

CYBER INVESTOR DAY

14 May 2019 // Madrid, Spain

#InvestCyber

CYBER INVESTOR DAY

5th edition of the cyber security Business Matchmaking events across Europe

By the European Cyber Security Organisation (ECSO)

14 MAY 2019 – MADRID, SPAIN



BROCHURE

INSTITUTIONAL PARTNER



SPANISH NATIONAL CYBERSECURITY INSTITUTE

BUSINESS MATCHMAKING COORDINATORS



Conecte su empresa a Europa

PROGRAMME

PITCHING SESSIONS & BUSINESS MATCHMAKING

The address information is limited to the registered participants
(more information: wg2_secretariat@ecs-org.eu)

- 09:00 – 09:30 **REGISTRATION AND INSTALLATION**
- 09:30 – 09:40 **OFFICIAL WELCOME**
Alberto Hernández, *CEO*, Spanish National Cybersecurity Institute (INCIBE)
Luigi Rebuffi, *Secretary General*, European Cyber Security Organisation (ECISO)
- 09:40 – 10:40 **PITCHES OF CYBER SECURITY STARTUPS**
4securitas; Alias Robotics; Antiopea; Autom8; Baffin Bay Networks; Build 38; Gaptain; Keynetic
Selected startups & SMEs will pitch their solutions for 5 min-lengths each, followed by short Q&A.

Moderator: **David Ofer**, *Vice-President*, ITrust
- 10:40 – 11:00 **Networking Coffee Break**
- 11:00 – 12:00 **PITCHES OF CYBER SECURITY STARTUPS**
Keystroke DNA; Kymatio; Protect-ID.com; Randed; Samoby; smartfense; Swascan; Trapmine; Webtotem
Selected startups & SMEs will pitch their solutions for 5 min-lengths each, followed by short Q&A.

Moderator: **Csaba Virág**, *Head of Cybersecurity Competence Centre*, Cyber Services Plc
- 12:00 – 13:30 **Networking Lunch Break**
- 13:30 – 16:30 **BUISINESS MATCHMAKING SESSION**
Scheduled meetings between startups and investors organised individually on the B2Match platform.

 #InvestCyber

CATALOGUE

SELECTED CYBER SECURITY STARTUPS & SMEs Pitching Sessions & B2B Sessions

4SECURITAS, IRELAND

Capital Seeking: € 500K

Table 1

Company specializing in cybersecurity and AI. It developed ACSIA, a next generation automated cybersecurity monitoring and defence tool, designed to protect Servers from the full range of cyberattack and threats. 4Securitas is graduate of New Frontiers (an Enterprise Ireland program) program at the Synergy innovation centre at Technology University Dublin and an alumnus of Bank of Ireland, StartLab, and Fintech Program. ACSIA (Automated Cybersecurity Interactive Applications) is a simple solution that allows all enterprises and non-technical staff members to understand cybersecurity and take actions against threats without breaking the bank. ACSIA is an efficient real-time security monitoring tool that implements an all-in-one solution. It acts as a security engineer that never sleeps by automatically identifying and mitigating threats. Accessible via: www.4securitas.com



ALIAS ROBOTICS S.L, SPAIN

Capital Seeking: € 3M

Table 14

A security firm focused on robots. Alias Robotics provide assessment on how to build, program and deploy robots while caring about safety, security and privacy. Robots are conquering our homes industries, industries, offices and hospitals, operating hand to hand with humans. However, robot security is being largely underestimated. Alias Robotics offers two solutions: 1) Hardware product - the RIS (Robot Immune System) protects and analyses the malfunctions and cyberattacks, 2) Security assessments - offensive security for robot manufacturers (market ready) and consulting services. Accessible via: www.aliasrobotics.com



ALIAS ROBOTICS
Robot Cybersecurity

ANTIOPEA, FRANCE

Capital Seeking: € 500K

Table 3

Antiopea is a French cyber security startup specialized in Blockchain that offers companies original software solutions to manage, exploit and trace their exchanges of messages and documents in an autonomous and highly secured manner. Antiopea's first software, Axiom NRM, tackles several uses cases based on secured and certified transmission of critical documents such as Due Diligences, KYC or Whistleblowing procedures. Antiopea is an Oracle and IBM start-up business partner, as well an ECSO Member. Accessible via: www.antiopea.com





