to gain better chances not only to discover foreign business partners, also develop international trade with many other countries. Furthermore, we make consistent contributions to improvement of national policy by communicating closely with the government and producing the research reports on the information security field in Korea. KISIA seeks to create a concerted approach among companies, governments and organizations across the world for the comprehensive development of the security communities.



AI Spera

AI Spera

COMPANY OVERVIEW

Name	OkHee Jun
Title	Marketing and Project Manager
Department	Public Relations Department
Company Address	7, Yeonmujang 5ga-gil, Seongdong-gu, Seoul, 04782, Republic of Korea
Phone	+82-10-3255-5662
E-mail	tianyumi@aispera.com
Website	www.aispera.com

ABOUT COMPANY

AI Spera, a frontrunner in cyber threat intelligence, was founded at the Hacking Response Research Center, Korea University. Our data-driven security solutions are principally based on anomaly-behavior detection combined with AI and machine learning technology. Dedicated to ensuring ongoing visibility, we effectively manage assets that are scattered across the attack surface in order to safeguard them from attackers. The more sophisticated methods of attackers become, the harder we strive to contain threats lurking in the cyberspace.

MAIN PRODUCTS

· **RMR**

Our foremost flagship product RMR(Risk Management Report) is a SaaS-based enterprise Attack Surface Management solution powered by AI and machine learning. Securing clear visibility into enterprise IT assets on the attack surface, its simple integration gives you the most exhaustive data feeds that cover all the externally exposed digital assets and vulnerabilities within.

· **Prime Use Cases**

1. Detection of new vulnerabilities
2. Closure of dangerous ports left wide open
3. Discovery of new corporate assets

· **Integration with Criminal IP**

Paired with our advanced Criminal IP, a Cyber Threat Intelligence search engine, conduct a more deeply contextualized search of the assets already identified through RMR and receive enriched threat intelligence via API integration.

DIFFERENTIATION

1. Streamlined security control

Automatically generated threat report alleviates the burden compounded by outdated security control infrastructure

2. Coverage of threat data

4.2 billion IP addresses, domains, ports, and all types of internet-facing information are refreshed and streamed around the clock

3. Easy accessibility via web-interface

Adoption requires only one primary domain address of assets in operation

REFERENCE CUSTOMERS and KEY PERFORMANCE

· **Performance Milestones**

- Korean Natural Language Processing Analysis (Recorded Future, 2020-2021)
- RMR selected as one of the products included in the “Security Solution Supply Pool”(Korea Internet &Security Agency, 2021)
- AI Security Analysis System – Implementation of Criminal IP to monitor malicious IPs for a leading Korean information technology company (KT ds, 2020)
- Fraud Prevention Algorithm/Consignment Research – Integration of Criminal IP with Korean cryptocurrency exchange giant Upbit (Dunamu, 2019-2020)
- Cyber Threat Intelligence Information – Implementation of Criminal IP to detect malicious users and bots for game operators (Netmarble, 2018-2020)
- Provision of Criminal IP Academic License for incorporation into the university curricula (Korea University, 2020)

CERTIFICATIONS

· U.S. patent filed for “IP-based security management methods, devices, and computer programs”, “Device and method for recognizing the behavior of a person in a video”

· Korean patent registered for “Malicious domain classification method and program based on AI technology”, “Devices, methods, and programs that provide information related to the distribution of illegal content in a P2P network”

· 2019 ISO-9001 Quality Management Certificate (obtained for CRIP development process)

EYL

COMPANY OVERVIEW

Name	Junghyun Baik
Title	Chief Marketing Manager
Department	Marketing Dept.
Company Address	#401, 52, Singu-ro, Ciheung-gu, Yongin-si, Gyeonggi-do, 16971, Republic of Korea
Phone	+82-10-3168-1418
E-mail	jhbaik@eylpartners.com
Website	www.eylpartners.com

ABOUT COMPANY

Pseudo random number generators are vulnerable to hacking because they tend to have a predictable pattern hackers can exploit. The weak entropy problem is compounded for FinTech & IoT devices with limited access to physical random events such as mouse movement. EYL provides Quantum random number generator that extracts randomness from radioactive isotope put in the very tiny chip(2mm) in order to generate perfect encryption keys. EYL is the Diamond Winner of MassChallenge Boston last year among 2,600 startups from 80 countries.

