INNCYBER Innovation HUB
Digital transformation, Cyber & IoT

INNCYBER - *CALL FOR PROJECTS*

4th Edition | 2023

REGULATION

PREMIVALOR Consulting
Your Value Partner

Index

Article 1.

Scope

1. **INNCYBER - Call for Projects - 4th Edition** is a joint initiative of partner entities (promoters) that aims to promote, among Researchers, University Students, Professors and STARTUPS, the development and implementation 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 solutions 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.
2. The promoters of **INNCYBER - Call for Projects - 4th Edition** are PremiValor Consulting, EDP - Energias de Portugal, PwC Portugal, MINSAIT INDRA, Altice Portugal, Altice Labs, in articulation with other partner entities.

Article 2.

Objective

1. The objective of **INNCYBER - Call for Projects - 4th Edition** is to stimulate minds from different education backgrounds to collaborate on the development of projects related with **cybersecurity** and **cyberdefence**, 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:

- **Students Category:** projects developed by Master, Postgraduate, and Undergraduate students from national and international Universities and Institutes;
- **PhD and Researchers Category:** projects developed by PhD, Researchers and PhD students from national and international Universities, Institutes and Research Centers;
- **STARTUPS Category**: STARTUPS that are developing innovative products / solutions with high potential of growth / internationalization on cybersecurity or cyberdefence.

2. The participants with the best projects of each category will have the opportunity to present the project on the Pitch Ceremony 2023 on the CYBER SUMMIT 2023.

Article 3.

Call for Projects Regulation – 4th Edition

1. The **INNCYBER - Call for Projects - 4th Edition** 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 and STARTUPS, 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 **INNCYBER - Call for Projects - 4th Edition** are reserved the right not to select winning projects in a given category 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 - 4th Edition** will take place between February and November 2023.

2. The participation in **INNCYBER - Call for Projects - 4th Edition** comprises the following phases according to the calendar presented on the number 3 of this article:

   a) **Registrations Phase;**

   b) **Project development**;

   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 projects and STARTUPS evaluation process will begin after the Project and Pitch Deck Delivery deadline. The evaluation and selection of the projects and STARTUPS that will attend the Pitch Ceremony is responsibility of the jury;

   e) **Pitch Ceremony**: the Pitch Ceremony is the event where the selected groups of Students Category, PhD and Researchers Category and the selected STARTUPS are invited to present their projects to the Jury in an Elevator Pitch format. The winning groups and STARTUPS of each category will only be selected during the Pitch Ceremony.

3. **INNCYBER - Call for Projects - 4th Edition** has the following schedule:

<u>Students Category and PhD Research Category</u>

Registrations Opening: January 30th, 2023

Registration deadline: April 21st, 2023

Submission deadline of follow-up questionnaire: April 30th, 2023

Project Delivery deadline: June 15th, 2023

<u>STARTUPS Category</u>

Registrations Opening: January 30th, 2023

Registration deadline: May 2nd, 2023

Pitch Deck Delivery deadline: June 15th, 2023

Article 5.

Topics/themes of projects

1. **INNCYBER - Call for Projects - 4th Edition** aims to promote the development of innovative projects with local, 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 - 4th Edition** a set of actions take place to communicate the project in Universities, Institutes and Research Centres and STARTUPS.

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

www.inncyberinnovationhub.com

Article 7.

Application requirements

The conditions to participate in each category of the **INNCYBER - Call for Projects - 4th Edition** are the following:

1. **Students Category:**

   1.1 Students interested in participating in the **INNCYBER - Call for Projects - 4th Edition** can **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 2022/2023;

   b) Have completed a bachelor, postgraduate or master’s degree in the academic year 2021/2022 or 2020/2021;

   1.2 Participants in the previous editions of **INNCYBER - Call for Projects** may reapply to this edition if they fulfil the requirements established in paragraph 1.1, a) or in paragraph b) of this article;

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

   1.4 The individual applications or groups can include up to three professors as supervisors/advisors with knowledge and skills in the areas covered by

INNCYBER - Call for Projects - 4th Edition. The absence of a professor as supervisor/advisor is not an exclusion factor.

1.5 It is not allowed to Students to participate in more than one application.

1.6 Professors providing mentorship as supervisors/advisors are allowed to participate in more than one group.

2. PhD and Researchers Category:

2.1 The requirements to participate in PhD and Researchers category are:

a) To have a PhD/Doctorate degree; or

b) To attend in the present academic year (2022/2023) a PhD program; or

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

2.2 Applications can be individual or in group.

2.3 Participants are not allowed to participate in more than one application.

3. STARTUPS Category:

3.1 STARTUPS at different levels of development / TRL can apply to **INNCYBER - Call for Projects - 4th Edition** if they focus on cybersecurity or cyberdefence;

3.2 Early stages startups can apply to **INNCYBER - Call for Projects - 4th Edition** 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.

4. Applicants are not allowed to compete simultaneously in the Students Category, PhD and Researchers Category and STARTUPS Category with the same project.

5. Projects that received an award in previous editions are not eligible to participate again in the same category of **INNCYBER - Call for Projects - 4th Edition**.

6. Exceptions are for projects and STARTUPS that participated in previous editions and were awarded but in the current edition **evidence a strong and robust evolution compared to the previous editions**. The Jury for these participants will be more demanding in terms of evolution of the projects or STARTUPS in order to assess if they qualify to be again in the short list to be selected to participate in the Pitch Ceremony.

Article 8.

