INNCYBER Innovation HUB
Digital transformation, Cyber & IoT

INNCYBER - *CALL FOR PROJECTS*

3rd Edition | 2022

REGULATION

PREMIVALOR Consulting
Your Value Partner

Index

Article 1.

Scope

1. **INNCYBER -** ***Call for Projects*** **- 3rd Edition** is a joint initiative of partner entities (promoters) that aims to promote, among researchers, university students, professors and Startups, the development of innovative projects with local, national and international impact stimulating:

   a. Technological and Digital Innovation in cybersecurity and cyberdefense;

   b. Knowledge transfer between universities, research centers and INNCYBER's partner entities (companies and public organizations);

   c. Development of new business models, new products, new services and STARTUPS aimed at cybersecurity innovation, including areas such as Security Automation, Threat Modeling Applied to Networks, Certification, Security by Design, AIML applied to Cybersecurity, Cloud Security, Quantum Computing, etc.

1. The promoters of **INNCYBER -** ***Call for Projects*** **- 3rd Edition** are PremiValor Consulting, Altice Portugal, Altice Labs, EDP - Energias de Portugal and PwC Portugal, in articulation with other partner entities.

Article 2.

Objective

The objective of **INNCYBER -** ***Call for Projects*** **- 3rd Edition** is to bring minds from different education backgrounds collaborating on the development of ideas that can improve the cybersecurity and cyberdefence areas, while awarding the best projects and Startups focused on innovation and entrepreneurship in the areas of digital transformation, cybersecurity and IoT on each of the following categories:

- Student's category: projects developed by Master, Postgraduate or Undergraduate students from national and international Universities and Institutes;
- PhD and researcher's category: projects developed by PhD, researchers or PhD students;
- Startup's category: Startups that are developing innovative products / services / solutions with high growth potential on cybersecurity.

Article 3.

Call for Projects Regulation

1. The ***Call for Projects*** is governed by the present regulation in which the Monitoring Committee and the Jury are sovereign in their interpretation, application and gap integration.
2. The selection criteria and decision grounds, including the attribution of the awards to the winning projects, are exclusive competence of the promoters of the initiative. The decisions of the Monitoring Committee and Jury cannot be object of complaint or appeal, being always and in any circumstances unquestionable and definitive.
3. The promoters of the ***Call for Projects*** are reserved the right not to select winning projects in any categories if they conclude that there are no projects in the current edition that fit the minimum distinction requirements.

Article 4.

Duration, main phases and deadlines

1. The **INNCYBER - *Call for Projects* - 3rd Edition** will take place between January and November 2022.

2. The participation in **INNCYBER -** ***Call for Projects*** **- 3rd Edition** comprises the following phases according to the calendar presented on the number 3 of this article:

   a) Registration: will occur in 2021/2022 academic year;

   b) Project development: will occur in 2021/2022 academic year;

   c) Follow-up questionnaire: during the project development phase, the participating groups will have to answer a brief follow-up questionnaire concerning the project development process;

   d) Evaluation: the project's evaluation process will take place after the reception of all projects. The analysis of all participating groups and selection of the projects that will attend the Pitch Ceremony is responsibility of the Jury;

   e) Pitch Ceremony: the Pitch Ceremony is the event where the individuals or groups with the best projects of each category are invited to present their projects. The winning groups of each category will only be selected during the ceremony.

3. **INNCYBER -** ***Call for Projects*** **- 3rd Edition** has the following schedule:

2nd Semester – Academic year 2021/2022

Project promotion kick-off: January 5th, 2022

Registration deadline: March 15th, 2022

Submission deadline of follow-up questionnaire: April 8th, 2022

Project submission deadline: June 24th, 2022

Article 5.

Topics/themes of projects

1. **INNCYBER - *Call for Projects* - 3rd Edition** aims to promote the development of innovative projects with national and international impact, leveraging the capacity for innovation in cybersecurity and cyberdefence areas.

