Profile Status: Published

Technology Offer

Speech Recognition Emergency Bells

Summary

A Korean SME has engaged in the industry of speech recognition services and emergency divisions. The rate of crimes against women has risen sharply. The company has an idea which is crime prevention through environmental design, so voice emergency platform is their representative technology and product. The company is open to license and commercial agreement with technical assistance, and financial agreement as well.

Creation Date	20 June 2018
Last Update	10 July 2018
Expiration Date	11 July 2019
Reference	TOKR20180620001
Public Link	https://een.ec.europa.eu/tools/services/PRO/Profile/Detail/c13dcfc9-5392-4961-aac6-abab08bfed3e

Details

Description

A Korean company has specialized in the development of technology applicable to an emergency platform. The firm did research about the rate of crimes. Sexually related crimes are increased up to 60.3% since 2006, and it does not resolve the problems with other ways to prevent the crimes. Therefore, the company developed an emergency platform, especially voice recognition. It performs when a person who is at risk says “Help Me” both in a noisy and quiet situation.

For example, it sensors the person’s voice in the case of emergency, and it sends the signals to police stations close to where it happened. It is designed firmly not to be damaged by a physical attack, and It could be installed inside the public restrooms and elevators as well.

Moreover, the products would be also used as emergency calls for disabilities and elders who live alone. Its principal technology is the same as speech recognition sensors for public usages. Thus, the company wishes to take the form of partnerships under a commercial agreement with technical assistance in order to contribute to crime prevention by decreasing the frequency of crimes. The faster it stops the dangerous situation, the safer they would be with the innovative devices applicable to various types of circumstances.

Under the license agreement, their technology would be licensed in other products to be more improved and utilized to result in lowering the rate of crimes that do not have to happen. Furthermore, a financial agreement would enable the technological support.

Advantages and Innovations

The company's technology has following advantages of

- Applicable on an emergency platform
- Contribution to decrease the rate of crimes by preventing them
- Hands-free devices for signals transmitting only with voice
- Availability of Crimes prevention through environmental design
- The technology could be applicable to a variety of fields, such as schools and vehicles for children.

Stage of Development

Prototype available for demonstration

IPR Status

Patents granted

Profile Origin

Private (in-house) research

Keywords

Technology

01003017	Speech Processing/Technology
01003018	User Interfaces, Usability
01006001	Audiovisual Equipment and Communication

Market

02007003	Operating systems and utilities
02008002	Voice recognition

Network Contact

Issuing Partner

ASTER - SOCIETA CONSORTILE PER AZIONI

Contact Person

Vera Lullo

Phone Number

+39 0516398090

Email

vera.lullo@aster.it

Open for EOI : Yes

Dissemination

Send to Sector Group

ICT Industry and Services

Client

Type and Size of Organisation Behind the Profile

Industry SME 11-49

Year Established

0

Already Engaged in Trans-National Cooperation

No.

Languages Spoken

English

Client Country

South Korea

Partner Sought

Type and Role of Partner Sought

- Type of partner sought: SEM, large company
- Specific area of activity of the partner: Partners should be in the area of supplier or developer for emergency equipment.
- Task to be performed: The Korean company's products should be commercialized for the public usages under commercial agreement with technical assistance and license agreement, and partnerships with financial agreement would support commercialization and improve more innovative the function of technology on the products as well.

Type of Partnership Considered

License agreement
Financial agreement
Commercial agreement with technical assistance

Attachments

Profile Status: Published

Technology Offer

A Turkish company specialized in software development offers its dairy and breeding farm management software under commercial agency agreement with technical assistance

Summary

A Turkish software developer SME is looking for enterprises that can help the market launch in the European market of their premium software developed for fattening and dairy farming management. Framework of cooperation would be commercial agency agreement with technical assistance.

Creation Date	04 June 2018
Last Update	06 July 2018
Expiration Date	07 July 2019
Reference	TOTR20180604002
Public Link	https://een.ec.europa.eu/tools/services/PRO/Profile/Detail/11b06784-27b2-4bf4-9042-e1dc0b578f69

Details

Description

The Turkish company has been delivering software development and project implementing solutions to clients ranging from large corporations to dynamic startups with their long years of IT experience. The company is highly experienced in business intelligence applications and developed software enables users to easily transform complex data into instant insights. Business intelligence applications add value to many sectors such as finance, telecommunication, retail, and manufacturing. Data mining technology is integrated into the solutions in order to increase benefits of the applications. The company provide solutions to the clients to let them increase productivity by re-planning their workflows with the reports provided by business intelligence systems.

