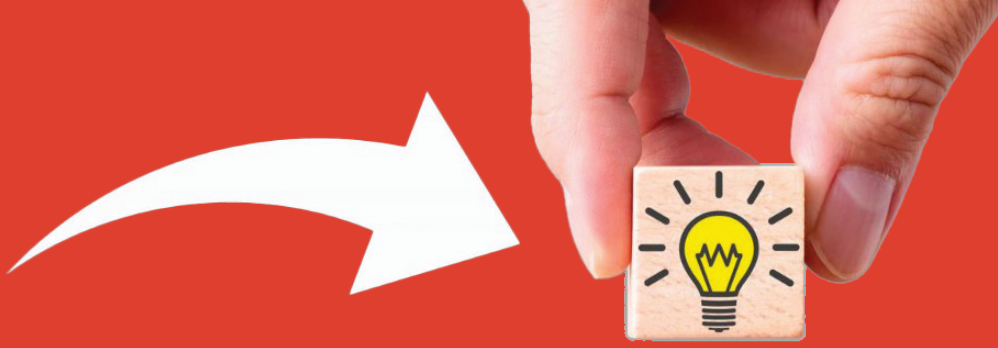


APPLICATION SECURITY

EXPERIENCE SHARING DAY

15 JUNE

FACULTY CLUB
LOUVAIN

CYBER SECURITY COALITION.be

SecAppDev

WELCOME

In June 2023, the 15th edition of the yearly SecAppDev course takes place in Leuven. As usual, experts from industry and academia (The SecAppDev Course) will teach about various aspects of secure application development. At SecAppDev, developers, architects, and technical managers get a unique deep dive into current best practices for security.

The programme for 2023 offers a dual track of twenty-two in-depth lectures and four hands-on workshops. The lectures are 90 minutes each and offer deep knowledge on a variety of security topics. The one-day workshops offer hands-on experience in Web and API security, AI and ML security, Cryptography, Threat modelling, Supply Chain security and Vulnerability management.

For the fifth time, the Cyber Security Coalition has the honour to collaborate with SecAppDev and to organize a joined full day event at the same venue. The event is hosted by the Cyber Security Coalition in the Faculty Club and as usual there will be plenty of networking moments.

We are pleased to announce that on Thursday morning June 15th, the following renowned speakers will give a summary presentation of their lectures:

Gary McGraw, CEO Berryville Institute of Machine Learning

Lukas Weichelsbaum, Senior staff security engineer, Google

Abhay Bhargav, Founder and Chief Research Officer, AppSecEngineer

Claudio Merloni, Security research manager, Semgrep and **Pieter De Cremer**, Senior security researcher, Semgrep

In the afternoon, other experts and/or Cyber Security Coalition members will share many of their experiences with you.

Jesse van der Zweep, AI & Cybersecurity developer, will explore different ways in which you can leverage Large Language Models (LLMs) across all cyber security services. It will go beyond theory, instead showcasing tangible demonstrations of LLM applications through working demos built on top of the OpenAI API. Attendees will also have the opportunity to access and explore these demos for themselves after the talk. The goal is to inspire and encourage active exploration of LLM applications within cyber security.

After this demo, **Kim Wuyts**, Senior privacy researcher at DistriNet, KU Leuven, will dig into the world of privacy engineering and explore what privacy is about, why it matters, and how threat modelling can help you introduce it early in the software development lifecycle.

Sebastien Deleersnyder, Co-founder & CTO at Toreon and COO & Trainer at DPI, will explain us how to evolve from Good to Great using the OWASP SAMM Threat Modelling.

To conclude our afternoon programme, **Mark Curphey**, Co-founder Crash Override, has 'looked behind the curtains' of industry security surveys, and is going to unravel some of the myths of software security. Mark will also show us how to 'lie with statistics', just like the cosmetics industry does on TV.

AGENDA

MORNING SESSION

09:00 **Security engineering for machine learning**

Gary McGraw
CEO, BERRYVILLE INSTITUTE OF MACHINE LEARNING

09:45 **Modern security features for web apps**

Lukas Weichelsbaum
SENIOR STAFF SECURITY ENGINEER, GOOGLE

10:30 COFFEE BREAK

11:00 **Fantastic software supply-chain vulnerabilities**

Abhay Bhargav
FOUNDER & CHIEF RESEARCH OFFICER, APPSECENGINEER

11:45 **Secure defaults: developer-friendly security**

Claudio Merloni
SECURITY RESEARCH MANAGER, SEMGREP

Pieter De Cremer
SENIOR SECURITY RESEARCHER, SEMGREP

12:30 LUNCH BREAK

AFTERNOON SESSION

13:30 **AI in Cybersecurity: building an adversarial machine learning platform**

Jesse van der Zweep
AI & CYBERSECURITY DEVELOPER

14:15 **A Taste of Privacy Threat Modeling**

Kim Wuyts
SENIOR PRIVACY RESEARCHER AT DISTRINET, KU LEUVEN

15:00 COFFEE BREAK

15:30 **OWASP SAMM Threat Modeling: From Good to Great**

Sebastien Deleersnyder
CO-FOUNDER & CTO TOREON COO & TRAINER DATA PROTECTION INSTITUTE

16:15 **The Myths of Software Security**

Mark Curphey
CO-FOUNDER CRASH OVERRIDE

17:00 CLOSING RECEPTION

SPEAKERS

Gary McGraw

CEO, BERRYVILLE INSTITUTE OF MACHINE LEARNING

Gary McGraw is author of the bestselling security books: Software Security (Addison-Wesley, 2006), Exploiting Software (Addison-Wesley, 2004), Building Secure Software (Addison-Wesley, 2001), Java Security (Wiley, 1996) and seven other books. CEO and Founder of the Berryville Institute of Machine Learning, Dr. McGraw is a world authority in software and application security.