Application procedures

1. Candidates who fulfil the conditions required in the previous article must formalize their applications by completing the Application Form available on the website of **INNCYBER INNOVATION HUB -** *www.inncyberinnovationhub.com*.
2. Along with the Application Form, participants should provide to the email address **INNCYBER_innovation_HUB@premivalor.com** the following documents:

<u>Students and PhD and Researchers categories</u>

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 2022/2023 (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 2021/2022 or 2020/2021.

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 a document proving attendance at a PhD program.

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 The Monitoring Committee 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 - 4th 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 an estimated period of two weeks following the follow-up questionnaire submission deadline, the Monitoring Committee will provide feedback to all participants.
6. If necessary, the Monitoring Committee may request the participants to submit additional information or to provide some clarifications regarding the project they are developing.
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. Participants of all categories must submit a report presenting their project.
2. The report must be delivered in PDF format.
3. The report can be written in English (preferably), Portuguese or Spanish. If the report is written in Portuguese or Spanish, it should include a detailed abstract in English.
4. It is suggested that the reports submitted by participants of the **Students Category** and **PhD and Researchers Category** do not exceed 30 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.
5. The report to be submitted by STARTUPS should follow the **Pitch Deck Template guidelines** made available to the participants. It is suggested that the projects do not exceed 50 slides (PowerPoint format), excluding appendixes such as graphic material, videos, market research studies/analysis, programming code or other relevant elements.

6. The projects submitted can include one or more videos.

7. 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.

8. 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.

9. With the project's submission, the individuals or candidate groups must also send the **Final Project Summary**, available on the **INNCYBER - Call for Projects - 4th Edition** website.

10. Any questions or doubts regarding project submission procedures should be emailed to **INNCYBER_innovation_HUB@premivalor.com**.

11. 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 - 4th Edition** is responsibility of the Monitoring Committee, composed by members of PremiValor Consulting, EDP - Energias de Portugal, PwC Portugal, MINSAIT INDRA, Altice Portugal, Altice Labs and other partner organizations of **INNCYBER INNOVATION HUB**.

2. The members of the Monitoring Committee and the Jury are responsible for analysing all the candidate projects and selecting the best 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.

Article 12.

Evaluation Criteria

1. The evaluation of the projects developed under **Students Category** and **PhD and Researchers Category** 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%

2. 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%

3. The presentation performed at the Pitch Ceremony is also an element of the Evaluation Criteria for all categories that will be considered by the jury members.

4. If a project submitted by a participating group or STARTUP in the **INNCYBER - Call for Projects - 4th Edition** has already been selected as a Finalist of the Pitch Ceremony in a previous edition, it will be taken into consideration as evaluation criteria the **advancements of the project** since the previous edition, in addition to the evaluation criteria presented in paragraph 1 and paragraph 2.

Article 13.

CYBER SUMMIT 2023 Ceremony

1. The **CYBER SUMMIT 2023** constitutes an **international event** that features a **conference** and a **fair event** that brings together **the key players of the cybersecurity and cyberdefence areas.**
2. At the conference, **internationally renowned speakers** will address the most critical topics and challenges related with cybersecurity and cyberdefence.
3. On the **fair event, Companies, Organisations, Universities and STARTUPS will have the opportunity to presented their most innovative solutions related with cybersecurity and cyberdefence**, constituting an opportunity for participants of the event to Network, identify Business Development Opportunities, present their products, services and solutions, share knowledge and recruit talent.

Article 14.

Pitch Ceremony

1. The Pitch Ceremony is the event in which the best projects (finalists) from each category will be presented publicly in an Elevator Pitch format:
    a. **Students Category:** A maximum of 10 projects will be selected for the Pitch Ceremony;
    b. **Doctorates and Researchers Category:** A maximum of 10 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 - 4th Edition.**
3. 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.
4. The Pitch Ceremony is an event integrated on the **CYBER SUMMIT 2023**.
5. The procedures regarding the participation in the Pitch Ceremony will be made available to the finalist groups.
6. The groups invited to the Pitch Ceremony expressly commit to the disclosure of their image and data regarding the **INNCYBER - Call for Projects - 4th Edition** promotion, the beneficiaries themselves, their Academic Institutions and of the Promoters of the event.

Article 15.

Communication of the decision

1. After the evaluation of the finalist projects and STARTUPS, the decision on who are the winners of the **INNCYBER - Call for Projects - 4th Edition** will be disclosed and communicated during the Pitch Ceremony.
2. There will be no isolated communications about the projects concerning the evaluation process and evaluations.

Article 16.

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 17.

Award Rights

1. Awards will be assigned based on the technical evaluation of the participating projects and STARTUPS of the **INNCYBER - Call for Projects - 4th 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 and business development.

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 and business development.

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 and business development.

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 and business development.

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 and business development.

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 and business development.

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

2 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 and business development.

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 and business development.

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 and business development.

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

3 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.

4 The award of the prize presumes a **minimum** of 10 received projects in each category. In case the minimum number of projects is not met in a given edition, the submitted projects are automatically enrolled for the following edition, giving the opportunity to the candidates to work in their development/improvement if they desire.

Article 18.

Changes to deadlines and dates in this Regulation

1. The deadlines and dates contained in this Regulation may be changed by decision of the promoters of **INNCYBER - Call for Projects - 4th Edition**, who will publicly announce it.

Article 19.

Processing of Personal Data

1. Enrolment and participation in **INNCYBER - Call for Projects - 4th 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 - 4th Edition**. Failure to provide or incomplete or incorrect data may make it impossible to participate in **INNCYBER - Call for Projects - 4th 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 - 4th 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 - 4th 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

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.