MAIN PRODUCTS

· **Quantum entropy chip**

- enables us to harvest ultimate randomness from nature using radioactive isotope decay
- Can dramatically improve security of all IoT devices because they can provide more secure encryption powered by quantum entropy chip

· **Quantum random number generator**

- USB, modular, PCI-Express type of quantum random number generators with varying speeds and user interface to meet the customer needs using Quantum entropy chip

· **Quantum Shieldz® Cipher™**

- is a self-sufficient voice encryption device that works with your personal smartphone.
- It uses an encryption key generated by a quantum random number generator (QRNG) to securely encrypt the user’s voice, completely blocking eavesdropping or unwanted recording through spyware.

DIFFERENTIATION

- ·Can be deployed on any kinds of IoT devices since it is very small(2mm) and affordable
- ·Post processing is not needed to meet the NIST requirements because it provides ultimate randomness
- ·Compare to competitor’s quantum random number generator, EYL’s products are 3 others of magnitude smaller and cheaper
- ·Other companies commercialized quantum random number generator using optical methods that provide quantum entropy at high speed, but they are prohibitively expensive and bulky.

REFERENCE CUSTOMERS and KEY PERFORMANCE

· **Customer**

- Government security agency (no-name country)
- Several private enterprises

· **Awards**

- “Diamond winner” of MassChallenge 2016 Boston
- Selected as Disrupt100 company MISP, IoT Security competition “Top Award”

CERTIFICATIONS

- ·NIST CMVP (as an Entropy Source)

F1Security

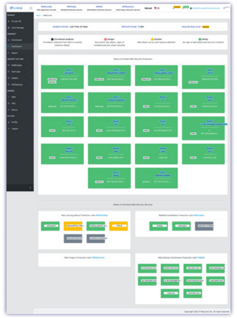
COMPANY OVERVIEW

Name	Hwang dong-hwa
Title	Developer
Department	DevOps Dept.
Company Address	#1402, 234, Beotkkot-ro, Geumcheon-gu, Seoul, 08513 Republic of Korea
Phone	+82-10-9759-6428
E-mail	hdh@f1security.co.kr
Website	www.uwss.us www.f1security.co.kr/English

ABOUT COMPANY

F1 Security provides web security solutions developed by industry consulting experts in cyber security. We have a family of web-based solutions that contribute to building a more secure web environment from hacking through web application firewalls, web shell detection solutions, and web shell scanners. Our solution has many practical use cases in Government, enterprises s , SMEs, and MSSPs.

MAIN PRODUCTS



F1Security develops and services four types of web security products.
All production is Software-Based.

·WebCastle (Web Application Firewall)

-Support to cloud environment and existing network infra

-Support to centralized management system

· WSFinder (Anti-WebShell)

-WebShell detection/response solution

-support to the centralized management system

·WMDS (Website Malware Detection System)

-detecting malicious code link distributed via websites

-140,000+ detection patterns

·UWSS(Unified Web Security Service)

-On-premise & Cloud-Based SECaaS type service

-includes products from WebCastle, WSFinder, and WMDS

DIFFERENTIATION

·F1Security is applying the web security technology learned through consulting services to the solution.

-holds a total of 30 intellectual property patents relating to web security.

-The patent also includes U.S. intellectual property rights relating to "Method and System for Detecting structured Malicious Code Using Process Behavior Prediction Technique."

-In addition, holds patents on artificial intelligence methodologies for the detection of webshell and website malware distribution.

·F1Security provide all-in-one web security solution with one platform

-support to cloud and existing infrastructure without changing the configuration of customer network.

-Customer can use one platform for centralized management F1Security's solution for all of products.

REFERENCE CUSTOMERS and KEY PERFORMANCE

·Shinsegae-inc (iDC & MSSP)

-Shinsegae-inc is an affiliate of the Shinsegae Group and is an MSSP that provides security services while operating iDC. Shinsegae-inc is providing external services by building F1 Security's UWSS as a dedicated platform.

·CJ O SHOPPING (Enterprise, E-Commerce)

-CJ O Shopping is Korea's first large home shopping channel and uses F1Security's WMDS to monitor whether malware is distributed via its website.

·Maru Internet (web hosting company)

-Maru Internet is a web hosting company and operates a WebCastle(web application firewall) of F1Security to protect its customers' websites.

