CONCORDIA

Cyber security cOmpeteNCe fOr Research anD InnovAtion

EDITORIAL

Thank you for being part of our Pan-European Cybersecurity Start-Up Community!!!

As always, we are very excited to share this issue with you and your contacts

This Issue

Meet Community Members: Collider

Guest Article: Bug Hunting for and by start-ups

Event Report: From COD to COD

Featured Article: How does large organisation relate to start-ups?

Dual Purpose Vehicle: Telefonica Tech Ventures

Should I stay or should I go: Bitdefender experience

EU Cybersecurity Investment Platform: ECSO initiative

More Letters Have Been Signed: EIT and EIC

Past Events

Future Events

www.concordia-h2020.eu

Meet Community Members: Collider

In this newsletter we present you the *Collider, an innovation programme of* bridges the gap between science and market to create disruptive technology-based start-ups. They foster entrepreneurial attitude in universities and uses the researcher – entrepreneur formula to create new high-value companies. On the other hand, Collider also actively encourage corporations to take part in the programme as well. They conduct innovation sessions to identify the main sectorial challenges and look for technologies in the local research ecosystem that can potentially help corporations. Later, they bring on board entrepreneurs that together with scientists build deep tech start-ups and launch pilots with corporate partners.

Check further details, portfolio and funding opportunities at: *https://thecollider.tech/*

If you want to get in touch with Collider or MWC directly please let us know.
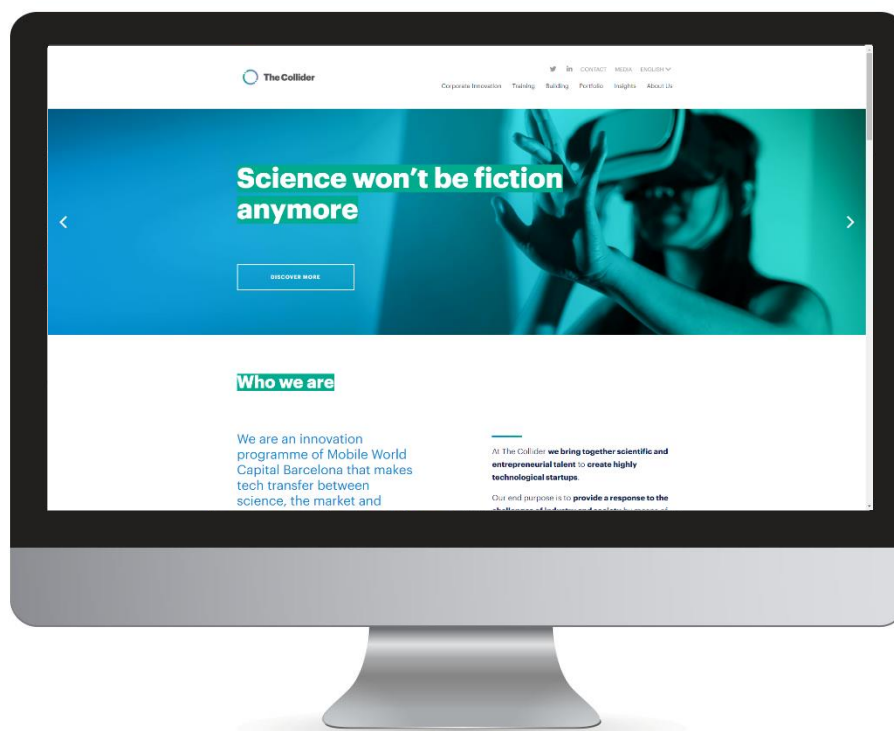
Guest Article: Bug Hunting for and by start-ups

Bug bounty is the name given to a kind of offering given by websites, organizations and software developers by which bug hunters can receive recognition and compensation for discovering, reporting or resolving bugs before the general public is aware of them. It used to be something reserved to larger organisations, but recently there are also bug bounty programmes or platforms specialised for start-ups. RISE, for example, is a managed bug bounty program designed specifically for start-up companies and is connecting start-ups to hundreds of security researchers. RISE belongs to Safehats company, based in India, but with offices in Germany. Secuna, headquartered in Philippines, is yet another non-EU company that specialises in bug bounty for start-ups. However, many European companies are also entering bug bounty business, although they target mainly larger organisations.