AUTOM8, ESTONIA

Capital Seeking: €750K

Table 8

autom8 provides super-fast and accurate source code security analysis enabled by machine learning. Up to now, autom8 has analysed 1B Lines of code and has a unique approach to secure software applications super-fast. Existing products use parser technologies invested in 50s/60s, which are too slow (500 million lines of code in 3-5 days), reporting too many false positives (%45-60). Existing products have an outdated quality model updated on a quarterly/yearly basis. Autom8 solution is an NLP (Natural Language Processing) which is based on a super-fast code analyser (e.g. 50 million lines of codes in minutes). It has a lower false positive ration (99% accuracy) using a self-learning quality model updated in real time. Autom8 is part of the CyberNorth Accelerator Program financed by the Estonian Ministry of Defence. Accessible via: www.autom8now.com

BAFFIN BAY NETWORKS, SWEDEN

Table 18

Since 2017, Baffin Bay Networks' Threat Protection solutions have been keeping businesses safe from cyber-attacks and providing customers with data and insights about their security state of health and evolving threats. Baffin Bay Networks has developed a Threat Protection Platform that protects organisations against both network and application level attacks, backed by machine learning and threat intelligence to keep up with the everchanging threat landscape. It is a fully controlled vendor independent platform and in-house developed service. For instance, the platform utilizes a unique algorithmic approach that detects and mitigates threats and blocks bad traffic in an automated, unsupervised manner.

Accessible via: www.baffinbaynetworks.com

BUILD 38, GERMANY

Capital Seeking: €8M

Table 16

Build38 develops solutions for securing the mobile market for end customer apps and approaches. Our customers tackle the mobile market easily, securely, compliant and much faster and more efficiently. Increasing top line with new markets and customers while saving bottom line with an SDK as a service development, quality assurance, and analytics. The Build38 trusted Application Kit (T.A.K) transforms an App into a Self-Defending App as a Service. Build38 offers investors a ready solution and portfolio with sound and proven business model for a growing market (best investor revenue). The company is founded by a long-established team with a technologically superior product and situated in Barcelona (DevOps), Singapore (APAC market) and Munich (HQ). Build38 is a carve out of the Giesecke+Devrient Group.

Accessible via: www.build38.com

GAPTAIN, SPAIN

Capital Seeking: 300K

Table 9

Gaptain tackles the problem posed by the lack of education of kids and teenagers in the digital field. Its solution is to coordinate and train schools and families in the 3 pillars supporting people's digital well-being: cybersecurity, digital skills, and security and supervision technology. Gaptain's solution, Segureskola, is a program for schools which includes a cybersecurity annual audit, ethics and digital skills training for students and teachers, families awareness about digital risks. It also includes an artificial intelligence platform to detect bullying, harassment, and segregation at



school. Segureskola is a security software in the school device and in the school network. Finally, Segureskola provides a digital certification differentiating those schools engaged in digital education and positive living. Accessible via: www.gaptain.com

KEYNETIC, SPAIN

Capital Seeking: €200K

Table 2

Networks have become an innovation enabler for new verticals such as Industry 4.0, offering great benefits and opportunities. However, by connecting machines they are exposed to new risks and threats, thus increasing the attack surface exposed by the industry. flowNAC provides a cutting-edge solution to this problem leveraging on Software Defined Networking (SDN) and Network Function Virtualisation (NFV) to bring a paradigm shift. flowNAC evolves from a trusted-segment model to a Zero-Trust model, thus increasing the security of connected assets without any impact on the production process. flowNAC implements micro segmentation to enforce the control over who has access to the network and which services are granted for each device, following a white-list model. Finally, flowNAC improves the visibility within the segment, by exposing an updated dashboard with devices connected to the network. Accessible via: www.keynetic.tech



KEYSTROKE DNA, ESTONIA

Capital Seeking: €225K

Table 12

Keystroke DNA verifies and protects businesses and identities online against fraud using behavioural biometrics for any business, using any platform and on any device. Cybercrime is an epidemic which costs billions of euros each year. Keystroke DNA strengthens access security as an invisible 2nd or 3rd authentication factor to eliminate unauthorized access in real-time due to the lost, shared, or stolen credentials. We also provide identity verification, retrospective identity analysis and represent the “What You Are” (i.e. inherence) aspect of a layered approach to security with greater accuracy than voice and facial recognition. The ability to authenticate using a low character count makes their service ideally suited to work with corporate identifiers. Accessible via: www.keystrokedna.com



