Programme

Associated Events

CFI CYBERSECURITY FOR INDUSTRY

ID &KYC FORUM

TRUST &SAFETY FORUM

W3S WEB3 SECURITY SUMMIT

INCYBER INVESTOR DAY

OSINT DAY

INCYBER FORUM EUROPE

26–28 MARCH 2024

LILLE GRAND PALAIS

Ready for AI?

Reinventing cybersecurity in the age of AI

IN CYBER FORUM

EUROPE

Between dystopian fantasy and techno-bliss, it is hard to determine where artificial intelligence (AI) will lead humanity. One thing is certain: nothing will ever be the same again.

Our professional activities, our personal lives, our ways of thinking, of deciding, of acting, of consuming, of producing, of caring for ourselves, are all going to be permanently disrupted. But tomorrow's world will depend above all on what we collectively decide to do - or not to do - with artificial intelligence, and on the «trust» we manage to build "in" and "through" these technologies.

To be "trusted", AI must, according to the European Commission, respect 7 principles, including technical robustness and security, respect for privacy and data governance. The widespread use of these technologies will introduce new risks, not only because of the increased attack surface, but also because of their intrinsic vulnerabilities (poisoning attacks, adversarial attacks, etc).

As technological progress is ambivalent by nature, AI is also used by attackers all along the "kill chain" to recognize a target, bypass protection mechanisms, build "deep fakes", automate an attack and so on.

The first challenge is therefore to secure not only artificial intelligence, but also the data it absorbs and produces. Data and artificial intelligence are inextricably linked. And the figures are staggering: every second, 7 megabytes of data are created for each person, resulting in a global quantity of data that will reach 181 zettabytes in 2025, compared with 2 zettabytes in 2010.

Fortunately, AI is also revolutionizing the "art" of cybersecurity, enabling us to improve our authentication, data security, threat detection, code analysis, orchestration, incident response and other capabilities. A technological leap that should also lead us to radically reinvent our policies, organizations and skills, so that they are "AI - ready".

List of thematic tracks

→ ROUND TABLES

CFI

ID&KYC Forum

Trust & Safety Forum

Web3 Security Summit

InCyber Investor Day

OSINT Day

CF

CYBERSECURITY
FOR INDUSTRY

IN CYBER FORUM
EUROPE

26–28 MARCH 2024

LILLE GRAND PALAIS

Cybersecurity For Industry is the event associated with the InCyber Forum, dedicated to cybersecurity issues in the industrial world. The only one of its kind in Europe, it provides a forum for the exchange and discovery of cybersecurity solutions for industry, as well as secure industrial solutions.

Round Tables

Implementing Cybersecurity in OT and Industrial Systems: Insights from the Field

Operational Technologies (OT) and Industrial Control Systems (ICS) play a crucial role in critical infrastructures such as energy, transportation, and water supply. However, these systems are increasingly facing threats from malicious actors.
Understanding how attackers exploit specific vulnerabilities in these systems and assessing the potential consequences of a successful intrusion is essential. Strengthening the resilience of OT/ICS systems is of the utmost importance toensure the continuity of essential services in our modern society. This session provides practical insights from the field to address these critical challenges.

Ensuring the Security of Autonomous Systems

The rise of autonomous systems, including autonomous vehicles, drones, and industrial robots, promises to enhance efficiency, precision, and safety in various domains. However, this growing autonomy poses a significant cybersecurity challenge, especially in Operational Technologies (OT). The central question is how to reconcile system autonomy with cybersecurity. How can autonomous systems be designed to make complex decisions while resisting sophisticated attacks? What measures can be taken to protect critical infrastructure based on autonomous OT systems?