Thanks to deep experience in IT sector, the company has been developed a farm management software system that provides animal welfare, makes comparison with instantaneous, real data and farm and livestock performance, accurate orientation of resources and proper planning. It helps the management of the enterprise efficiently and successfully by providing support to the manager’s decision processes on issues related to implementation, evaluation and inspection.

Developed software is a dairy and breeding farm management software to optimize farm’s performance and increase productivity.

The software has mobile application version. Animal history can be followed from mobile and monitoring current activities on the stall is performed throughout running checklist reports

The modules of the management software includes:
Animal assets management
Purchases
Breeding
Health
Feeding
Production
Leaving
Sales
Alerts & Tasks
Costing
Integration
Inventory Management
Reporting, Business Intelligence

The company has been already implanting the farm management system on a number of large milk and dairy products manufacturing companies and farms in Turkey and wants to expand its business in European countries.

The company is looking for partners to cooperate them on implementing the software in the European countries under commercial agency agreement. Technical assistance will be delivering throughout implementation of the system.

Advantages and Innovations

Advantages of the software include:
• Offers both desktop and web versions with proven hybrid solutions, without having to choose between desktop applications or Web applications.
• Farms can use a single app that covers the desktop version or web version.
• Most flattering feature is its flexibility.
• Reports can easily be configured with many conditions and filters. In addition, the software includes a complete and powerful Report Designer that enable creating almost any kind of report.
• Provides users with a relational database structure that allows real data mining.
• It is user friendly and does not require any expert computer knowledge.
• There is no need to re-enter data, correct data entry errors, or prepare checklist reports.
• Get real-time data and are ready to run custom reports or export to Excel.
• Run data mining tools, design chart or any other report.
• The company is able to offer tailor-made solutions

Stage of Development

Already on the market

IPR Status

Trade Marks

Profile Origin

COSME

Keywords

Technology

01003010	Databases, Database Management, Data Mining
01003015	Knowledge Management, Process Management

Market

02007001	Systems software
05009003	Animal health

NACE

J.62.0.1	Computer programming activities

Network Contact

Issuing Partner

ASTER - SOCIETA CONSORTILE PER AZIONI

Contact Person

Vera Lullo

Phone Number

+39 0516398090

Email

vera.lullo@aster.it

Open for EOI : Yes

Dissemination

Send to Sector Group

ICT Industry and Services

Client

Type and Size of Organisation Behind the Profile

Industry SME 11-49

Year Established

2014

Already Engaged in Trans-National Cooperation

Yes

Languages Spoken

Turkish
English

Client Country

Turkey

Partner Sought

Type and Role of Partner Sought

The Turkish company searches for a long term partnership with companies that are experienced in both fattening and dairy farming. The ideal partners would be producer of animal tracking and data collection devices
The right partner will receive product training and support with marketing activities.

Type and Size of Partner Sought

SME 11-50,R&D Institution,SME <10,>500 MNE,251-500,SME 51-250,>500

Type of Partnership Considered

Commercial agreement with technical assistance

Attachments

Profile Status: Published

Technology Offer

UK university seeks a commercial agreement with technical assistance or financial agreement for the market validation/technical development of a big data reduction and AI analysis engine for cyber threat detection and quarantine.

Summary

This UK university is developing a threat detection and neutralisation ecosystem in high throughput, big data network traffic environments; such as cloud providers, industrial control systems, Internet of Things and Smart Cities. The university seeks partners for a commercial agreement with technical assistance or a financial agreement for market validation and the further technical development of ecosystem elements.