The American leader HackerOne was founded in 2012 by two Dutch hackers and the ex-Head of Product Security at Facebook. It uses a network of freelance hackers who are paid from 1000 to 100.000 euros. The company is now headquartered in the U.S.

where majority of its business comes from (Verizon Media, Paypal, Airbnb, Twitter, the U.S. Department of Defence) but it is growing in Europe and Asia. Bugcrowd is another American Bug Bounty platform with a very similar model.

In Europe, the start-ups are plenty and divided by their business model: private bug bounty programs (bug hunters are selected and the program is secret) or public ones (to whole community of bug hunters).

The Belgian Intigriti has recently announced raising €4.1 million in their Series A round, led by European based venture capital firm ETF partners. Intigriti was founded in 2016 and uses a network of 15.000 ethical hackers that serve more than 75 customers. Similar number of hackers is also used by YesWeHack platform. Launched in 2013 and raised the same amount as Intigriti two years ago they also claim to be the leader among bug bounty platforms in Europe (offices in Paris, Germany and Switzerland), they start growing in Asia with an office opened in Singapore in the last year. Their last innovation is using blockchain to improve smartly the Coordinated Vulnerability

Disclosure (CVD). In January 2020, YesWeHack wrote a white paper about this topic for the European Union context. They are also using students who are trained with another bug bounty platform.

Yogosha, another French company that raised 2 million in January, is specialized in private Bug Bounty (500 shortlisted bug hunters) in Europe. They recently increased their offer in all of Europe, especially in Germany and Spain.

The Dutch Zerocopter is another European bug bounty platform with 3 000 hackers. Among newcomers we can mention Hackrate from Hungary, which is listed in EU start-up directory and is looking for the investment to further develop their platform. CazHack is an example of new platform active in Spain.

Hype or not, bug bounties program are an interesting option to complement internal testing process, while incentivizing ethical hackers to report bugs and issues and get paid for their work. Crowdsourcing of pen testing is considered as a long-term innovation in the existing cybersecurity processes.

This article has been co-written with Louise Bautista.

After a first experience in Capgemini consulting group, Louise Bautista worked as an account executive for YesWeHack, the European Bug Bounty platform. She is working now for VPN client software company, TheGreenBow. She is also Secretary general of the non-profit organization: the French club of Cryptocurrency and founder of its delegation in Malta. Louise wrote many articles about cybersecurity, blockchain and innovation for Cryptonaute, Harvard Business Review France, Security and Defence magazine. Louise will be also speaking at CONCORDIA Woman in Cybersecurity webinar dedicated to entrepreneurship, scheduled for December 14th at 16.30. More details in EVENTS section.

Event Report: From COD to COD

The CONCORDIA project runs annual event called CONCORDIA Open Door (COD) that is used as an enabler of an open and constructive dialogue about the whole spectrum of cybersecurity, from research to technology, from legal to business, but also to collect important feedback about what can the community expect and offers to the future European Cybersecurity Competence Centre. This dialogue conclusions and the feedback that is received is then used to align CONCORDIA activities with the needs of a wider cybersecurity community.

COD2019 was held at Hotel Parc Alvisse, Luxembourg on the 16th and 17th of October 2019 with around 100 participants.

During this first edition of COD event, ID Quantique, one of the members of PECS-UP community, presented their work on quantum key distribution (QKD) systems, quantum safe network encryption, and hardware random number generators. This Swiss company, founded as a spin-off of the Group of Applied Physics at the University of Geneva, also gave insights in best practice collaboration between small and large enterprises.

For those that are interested in this topic, we recommend recently published white paper on "How quantum technologies are helping to secure our digital future".

www.idquantique.com

This year, CONCORDIA Open Door event 2020 was virtual event due to the circumstances related to COVID-19. It was held on 28th and 29th of October 2020 and included two panel sessions related to start-ups and SMEs, namely "Startups, SMEs, and the future European Cybersecurity Competence Center and Network" and "Big vs Small Industries: Approach to Cybersecurity".