·Hankook Tire Affiliates (Manufacturing, Smart Factory)

-Used to protect against hacking of web-based MES systems built in cloud environments

CERTIFICATIONS

·Cloud Service Accredited by KACI

·Cloud Quality Performance Test Results (NIPA, TTA)

MONITORAPP

MONITORAPP

COMPANY OVERVIEW

Name	Suna Choi
Title	Global Sales Manager
Department	Global Business
Company Address	9f, 27 Digital – ro 27 ga-gil, Guro-gu, Seoul, 08375, Republic of Korea
Phone	+82 10 5848 7749
E-mail	suna.choi@monitorapp.com
Website	www.monitorapp.com

ABOUT COMPANY

MONITORAPP, Inc., is a cyber-security software and services vendor, currently holding the number one market share in the Korean WAF appliance market.
Founded in 2005, MONITORAPP has spent the last 16 years perfecting cybersecurity solutions. Due to the success with our physical appliances(AIWAF, AISWG, AISVA), we've decided to bring the reliability and stability of their physical security appliances to the flexibility and ease of access of the cloud. In 2016, MONITORAPP launched SECaaS platform AIONCLOUD to provide a full-stack network security service and website protection services on our platform so our clients can enjoy our full range of services on a zero-trust network solution.

MAIN PRODUCTS

- **AIONCLOUD**

AIONCLOUD is an All-in-One SECaaS platform which provides both Website Protection securing web servers and Secure Internet Access protecting users and organizations. AIONCLOUD Website protection is an integrated platform which brings a comprehensive set of advanced security features ensuring a complete web server security. It includes WAF, WMS, DDoS protection and CDN. AIONCLOUD Secure Internet Access is a cloud native SASE (Security Access Service Edge) solution offering a comprehensive Zero Trust approach which includes SWG, CASB, NGFW, ZTNA

- **AIONCLOUD WAF(Web Application Firewall)**

AIONCLOUD WAF is a cloud-delivered application security service providing a comprehensive Web Application and API Protection against the most sophisticated security threats.

- **AIONCLOUD SWG(Secure Web Gateway)**

AIONCLOUD SWG is a network security solution which keeps unauthorized traffic from entering a network. It delivers a safe web experience by offering URL filtering, application access control and threat protection.

- **AIONCLOUD CASB(Cloud Access Security Broker)**

AIONCLOUD CASB is a gatekeeper that allows users and organizations to gain visibility into the cloud Software-as-a-Service (SaaS) applications. It enables users to handle the data in the most secure way and elevates the SaaS usage to new heights by offering control over data and cloud activity, full visibility into all cloud and protection against cloud threats.

DIFFERENTIATION

- MONITORAPP implements AIONCLOUD, Korea's first SASE platform, as its own development technology, and provides security services such as WAF, SWG, and NGFW on the all-in-one cloud-native platform.
- AIONCLOUD is the first security platform in Korea to obtain SaaS edge computing CSAP certification.(Cloud Security Assurance Platform)
- AIONCLOUD provides both 'Website Protection' securing business-critical web servers and 'Secure Internet Access' to protect users and organizations on a single platform.

REFERENCE CUSTOMERS and KEY PERFORMANCE

- Reference – Samsung, LG, Nintendo Korea, SK, KT, Naver Cloud
- Global Corp & Partnership – USA, Japan, Malaysia, India, Thailand, UAE, Sweden.
- #1 Web Application Firewall Market Share in Korea – 30% Increase in Web Application Firewall supply as of 2021 compared to 2020.

CERTIFICATIONS

- 15 Certifications for the last three years (CC, CSAP, GS, KC, FCC, CE)
- 17 Patents

NETAND Co., Ltd

ND HIWARE

CONTACT INFORMATION

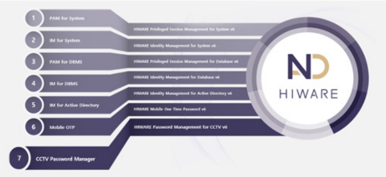
Name	Hyemin Yeon
Title	Senior Marketing Manager
Department	Global Business Development
Company Address	10F, Hanam Bldg, 25, Uisadang-daero 1-gil, Yeongdeungpo-gu, Seoul, 07333, Republic of Korea
Phone	+82-10-9172-0618
E-mail	jenny07@netand.co.kr
Website	www.netand.io