2. The projects to be developed should focus on strategic areas of Cybersecurity and Cyberdefence, namely:

   a) **Security Automation**:

   - Mechanisms for testing vulnerabilities in implementations using Security-by-Design

   b) Threat Modeling applied to IoT:

   - Security mechanisms applicable to IoT communication, in terms of data protection

   c) Threat Modeling applied to Networks:

   - Identification of vulnerability testing mechanisms applied in 5G private network scenarios, based on OPEN-RAN and Edge Computing approaches

   d) **Critical Infrastructures and essential services protection**;

   e) Security and vulnerabilities in the **5G World;**

   f) **Artificial Intelligence & Machine Learning applied to cybersecurity**;

   g) **Cloud Security**;

   h) **Security-by-Design (SbD);**

   i) Cybersecurity **Certification**;

   j) Cybersecurity **Risk Management and Identification**;

   k) New strategies to address **social engineering attacks**;

l) **Ethics & Human Element of Cybersecurity –** bridging the gap between machines usage in cybersecurity and the human decision-maker;

m) **Cyber Hygiene and GDPR:** Training program for the dissemination of good practices among users;

n) **Cybersecurity risks, awareness** (marketing/communication plan);

o) **Microeconomics** applied to cybersecurity;

For more details regarding some of the topics, please go to Annex I.

Article 6.

INNCYBER - Call for Projects Promotion

For a better understanding of the scope and objectives of INNCYBER - *Call for Projects* - 3rd Edition a set of actions take place to communicate the project in Universities, Institutes and Research Centres.

Nevertheless, participants can also contact PremiValor Consulting team to obtain clarifications. Please see the contacts on:

www.inncyberinnovationhub.com

Article 7.

Application requirements

The requirements to participate in the **INNCYBER - *Call for Projects* - 3rd Edition** are:

1. Students Category:

Candidates interested in participating in the INNCYBER - *Call for Projects* - 3rd Edition must apply individually or join a group of up to five members and meet the following requirements at the time of the application:

a) Attend a Master, Postgraduate or Undergraduate course in the academic year 2021/2022;

b) Candidates who have completed their bachelor, postgraduate or master's degree in the academic years 2020/2021 or 2019/2020;

c) Participants in the previous edition of INNCYBER - *Call for Projects* may reapply to this edition if they fulfil the requirements established in a) or b) of this article;

d) The groups can be composed by elements from different universities, levels of graduation (Master, Postgraduate or Undergraduate) and from different areas of knowledge to foster multidisciplinary and complementarity;

e) The candidates (individuals or participating groups) can include one or more supervisors or advisors with knowledge in the areas covered by INNCYBER INNOVATION HUB. Nevertheless, the absence of a supervisor or an advisor is not an exclusion factor of the individual or group in the competition.

2. PhD and Researchers Category:

The requirements to participate in PhD and Researchers category are:

a) Have a PhD/Doctorate degree; or

b) To attend in the present academic year (2021/2022) a PhD program;

c) To be a researcher in a University, Institute or Research Center.

3. Startups Category:

a) Startups at different levels of development / TRL can apply to INNCYBER - *Call for Projects* if they focus on the cybersecurity or cyberdefence areas;

b) Early stages startups are accepted but they need to have a clear market orientation and the vision to have a commercial product/service in a maximum time frame of 2 or 3 years.

It is not allowed to compete simultaneously in Students, PhD and Researchers and Startup categories with the same project.

Article 8.

Application procedures

1. Candidates who fulfil the conditions required in the previous article must formalize their applications by completing the form provided by the Monitoring Committee of INNCYBER - *Call for Projects*.

2. Along with the application form, all participants should provide the following documents:

   Students and PhD and Researchers categories

   2.1 For those who fit in article 7.1 a) should provide a document proving attendance of a university/institute in the academic year 2021/2022 (e.g. student card).

   2.2 For those who fit in article 7.1 b) should provide a document proving attendance of a university/institute in the academic years 2020/2021 or 2019/2020.

   2.3 For those who fit in article 7.2 a) or 7.2 b) should provide a copy of the certificate/document of the PhD degree or PhD student.

   2.4 For those who fit in article 7.2 c) should provide a document proving their condition from University, Institute or Research Center.

   Startup category

   2.5 Formal document with information about the company, namely area of activity, indication of the owners/shareholders of the company, foundation date, etc. (e.g. “certidão permanente”/legal constitution document or equivalent). A written declaration from the founders of the startup monitoring committee is also accepted.

2.6 INNCYBER may request additional information.

3. The formalization of the application means the acceptance, without reservation or conditions, by the interested parties of the terms and regulation of this competition, as well as the express authorization to verify the authenticity of the respective documents made available.

Article 9.