Creation Date	19 September 2017
Last Update	25 September 2017
Expiration Date	25 September 2018
Reference	TOUK20170919001
Public Link	https://een.ec.europa.eu/tools/services/PRO/Profile/Detail/5321d01a-00da-426a-95b0-5bf8f6bfc5c0

Details

Description

Threat intelligence feeds come from a variety of sources; such as network traffic data, system logs and event management (SIEM). In a high throughput network, this can rapidly escalate into a big data challenge. A single packet capture probe on a 10 Gbps network backbone has the potential to capture Terabytes of data over the course of a day. Large, disperse networks require many probes to cover the entire network.
Organisations have started to use NetFlow flow export protocols to attempt to reduce data volumes. However, proprietary NetFlow v5 and NetFlow v9 are network management protocols, which were not specifically designed with threat intelligence and digital forensics in mind.
The University has developed a technique using the IPFIX (Internet Protocol Flow Information) export protocol. IPFIX supports template extensibility, variable length fields, and probe protection against flow interception, tampering attacks, replay attacks and probe DoS (Denial of Service) attacks. Furthermore, as an open standard IPFIX is vendor neutral. This traffic capture method takes advantage of IPFIX templates to capture any data from within a traffic packet at network or application level. Thus allowing network analysts to tune traffic data capture at both

the network and application layer; either for pre-emptive, pre-attack forensics or on-going incident analysis.
Reducing the volume of captured data makes data analysis more efficient, which in turn decreases threat reaction time. The University is looking to develop machine learning algorithms to further automate the detection process, so as to distinguish between actual threats and threat characteristics that initially appear to malicious but are in fact benign. In parallel to this work, the University is developing threat neutralisation techniques based upon Software Defined Networking.
A concept demonstrator has been developed for the detection of botnets. The demonstrator also shows how this can be applied to Internet of Things sensor networks. Current research is also developing templates to detect malicious HTTP content, SPAM and attacks upon SCADA (Supervisory Control and Data Acquisition) devices. Design of capture templates is limited only by the imagination of our partners and research team.
The University seeks commercial partners for a commercial agreement with technical assistance to further test the market viability of the product and develop it or partners who would like to invest in the technology for a financial agreement to develop the solution further.

Advantages and Innovations

Cyber threat detection can rapidly generate big data volumes of analysis traffic. This innovative traffic capture mechanism allows organisations to capture only the data that matters, reducing data capture volumes by up to 98% over traditional packet capture based systems.
One obvious advantage of this technique is the reduction in data storage requirements. However, reducing big data volumes of traffic means that SOC (Security Operations Centre) analysts can react more quickly to an event.
The capture mechanism takes advantage of the IPFIX (Internet Protocol Flow Information Export) protocol. Capture templates are custom designed around specific threat indicators or data attributes from the network layer through to application level, allowing detection within protocols that are often misused in cyber security attacks such as HTTP (Hyper Text Transfer Protocol), SMTP (Simple Mail; transfer Protocol) and DNS (Domain name system).
Many packet capture solutions rely on mirrored or SPAN (Switched Port Analyser) ports, which can mean large volumes of replicated data must be transported across a network to an analyse system. Our in-band capture system uses aggregation techniques and TAP(Test Access Point)ports. Resulting manageable quantities of data means network traffic can be efficiently stored for pre-event application and network forensics, or lawful interception.
The solution developed by this University is a proof of concept case study, a template that captures botnet traffic in cloud services providers. Compared to PCAP (packet capture) the captured data volumes were 8000% smaller. When compared with NetFlow, and industry leader, the University solution was 27% faster.

Stage of Development

Available for demonstration

Comments Regarding Stage of Development

The University has developed a proof of concept study to capture botnet traffic in cloud service providers which demonstrated data capture reduce volumes of over 8000%. Additional templates are under development to target HTTP threats, DDoS (Distributed Denial of Service) and SPAM.
A concept demonstrator has been built to show how it and other templates can be introduced into small footprint IoT sensor networks.
Further research is being conducted to feed captured data into artificial neural network learning environments to support SOC analysts in threat detection.

IPR Status

Secret Know-how,Copyright

Comment Regarding IPR status

Trade Marks currently under consideration as are patents

Profile Origin

COSME

Keywords

Technology

01003006	Computer Software
01003009	Data Protection, Storage, Cryptography, Security

Market

02006005	Big data management
02007001	Systems software
02007022	Software services
02007025	Consulting services

NACE

J.62.0.1	Computer programming activities
J.62.0.2	Computer consultancy activities
J.62.0.9	Other information technology and computer service activities