Lukas Weichselbaum

SENIOR STAFF SECURITY ENGINEER, GOOGLE

Lukas Weichselbaum is a senior staff tech lead and manager at Google's Information Security Engineering team with over a decade of industry experience and regularly speak at infosec and developer conferences. At Google, he leads a team of 10+ professionals focusing on securing Google's web ecosystem by making web frameworks secure by default and by deploying web platform security features like CSP, Fetch Metadata, Trusted Types, COOP, etc. at scale. As a member of W3C WebAppSec WG, Lukas is passionate about improving the security of the web platform as a whole and contributed to specifications such as CSP3.

Abhay Bhargav

FOUNDER & CHIEF RESEARCH OFFICER, APPSECENGINEER

Abhay Bhargav, Founder & CRO of AppSecEngineer, specializes in AppSec, Cloud-Native Security, Kubernetes Security & DevSecOps training. With a start in pentesting & red-teaming, Abhay now focuses on scaling AppSec through innovative solutions. He pioneered the world's first hands-on DevSecOps training programme, emphasizing AppSec Automation, and actively researches new technologies' impact on security. A sought-after speaker and trainer at events like DEF CON, BlackHat, and OWASP AppSec, Abhay has also authored publications on Java Security and PCI Compliance.

Pieter De Cremer

SENIOR SECURITY RESEARCHER, SEMGREP

Pieter De Cremer's career started as an intern at Secure Code Warrior where he wrote more than 100 rules for their security tool, Sensei. He was closely involved in the early designs of the tool and after graduating, Pieter decided to pursue a PhD at this company. During his research, Pieter designed, implemented, and evaluated improvements for both training and tools provided by SCW. Currently Pieter works as a Security Researcher at Semgrep, he frequently presents and hosts workshops at conferences such as BruCON and OWASP BeNeLux.

Claudio Merloni

SECURITY RESEARCH MANAGER, SEMGREP

Claudio Meloni is a veteran security expert. After completing his Master in Computer Engineering at the Politecnico di Milano University, he started a now more than 15-year long journey in the security space. Security consultant first, then moving through different roles, from sales engineering to security research and product engineering. He fell in love with static source code analysis early on and spent most of his career working with, and on, the leading solutions. He is now leading the security research team at Semgrep, and trying to make the world a safer place, one rule at a time.

Jesse van der Zweep

AI & CYBERSECURITY DEVELOPER

Jesse van der Zweep is researching and building solutions that improve the security of machine learning models. He has an academic background in AI and extensive, practical pen-testing experience. For the past few years, he has been working on the intersection of cybersecurity and machine learning. He is currently building an adversarial machine learning platform at NavInfo Europe.

Kim Wuyts

SENIOR PRIVACY RESEARCHER AT DISTRINET, KU LEUVEN

Kim Wuyts is a senior privacy researcher at the imec-DistriNet research group at KU Leuven (Belgium). She has more than 15 years of experience in security and privacy engineering. Kim is one of the driving forces behind the development and extension of LINDDUN, a privacy threat modelling framework. She is also a co-author of the Threat Modelling Manifesto, programme co-chair of the International Workshop on Privacy Engineering (IWPE), and a member of ENISA's working group on Data Protection Engineering.

SPEAKERS

Sebastien Deleersnyder

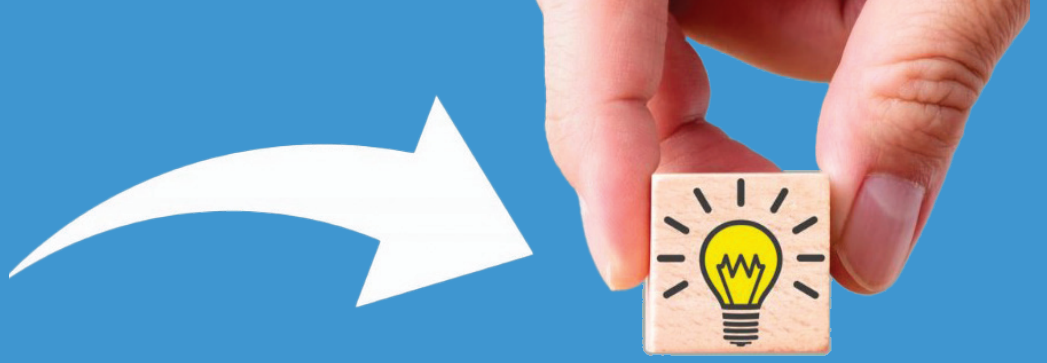
CO-FOUNDER & CTO AT TOREON | COO & TRAINER AT DPI