Monitoring process

1. The monitoring process aims to assist the participants during the development of the projects.
2. The follow-up process includes the fulfilment of a questionnaire provided by the **INNCYBER - *Call for Projects* - 3rd Edition** Monitoring Committee to the participants.
3. The follow-up questionnaire is available on the website of INNCYBER INNOVATION HUB (www.inncyberinnovationhub.com).
4. The submission of the follow-up questionnaire should be done in accordance with the number 3 of article 4 of the current regulation.
5. Within a period of two weeks following the follow-up questionnaire submission deadline, the Monitoring Committee will provide feedback to each individual or candidate group.
6. If necessary, the Monitoring Committee may request the individual or group candidates to submit additional information or to provide some clarifications regarding the project they aim to develop.

7. The participants may contact the Monitoring Committee during the project development period to obtain any clarifications (important note: The Monitoring Committee will not provide any reserved or non-public information or information that may affect the competitiveness and independence of the competition).

Article 10.

Project submission procedures

1. The report must be submitted in a PDF format.
2. The report can be written in English (preferably), Portuguese or Spanish languages. If the report is written in Portuguese or Spanish, it must include a detailed abstract (1 page) in English.
3. As a guideline, it is suggested that the projects do not exceed 25 pages (Word format) or 50 slides (PowerPoint format), excluding appendixes such as graphic material, videos, market research studies/analysis, programming code or other relevant elements.
4. The projects submitted can include one or more videos.
5. The report and any content related to the project should be submitted to the following email: **INNCYBER_innovation_HUB@premivalor.com**. Files should be sent in non-editable format such as PDF format. If the project is composed by several documents, the participants should send a ZIP file containing all the documents.
6. If the uploaded files exceed 5 Mb they can be placed on online platforms (e.g. WeTransfer, Google Drive, etc.) and an email should be sent to **INNCYBER_innovation_HUB@premivalor.com** sharing the link for download.
7. With the project's submission, the individuals or candidate groups must also send the Final Project Summary, available on the *Call for Projects* web page.

8. Any questions or doubts regarding project submission procedures should be emailed to **INNCYBER_innovation_HUB@premivalor.com**.
9. The projects and the Final Project Summary should be delivered according to the deadlines stipulated in Article 4 of the present regulation.

Article 11.

Monitoring Committee and Jury

1. The whole process of launching, processing, interpretation of the Regulation, awarding and implementation of the **INNCYBER - *Call for Projects* - 3rd Edition** is responsibility of the Monitoring Committee, composed by members of PremiValor Consulting, Altice Portugal, Altice Labs, EDP - Energias de Portugal, PwC Portugal and other partner organizations of the INNCYBER INNOVATION HUB.
2. The members of the Monitoring Committee and the Jury will be responsible for analyzing all the candidate projects to select the projects of each category to attend the Pitch Ceremony.
3. The Jury has sole authority, and decides sovereignly, according to the most appropriate criteria considering the objectives of INNCYBER INNOVATION HUB, which are outlined in the article 12 of the present regulation.
4. The Jury is responsible for the final decision of the award attribution in each category. It is composed by members of the Monitoring Committee, joined by at least three other members, at minimum one of them being independent of the promoters of the initiative.

Article 12.

Evaluation Criteria

The evaluation of the projects developed under Students and PhD and Researchers categories is based on the following criteria:

a) Methodology applied in the development of the project (technical development and scientific component) - 20%

b) Innovation of the project / solution - 40%

c) Robustness of the product, service or solution proposed in terms of possible implementation - 15%

d) Business model (including economic viability of the project) (if applicable) - 15%

e) Project presentation (formal report) - 10%

The evaluation of the participating Startups on the Startups category is based on the following criteria:

a) Innovation of the product, service, solution or process - 30%

b) Business model (including economic viability of the project or solution) - 30%

c) Potential of scalability - 20%

d) Importance of the product/service or solution for organizations and society - 20%

The presentation performance at the Pitch Ceremony is also an Evaluation Criterion for all categories that will be considered by the jury members.

Article 13.

Pitch Ceremony

1. The Pitch Ceremony is the event in which the best projects from each category will be presented publicly in an Elevator Pitch format:

    a. **Students Category:** Top 10 projects will be selected for the Pitch Ceremony;

    b. **Doctorates and Researchers Category:** a maximum of 5 projects will be selected for the Pitch Ceremony;

    c. **Startups Category:** A maximum of 10 Startups will be selected for the Pitch Ceremony.

2. At the Pitch Ceremony, the jury will evaluate the finalist projects and decide the winners of each category of **INNCYBER -** ***Call for Projects*** **- 3rd Edition.**

4. At least one group member must attend the Pitch Ceremony. If no element of a group attends the Pitch Ceremony that group will be excluded.

