Newsletter # 2 | 2020

CONCORDIA

Cyber security cOmpeteNCe fOr Research anD InnovAtion

Stakeholders' Newsletter

Thank you for joining our mailing list and be part of the EU Cybersecurity Competence Network!

This second issue will point out some interesting articles related to the post-lockdown cybersecurity situation and other updates you may have missed during this summer. Take particular attention to the CONCORDIA open door 2020: our annual event is probably what you were looking for boosting your network and ideas. This year is even easier to join because we are going online.

Enjoy your reading, and don't hesitate to provide feedback.

This issue

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 830927.

CONCORDIA Education

CONCORDIA Methodology for the creation and deployment of new courses and/or teaching materials for cybersecurity professionals

CONCORDIA proposes a Methodology for designing and deploying courses for professionals while considering the specificities of the cybersecurity area. Based on this Methodology, new courses will be developed targeting mainly industry mid-level management and/or executives.

Read more at:
https://www.concordia-h2020.eu/wp-content/uploads/2020/06/CONCORDIA-methodology-courses-professionals-for-publication.pdf

Education workshop – post event report

On June 2nd and 3rd, the first CONCORDIA workshop on education for cybersecurity professionals took place. The workshop ran in the framework of the CONCORDIA project, linked to the activities on developing (1) a framework for skills certification and (2) course content creation for cybersecurity professionals.

Read the report at:
https://www.concordia-h2020.eu/wp-content/uploads/2020/07/CONCORDIAWorkshoponEducation2020-forpublication.pdf

Feasibility study on existing skills certification schemes

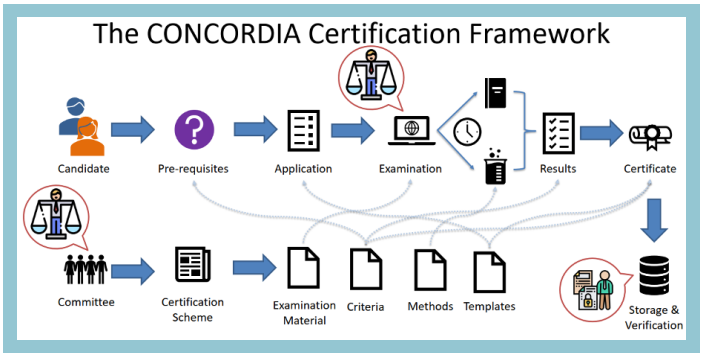
This document contains the results of the analysis of the current situation regarding the certification of cybersecurity skills and the conclusions regarding the gaps derived by the project team.

Document at: https://www.concordia-h2020.eu/wp-content/uploads/2020/06/CONCORDIA-SkillsFeasibilityStudy-forpublication.pdf

Preparing to fight Cyber Threats – The Human aspect

It is news to no one that everyday organizations experience incidents related to Cybersecurity. Cyber threats follow an increasing progression for the last five years. What can organizations do in order to be better prepared and more resilient?

Read more at:
https://www.concordia-h2020.eu/blog-post/preparing-to-fight-cyber-threats-the-human-aspect/



CONCORDIA OPEN DOOR 2020

When? 28th and 29th of October 2020
Where? Online, powered by tame.events

CONCORDIA Open Door (COD) is a chance for stakeholders of all backgrounds (such as IT, entrepreneurship, education, economy, and policy) to discuss societal and technological needs in the cybersecurity field and to discover others' competences for potential collaborations.

CONCORDIA Open Door event 2020 goes virtual to allow a broader audience during the current situation. However, CONCORDIA advocates social networking: the virtual event platform will allow breakout and networking sessions, besides outstanding talks and panels. Further, the platform is GDPR-compliant and EU-based.

Registration are now open!!! Joining the event is free of charge and you can do it registering (RSVP button) at https://opendoor.concordia-h2020.eu/2020/register.

If you want your company or start-up to gain visibility during this virtual two-days, please consider joining the expo area with full access to your own virtual booth. For further info, don't hesitate to contact opendoor@concordia-h2020.eu.

COD2020: https://opendoor.concordia-h2020.eu/

Previous edition:
https://opendoor.Concordia-h2020.eu/2019/index.html

Suggested articles and webpages

CPO Magazine. The COVID-19 crisis accelerated the need for digital transformation for many companies, as communication and collaboration became even more important for employees working from home. As enterprises rapidly pivoted to increase their digital footprint and ramp up a remote workforce, they faced increasing security challenges for protecting enterprise networks, devices and data. Unmanaged devices, shadow IT and rapidly deployed remote access networks introduced larger attack surfaces for cyber criminals, making securing the enterprise even more difficult for CSOs and their teams.

