2022
CYBERWAL IN GALAXIA PROGRAM

INVESTING IN CYBERSECURITY FOR A SECURE FUTURE

12 - 16 DECEMBER
EURO SPACE CENTER
TRANSINNE

HANDBOOK

Cyberwal in GALAXIA

IDELUX DÉVELOPPEMENT

Cyberwal by digital wallonia .be

Table of contents

Presentation of the CyberWal in Galaxia Program 4

Organizers 5

IDELUX 5

CyberWal by Digital Wallonia 6

Program of the Cyberwal in Galaxia 7

Speakers 14

Certificate of Participation 19

Gala dinner 19

Goodies sustainability 19

Presentation of the CyberWal in Galaxia Program

In order to meet the challenges of cybersecurity, and particularly the threats linked to cybercrime, Wallonia has decided to set up a center of excellence to protect its territory, society and also all the players involved.

Wallonia therefore responds to the objectives of the European Commission, but also of the Walloon Recovery Plan; by creating a structuring and large-scale Walloon ecosystem, involving the local industrial scenery, but also by creating bridges with training, research and innovation.

In this context, and among the strategic tools and services that will be put into place, the “Cyberwall in Galaxia Program” school, organized at the Euro Space Center in Transinne, is the first international school linked to the Cyberwal initiative. You are nearly 80 to have registered!

This school, whose funding is provided by the Walloon Region, is organized by IDELUX Development, under the authority of a Scientific Committee chaired by Mr Axel LEGAY, Professor of Cybersecurity at UC Louvain.

This edition will therefore take place on the Galaxia site, which forms, with the ESEC center of the European Space Agency (ESA) in Redu, a leading space center in Europe. It is in this ESEC center in Redu that ESA has also decided to base its cybersecurity center, which will be responsible for ensuring the cyber protection of the Agency's ground and in-flight activities.

Organizers

IDELUX

The IDELUX Group is the territorial development agency in the province of Luxembourg.

The group is active in four main areas: economic development, support for municipalities in the creation of their projects, water management and waste management.

Composed of five intermunicipal companies, its mission of general interest is to "contribute to the improvement of the well-being of the population in the territory it serves".

Among the priority economic sectors for IDELUX, the space field is strategic with the establishment of one of the 7 operational centers of the European Space Agency (ESA) in Redu in the province of Luxembourg. The role of IDELUX is to create a real cybersecurity ecosystem around Redu-Galaxia (Transinne), an economic activity park dedicated to space and high technologies, managed by the Intercommunale.

In concrete terms, ESA, with which IDELUX has a close relationship, is working hard to set up its knowledge center as well as its CSOC (Cyber Security Operation Center) in order to ensure, essentially from Redu, the Agency's ground and in-flight cybersecurity operations.

On the strength of its commitment in this priority sector, IDELUX has supported the "Cyberwal" initiative which brings together, thanks to the decisive work of Professor Axel LEGAY, all the Walloon actors involved in cybersecurity.

The Cyberwal initiative, inaugurated at Galaxia, positions the province of Luxembourg as one of the key players in the Belgian regional cybersecurity policy.

It is in the context of Cyberwal that an international school dedicated to cybersecurity is organized during the week of December 12th 2022 at Galaxia. This school is part of the Walloon Recovery Plan funding and has been supported by the Minister Willy BORSUS.

CyberWal by Digital Wallonia

Walloon and Brussels actors active in the field of cybersecurity have come together to create the "CyberWal" ecosystem (Cyber Security for Wallonia).

This virtual institute aims to promote research, innovation and training, but also aims to reach as many players as possible, by raising their awareness towards issues related to cybersecurity.

CyberWal brings together all the researchers working on cybersecurity within the Universities of the Wallonia-Brussels Federation and Walloon Approved Research Centers (CRA). It also includes the skills centers that will train the cybersecurity technicians and talents of tomorrow. The latter will also benefit from advanced training on the most recent research results, but also on the "basics" of cybersecurity.

Internationally recognized for his expertise in cybersecurity, member of the Digital Council and Professor at the Catholic University of Louvain, Axel LEGAY is the scientific coordinator of the CyberWal alliance by Digital Wallonia. He is also one of the initiators-designers of the CoronAlert application, and the President of the Scientific Committee of the “Cyberwal in Galaxia Program” School.

The CyberExcellence project, validated today by the Walloon Government, represents the first research project linked to the activity of CyberWal.