5. All participant individuals or groups will be invited to attend the Pitch Ceremony.

6. Details of the participation in the Pitch Ceremony will be made available to the finalist groups with sufficient time advance so that they can prepare their presentations.

7. The groups invited to the Pitch Ceremony expressly commit to the disclosure of their image and data regarding the *Call for Projects* promotion, the beneficiaries themselves, their Academic Institutions and of the Promoters of the event.

Article 14.

Communication of the decision

1. After the evaluation of the finalist projects, the decision on who are the winning individuals or group candidates of the **INNCYBER - *Call for Projects* - 3rd Edition** will be disclosed and communicated during the Ceremony.
2. There will be no isolated communications about the projects concerning the evaluation process and evaluations.

Article 15.

Intellectual Property of Candidate Projects

1. The intellectual property of the candidate projects belongs to their authors.
2. The reports related to the projects submitted to the contest will not be returned to the candidates, with the management of the contest allowed to disclose them in general terms.

Article 16.

Award Rights

1. Awards will be assigned based on the technical evaluation of the projects carried out by the **INNCYBER - *Call for Projects* - 3rd Edition** Jury.

   1.1 Students Category:

First Place

The first-place project will be awarded a prize of an amount equivalent to €5,500 (five thousand and five hundred euros), comprised of a monetary amount of € 2,500 (two thousand and five hundred euros) and € 3,000 (three thousand euros) in dedicated mentoring hours from experienced professionals with expertise in business modelling, finance, business development and other relevant areas.

If the winning group is accompanied by one or more supervisors or advisors, a total gross monetary amount of €1,000 (one thousand euros) will be awarded to the supervisor(s) or advisor(s).

The first-place winners also receive a formal declaration of their achievements for academic/professional CV enrichment purposes.

Second Place

The second-place project will be awarded a prize of an amount equivalent to €2,500 (two thousand and five hundred euros), comprised of a monetary amount of € 1,000 (one thousand euros) and € 1,500 (one thousand and five hundred euros) in dedicated mentoring hours from experienced professionals with expertise in business modelling, finance, business development and other relevant areas.

If the group is accompanied by one or more supervisors or advisors, a total gross monetary amount of €750 (seven hundred and fifty euros) will be awarded to the supervisor(s) or advisor(s).

The second-place winners also receive a formal declaration of their achievements for academic/professional CV enrichment purposes.

Third place

The third-place project will be awarded a prize of an amount equivalent to €1,000 (one thousand euros) in dedicated mentoring hours from experienced professionals with expertise in business modelling, finance, business development and other relevant areas.

The third-place winners also receive a formal declaration of their achievements for academic/professional CV enrichment purposes.

1.2 PhD and Researchers Category:

First Place

The first-place project will be awarded a prize of an amount equivalent to €7,000 (seven thousand euros), comprised of a monetary amount of € 2.000 (two thousand euros) and € 5,000 (five thousand euros) in dedicated mentoring hours from experienced professionals with expertise in business modelling, finance, business development and other relevant areas.

The first-place winners also receive a formal declaration of their achievements for academic/professional CV enrichment purposes.

Second Place

The second-place project will be awarded a prize of an amount equivalent to €3,500 (three thousand and five hundred euros), comprised of a monetary amount of €1,000 (one thousand euros) and €2,500 (two thousand and five hundred euros) in dedicated mentoring hours from experienced professionals with expertise in business modelling, finance, business development and other relevant areas.

The second-place winners also receive a formal declaration of their achievements for academic/professional CV enrichment purposes.

Third Place

The third-place project will be awarded a prize of an amount equivalent to €1,000 (one thousand euros) in dedicated mentoring hours from experienced professionals with expertise in business modelling, finance, business development and other relevant areas.

The third-place winners also receive a formal declaration of their achievements for academic/professional CV enrichment purposes.

1.3 Startups Category

First Place

The first-place will be awarded a prize of an amount equivalent to €6,500 (six thousand and five hundred euros), comprised of a monetary amount of € 1.500 (one thousand and five hundred euros) and € 5,000 (five thousand euros) in dedicated mentoring hours from experienced professionals with expertise in business modelling, finance, business development and other relevant areas.

The first-place winners also receive a formal declaration of their achievements for academic/professional CV enrichment purposes.