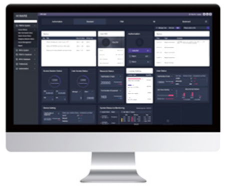
ABOUT COMPANY

NETAND is a Privileged Access Management and Identity Management software vendor. Our solution, HIWARE, helps you strengthen your system security by detecting threats with identity/account management, and protects your data from malicious attacks by restricting and controlling user access. As ID life-cycle management is carried out actively, you can decide on your password policies in detail. With authentication options we provide you, users need to complete set of protection steps to access the information that is restricted to their use, with restricted commands. You can also monitor you users in real-time and through audit reports. HIWARE supports system, database and active directory. Reach out to us to learn more about the functions and details of our product and how we provide you the best PAM solution in the market. It has been 15 years since our company was founded. Internationally we are mostly active in South East Asia and we also have customers in Europe, North America and Latin America. We are the market leader with the biggest market share in South Korea with more than 1,200 customers. Some of our customers are big international companies like Samsung, Hyundai, LG, ING Bank, etc. Currently we are working with Shinhan Bank in Vietnam and Nicepay in Indonesia.

MAIN PRODUCTS

- **HIWARE Privileged Access Management**
  - Privileged Access Management for System
  - Privileged Access Management for Database
- **HIWARE Identity Management**
  - Identity Management for System
  - Identity Management for Database
  - Active Directory
- **HIWARE Multi Factor Authentication**
- **HIWARE Password Management for CCTV**


1 PAM for System
2 IM for System
3 PAM for DBMS
4 IM for DBMS
5 IM for Active Directory
6 Mobile OTP
7 CCTV Password Manager
HIWARE Privileged Session Management for System v6
HIWARE Identity Management for System v6
HIWARE Privileged Session Management for Database v6
HIWARE Identity Management for Database v6
HIWARE Identity Management for Active Directory v6
HIWARE Mobile One Time Password v6
HIWARE Password Management for CCTV v6
ND HIWARE



DIFFERENTIATION

- Our flagship software product, HIWARE provides integrated access and account management solutions in a single user interface. By using HIWARE, customers can manage users conveniently and benefit from efficient customization options.
- HIWARE provides both PAM for System and PAM for DB. Our strongest feature of the solution is PAM for DB, which functions with most databases such as Oracle, MariaDB, Sybase, etc. In addition, there is no limit to the number of users and devices that can stably access our solution. HIWARE is installed in large infrastructure environments with more than 500,000 different types of devices and more than 40,000 users.

REFERENCE CUSTOMERS and KEY PERFORMANCE

- NETAND, a leading vendor in PAM (Privileged Access Management) and IM (Identity Management) vendor, has more than 1200 customers; Finance, Manufacturing, and Telecom are the Top 3 Verticals.
- We export our product, HIWARE, to 11 countries with more than 1,200 domestic customers and engaging actively marketing activities through overseas partnerships of more than 20 countries.

CERTIFICATIONS

- Domestic: patents (22), copyright registration (12), GS certification (11), and CC certification (3)
- International Application: PCT application (2), US Patent and Trademark application (1)

Quad Miners

Quad Miners

COMPANY OVERVIEW

Name	David Kim
Title	Global Sales, Partner Enablement
Department	Sales
Company Address	DREAUM Sunghong Tower 6F, #138 Teheran-ro, Gangnam-gu, Seoul, 06236, Republic of Korea
Phone	82+10-2090-1573
E-mail	david@quadminers.com
Website	www.quadminers.com

ABOUT COMPANY

Quad Miners create network & cloud security solutions that detect and respond to cyber threats. Our technology gives complete visibility to a company's network that enters or exits the environment and all traffic that moves.

MAIN PRODUCTS

"Only those who know the truth can respond."
Network Blackbox a next-generation solution for detecting and responding to threats. Quad Miners provides a solution called the Network Blackbox. This is a next-generation network detection and response solution that records, stores, and analyses all data flows using the Network Blackbox, from the initial point in time when an event begins, to the time that it is completed and even beyond. The Network Blackbox as it applies to network security is similar to the black box concept used in aircraft.
The most notable feature of the Network Blackbox is that it saves and analyses 100% of packets to detect and respond to all types of cyber security threats. The Network Blackbox consists of 1) threat detection using over 50,000 rules, 2) scenario-based user behavior analysis, 3) extraction and analysis of a variety of content (email, search, translation, etc.), 4) Supervised-learning anomaly detection analysis, 5) internal breach detection through "cyber kill chain" monitoring, 6) detection of malware and determination of whether such code has infected the network internally and 7) forensic analysis, collecting and saving all traffic, while also performing full packet-based information analysis.