Securing the Entire Supply Chain in the Connected Factory

Securing the entire supply chain within a connected factory is a major concern in the era of Industry 4.0. The primary goal is to ensure operational continuity while safeguarding sensitive data and industrial processes. Connected factories integrate advanced technologies such as the Internet of Things (IoT), automation, robotics, and computerized management systems. While this enhances efficiency, inventory management, and traceability, it also exposes the entire supply chain to new security risks. What are the potential risks in the connected factory, and how can they be assessed to implement appropriate security measures? How can cybersecurity for Industrial Control Systems (ICS) be ensured while maintaining the availability and performance of equipment in a connected factory?

Micro-Segmentation: Key to OT Resilience?

Micro-segmentation in the industrial environment is a significant challenge in the era of increasing digitization and automation. This approach involves dividing computer networks into segments, thereby isolating different parts of the industrial infrastructure and reinforcing the security of industrial systems. By isolating each component or device, it limits the spread of potential threats within the network. Each segment can be configured with specific rules, allowing or disallowing communication with other segments. As a result, it offers a proactive response to cyber threats, preserving the integrity and performance of industrial enterprises. How can micro-segmentation help companies enhance their security in an industrial context? What are the best practices for maintaining effective micro-segmentation in the long term in an industrially evolving environment?

ID &KYC FORUM

INCYBER FORUM EUROPE

26–28 MARCH 2024

LILLE GRAND PALAIS

2024 THEMES

The customer at the heart of technological change

Health, banking, transport, education,
e-government... digital identity is now
at the heart of economic activities and civic life.

Round Tables

Special 5th birthday ID&KYC Forum
Review and perspectives of digital identity (and KYC) in France and in Europe

On its fifth anniversary, the ID&KYC Forum invites several national and international personalities to speak on the results and prospects of digital identity. What has been achieved in France over the last five years? What were the failures and successes? Where does France stand in relation to the evolution of the European landscape and the progress made by its neighbors? How do different market segments use the solutions offered by the government and the private sector? What is the adoption curve by the public? What are the priorities for the next five years? Is there a consensus on these priorities?

"Anti-money laundering package" and new "European digital identity framework": what will be the impacts?

At the heart of the issues of digital identity and knowledge of customers and partners, two major European regulations follow parallel timetables and will in all probability be definitively adopted during our Forum. How will they impact business activity and societal-household life? How do these texts mark an evolution or even a revolution in customer relations practices and the distribution of digital services? Are there synergies and interactions between these regulations? What will be their respective and combined impacts? How to prepare for the arrival of the new rules? What are the accompanying texts and implementations? How to interpret them? What developments or updates should be expected for businesses?

Electronic wallet how to adjust to new intermediation strategies for tomorrow?

Today, more than one in two e-commerce transactions in the world are carried out via mobile phones. Through the provision of ergonomic simplicity, application security and a legal guarantee, the rise of electronic identity, payment and digital currency wallets creates a new intermediation capacity for transactions and services of tomorrow. How big is this development? Who will benefit from this new intermediation? What do businesses and financial services need to do to participate? Will European digital portfolio projects be able to compete with the digital giants? How do transactional ecosystems build ton banking/postal or telecom/sectorial networks using digital id* will cope with that? What are the societal consequences of this new form of intermediation?

"EUDI Wallet": which functions for promoting a new life on mobile?

Authentication, electronic signature, payment: what are the functionalities promised by the European mobile wallet (EUDI)? How will they relate to each other? For what uses? Halfway through the European pilots of the four consortia, what lessons have emerged? Digital services, travel, opening a bank account, professional identities: where are the most significant innovations located? What are the impacts on technical architectures? The "high" Security level of the European portfolio: how to understand it? how to implement it? how will it be used? What are the options? Will European citizens and consumers benefit from a new life on mobile with these journeys?

Round Tables

How to optimize digital journeys with KYC and AI, to improve customer engagement?

Data governance allows organizations to test and implement digital strategies. Customer Knowledge (KYC) tools and Artificial Intelligence (AI) techniques make it possible to go further, by combining proposals better calibrated in terms of risk and opportunities, and by improving the personalization of the service. What are the benefits of KYC automation and Artificial Intelligence on user experiences (UX)? How to combine the two approaches? What are the impacts on real-time data verification, customer enrollment, consent management and transaction monitoring? What is the feedback on the market?