Read more at:
https://www.cpomagazine.com/cyber-security/building-cyber-resilience-post-covid-19/

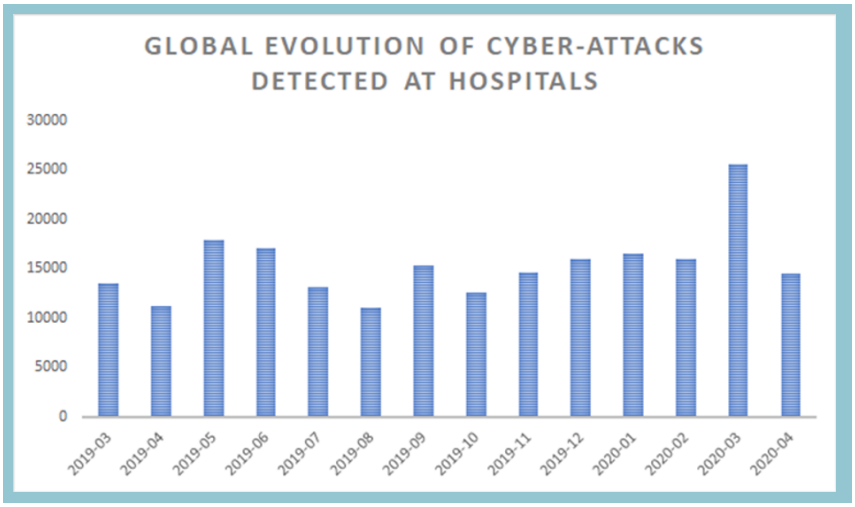
ITProPortal. According to current government guidelines, everyone who cannot do their job from home should now go to work, provided their workplace is open. As people start to trickle back into the workplace over the next few months, we're going to see the emergence of a very different workplace. More people are going to continue to work remotely, whether full-time or part-time, and businesses are going to have to deal with the impact of the predicted recession.

This 'new normal' brings with it many challenges, not least for cybersecurity teams who will have to develop new short- and long-term plans to ensure resiliency.

Read more at:
https://www.itproportal.com/features/the-top-cybersecurity-challenges-post-lockdown/

BITDEFENDER. Two things also spread along with the virus: panic and misinformation. In a digital world, these two can be very effective weapons in the hands of cybercriminals, especially when their goals are financially motivated. And make no mistake, everything in the cybercriminal community is financially motivated; from data that is stolen in transactions through obscured forums, to ransom demands from cybercriminals who lock you out of your data.

Read more at:
https://www.concordia-h2020.eu/blog-post/opportunistic-cyber-threats-in-a-time-of-pandemic/



Updates

Security vulnerabilities allow hackers to remotely gain access a Mercedes-Benz

Security researchers recently revealed during a virtual conference that they had discovered more than a dozen vulnerabilities in a Mercedes-Benz E-Class. The researchers were able to tamper with the TCU file system of the car which is also considered the "most crucial" part of the car since it enables the car to communicate with the internet. By doing so, they had the highest level of access to the car's internals and were also access the car's passwords and certificates.

While the safety of internet-connected cars has improved over the years, it is far for from being perfect. Previous incidents have shown that not only can hackers gain access to personal data of drivers and passengers that is stored in such vehicles but they can also jeopardise the physical safety of its passengers and those around the vehicle as well. Car manufacturers need to take into account that resilient security and protection (and in case of mobility also: safety) need to be built into systems, devices and services – including mobility platforms of any sort and capabilities –, not bolted on.

Read more at: https://techcrunch.com/2020/08/06/security-bugs-mercedes-benz-hack/

MARRIOTT: new data breach affects 5 200 000 customers

On March 31, Marriott International announced that it had experienced a data breach making it the second data breach faced by the hotel chain in three years. Marriott said it discovered that information had been accessed by hackers who used the login credentials of two of its employees. The hotel conglomerate stated that it had no reason to believe that payment data had been stolen, however, information such as names, addresses, phone numbers and date of birth may have been compromised.

Read more at:
https://techcrunch.com/2020/03/31/marriott-hotels-breached-again/

EU aims to strengthen critical infrastructure against cyber threats, grants €38 million

The Horizon 2020 programme is the EU's research and innovation programme aimed at supporting innovative projects to provide the requisite critical infrastructure to protect against cyber and physical threats. Through this programme, the European Commission has announced that it is committing more than €38 million to bolster innovative projects that ensure protection of critical infrastructure from cyber and physical threats, thereby making cities smarter and safer.