Second Place

The second-place will be awarded a prize of an amount equivalent to €3,000 (three thousand euros), comprised of a monetary amount of € 500 (five hundred euros) and € 2,500 (two thousand and five hundred euros) in dedicated mentoring hours from experienced professionals with expertise in business modelling, finance, business development and other relevant areas.

The second-place winners also receive a formal declaration of their achievements for academic/professional CV enrichment purposes.

Third Place

The third-place will be awarded a prize of an amount equivalent to €1,000 (one thousand euros) in dedicated mentoring hours from experienced professionals with expertise in business modelling, finance, business development and other relevant areas.

The third-place winners also receive a formal declaration of their achievements for academic/professional CV enrichment purposes.

2 The right to the award is automatically and definitively extinguished, and without the need for any specific formalism, if any of the following occur:

a) It is concluded that there is some irregularity in the application of the winning individual(s), group or project;

b) There is evidence of the project being carried out by other members other than the members of the awarded group or project;

c) Evidence of plagiarism;

d) If the prize is not claimed within one year from the date of the Pitch Ceremony;

e) If, pending the benefit of the award, the winners are subject to any criminal proceedings instituted by the State or disciplinary proceedings instituted by the institution of attendance of the course or working institution, or the winners assume a behaviour regarding the promoters, sponsors or third parties that, due to its severity, determine damage to the image or honourability of the participants or discredit or injury to the entities involved or to themselves.

3 The award of the prize assumes an assumption of a **minimum** of 10 received projects in Students category, 3 projects in PhD and Researchers category and 3 Startups. In case the minimum number of projects is not met in a given edition, the submitted projects are automatically enrolled to the following edition, giving the opportunity to the candidates to work in their development/improvement if they desire.

Article 17.

Changes to deadlines and dates in this Regulation

The deadlines and dates contained in this Regulation may be changed by decision of the promoters of **INNCYBER - *Call for Projects* - 3rd Edition**, who will publicly announce it.

Article 18.

Processing of Personal Data

1. Enrolment and participation in **INNCYBER - *Call for Projects* - 3rd Edition** implies the collection and processing of personal data of the interested parties, for which PremiValor Consulting and the project partner entities are responsible, with the data to be processed for the purposes of verifying compliance with the conditions of participation, pursuing the due diligence and communications necessary for the participation and development of the projects and the delivery of the award, holding questionnaires, monitoring, development of the project evaluation process and public disclosure of the image and identification data of the interested parties classified for the award. These purposes are based on the consent of the data subject, provided through the application form.

2. The responsible undertake to comply at all times with the legal duties arising from the processing of personal data, including compliance with the appropriate technical and organizational security measures to ensure data protection with a view to compliance with applicable legislation on the protection of personal data, in particular Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

3. The collection and processing of personal data of interested parties is a necessary requirement for entry and participation in **INNCYBER - *Call for Projects* - 3rd Edition**. Failure to provide or incomplete or incorrect data may make it impossible to participate in **INNCYBER - *Call for Projects* - 3rd Edition.**

4. In cases where the processing of personal data is performed solely on the consent of the holder, the holder has the right to withdraw his consent at any time. The withdrawal of consent, however, does not compromise the legality of the treatment based on the consent previously given.

5. Anyone wishing to participate in **INNCYBER - *Call for Projects* - 3rd Edition**, by submitting an application identifying a third party's personal data, must first ensure that has provided the third party with the information present in this Regulation and obtained the respective consent of the third party for the communication of their personal data to the responsible for the strict purposes set out in this clause.

6. The personal data of participating students and professors will be retained by the holder until the conclusion of the edition of **INNCYBER - *Call for Projects* - 3rd Edition** in which they participated, after which it will be deleted unless, under applicable law or regulation, or due to pending litigation, retention for a longer period is mandatory.

7. To the data holders are guaranteed the rights of access, rectification, deletion and portability of their personal data, as well as the right to object and to limit their processing, under the applicable legal terms, ought the responsible to be contacted through the following contacts: PremiValor Consulting, Avenida 5 de Outubro, n. º 75 - 7th floor, 1050-049 Lisbon or by the email **INNCYBER_innovation_HUB@premivalor.com**.

8. Data holders also have the right to file complaints regarding the processing of their data with the National Data Protection Commission or other competent supervisory authority.