Which are the pillars to build the digital identity of the future (2030–2050)?

Besides mobile wallets, what are the most structuring approaches for the digital identity of the future? We address several essential themes here. Digital Identity Infrastructure is a concept that considers that digital identity must be inserted into a broader "digital public infrastructure" approach (ITU/G20). The resulting ecosystem notably combines data exchange and transaction management, allowing digital society to function more optimally. Several approaches or architectural models can then be adapted (eg: decentralized, centralized, federated) for different applications. Identity & Attributes Trust Frameworks are sets of rules and standards to which trust operators can adhere and against which they can also be certified to demonstrate their ability to deliver data whose integrity and compliance are guaranteed. The Central Bank Digital Currency (CDBC) has progressed, like the European digital currency or the Swedish e-krona. However, it still faces the need to be able to identify people and/or accounts effectively before it can be implemented for the public.

Round Tables

Improving the fight against digital fraud in consumption, identity, and payment

Inflation and the increase in the cost of living have led several European authorities and organizations (EUROPOL, EBA, EPC, CIFAS UK) to warn against the proliferation of threats of scams and cyber fraud penalizing consumers. in their purchase, payment, or service transactions. Identity thefts, online or telephone manipulation, scams, false commercial offers, spyware, hacking and data interceptions, the risks are everywhere.

What are the most targeted transactions? What are the goals of fraudsters? How can we better detect fraud and prevent threats? Who to alert and what are the possible remedies? How to manage relationships with customers in a context of high risks? How to strengthen the culture of risk and fraud management within companies? What are the feedbacks and best practices to put in place?

IAM-CIAM: increasing data fluidity through identity orchestration

More fluidity and less friction for users: this seems to be the motto of corporate identity management today. A practice which affects all internal and external customers of the company: employees, partners, customers, non-human entities such as applications or connected objects. Thanks to orchestration platforms, not only are the company's different audiences onboarded, authenticated, and supported in authorizations, but they also free themselves throughout their digital journeys, from the complexities of the various IT environments.

Without programming, without effort, without passwords, how can identity orchestration generate fluid management of company data? How are user interfaces, connectors and APIs managed? Which parts of the life cycle can be automated and according to what criteria? How do management event notifications automatically reprovision identities and access? What are the profits according to the size of the companies?

ID &KYC FORUM

Round Tables

Trust of business organizations and professional identities: a breath of modernization

Driven by electronic invoicing, digital signatures and the development of transnational exchanges, the digital identities of companies and professionals are the subject of intense work of reflection with a view to modernization and increased interoperability. While respecting the very strict security requirements, new possibilities are emerging for the management of the trust attributes of companies and professionals: company registers, professional e-wallets, certification schemes, solvency information, management of mandates.

What are the structuring initiatives? What legal confidence should be given to digital identities? What are the developments in the management and use of business registries in France and Europe? Who are the stakeholders in this evolution? How will digital certificates evolve? Will the digital identity of organizations move from concept to reality? What are the next steps?

Towards more accountability in the use of the Internet, social networks, and platforms?

While online societal life has taken on an essential dimension, initiatives are progressing to better secure online digital services, clarify the content of offers and better protect children and teenagers from manifestations of hatred, pornography, and violence. In the United Kingdom, a new law called the "Online Safety Bill" (OSB) aims to make the United Kingdom "the safest place in the world for the Internet". Strong measures have been taken to protect children and make platforms responsible for hosted content. In France, the bill aimed at securing and regulating the digital space (SREN) has very similar objectives in the fight against online scams and in child protection. European DMA, OSB, SREN: will the new legislative and regulatory framework finally support more responsible use of the Internet? How will we be better protected online? What are the obligations for online platforms and services? What certification practices will be used? What measures are taken for age verification? What role will digital identity play in making the Internet more secure?