Program of the Cyberwal in Galaxia

Day 1
Monday 12/12

9:30 AM – 10:30 AM
REGISTRATIONS

10:30 AM – 11:00 AM | Auditorium
Luxembourg Seminar - 2nd Greater Region Software Engineering Research Days (SOFTER)

Each year, SOFTER brings together researchers from academia to discuss foundations, techniques, and tools for automating the analysis, design, implementation, testing, and maintenance of complex software systems. A special emphasis is put this year on Machine-Learning Systems.

Yves Le Traon - Full Professor in Computer Science - Systems and Software Reliability - Deputy Director of SnT

11:00 AM – 01:00 PM | Auditorium
Research presentations

01:00 PM – 02:30 PM
LUNCH TIME

02:30 PM – 03:45 PM | Auditorium
Panel on career progression

Axel Legay - Professor of Cyber Security - UCLouvain - President of the Scientific Committee

03:45 PM – 04:00 PM
COFFEE BREAK

04:00 PM – 06:00 PM | Auditorium
Research presentations

The objective of this presentation is to briefly retrace the evolution of the careers of researchers. The second part of the presentation consists of listing the questions I asked myself when I was in your place and discussing the possible answers with you.

Axel Legay - Professor of Cyber Security - UCLouvain - President of the Scientific Committee

OR

02:30 PM – 04:15 PM | ESEC (Redu)
Cyber Range technology and state of the art capabilities

Cyber Range is a powerful tool for creating digital twin of any IT environment and Cybersecurity scenario. This session explains how Cyber Range can be used for training, validation & testing, as well as for cyberattack simulation.

Pascal Rogiest - Managing Director of the Cybersecurity Division of RHEA Group, Chief Strategy Officer of RHEA Group, Vice President of RHEA Belux

Matteo Merialdo - Deputy Director of the Operational Security Services Unit (ESEC - ESA) in Redu.

03:45 PM – 04:00 PM
COFFEE BREAK

04:30 PM – 06:00 PM | ESEC (Redu)
CyberExcellence@ESEC
Building a State-of-the-Art Space Cyber Security Capacity
Be part of the game

Jean-Luc Trullemans - Head of the European Space Security and Education Centre (ESEC)

Day 2
Tuesday 13/12

8:30 AM – 9:00 AM
REGISTRATIONS

9:00 AM – 9:30 AM | Auditorium
Welcome to 2022 Cyberwal in Galaxia Program

Axel Legay - Professor of Cyber Security - UCLouvain - President of the Scientific Committee

Georges Cottin - Deputy General Manager of IDELUX

9:30 AM – 10:30 AM | Auditorium
EU NIS2 Directive : enabler for more IT/OT security

Kurt Callewaert - Howest Valorisation Manager Digital Transformation.

Benoit Balliu - Howest Researcher in Industrial Security.

Tijl Atoui - Howest Cybersecurity Teacher and Researcher in Industrial Security and Fictile Factory maintaining.

10:30 AM – 11:00 AM | Auditorium
Introduction to OT/ICS Security

Kurt Callewaert - Howest Valorisation Manager Digital Transformation,.

Benoit Balliu - Howest Researcher in Industrial Security.

Tijl Atoui - Howest Cybersecurity Teacher and Researcher in Industrial Security and Fictile Factory maintaining.

12:30 PM – 02:30 PM
LUNCH TIME

11:00 AM – 12:30 PM | Auditorium
Industrial Environment Scanning and Enumeration

Kurt Callewaert - Howest Valorisation Manager Digital Transformation.

Benoit Balliu - Howest Researcher in Industrial Security.

Tijl Atoui - Howest Cybersecurity Teacher and Researcher in Industrial Security and Fictile Factory maintaining.

2:30 PM – 3:30 PM | Freedom & ISS
Exploitation in an Industrial Environment

Fictile is a fast-growing fiction tile-producing company. Under the steady and continuous leadership of J.C. they are the unrivaled market leader in their sector since 2016. Their factory contains three halls. A hall with hydraulic presses, baking installation and a painting hall. To remain brand independent, the lead engineer of the factory decided to equip each hall with different types of industrial controllers. The three market leaders were chosen: Siemens, Beckhoff, and Phoenix Contact. According to investor K.C., there is no room in the budget for cyber-security. “Production must come first.”

Can you prove them wrong, by capturing all the flags?