ANNEX I

Annex I

Details of topics referred on Article 5

Topic: **Security Automation**

Area: Mechanisms for testing vulnerabilities in implementations using security by design

- DevOps processes enable businesses to bring applications to market quickly and efficiently. Many companies are now realizing these benefits by automating the continuous integration and continuous delivery (CI/CD) of their applications. However, the need for safe and secure software is paramount. The term DevSecOps is used to describe the integration of security at every phase of the software development lifecycle, from initial design through integration, testing, deployment, and software delivery. It advocates that security should be built into the product, rather than applied to a finished one.

- DevSecOps builds on the learnings and best practices of general DevOps. The application of DevOps values to software security means that security verification becomes an active, integrated part of the development process. The CI/CD processes introduced by DevOps ensure the active testing and verification of code correctness during the agile development process. Similarly, DevSecOps injects active security audits and penetration testing into agile development.

- The main goal of this project is to understand how security can be automated as part of the CI/CD pipeline, with a special focus on container security automation.

The increased attack surface of container infrastructures makes security even more important, but security and DevOps teams can't afford to slow the pipeline with manual processes. In a broader context, security testing tools, such as security unit tests, SAST, DAST, dependency checks, etc., should be analyzed. The tools more appropriate for containers should be further evaluated, tested, and possibly extended to comply with additional security requirements.

Topic: **Threat Modeling Applied to Networks**

Area: Identification of vulnerability testing mechanisms applied in 5G private network scenarios, based on Open-RAN and Edge Computing approaches.

- Data networks have enabled extraordinary growth in capabilities such as email, the web, and social media. Today it forms the technical basis for our information-centric economy. However, physical networking cannot support the complexity and pace of innovation in emerging applications such as Virtualized / Cloud Computing, IoT, Mobile Computing, and Big Data Analytics. The industry norm of deploying special purpose, fixed-function hardware appliances (e.g., routers, switches, firewalls, load balancers) that implement standardized protocols no longer scales with the required pace of innovation for new services, nor the economics of modern virtualized computing. In response, the industry has developed new initiatives regarding Network Function Virtualization (NFV) and Software-Defined Networking (SDN), in which they abstract the implementation of new network functions and decouple them from specific hardware platforms and topological constraints. While network virtualization allows organizations to segment different virtual networks within a single physical network, or to connect devices on different physical networks to create a single virtual network, software-defined networking enables a new way of controlling the routing of data packets through a centralized server.

- The key difference between NFV/SDN and traditional networking is infrastructure: NFV/SDN is software-based, while traditional networking is hardware-based. Because the control plane is software-based, NFV/SDN is much more flexible than traditional networking. There are also security differences between NFV/SDN and traditional networking. While significant improvements may be achieved in network security by centralization and programmability (due to greater visibility and the ability to define secure pathways), these two concepts can also attract a new level of threats and attacks. Security within the SDN paradigm is a challenge, as all layers, sub-layers, and components need to communicate according to strict security policies. Additionally, because SDNs use a centralized controller, securing the controller is crucial to maintaining a secure network, and this single point of failure represents a potential vulnerability of SDN.

- The main goals of this project are to identify sensitive assets in both traditional and virtual networks, threats to those assets, and vulnerabilities that make the threats a necessary concern, as well as to propose possible mitigations for those threats. A template for Microsoft Threat Modeling Tool should be created with that information and used over a lab network environment in Altice Labs using 5G, Open-RAN and Edge computing.

Topic: **Threat Modeling Applied to IoT**

Area: Security mechanisms applicable to IoT communication, in terms of data protection

- Nowadays, information is constantly collected from multiple devices (smartphones, sensors, gateways, …), which can vary from basic network statistics to sophisticated data and detailed user information. With an exponential increase in devices that connect to the internet, people see huge benefits for communications and productivity. Internet of Things (IoT) plays a big part in this context, with IoT solutions trending at an explosive rate.

- Although this new data collection paradigm offers great business opportunities, these devices can also leave systems and networks exposed to a growing number of new cyber threats. It is well known that IoT devices are generally lagging in terms of network and information security, due to a lack of manufacturing standards and IoT regulations, as well as the reduced computational power and storage space of those devices. Even if one device is properly secured, unsecured devices can still exist in a certain ecosystem, opening up entire networks to data breaches.

- Architecturally based IoT threat modeling can help to identify privacy and security issues in this context. The main goals of this project are to identify sensitive assets in IoT ecosystems, threats to those assets, and vulnerabilities that make the threats a necessary concern, as well as to propose possible mitigations for those threats. A template for Microsoft Threat Modeling Tool should be created with that information and used in a practical use case for Altice Labs.