ITEA Cyber Security Advisory Board (CySAB) report

Meeting 6 July 2022, online

On 6 July 2022, the third ITEA CySAB meeting took place with the following Advisory Board members:

Company/Organisation	Country	Represented by
Academic Medical Center of the University of Amsterdam	The Netherlands	Silvia Olabarriaga
Armengaud Innovate GmbH	Austria	Eric Armengaud
Ericsson	Turkey/Sweden	Emrah Tomur
Koçfinans	Turkey	Özden Gebizlioğlu Özvural
Koçfinans	Turkey	Zühal Dilek Ataman
Siemens Mobility	Germany	Andres G. Guilarte
Signify	The Netherlands	Sandeep Kumar
Turkcell	Turkey	Emin İslam Tatli

ITEA is a Eureka Cluster instrument to build innovative RD&I projects that are funded by national funding agencies and that are based on urgent needs and requirements of end-users.

The ITEA Cyber Security Advisory Board (CySAB) is established to understand the urgent customer needs and requirements in this domain to build up innovative research projects by the ITEA Community solving Cyber security challenges. In addition, this Board enables the member organisations to learn and to get inspired from each other and to create collaboration among members and between members and the ITEA RD&I Community.

This CySAB meeting was set up to review the State-of-the-Art in cyber security with an analysis of the main trends regarding cyber security threats and how to protect against these risks. It was also the opportunity to listen to the Board members providing insights into their important Cyber security issues. Finally, a discussion took place regarding the set-up of an ITEA CySAB portal dedicated gathering the challenges and solutions at one spot.

Cyber security landscape and defence strategies

Vasco Gomes, Chief Technology Officer for Cybersecurity products at Atos, gave a keynote speech. First, he presented the Atos Cybersecurity Technology Radar which follows more than 100 technological trends in the field of Cyber security. All the information is shared and can be found at https://atos.net/en/lp/cybersecurity-tech-radar

He then discussed the key threats in 2022 covering the following topics:

- Ransomware threats
- Supply chain threats
- Vertical specialised threats
- Cloud threats
- API threats
- External remote service threats
- Conventional threats

This keynote speech was followed by an interesting discussion with the Board members. The questions and subsequent discussion focused around the following topics:

- Good balance between privacy and duration of logged data to detect risks such as supply chain attacks
- Distributed logs and impact on attack detection
- Identity management (for internal applications but also for cloud applications)

Main priorities seen by the CySAB members

1. Supply chain

Large companies have a large supply chain with hundreds of vendors. Some of the key operational tools are outsourced creating a bigger risk. Audit and certification have to continuously evolve to adapt to the moving threat landscape. Any idea to lower the risk could be a good focus for a research project.

2. Management of new multi-stakeholder services

Today, new services involve a complex value chain with a lot of stakeholders that are interconnected to provide the service. Cyber security is a bigger challenge. In this domain, we see some projects around C-ITS (Cooperative Intelligent Transport Systems) to develop these cooperative services, but other research initiatives could be complementary.

3. Real-time detection of threats

With the high number of devices and systems, the high speed of the exchange of data, manual security monitoring is not a solution anymore. The development of real-time detection systems based on AI is mandatory.

In the banking sector, new applications will also have to be monitored and decisions need to be taken in real time to allow or deny transactions. The development of a framework to monitor in real time compared with normal behaviour would help to provide the needed security level of these applications.

4. Internal attacks

In Healthcare there is a big issue related to the detection of non-compliant data access. In the IT system users have to obey to regulations and there is a need to prevent any unauthorised data access. The idea could be to develop additional checks specific to the privacy aspects. The management of credentials is a central topic for progressing on this domain.

5. Cloud service management

Growing numbers of connected objects deliver services that are implemented by cloud applications. The security of these cloud services needs to be monitored. The service providers have to implement the security check and the data storage with the right balance between, on one hand, the capability to detect attacks and on the other hand the privacy of the object users.

6. Regulations

More and more regulations are put in place at national or international levels. The management of all these regulations for an international company can be a concern. It could be useful to have tools to help to handle all the regulations.

7. Effective use of new regulation

In the transportation sector, CENELEC has issued a new norm on cyber security - TS 50701 - which is based on the IEC 62443. This norm will be mandatory for any development from July 2023 onwards. The main concern now is to adapt all the design processes to this norm. New tools are again welcome to help to enforce this new regulation.

CySAB portal

ITEA plans to prepare a portal for the CySAB members and the ITEA Community to build connections among them and to build a bridge between the CySAB and the ITEA Community. The ITEA Communications team presented the Smart City Advisory Board portal which has been developed to serve the other existing Advisory Board. Based on this presentation, the customisation of this portal to the CySAB needs has been discussed. The following set of functions and elements of the portal are under consideration:

- Information related to the CySAB meetings
- Introduction of the CySAB members
- Cyber security related news from CySAB members / ITEA (projects)
- Cyber security related ITEA projects
- Innovative outcomes from ITEA projects
- Discussion on challenges / project ideas

Conclusion - Next steps

This CySAB meeting was a great opportunity to discuss the Cyber security evolutions and to identify potential opportunities for new ITEA projects that could be submitted to the upcoming ITEA Call 2022. We want to thank Vasco Gomes from Atos and the CySAB members for sharing their views.

It is now up to the ITEA Community to prepare related cyber security projects based on this valuable information. For this purpose, you can benefit from the ITEA PO Days 2022 taking place on 13-14 September in Helsinki. More information about this event can be found at https://itea4.org/podays2022/po-days-2022.html. This 2-day networking event offers a great opportunity to find skilled partners to create new Cyber security solutions together, so we hope to see you in Helsinki!

The next CySAB meeting is planned for Q4 2022, where we would like to re-discuss the CySAB portal and to interact with a set of Cyber security focused ITEA projects.