Before first panel session there was a keynote presentation from Maria Lundquist, from European Investment Bank (EIB), about the ecosystem provided by EIB in the context of cybersecurity. This institution is helping start-ups and SMEs to overcomes barriers and funding gaps that correspond to "valleys of death", as they are known in innovation management and growth strategies. Maria also presented Cybersecurity Related Investment Estimation method, a kind of methodology to estimate values of investment that go into cybersecurity, when it is difficult to separate it from the other IT investments. Finally, she also briefly mentioned InnovFin funds, such as AI and Blockchain fund, and several projects that they selected for financing.

Panel session started with an introduction about pooling Europe's Cybersecurity expertise and implementing European Cybersecurity Competence Centre and Network. The first panellist Jean Diederich (Wavestone) gave overview of current cybersecurity start-up landscape and mentioned that there are segments, such as cloud security, which not currently addressed by start-ups. José Ruiz Gualda from jtsec and CONCORDIA PECS-UP start-up community was stressing the importance to choose the best solution in EU, overcoming fragmentation and support of "national start-up champions". Victoria Villanyi from ELTE addressed entrepreneurship gap, and made a link to the cultural factors, while Danilo D´Elia from ECSO presented several new initiatives started in this organisation, such as cybersecurity start-up award and letter of intent to start a dialogue on creation of Pan-European cybersecurity specific investment fund.
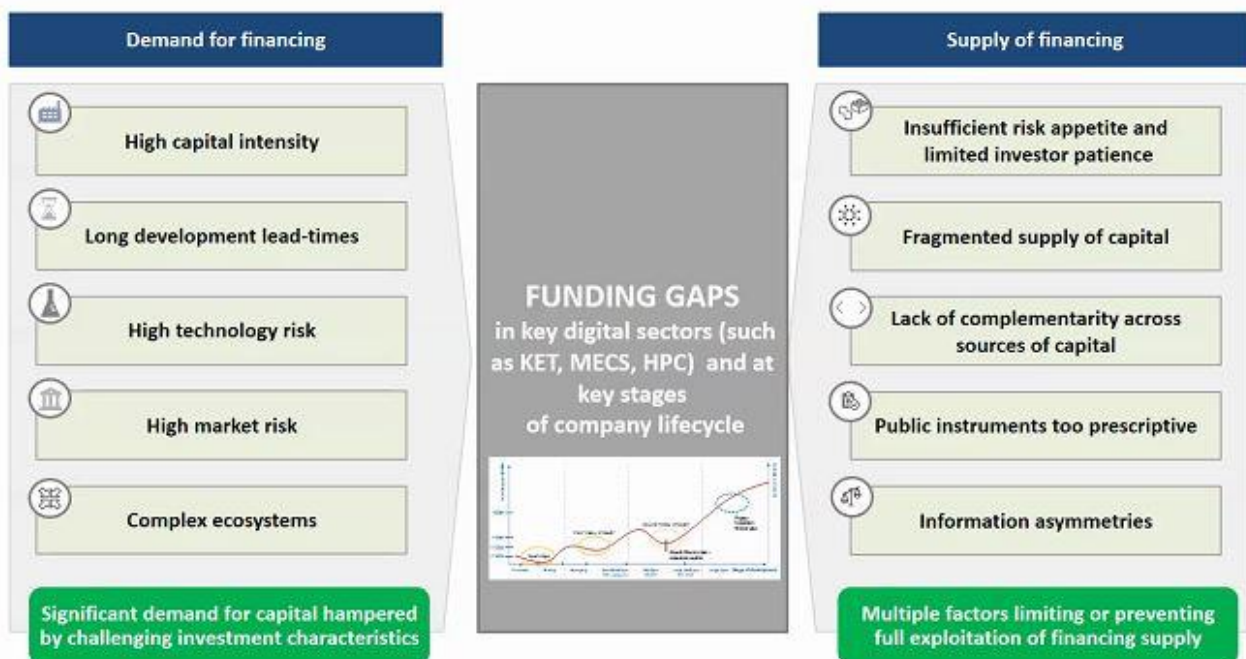
The challenge is, all panellists agree, on how to coordinate what is useful for EU in emerging start-up landscape (e.g. which are strategic segments), how to move from proof of concept to the next stage that involves real operational deployment, as well as how to keep start-ups in Europe,