Network Contact

Issuing Partner

ASTER - SOCIETA CONSORTILE PER AZIONI

Contact Person

Vera Lullo

Phone Number

+39 0516398090

Email

vera.lullo@aster.it

Open for EOI : Yes

Dissemination

Send to Sector Group

ICT Industry and Services

Client

Type and Size of Organisation Behind the Profile

University

Year Established

1858

Turnover

<1M

Already Engaged in Trans-National Cooperation

Yes

Languages Spoken

English

Client Country

United Kingdom

Partner Sought

Type and Role of Partner Sought

The University is looking to partner with
• investors
• commercial organisations who wish to proactively threat monitor their own network infrastructure or applications
• managed service providers who are interested in developing the technology further in order to bring to the market
• commercial organisations with large threat and non-threat PCAP samples or other network traffic capture repositories
• IoT developers looking to incorporate situational awareness into their products

The University is looking for assistance in establishing the market viability of the solution and well as cooperation to develop the product further according to market needs. The University seeks partners for a commercial agreement with technical assistance or financial agreement.

Type and Size of Partner Sought

SME 11-50,University,R&D Institution,SME <10,>500 MNE,251-500,SME 51-250,>500

Type of Partnership Considered

Financial agreement
Commercial agreement with technical assistance

Attachments

Process.jpg

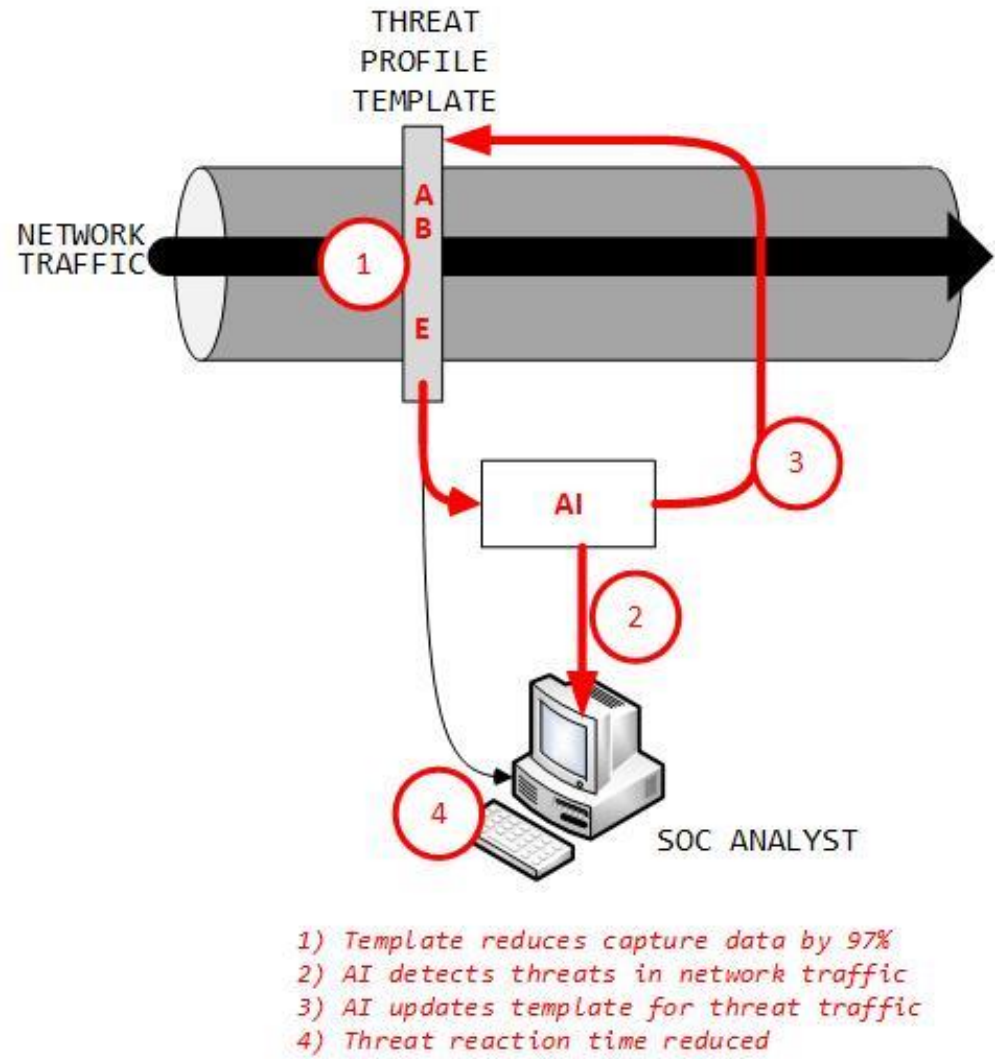
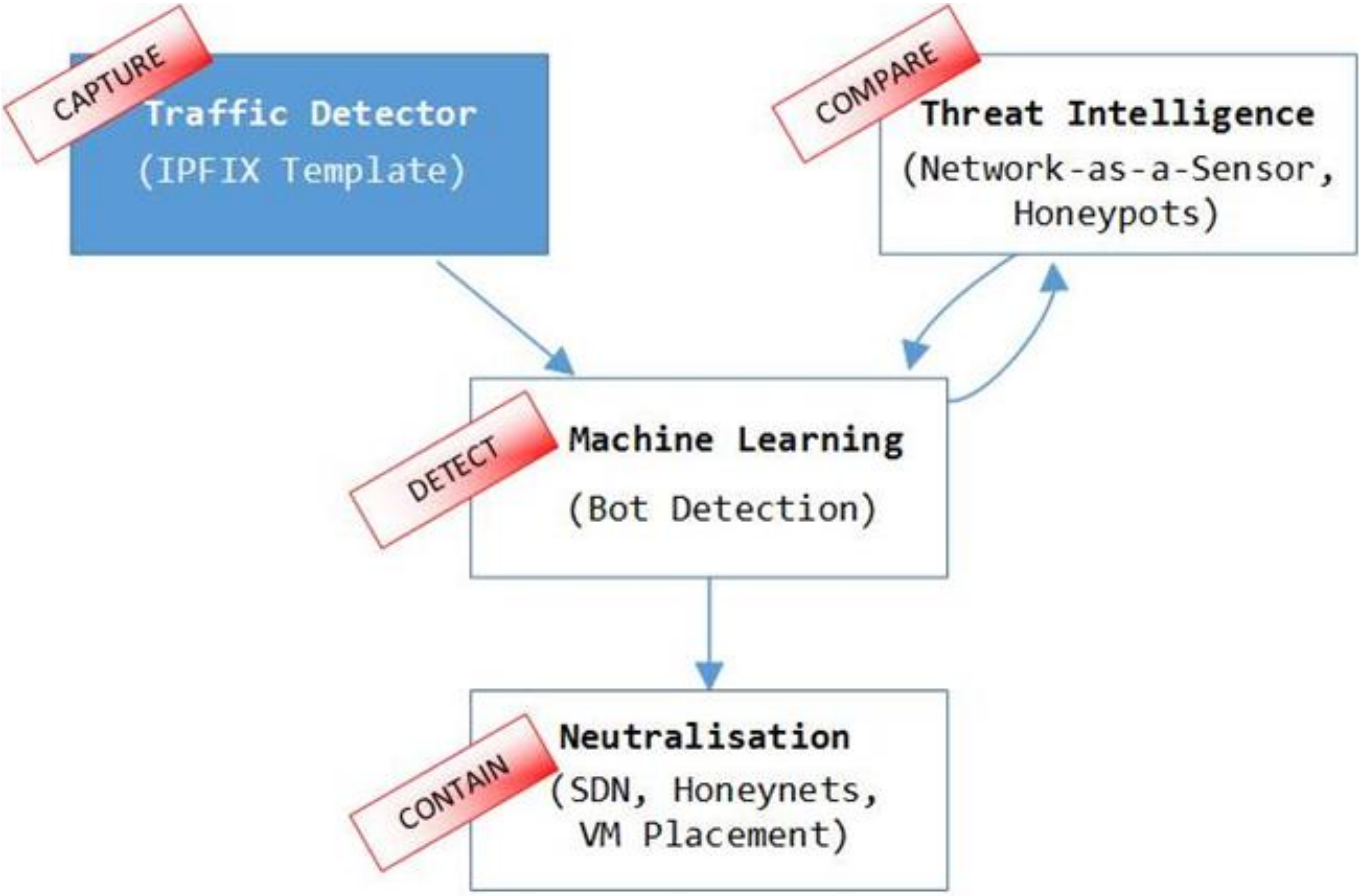


image1.jpg



Conceptual botnet mitigation eco-system