Read more at:
https://ec.europa.eu/digital-single-market/en/news/eu-grants-eu38-million-protection-critical-infrastructure-against-cyber-threats

Updates

1st ENISA Advisory Group Meeting: Members to Strengthen Agency's Work Towards a Cyber Secure Europe

The Advisory Group of the European Union Agency for Cybersecurity, ENISA, is meeting for the first time to discuss the Agency's new strategy and the current political landscape of Europe's cybersecurity ecosystem. Established under the EU Cybersecurity Act (Article 21, CSA) of 2019, the group will serve a 2.5-year term to assist the Agency with its numerous tasks, to advise the Executive Director on drawing up a major part of the annual work programme and to engage effectively on the programme with stakeholder communities.

Read more at: https://www.enisa.europa.eu/news/enisa-news/1st-enisa-advisory-group-meeting-elected-members-to-strengthen-agency2019s-work-towards-a-cyber-secure-europe

False Flags in Cyber Threat Intelligence Operations

TELECOM ITALIA. Like "fake news" also in the security world there is the risk of "false flags".
There are tons of information in the form of paid and OSINT (Open Source Intelligence) feeds that enrich and add value to any indicators used to protect the networks.

Read more at:
https://www.concordia-h2020.eu/blog-post/false-flags-in-cyber-threat-intelligence-operations/

The DNS in IoT: Opportunities, Risks, and Challenges

SIDN LABS, UNIVERSITY OF TWENTE, et al.. The Internet of Things is widely expected to make our society safer, smarter, and more sustainable. However, a key challenge remains, which is how to protect users and Internet infrastructure operators from attacks on or launched through vast numbers of autonomously operating sensors and actuators.

Article at:
https://www.sidnlabs.nl/downloads/49DguF5OpLVw5HCXfROdzW/9c7126fce8ddc80b0850d85f04d64139/The-DNS-in-IoT-Authors-Version-2020-SIDN-Labs.pdf

BloSS - The Full View and Evaluation

UZH. In the blockchain-based collaborative defense system BloSS, members of the platform perform the on-chain signaling of DDoS (Distributed Denial-of-Service) attack information, establishing bilateral contracts defining the terms of a mitigation service. BloSS stimulates the cooperative behavior in the collaborative defense environment by providing valuable incentives defined in terms of the mitigation service contract and combining it with a reputation system in its protocol for the bilateral evaluation of the service.

Read more at: https://link.springer.com/article/10.1007/s10922-020-09559-4

More cybersecurity research and innovation updates are available through CONCORDIA services https://www.concordia-h2020.eu/concordia-service-catalog/

Next Events and Open Calls

IoTSC20 - conference
Online – 7, 14, 21 October 2020
https://www.enisa.europa.eu/events/4th-iot-securiity-conference-online-series/

S&P Oakland 2021 – conference
San Francisco, California, USA – 23 to 27 May 2021
https://www.ieee-security.org/TC/SP2021/
Submission deadline: 3 September 2020, 3 December 2020

ACM CCS 2020 – conference
Online – 9 to 13 November 2020
https://www.sigsac.org/ccs/CCS2020/

AsiaCCS 2021– open calls
Hong Kong, China – 7 to 11 June 2021
https://asiaccs2021.comp.polyu.edu.hk/
Submission deadlines: 12 December 2020

CONCORDIA
OPEN DOOR 2020
Online (tame.events) – 28 and 29 October 2020
https://opendoor.concordia-h2020.eu/

Trust Services Forum - CA Day 2020
Berlin, Germany – 22 and 23 September 2020
https://www.enisa.europa.eu/events/tsforum-caday-2020/tsforum-caday-2020

2020 CEF Telecom Call – Cybersecurity – open calls
https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2020-cybersecurity
Submission deadlines: 5 November 2020

Cybersecurity Luxembourg Startup Pathway – event
Online – 21 and 22 October 2020
https://www.startupluxembourg.com/startuppathway

CONCORDIA

Cyber security cOmpeteNCe fOr Research anD InnovAtion

@concordiah2020

CONCORDIA Project

Concordia-h2020.eu

concordiah2020

This is the CONCORDIA stakeholders' newsletter. If this newsletter was forwarded to you and you are interested to receive it directly, you can subscribe here. You may unsubscribe here.
For any questions please contact us at:

antonioken.iannillo@uni.lu

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 830927.

www.concordia-h2020.eu