DIFFERENTIATION

- **Quad Miners' NDR product, Network Blackbox,**
- Collect and analyze all network traffic (S-N/E-W).
- Detects all threats (Known/Unknown, Internal/External) and visualizes them based on MITER ATT&CK Matrix and TTPs.
- Supports various threat detection methods such as threat detection rules, non-rule, and supervised/unsupervised machine learning-based detection.
- Based on Full Packets, it provides sufficient content (why and how it was detected as a threat) for IT personnel to understand.
- Provides detailed evidence for Network Forensics, such as recovering user web screens, extracting attachments to mail, extracting uploaded/downloaded files, and isolating and downloading PCAPs.

REFERENCE CUSTOMERS and KEY PERFORMANCE

- Network Blackbox has been listed in Gartner's NDR report for three consecutive years.
- 35 customers from national defense, tier 1 banks, national infrastructures, global enterprise
- Global Branches in Japan and USA

CERTIFICATIONS

- **International patent application (PCT, United States of America, Japan)**
- A network forensic system and its method using the system (PCT-KR2019-008860)

- **Patent applications in South Korea**
- A high-performance packet stream storage system and its method using the system (10–2080477)
- A pattern-based index processing system and its method using the system (10–2080478)
- A scenario-centered real-time attack detection system and its method using the system (10–2080479)

S2W.Inc

COMPANY OVERVIEW

Name	Ted Suh
Title	Director
Department	Global Business Team
Company Address	3F, 12, Pangyoyeok-ro 192beon-gil, Bundang-gu, Seongnam-si, Gyeonggi-do, 13524, Republic of Korea
Phone	+82-10-9663-0321
E-mail	hm@s2w.inc
Website	www.s2w.inc

ABOUT COMPANY

Safe & Secure World, S2W is a data intelligence company that solves the problems with technology for good. In a data-driven hyper-connected society, we propose solutions that benefit individuals, corporations and society so that everyone's safety is guaranteed and brand value is protected. S2W specialize in cyber threat intelligence, brand/digital abuse detection, and blockchains of illegal virtual assets. We provide customized solutions to customers through technology such as big data and algorithm analysis, blockchain on-chain data analysis, and machine/deep learning.

MAIN PRODUCTS

- **Quaxar**

Quaxar is tailored intelligence specifically designed for the enterprise's optimized operational environment. It features the ability to mount customer CTI-related data within Quaxar to quickly and accurately respond to threats and allows you to monitor a variety of exclusive information by linking external threat information with Quaxar. This helps clients make better decisions for sustainable growth beyond protecting their core assets.

- **Xarvis**

Xarvis is an integrated search engine for deep/dark web, which helps clients comprehensively grasp all the information on the surface web and hidden channels. Through integrated web monitoring, it allows to collect pieces of information related to the case and criminal and derives meaningful intelligence through data refinement and in-depth analy

DIFFERENTIATION

S2W's CTI solution is differentiated by its unique external threat monitoring coverage and high-accuracy risk factor detection based on relationship analysis. It monitors more than 100 digital channels, including social media, blockchain, and Telegram focusing on more than 90 million dark web pages and 1.5 million dark web domains and covers more than 20 risk factors such as source code, assets, API keys, malware, privacy documents, phishing/smishing. It also provides immediate actionable intelligence based on an understanding of the attack group, providing customized response in the event of a threat.

REFERENCE CUSTOMERS and KEY PERFORMANCE

S2W provides cyber threat intelligence solutions to major Korean companies in various industries such as financial, telecommunications, mobility, retail and commerce, games as well as public institutions. (KISA, NSR, etc.) Furthermore, we officially signed contribution agreement with Interpol to have a partnership and supply threat intelligence data to contribute to international cybersecurity. We did a Clop Ransomware arrest operation which provided Interpol with analysis of Clop-related infrastructure information to track its origin, Bitcoin flow analysis and profiling Clop ransomware operations on dark web and Grandcrab&Revil Sodinokibi arrest operation which provided cyber and malware technical expertise to Interpol and its member countries.