Sebastien Deleersnyder, also known as Seba, is a highly accomplished individual in the field of cybersecurity. He is the CTO and co-founder of Toreon, as well as the COO and lead threat modelling trainer of Data Protection Institute. Seba holds a Master's degree in Software Engineering from the University of Ghent and has extensive experience in the development and training of secure software. He is the founder of the Belgian chapter of OWASP and a former member of the OWASP Foundation Board. In 2022, Seba was honoured as Belgium's Cyber Security Personality of the Year by the Cyber Security Coalition, where he currently serves as the chair of the new Application Security focus group. Through his leadership on OWASP projects such as OWASP SAMM, Seba has made a significant impact in improving global security. He is currently focused on adapting application security models to the evolving landscape of DevOps and raising awareness of the importance of threat modelling among a wider audience.

Mark Curphey

CO-FOUNDER CRASH OVERRIDE

Mark Curphey is the co-founder and Chief Marketing Officer at Crash Override, a venture backed security startup founded in 2022. Mark is a well-known security expert, author, and public speaker. He has more than 25 years of experience in the security and software development fields holding executive leadership, technical leadership and community advocacy roles. Prior to Crash Override he was the co-founder and CPO/CTO of Open Raven, a data classification company, founder and CEO of SourceClear (acquired by Veracode in 2018) the first pure play security software composition analysis company and led the MSDN subscription team at Microsoft. In 2002, he founded the Open Web Application Security Project, the de facto online community dedicated to improving software security. He has a Master's Degree In Information Security from Royal Holloway and Bedford New College, University of London. Mark lives in the UK.



TAKE THE SURVEY!

We hope you enjoyed the presentations.
Your feedback is greatly appreciated.
This short questionnaire will take only a few minutes to complete.
Thank you in advance.

MORNING SESSION

AFTERNOON SESSION

BELGIUM'S CYBER SECURITY *Awards*

WELCOME TO THE THIRD EDITION OF BELGIUM'S CYBER SECURITY AWARDS, recognizing professionals who demonstrate excellence, innovation and leadership in cybersecurity in Belgium. The awards campaign launched by the Cyber Security Coalition is a totally independent event whereby a multidisciplinary, impartial jury can make its decision on merit alone.

WE ARE HANDING OUT 4 CYBER SECURITY AWARDS:

BELGIUM'S CYBER SECURITY *Personality* of the Year

BELGIUM'S CYBER SECURITY *CISO* of the Year

BELGIUM'S CYBER SECURITY *Researcher/Educator* of the Year

BELGIUM'S CYBER SECURITY *Young Professional* of the Year

Why these four Cyber Security Awards?

It has never been more important to recognize excellence in the field of cyber security. Malicious attacks increase day by day and cyber security teams are constantly countering evolving threats. It is essential that we identify and celebrate the extraordinary achievements of the professionals who undertake this challenging work in the Belgian cyber security sector. The awards showcase the vast range of activities ongoing in Belgium to keep us safe in the virtual world. Winners and finalists are an inspiration to other individuals, who wish to work to protect others in the same manner.

We encourage all those, who are committed to progressing the Belgian cybersecurity industry, to apply.

Our jurors come from varied backgrounds across the three sectors and are some of the most well-regarded individuals within the industry. They will review all shortlisted applications in the four categories, deciding the four winners collectively at judging day, held on November 10th.

APPLY NOW

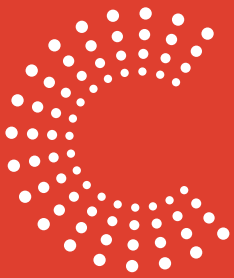
OR NOMINATE A CANDIDATE

The closing date for the submission of applications is October 6th. You can submit your application through award.cybersecuritycoalition.be. Do you know someone eligible for one of the Cyber Security Awards? You can also nominate one or more candidates.

Belgium's Cyber Security trophies will be handed over to the winners during a Gala dinner in the Africa Palace in Tervuren on December 6th. Minister Vincent Van Quickenborne has already confirmed his attendance

AWARD.CYBERSECURITYCOALITION.BE

APPLICATION SECURITY



The mission of the Cyber Security Coalition is to bolster Belgium's cyber security resilience by building a strong cyber security ecosystem. We do so by bringing together the skills and expertise of the academic world, the private sector and public authorities on a trust-based platform aimed at fostering information exchange, operational peer-to-peer collaboration, making recommendations for more effective policies and guidelines, and finally carrying out joint awareness-raising campaigns aimed at citizens and organizations.

cybersecuritycoalition.be

The annual SecAppDev course is run by secappdev.org, a non-profit organization that aims to broaden security awareness in the development community and advance secure software engineering practices. At SecAppDev, experts from industry and academia offer insights into security best practices and the implications of the latest cutting-edge research. Each year, a dual-track program consisting of in-depth lectures and hands-on workshops takes participants on an immersive journey into the world of software security.

secappdev.org