Kurt Callewaert - Howest Valorisation Manager Digital Transformation.

Benoit Balliu - Howest Researcher in Industrial Security.

Tijl Atoui - Howest Cybersecurity Teacher and Researcher in Industrial Security and Fictile Factory maintaining.

PROGRAM

3:30 PM – 5:30 PM | Freedom & ISS

Lab work: Hands on - Industrial CTF on the Fictile Factory

Kurt Callewaert - Howest Valorisation Manager Digital Transformation, Former Head of Research Applied Computer Science.

Benoit Balliu - Howest Researcher in Industrial Security.

Tijl Atoui - Howest Cybersecurity Teacher and Researcher in Industrial Security and Fictile Factory maintaining

6:00 PM – 8:00 PM

VIP Eurospace Center visit

Join us for an unique experience at the Euro Space Center on Tuesday, 13th of December.

Day 3
Wednesday 14/12

9:00 AM – 9:30 AM
REGISTRATIONS

09:30 AM – 12:30 PM | Auditorium
Theoretical part: Malware Reverse Engineering

Software reverse engineering aims to analyse binary code, for which there is no corresponding source code available to the analyst, with a view to understand what it does and how it works. For malware analysis, it also aims to identify, defeat and eliminate the malware.

In this course, we introduce the four phases of reverse software engineering in the context of malware analysis:

Basic static analysis reviews ways to get information from the structure of a binary executable. Important functionality and clues about the type of network communications used can be derived from the libraries the executable depends on.

Basic dynamic analysis requires running the executable in an isolated or virtualised environment, in order to identify high level observable behaviour, such as modifications made to the system (e.g. created files, modified registry entries, etc) and network addresses the executable connects to, which can all be used to derive identification signatures.

Advanced static analysis consists of analysing the actual instructions of the program, to gain a fine grained understanding of its operations.
This requires familiarity with assembly language constructs, which not only depend on the platform instruction-set, the operating system, but also the language and compiler used to create the executable.

Advanced dynamic analysis is essentially binary debugging, used to examine the internal state of the running executable, giving not only a very detailed view of the operations of the executable, but also how it reacts to changes made to its internal state.

Laurent Mathy - Professor of Systems and Security in the Electrical Engineering and Computer Science.

12:30 PM – 02:30 PM
LUNCH TIME

02:30 PM – 05:30 PM | Freedom & ISS
Lab work: Malware Reverse Engineering

For these topics, after a theoretical review, we also present some anti-analysis techniques used in malware to prevent or hinder analysis, as well as labs to illustrate and put the acquired knowledge into practice.

Laurent Mathy - Professor of Systems and Security in the Electrical Engineering and Computer Science.

06:30 PM – 07:30 PM| Hub
Aperitif

07:30 PM – 10:30 PM | Voyager Café
Gala Dinner at the Euro Space Center

Day 4
Thursday 15/12

On this day, students have the opportunity to choose between two courses, one on testing which starts at 9:30 am and the other on Federated Learning which starts at 10:30 am. The syllabus of both courses is given below.

9:00 AM – 9:30 AM
REGISTRATIONS

09:30 AM – 12:30 PM | Freedom & ISS

Theoretical part: Certification oriented cybersecurity testing of cyber physical systems with fuzzing techniques

The course aims to teach students how to use fuzzing techniques for cybersecurity testing of cyber physical systems. The course introduces relevant cybersecurity certification schemes and explains how to design the testing process for certification evidence gathering.

The course is composed of three parts: 1) cybersecurity certification and testing, 2) cybersecurity testing processes, and 3) Dynamic testing and fuzzing techniques.

The course starts by providing an overview of product and process cybersecurity schemes and introducing the NIS directive with it's focus on risk analysis.

The course then describes the requirements that certification schemes impose on the testing process such as maintaining traceability between risk analysis and testing.

The course then introduces the Common Criteria product certification scheme and its concepts of protection profile and evaluation assurance level that will be used in the practical work.

The second part of the course then provides an overview of the different phases of the penetration testing process and the tools that can be used during each phase.

The third part of the course focuses on dynamic testing fuzzing techniques and how to use them to test cyber physical systems. The general fuzzing process is then introduced along with a description of black-box, white-box and grey box-fuzzing. The state of the art in fuzzing is then presented with an overview of fuzzing tools.

Xavier Devroye - Assistant Professor of Software Engineering at the Namur Digital Institute and the Faculty of Computer Science of the University of Namur.