CERTIFICATIONS

- Patents: 'Methods and systems for analyzing cryptocurrency transactions', 'Methods, devices and computer programs for providing cybersecurity using knowledge graphs', 'Methods and devices for analyzing cryptocurrency transactions', 'Methods and devices for collecting data in multi-domain'
- Award: 'Dark web/OSINT Solution' Grand Prize at the 'Security Awards Korea 2021'
- Plaque of appreciation: Interpol 2021

SecuLetter

SECULETTER

COMPANY OVERVIEW

Name	Julie Sohn
Title	Manager
Department	Global Business
Company Address	3rd Floor, MELFAS B/D, 255-14, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeongi-do,13494, Republic of Korea
Phone	+82-31-608-8860
E-mail	julie.sohn@seculetter.com
Website	www.seculetter.com

ABOUT COMPANY

SecuLetter is an Advanced File-based (Non-PE) Malware Analysis Expert which provides the proactive security against the advanced cyber threats. With SecuLetter product you can protect internal system from malicious code attacks by blocking malicious contents before reaching to your email and file systems. SecuLetter's all products are based the company's own patent technology, 'Automatized Reverse-Engineering Techniques'.

MAIN PRODUCTS

· **MARS SLE – Advanced Email Security (Server, Cloud Edition)**

MARS SLE is an advanced email security solution protecting corporate system from cyber attacks such as APTs, phishing, malware, ransomware, impersonation attacks inflowed through email.

- Analyze malicious code embedded in file attachments.
- Quarantine and archive malicious email.
- Scan malicious URL which malicious code can be downloadable from the link.
- Provide the malicious code detection result report.

· **MARS SLF – Advanced File Security (Server Edition)**

MARS SLF is a file-based malware protection solution which proactively scan and detect the hidden malicious code in the file transferred from external to internal network.

- Block malicious file transfer to internal network.
- Support unlimited file size scanning.
- Scan malicious content in file storage server.
- Provide malicious code detection result report.

DIFFERENTIATION

· **Proactive Prevention**

Proactively detect and block the malicious content before reaching to your internal systems.

· **Fast and Accurate Diagnosis**

5 times faster than existing sandbox-based solution and provide accurate diagnosis by analyzing assembly level.

· **Neutralize Evasive Malware**

Detect evasive threats which recognize the sandbox environment and does not take any action.

REFERENCE CUSTOMERS and KEY PERFORMANCE

· **USD 2 million Investment from Saudi Arabia (2020.01)**

· **Local partnership across the APAC and middle-east.**

· **Reference Customers**

- KEPCO E&C (Power plant design & engineering) → Block ransomware attacks.
- National Health Insurance Service (South Korea) → Block malicious threats embedded in files uploaded through civil application service.
- Korea Post → Block malicious threats at air-gap environment.
- KT Corporation (Telco) → Launched "Intelligent Threat Email Analysis Solution" in cooperation with KT.
- BNK Busan Bank → Block APT threats invaded through digital documents.

CERTIFICATIONS

· **Patent**

- "Non-PE File Malicious Inspection Method by Memory Analysis and Device"
- "Malicious File Analysis Device and the Method by Using Virtual Environment"

· **ISO 9001 / ISO 14001 / ISO 27001**

Spiceware

COMPANY OVERVIEW

Name	Michelle Park
Title	Director of Global Marketing
Department	Global Business
Company Address	17F, 83 Uisadang-daero, Yeongdeungpo-gu, Seoul, 07325, Republic of Korea
Phone	+82-(0) 502-1930-7274
E-mail	michelle.park@spiceware.io
Website	www.spicewareone.com

ABOUT COMPANY

Established in 2017, Spiceware provides globally certified cloud protection services that safely manage data assets so that businesses can stay ahead of the changing market without losing their data asset competitiveness. The company offers a one-stop cloud security service Spiceware One which is a zero-trust security with PII (Personally Identifiable Information) Protection Service that safely protects companies' data dispersed through various clouds.

MAIN PRODUCTS

Spiceware One is a data-centric security service available as a subscription model designed to fit the growth cycle of all companies, from startups to large enterprises. It is a zero trust network access (ZTNA) security platform that has personal information anonymization and pseudonymization features for data analysis.