after the initial success. The conclusion of panel is that, besides addressing already mentioned and well-known gaps (funding, growth, territorial and educational differences), EU needs also to foster quality and not quantity in cybersecurity start-up ecosystem.

The second start-up and SME panel was named "Big vs Small Industries: Approach to Cybersecurity" and it was focusing on better understanding of how the European start-ups, SMEs and large enterprises are approaching the cybersecurity challenges. Despite a growing interest on cybersecurity, in 2020, a vast majority of start-ups and SMEs stakeholders are not aware of the impact of cyber breaches and threats on their businesses. This was confirmed by independent statistics as brought forward by the panel guests Georgiana Ghiciuc from Beaglecat and Christopher Richard from United Biometrics. Panellists also mentioned some other challenges, such as low cybersecurity budgets. The SMEs decision-makers are considering cybersecurity as an IT issue rather than an organisational governance issue and consequently they are setting-up smaller budgets compared with the real needs. These challenges are also encountered by the large corporations, but at a different scale as the representative of large enterprise, Frank Schubert from Airbus, confirmed.

Supply-side limitations compound sectoral challenges, resulting in significant funding gaps across various digital sectors

Demand for financing
- High capital intensity
- Long development lead-times
- High technology risk
- High market risk
- Complex ecosystems

Significant demand for capital hampered by challenging investment characteristics

FUNDING GAPS in key digital sectors (such as KET, MECS, HPC) and at key stages of company lifecycle

Supply of financing
- Insufficient risk appetite and limited investor patience
- Fragmented supply of capital
- Lack of complementarity across sources of capital
- Public instruments too prescriptive
- Information asymmetries

Multiple factors limiting or preventing full exploitation of financing supply

The second panel concluded that there is still a strong need to further encourage the actions and impact of joint cybersecurity initiatives such as CONCORDIA project, where different stakeholder, small and big, work together.

Featured Article: How does large organisation relate to start-ups?

Wait! Before going to "how" we should explain "why". Large organisations sometimes have problems in reorientation, transformation or revitalization of its product and service portfolio. Investing in or collaborating with a start-up company, that executes parts of the strategy not possible to execute in the large firm, could be a viable option, used by many large organisations.

Besides this motivation that can be describes as "one strategy, different tactics", there is also more traditional motivation, such as staying ahead of competition, even if this is done through adjacent start-up. Operational level activities include start-up scouting, monitoring of windows of opportunity etc.

Mind the Bridge, together with Nesta, annually elaborates the "Europe's Corporate Start-up Stars", a ranking of more 'start-up-friendly' corporates in Europe. Telefonica, for example, which is one of CONCORDIA partners, was praised for inversion in cybersecurity, among other into companies such as Countercraft and Imbox. While Telefonica is famous for its Wayra innovation hub and accelerator, there are other ways to invest or collaborate with start-ups, including direct or indirect corporate

venture. Sapphire, for example, was formerly known as SAP Ventures but rebranded as Sapphire in 2014, to reinforce its status as a firm independent from the German corporation. BBVA Ventures was transformed into a separate entity, Propel Ventures, while Banco Santander did something similar when transforming InnoVentures into Mouro Capital.

Siemens has also set up a separate venture capital unit called Next47, to foster disruptive ideas. Some companies from Next 47 portfolio entered Atos Scaler programme, where 15 start-ups are selected to develop their projects according to specific customer interests, and to contribute to enriching Atos offerings. One of this companies (United Biometrics) was recently present at CONCORDIA Open Door event (COD2020) exhibition space.