Christophe Ponsard - Research-Innovation-Exploitation Coordinator.

OR

10:30 AM – 12:30 PM | Freedom & ISS

Theoretical part: Secure Federated Learning

The course aims to introduce students to the understanding of different Federated Learning concepts with a focus on security vulnerabilities and cyber security challenges. The course will introduce the Federated Learning and compare it to other Machine Learning approaches.

The main concepts and process of Federated Learning will then be presented. The model aggregation phase will then be presented along with the security threats. The concept of differential privacy and its relevance for federated Learning explained. Homomorphic encryption techniques will then be introduced for securing the federated Learning process.

The course will then present open-source frameworks for federated learning that will be used in the practical work.

Xavier Lessage - Senior Research Engineer in the Data Science Department at CETIC.

12:30 PM – 02:30 PM
LUNCH TIME

02:30 PM – 05:30 PM | Freedom & ISS

Lab work: Certification oriented cybersecurity testing of cyber physical systems with fuzzing techniques

The practical work will apply the certification and fuzzing concepts presented in the course to a mobility case study composed of virtualized rovers that navigate on the road under the supervision of a traffic control system. The rover software and firmware needs to be updated on a regular basis. The practical work will involve performing an impact analysis to determine if certified components are impacted, performing fuzzing tests to detect possible vulnerabilities and reporting on the tests required by the impact analysis.

Xavier Devroye - Assistant Professor of Software Engineering at the Namur Digital Institute and the Faculty of Computer Science of the University of Namur.

Guillaume Ginis - Senior Researcher in Cybersecurity at CETIC.

OR

02:30 PM – 04:30 PM | Freedom & ISS

Lab work: Secure Federated Learning

The practical work aims at applying Federated Learning concepts with a practical exercise from the medical/hospital domain (classification of medical images (malignant or benign lesions)). The practical work will cover the steps required to train a neural network (CNN) with a Federated learning architecture. The practical work will involve adapting the model to meet cybersecurity challenges and performing cybersecurity tests.

Xavier Lessage - Senior Research Engineer in the Data Science Department at CETIC.

Day 5
Friday 16/12

8:00 AM – 8:30 AM
REGISTRATIONS

8:30 AM – 10:00 AM | Auditorium

Theoretical part: Machine Learning Security in the Real World

Adversarial attacks are considered as one of the most critical security threats for Machine Learning (ML). These attacks apply small perturbations to some original examples in order to produce adversarial examples, specifically designed to fool ML model decision.

In order to enable the secure deployment of ML models in the real world, it is essential to properly assess their robustness to adversarial attacks and develop means to make models more robust. A common way to assess robustness is to empirically compute the model performance on the adversarial examples that an attack produced from a set of original examples.

Similarly, the established way to harden ML models is adversarial hardening, i.e. training processes that make models learn to make correct predictions on adversarial examples.

Traditional adversarial attacks were designed for image recognition and assume that every image pixel can be modified independently to its full range of values. In many domains, however, these attacks fail to consider that only specific perturbations could occur in practice due to the hard domain constraints that delimit the set of valid inputs (e.g., financial transactions must have a positive amount, text must be linguistically consistent, medical images can change depending on the machine used and patients' morphology, etc.).

Because of this, they almost-always produce examples that are not feasible (i.e. could not exist in the real world).

As a result, research has developed real-world adversarial attacks that either manipulate real objects through a series of problem-space transformations (i.e. problem-space attacks) or generate feature perturbations that satisfy predefined domain constraints (i.e. constrained feature space attacks).

In this lecture, we will review the scientific literature on these attacks and report on our experience in applying them to real-world cases.

Maxime Cordy - Research Scientist at the Interdisciplinary Center for Security, Reliability and Trust (SnT)

10:00 AM – 12:00 PM | Freedom & ISS

Lab work: Machine Learning Security in the Real World

During the lab, the students will gain practical knowledge on adversarial attacks via an online game and a hands-on exercise.

Maxime Cordy - Research Scientist at the Interdisciplinary Center for Security, Reliability and Trust (SnT)

Speakers

Tijl Atoui

Howest Cybersecurity Teacher and Researcher in Industrial Security and Fictile Factory maintaining

Tijl graduated in 2020 and has a Bachelor Applied Computer Science. Now he is a Cybersecurity teacher and researcher for the Security and Privacy research group of HOWEST.