KYMATIO, SPAIN

Capital Seeking: €1M

Table 19

Kymatio is an Enterprise SaaS for continuous diagnosis and prevention of insider risk. With Kymatio, companies can understand their human internal risk, start guided actions to prevent incidents, and increase their cybersecurity posture while training and raising awareness of their employees. The company is a CyberSecurity Ventures alumni and is supported by the Spanish Ministry of Economy, Industry and Competitiveness, National Cybersecurity Institute (INCIBE). Accessible via: www.kymatio.com



PROTECT-ID (Elixir LLC), ESTONIA

Table 4

Today one can open an e-commerce site without having a legal name, address, bank account or even a company. This also means that if you get scammed while shopping online, no-one can help you. Protect-ID uses advanced algorithms to determine the integrity of any website. This helps website owners to ensure that all their used systems are secure. It is a set of powerful tools that help the user build better and safer websites. Protect-ID team makes advanced web security checks available for all website owners, wants to share this tool using user-friendly UX and APIs, and wants to offer real, powerful systems that help you build more secure websites and online shopping experiences. Accessible via: www.protect-id.com



RANDED, SPAIN

Capital Seeking: € 3.5M

Table 10

Web security solutions have traditionally focused on a tactical or reactive approach based on detection and analysis. Unlike traditional security solutions, Randed Isolation Technology (RITech) is based on a strategic and proactive approach. The technology, instead of distinguishing between good and bad content, prevents any external content from reaching the corporate networks. Thus, it keeps it secure. RITech isolates web communications by transforming all the html code into a visual safe streaming to eliminate malware, data breaches, zero-day attacks, confidential data extraction and many other attacks. RITech does not require an entire Operating System, and it uses only the browsing engine to optimize the performance and consumption of the resources. The solution only isolates browsing instances, which guarantees the persistence of users' browsing sessions. Accessible via: www.randed.com



SAMOBY, SPAIN

Capital Seeking: €500K

Table 11

Samoby detects in real time mobile threats from network, app, and device perspectives. It acts to block the attack on the device itself. All the events that happen on the device (e.g. connection, usage, data traffic, ect.) are stored. Therefore, they can enrich other sources of information for a complete forensic analysis if it is required. Samoby collects information directly on the mobile, it is not necessary to filter the data by a proxy server. Samoby provides the service as a SaaS, but for regulatory or specific privacy requirements (e.g. financial, healthcare, government), the service can be deployed on premises. Accessible via: www.samoby.com



SMARTFENSE, SPAIN

Capital Seeking: €900K

Table 15

Current security solutions neglect the most vulnerable factor: the user. Behaviour change is possible, but we are aware that people responsible for information security require fast and effective solutions. To prioritize users in security strategy, Smartfense is the Information Security training and awareness platform which develops safe habits for end-users. This turnkey solution is simple and accessible awareness platform and contains a pre-defined educational content which is editable. Finally, it also includes an Integrated Phishing and Ransomware Simulator to evaluate and measure behaviours. Accessible via: www.smartfense.com/es-es/





SWASCAN, ITALY

Capital Seeking: €2M

Table 20

Swascan provides an All-in-One platform to help companies secure their assets and guide those companies towards GDPR compliance. Swascan is the first 100% Italian CyberSecurity platform. It is completely in Cloud, SaaS and Pay for Use. It has four main services. The Web App Scan is the automated service for Web Vulnerability Scan which identifies security vulnerabilities and criticalities in terms of web sites and web applications. The online Network Scan tool scans the infrastructure and the devices to identify security vulnerabilities and criticalities. Source Code analysis is a process that – through the source code analysis of applications – verifies the presence and effectiveness of minimum-security standards. GDPR Assessment is the Online Tool that allows companies to verify and measure their Compliance level to provide guidelines and corrective actions. Accessible: www.swascan.com