·The all-in-one data security platform has the following features:

- Sensitive and Personal Information Detection
- Data Loss Prevention(DLP)
- DDos Defense
- MFA Certification for Users and Devices
- File Encryption and Decription
- Detection of Suspicious User Behavior
- Ransomeware Recovery
- SAML-based SSO Support

Spiceware One
Sensitive/Personal Information Detection
Data Loss Prevention
File encryption/ decryption
DDoS Defense
Detect Suspicious User Behavior
MFA Certification for User and Device
Ransomeware Recovery
SAML-based SSO support

DIFFERENTIATION

·Quick & Easy Installation

Service can be applied instantly, eliminating downtime cost

·Customizable Dashboard

Personalized dashboard provides an overview of information processing activities of the users, notifying the administrators of any abnormal behaviors 24/7

·Zero Installation Cost

Available as SaaS, charged monthly which can be cancelled at any time

REFERENCE CUSTOMERS and KEY PERFORMANCE

Spiceware products are available on AWS marketplace, Naver, SKT, and Seed Marketplace and will expand our reach to Google's GCP and Microsoft Azure in the coming years. In 2020, our product was added as an integral part of LG CNS' next generation SaaS package, and just last year, Tmap Mobility, South Korea's leading mobility platform, became our client and the product is being used to protect their 20 million registered users and 14 million monthly active users.

CERTIFICATIONS

Spiceware One is a CSA & ISO certified privacy protection service for the cloud. We have ISO/IEC 27001, 27017, and 27018 certification as well as CSA STAR and CSAP(Cloud Security Assurance Program) in cloud security.

STEALTH SOLUTION

COMPANY OVERVIEW

Name	Eric Li
Title	CTO
Department	R&D Lab
Company Address	4F, 83, Uisadang-daero, Yeongdeungpo-gu, Seoul, 07325, Republic of Korea
Phone	+82-10-3034-1633
E-mail	info@stealths.co.kr
Website	www.stealthsolution.co.kr

ABOUT COMPANY

Stealth Solution, located in Seoul, South Korea, is a startup that provides an intelligent security platform for a new security paradigm. They help companies invest in security infrastructure continuously, build a cyber-threat response environment and eliminate risk factors. Besides, Stealth Solution actively has responded to cyberattacks by applying next-generation MTD strategies to detect and block malicious attacks.

MAIN PRODUCTS

- **Stealth Moving Target Defense(SMTD)**

  SMTD is based on network host address mutation technology that mutates IP address and PORT number of network host continuously, network deception technology, and network reflection technology so that it makes impossible for attackers to identify the network host from the first attack stage.

DIFFERENTIATION

- **Hide major server address**

  The main server information can be hidden by continuously changing the properties of the attack surface(IP, Port, Protocol, Application, etc.)

- **Secure client communication**

  The client that needs to connect according to the hiding of the server address guarantee a secure communication channel that is similar to VPN communication by creating separate hidden tunneling to continuously track the server address.

- **Hacking Prevention**

  It can effectively defend against attacks in the reconnaissance and detection phases of the cyber kill chain. It is particularly effective to active and passive scanning attacks.

- **Zero Trust**

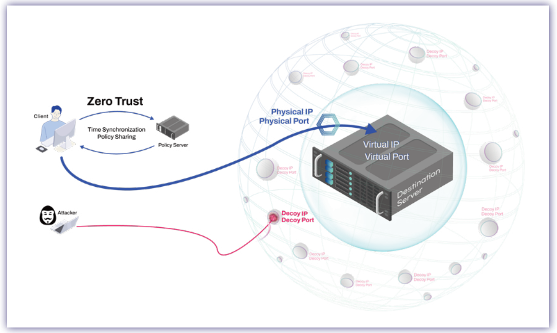
  Block unauthorized client server access and dealing with insider threats through zero trust policy

- **Ensure server stability**

  Adopting a secure gateway method of physical card type, which does not require installation of server agent, ensures server stability and installation of legacy solutions without compromise.

- **Advanced deception system**

  Construction of an advanced deception system that provides improved functions such as behavior analysis and abnormal behavior detection of unauthorized/unauthenticated clients along with network address changing technology.



REFERENCE CUSTOMERS and KEY PERFORMANCE

- Companies might worry about network performance because of the characteristic of SMTD that mutates the server attributes. However, a test shows only 6% of network latency when SMTD runs every second. Also, if you increase the amount of the client, rate of latency decreased.
- The overhead frequency when SMTD runs every second is only 0.04%. In other words, you take only 4 seconds more in the circumstance that you are originally able to download a 10GB file in 100 seconds. Considering that playing SMTD every second is quite unusual in the actual environment, it shows excellent network performance

TRANSFORM

kotra
Korea Trade-Investment
Promotion Agency

kisia
Korea Information Security Industry Association