The focus of his research is mainly Industrial Security and maintains the Fictile factory.

Benoit Balliu

Howest Researcher in Industrial Security

Previously head of cybersecurity at a multinational textile manufacturer, Benoit is now a researcher for the Security and Privacy research group of Howest College University.

He mainly focuses his research on Industrial Security.

Kurt Callewaert

Howest - Valorisation Manager Digital Transformation.

Kurt Callewaert (Master Mathematics) is Valorisation Manager Digital Transformation and former coordinator of the research group of Applied Informatics at HOWEST. He was responsible for the very well known Cyber Security Professional track. Kurt and his team conduct research on Blockchain, Cybersecurity (including Industrial security), Data Protection (GDPR), RPA, AR and AI. Kurt is the project leader of the various projects. Kurt is 'chair' of the NIS Focus Group of the Cyber Security Coalition asbl in Belgium to translate the new European Cybersecurity legislation NIS into concrete measures for the companies. Kurt is a member of the Cyber Security Coalition asbl and a founding member of the Beltug Blockchain Task Force and IoTbe asbl. He is also a member of the ISO TC307 Blockchain & DLT standardization committee. Kurt is part of the CEB-BEC 65 working group in Belgium (Industrial process measurement, control and automation) as a cybersecurity expert. Kurt is a member of the Physical Internet expert group of POM West Flanders and a member of ALICE Alliance for Logistics Innovation through Collaboration in Europe. Kurt is a much sought after speaker at C-level seminars around the topics of cybersecurity , AI and blockchain technology. Kurt can also add the RSA Conference in San Francisco to his list of speakers since 2020. Kurt Callewaert is a member of the Flemish Steering Committee Cyber Security - Outreach & Training. Kurt is a member of the steering committees IOF i4S and IOF M&F in the association UGent.

The content of the presentations was provided by the speakers.

Maxime Cordy

Research Scientist at the Interdisciplinary Center for Security, Reliability and Trust (SnT)

Maxime Cordy is a Research Scientist at the Interdisciplinary Center for Security, Reliability and Trust (SnT), University of Luxembourg, in the domain of Artificial Intelligence (AI) and Software Engineering (SE), with a focus on security and quality assurance for machine learning, software verification and testing, and the engineering of data-intensive systems.

He has published 70+ peer review papers in these areas. He is one of the four permanent scientists of the SnT's SerVal group (SEcurity, Reasoning and VALidation).

His research is inspired from and applies to several industry partners, mostly from the financial technology and smart energy sectors. He is deeply engaged in making Society benefit from results and technologies produced by research through the founding of a spin-off company and the leadership of private-public partnership projects at SnT.

He has worked as a program committee member and reviewer for top-tier AI and SE conferences incl. IJCAI, ECCV, NeurIPS, ESEC/FSE, PLDI, ISSTA, CAISE, etc. He is distinguished reviewer board member of TOSEM and regular reviewer for other top-tier SE journals.

Xavier Devroye

Namur University - Assistant Professor of Software Engineering at the Namur Digital Institute and the Faculty of Computer Science of the University of Namur

Xavier Devroey is an assistant professor of software engineering at the Namur Digital Institute and the Faculty of Computer Science of the University of Namur in Belgium. His main research interests include automated test case generation, test suite augmentation, and variability-intensive systems.

He received his PhD in Computer Science from the University of Namur in 2017. He worked as a postdoctoral researcher in the software engineering research group of the Delft University of Technology from 2017 to 2021.

Guillaume Ginis

CETIC – Senior Researcher in Cybersecurity at CETIC

Industrial engineer in electronics from the ISICHt (now HelHa)

Guillaume Ginis is an industrial engineer in electronics from the ISICHt (now HelHa) since 2006. He has worked for 11 years at ALSTOM TRANSPORT BELGIUM in Charleroi as Software Developer for test automation, System Engineer and System Engineering Manager for the Interlocking solution used mainly by INFRABEL. Then, he has worked for 2 years at THALES BELGIUM in Tubize as System Engineer and Test and Validation Manager for security products. He participated in some research projects, in collaboration with CETIC, when working at ALSTOM (mainly INOGRAMS and DIGITRANS). He has started working for CETIC in 2021 as Senior Researcher in Cybersecurity. He joined the MBEDIS department to bring his knowledge about cyber-physical systems (design, tests, safety, ...), test automation and cybersecurity.