In summary, there are different ways to achieve win-win situation between large organisations and start-ups and CONCORDIA ecosystem, with more than 50 partners, from which are more than 20 large organisations, is one opportunity to explore these links.

Dual Purpose Vehicle: Telefonica Tech Ventures

On October 22nd, 2020 Telefónica introduced Telefónica Tech Ventures, its investment vehicle specialized in cybersecurity. It is promoted by ElevenPaths, Telefónica Tech's cybersecurity company, and by Telefónica Innovation Ventures, Telefónica's Corporate Venture Capital, it starts with a portfolio of nine invested startups and investment plans for up to fifteen more over the next three years.

This new vehicle serves a dual purpose: to develop Telefónica Tech's own investment capabilities in the highly dynamic cybersecurity sector, and secondly, to detect the most disruptive innovation in this field.

More details on :
https://techventures.telefonica.com/
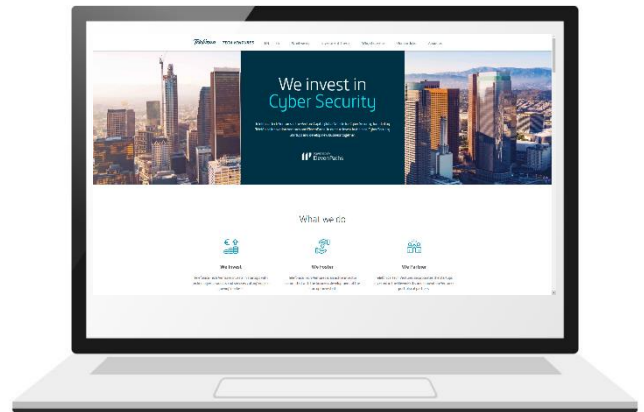
Should I stay or should I go: Bitdefender experience

In 2001, Florin Talpes started company in Romania that over time would become the role model for start-ups everywhere in the world. Bitdefender, partner of CONCORDIA, started in antivirus business, but is now doing also other cyber security products and services. It grew to more than 1600 employees worldwide.

During all these years, company preserved its headquarters in Romania. In one interview, Florin, who is CEO now, mentions the major milestone when the company started to employee abroad, first in Germany and then in US. This "nuclear explosion" moment, as he calls it, happened when Bitdefender decided to have a double HQ, partly in Romania and partly in the US.

EU Cybersecurity Investment Platform: ECSO initiative

European Cyber Security Organisation (ECSO) is a non-for-profit organisation, established in 2016 with more than 250 European cybersecurity stakeholders. ECSO Working Group 2, dedicated to Investment and Market deployment, organises regular technical workshop with private investors to discuss challenges and opportunities to invests in European companies. ECSO WG2, with the support of the European private investors, drafted a letter of intent to initiate a dialogue with the EU Institutions for the creation of a European cybersecurity investment platform (fund-of-funds) of at least €1 billion investment, with the duration up to 5 years.

In this letter, ECSO and investors identified several key challenges for the European cybersecurity companies to scale up in Europe and also outline objectives such as to stimulate the emergence of new pan-European cybersecurity specialised funds, or to encourage the creation of a pan-European "Cybersecurity Accelerator" as a network of regional ecosystems specialised in cybersecurity.

If you want to support ECSO in this initiative, please let us know.

More Letters Have Been Signed: EIT and EIC

Another Letter of Intent has been signed, this time between the European Innovation Council (EIC) and the first wave Knowledge and Innovation Communities (KICs), including EIT DIGITAL, one of CONCORDIA partners. European Institute of Innovation and Technology (EIT) is a European Union body, established in 2008, with designated Knowledge and Innovation Communities (EIT KICs), each set up as independent entities. EIT Digital has two main instruments for venture creation. The first one is Innovation Factory, that brings together organisations from all over Europe to launch deep tech ventures, while the second is the Venture Program that supports teams of entrepreneurs from the so-called RIS (regional innovation scheme) countries to launch their Minimum Viable Product. EIT Digital is also running Digital Challenge that in 2020 has established a new record: 403 scaleups from 32 countries applied to the 7th edition of Europe's flagship deep tech competition in digital, a 44% growth with respect to 2019. The 20 best companies are invited to an exclusive event to pitch in front of a jury of high-profile corporates and investors. Among them, the jury will select 5 winners that will receive prizes totalling €350,000 to boost their international growth.