TRAPMINE, ESTONIA

Capital Seeking: €1M

Table 13

Unlike traditional detection-based approaches like legacy antivirus, Trapmine combines proven technologies such as behaviour monitoring, forensic analysis, machine learning and cloud intelligence in a single multi-vector engine to detect and block cyber threats. Trapmine collects and analyses forensics from endpoint devices to discover hidden threats that AV/EDR solutions miss. Trapmine offers a unique approach to focus on post-breach detection with live forensic artefacts analysis, ensures a less false-positive rate, and is an easy-to-use product. Trapmine is part of the CyberNorth Accelerator Program financed by the Estonian Ministry of Defence. Accessible via: www.trapmine.com



WEBTOTEM, ESTONIA

Capital Seeking: €500K

Table 6

WebTotem is a website security platform with an Automated Incident Response as a service for startups, e-commerce and even entire countries. WebTotem is a service which helps prevent most website cyber-attack and increases the defence barrier without requesting any special knowledge from the user. Most important, it works without any human interaction. WebTotem is currently monitoring nearly 140 000 websites for one of their clients and use data from this as a learning model for cyber attack prevention in the entire country. WebTotem offers a highly scalable infrastructure tested for high loads. WebTotem is part of the CyberNorth Accelerator Program financed by the Estonian Ministry of Defence. Accessible via: www.wtotem.com



ADDITIONAL SELECTED STARTUPS

Participating to B2B Sessions

DFTOOLS, SPAIN

Capital Seeking: €300K

Table 7

DirectDump is a combination of hardware and software for monitoring systems in a transparent way. It is agentless and hotplug, it respects the integrity and permits the access to the blocked systems. DirectDump is a transparent and undetectable monitoring. It provides detection and counter-measures for cyber-attacks and extraction of volatile and non-volatile data. DFTools uses blockchain for data integrity, big data for analysis, and they adapt to industry 4.0.

Accessible via: www.dftools.net



NEWRALERS S.L

Capital Seeking: € 500K

Table 17

Newralers offers an automated fraud detection with intentionality analysis by means of artificial intelligence algorithms of own design. The operation in real time, with a strong increase in security and productivity and with a reduction in costs allowing to improve the control and supervision in a growing environment of fraud attempts, facilitating the adaptation in real time to any modification of the environment or circumstances criminal without human intervention. Newsralers' intelligence engine extracts the relevant elements of the communication and contrasts them, determining standard patterns and evaluating in a percentage manner the proximity of each communication of fraud to such patterns. This percentage probability of proximity helps detect the critical point from which that communication can be a fraud.

Accessible via: www.newralers.com



SYNEIDIS S.L. CYBERSECURITY

Capital Seeking: €700K

Table 21

Companies produce and exchange large numbers of files, inside and outside the organization and by various devices. This generates a lack of control, which complicates the task of maintaining the security of the files. HushApp aims to protect these files with high encryption technology, but without the need for technical knowledge. This means that it protects the files, without hindering communication and productivity. The main competitive advantages of HushApp are: ease of use and high encryption standards, it can send to anyone without the need for them to install anything nor register, it has zero knowledge enforced and constant R&D in cryptography to stay ahead of the curve.

Accessible via: www.syneidis.com



XOLIDO, SPAIN

Capital Seeking: €12M

Table 5

The logo for Xolido, featuring the word "xolido" in a bold, blue, lowercase sans-serif font.

XolidoSign Technology is currently used in more than 130 countries with millions of documents signed, time stamped and verified, on average. Are you interested in the opportunity to invest in a new global and unified platform for electronic document signing? XolidoSign Plus is a global and unified electronic signature platform with advanced software engine/AI that manages the processes of identification, authentication and restrictions, ensuring that the signer is who should be and providing legal certainty to all parties, regardless of the legal frameworks involved. The predictive legal model of XolidoSign Plus will ensure strict compliance with all legislation, related to electronic signatures, in force in each country, in a transparent way for the user. - XolidoSign Plus can be integrated in any system, supports all types of files (PDF, DOC, XML, JPG, MP4, etc.), types of signature (electronic certificate, biometric, OTP PIN, CSV for public sector, etc.), signature formats (PAdES, XAdES, CadES, etc) and multi device.. Accessible via: www.xolido.com

STRATEGIC COMMUNICATION PARTNERS