The content of the presentations was provided by the speakers.

Xavier Lessage

CETIC - Senior Research Engineer in the Data Science Department at CETIC

Secure Federated Learning

Xavier Lessage is a senior research engineer in the Data Science department at CETIC. His main interests are artificial intelligence, cloud computing, distributed data processing (high performance computing) and cyber security.

One of his interests in industry and digital technology is health, and more specifically, the use of artificial intelligence in health care.

Philippe Massonet

CETIC – Scientific Coordinator at CETIC

Philippe Massonet is scientific coordinator at CETIC, a Belgian ICT applied research center. His research interest cover the areas of software, service and security engineering, as well as distributed systems such as Grids and service oriented infrastructures. He was recently coordinator of the GridTrust IST European project (Strep) dealing with trust and security in next generation grids, and is responsible for dissemination and security in the RESERVOIR IST European project (Integrated project) led by IBM research. He is currently the coordinator of the PONTE eHealth project that is looking into using semantic web technologies to build decision support systems for the design clinical trials.

He is active in the NESSI ETP working groups, and the ERCIM working groups. At CETIC he also works as a consultant for industry and government in his areas of research. He has experience in the prototyping and commercial development of advanced requirements engineering tools. Previously he was manager of the requirements engineering team at CETIC. He has experience in the management of international R&D projects (Eurescom MESSAGE, IST FP6 GridTrust, and FP7 PONTE) and is or has been involved in several IST FP6/ FP7 research projects (RESERVOIR, HPC4U, AssessGrid, CoreGrid, GridTrust and Oldes).

Matteo Merialdo

RHEA Group - Deputy Director of the Operational Security Services Unit (ESEC - ESA) in Redu

Matteo is RHEA's Security Services Deputy Business Unit Manager. He is based in Belgium, working at RHEA's Centre of Excellence in Diegem and at the European Space Security and Education Centre (ESA ESEC) in Redu.

I have a degree in Telecommunication Engineering and another Master's degree in Software Engineering. In general, I have been fascinated by designing and building complex software systems since my twenties.

I've come quite a long way since joining RHEA in 2014.
I was hired as a software engineer, then I moved to software architect, then to project manager. After that, I become Manager of Security Services R&D – and recently Deputy Business Unit Manager of Security Services.

Within Security Services, I oversee all the operational and technical aspects of the business unit activities, including all projects, services, security operations and products roadmaps.

In 7 years, I've seen Security Services grow from two people (I was the first with the Director) to 50 extremely strong professionals. Being part of this endeavour was a once-in-a-lifetime opportunity and a life-changer for me. Our growth plans are ambitious, and being a key player is definitely an amazing aspect of my life!

Christophe Ponsard

CETIC - Research-Innovation-Exploitation Coordinator

Ir. Christophe Ponsard is Research-Innovation-Exploitation Coordinator. He holds a master in Electrical Engineering and Computer Science. His main area of expertise is software engineering, more specifically requirements engineering, model-driven engineering and the management of specific non-functionale requirements like security, sustainability and accessibility. After leading the Software and System Engineering department of CETIC for ten year, he is now focusing on business and research alignment.

He is actively contributing to a number of Regional and European applied research programs more specifically in the transportation and logistics domains. He is also involved in valorisation activities in local companies using co-innovation techniques. He is also regularly involved in computer science conferences.

Pascal Rogiest

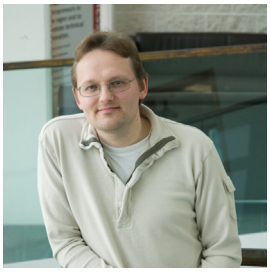
RHEA Group - Managing Director of the Cybersecurity Division of RHEA Group, Chief Strategy Officer of RHEA Group, Vice President of RHEA Belux

Pascal Rogiest is Acting Managing Director, RHEA Group Cybersecurity Division, Chief Strategy Officer for RHEA Group and Vice-President Belux. He joined the company in December 2020 as Chief European Institutions Officer and Managing Director of RHEA System Luxembourg S.A, bringing experience in both space and cybersecurity in order to further develop the commercial and institutional footprint of RHEA. In his role as Chief Strategy Officer, he fosters additional service offerings along the space and cybersecurity value chain and in related fields of strategic focus, leveraging the many competences present within the company.