On the other hand, the European Innovation Council (EIC), to be fully implemented from 2021 under Horizon Europe, was introduced to support the commercialization of high-risk, high-impact technologies in the European Union. Enhanced European Innovation Council (EIC) pilot has been launched since 2018 at the request of the European Council. While EIC Pathfinder is providing grants to high-risk cutting-edge R&D projects implemented by consortia exploring new territories aiming at developing radical and innovative technologies, the EIC Accelerator is providing support to single start-ups or SMEs dealing with innovation which are still too risky to attract private investments.

https://ec.europa.eu/
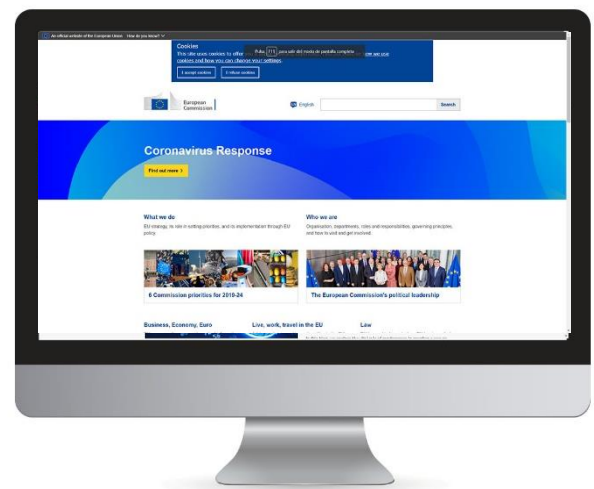
Past Events

We have been participating in Horizon Cyber event on October 2nd, 2020, co-organised by ECSO, SPARTA pilot project, ENISA and others, where several start-ups (mainly French) presented themselves. In addition, we participated in South Summit event and sessions dedicated to cybersecurity on October 7th, 2020. South Summit was created by IE Business School in 2012 and is currently the largest start-up gathering event in Spain and one of the most important in Europe. As a part of cybersecurity start-up scouting efforts to enlarge PECS-UP community, we also attended virtual event called Impact Week, more specifically dedicated session on start-ups that are working on key topics such as DLT and blockchain.

Future events

This year, in relation to its recently launched start-up award, ECSO was very active in co-organisation the local competitions, such as Cybersecurity Luxembourg Start-up Pathway on 15-16 September (Luxembourg), Horizon Cyber on 2 October (France), or European Cyber Week on 18 November in Rennes (France). The 8th edition of the ECSO Cyber Investor Days is organised together with eurobits e.V. on Nov 30th and Dec 1st . Here is the link for registration: *https://www.eventbrite.com/e/8th-cyber-investor-days-tickets-119427455735*

CONVERGENCE is the new name for the joint annual event of pilot projects for the European Cybersecurity Competence Centre, Network and Community. CyberSec4Europe, SPARTA, CONCORDIA and ECHO announced a two-day concertation event from 9-11 December to be hosted online. Registration is free of charge and you can find agenda here:


https://cybercompetencenetwork.eu/convergence/
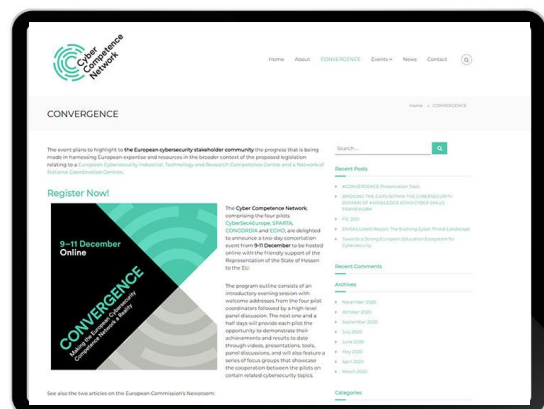
CONCORDIA will provide a series of webinars focusing on topics related to gender balance. The purpose of the webinar is to provide insights from relevant speakers and facilitate networking with the audience, to help women potentially interested in starting a new career path to be in touch with relevant speakers/organizations. The webinars are organized on two moments: first, a panel with relevant speakers (about 45 min) and second mentoring activity, implemented as private calls between people from the audience and a speaker (45 mins). We are happy to announce that the first webinar will be on women entrepreneurship, with Louise Bautista, Paola Bonomo and Sara Colnago. Registration is required, at the following link:

https://hopin.com/events/dc-women-entrepreneurship

Cybersecurity Ventures is an International Acceleration Programme for cybersecurity start-ups, which emerged from the initiative of the National Institute of Cybersecurity (INCIBE) in Spain. Cybersecurity start-ups can sign up to the programme until 1 March 2021. More about benefits and other details at tis link:

https://www.incibe.es/venture
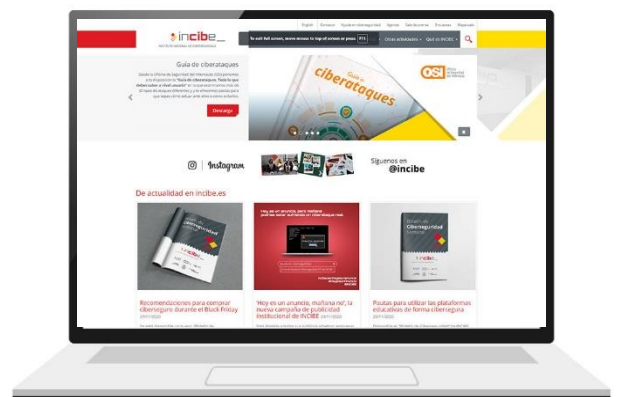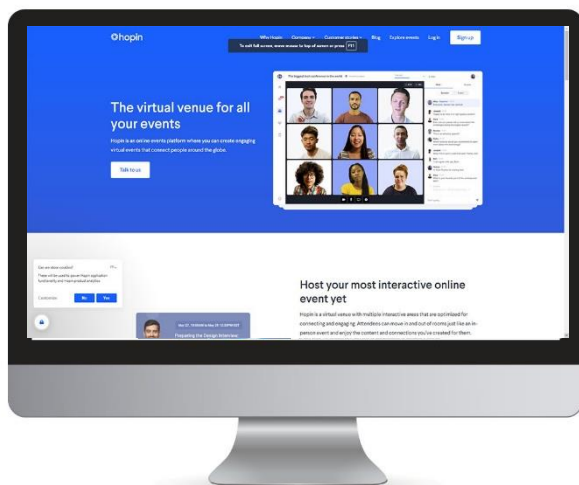
Feedback needed: How did COVID impact your business?

The World Economic Forum found that cyber-attacks and data fraud ranked third amongst Covid-related business concerns. It's a challenge for many organisations — but also an opportunity for start-ups. According to the LORCA Report 2020, investment into UK cybersecurity startups in 2020 has increased by 940%, compared to the same quarter in 2019 (which had already reached an all-time high of £521m). New cyber startups are springing up all the time, too; a new cyber business is registered every week in the UK, while vacancies for cybersecurity jobs climbed by 22% year-on-year in 2019. How did COVID impacted your business? Do you have a story to share?

Let us know and we will publish your story in the next newsletter.

Feedback needed: CONCORDIA released an open-source Cyber Range platform

This means that every start-up is now able to deploy a cyber range for teaching or training cybersecurity professionals for free. You can then focus on developing training and delivering them to their audience. KYPO Cyber Range Platform is open source under the MIT license, which means that anyone can customize the cyber range or extend it for its needs. If you decide to do it, or need more details, let us know.

More information at *https://www.concordia-h2020.eu/news/concordia-releases-an-open-source-cyber-range-platform/*

Thanks for your collaboration, for any questions or content

recommendation please contact us:

aljosa.pasic@atos.net

nicolas.kourtellis@telefonica.com

www.concordia-h2020.eu