Pascal spent most of his career at the satellite firm SES, where he held technical, commercial, business and corporate development positions until he became Vice President, Head of Mergers and Acquisitions. He was behind the creation and subsequent development of two subsidiaries at SES, namely SES TechCom and Redu Space Services, and has been involved in various international projects.

He joined LuxTrust, the Luxembourg-based digital trust services provider, in 2015, becoming CEO in March 2016 in order to foster the international, commercial and institutional development of the company, and transform it into a customer-centric organization based on end-to-end digital trust and identity solutions. In 2018, he won the IT Security CEO Award for the Benelux region (CEO Monthly Magazine).

Pascal has a background in electro-mechanical engineering and a PhD in aerospace.



Laurent Mathy

Liège University - Professor of Systems and Security in the Electrical Engineering and Computer Science

Professor of systems and security in the Electrical Engineering and Computer Science

Laurent Mathy is a full professor of systems and security in the Electrical Engineering and Computer Science (EECS) department of the University of Liège, and a Chinese Academy of Sciences (CAS) President's International Fellowship Initiative (PIFI) visiting scientist in the Computer Network Information Center (CNIC), CAS, in Beijing.

He was also a full professor of networked systems in the School of Computing and Communications at Lancaster University, and held positions as a visiting professor in the Institute of Computing Technology, CAS, in Beijing, visiting professor at the Universities of Louvain and Liège, visiting research director at LAAS-CNRS in Toulouse, and visiting researcher in the Center for Integrated Computer Systems Research (CICSR) at the University of British Columbia in Vancouver.

He received a PhD in computer science from Lancaster University in 2000, and an electrical engineering degree from the University of Liège in 1993.

He was also a full professor of networked systems in the School of Computing and Communications at Lancaster University, and held positions as a visiting professor in the Institute of Computing Technology, CAS, in Beijing, visiting professor at the of Louvain and Liège, visiting research director at LAAS-CNRS in Toulouse, and visiting researcher in the Center for Integrated Computer Systems Research.

Jean-Luc Trullemans

Head of the European Space Security and Education Centre (ESEC)

Jean-Luc Trullemans is currently Head of the European Space Security and Education Centre (ESEC) in Redu/ Belgium. He joined the ESA Security Office as security expert and advisor on July 2020 after a thirty-year law enforcement career, along with BE Government as Senior security advisor for David Clarinval, Belgian deputy Prime Minister and Francois Bellot, Minister of Transport.

Jean-Luc's initial curriculum is completed by a master's degree in public management and a certificate in cyber security of critical infrastructures (MIT).

The content of the presentations was provided by the speakers.

Certificate of Participation

At the end of the training, each participant will receive, by mail, a certificate of participation, with access to a personal web page containing the program of the courses followed.

You will then be able to easily share your experience on your CV or on social networks.

Gala dinner

On Wednesday, December 14th, starting at 6:30 p.m., we will be thrilled to welcome you to the gala dinner, which will be held in one of the most unusual places of the Euro Space Centre, the Voyager Café. We want your experience and this moment of conviviality to be unforgettable!

We are proud and honored that you are part of the 1st promotion of this 1st edition of the international school “Cyberwal in Galaxia Program”, linked to the CyberWal initiative.

Goodies sustainability

For this 1st edition of the CyberWal in Galaxia Program school, we wanted to be as eco-friendly as possible, by choosing sustainable goodies.

Upon your arrival, you will receive a ballpoint pen, a notebook, and a lanyard with your badge.

Made in France, the pen, from the BIC® Super Clip Ecolutions® brand, contains 83% of recycled materials, and recycled plastic granules from the automotive recycling industry. The printing, meanwhile, was made in Spain.

We are pleased to offer you a notebook, made of recycled cardboard and paper.

And finally, for your badge: no plastic! Your details will be attached to a metal clip.

We would like to thank you in advance for dropping off your lanyard when you leave.

Organized by

IDELUX DÉVELOPPEMENT

Cyberwal by digital wallonia .be

iddUP

Our best partners

The success of this CyberWal in Galaxia Program is also due to the support of our partners, a winning ecosystem! We are infinitely grateful!

This Program, which is financed by the Walloon Region, is organized by IDELUX Development and under the authority of the scientific committee chaired by Mr Axel Legay, Professor of cybersecurity at the UC Louvain.

Wallonie

European Space Applications Park GALAXIA

UCLouvain

Agence du Numérique

www.**cyberwalingalaxia**.be