TRUST & SAFETY FORUM

IN CYBER FORUM EUROPE

26–28 MARCH 2024

LILLE GRAND PALAIS

With 100,000 professionals worldwide,
and 20,000 companies soon to be impacted
by the forthcoming Digital Services Act,
Trust & Safety is striving to become a standard
discipline within the wider security family.

How is AI protecting personal data on platforms?

Everyone has built a digital identity over the last decade but how are we keeping it secure from it being stolen or misrepresented? AI and other emerging technologies can help individuals and companies to protect our digital identity.

The use of AI in T&S recruitment process

The job landscape in the Trust & Safety industry has undergone significant transformations in recent years, with numerous companies actively seeking candidates with unconventional backgrounds. Human resource departments are increasingly leveraging artificial intelligence in ethical ways to pinpoint suitable applicants while ensuring the secure handling of their personal data.

AviaTOR – Prioritizing CSAM reports through the use of AI

32 million reports of Child Sexual Abuse Material have been reported by platforms in 2022, and made subsequently available to law enforcement agencies. How can they prioritize such a large volume of reports ? AviaTOR is a tool which uses augmented intelligence and targeted research to help authorities to focus on identifying perpetrators and saving victims.

How will 79 elections in 2024 impact the online community

In 2024, around 80 countries will be holding political elections, with social media platforms being the main communication channel to target voters. How can AI help in detecting and preventing misinformation so that voters get the information they need?

AI generated intimate content is a new challenge to tackle

In the second half of 2023, hotlines and platforms have seen an increase in generative AI sexual content using real images of people. Abusers are generating nude images of their schoolmates and distributing them without realising the images can be considered CSAM. Child protection community is getting mobilised to increase awareness of the severity of this type of abuse, how to prevent it and minimise the distribution of such content. And adult survivors are standing up too, to contribute to a change of mindset of the society as a whole.

Round Tables

Staff welfare in the AI era

Until recently, Trust & Safety teams have been coping with harmful and illegal content with limited support from technology - such as AI - to analyse content and minimise exposure. Technology is now available, but what has been the impact on the professionals? Have staff welfare programs and best practices documents incorporated these developments?

Creativity in protecting content from criminal exploitation

We love to watch series, movies or live sports matches, and organised crime excel in catching our attention and bringing us into their underground economy, at our own risk. Professionals on the protection side collaborate and innovate with technology to ensure the digital world stays safe, and their insights enrich the Trust & Safety community and ensure the good guys win in the end.

TALK
AI and DSA Checkstep presentation

Learn how tech provider Checkstep is using Ai to ensure their customers are compliant with the DSA and its various rules.

CONFERENCE
Protecting IP rights through AI

AI is commonly discussed as a technology that is challenging the way we think about intellectual property (IP). In this presentation, we will explore the use of AI tools to protect IP rights. We will discuss the different types of AI tools that are available, how these tools can be used to identify and track infringement, prevent counterfeiting, and enforce IP rights. We will also discuss the ethical considerations of using AI to protect IP rights.

W3S

WEB3
SECURITY
SUMMIT

IN CYBER FORUM EUROPE

26–28 MARCH 2024

LILLE GRAND PALAIS

Web3 technologies promise to accelerate the circulation of assets and create a bridge between the real and the virtual.
But the absence of standards and centralized authority reinforces the need to establish a suitable risk management framework.

Round Tables

01 . What security challenges are involved in tokenization ?

02 . Blockchain and industrial integrity: an inevitable revolution

03 . What legal challenges does Web3 pose?

04 . How does Web3 redefine the protection of intellectual property?

INCYBER INVESTOR DAY

INCYBER FORUM

EUROPE

26–28 MARCH 2024

LILLE GRAND PALAIS

The cybersecurity investment match between Europe and the USA: how to close the gap on the old continent?

In the cybersecurity investment race between Europe and the USA, Europe is showing encouraging signs, despite lagging behind. In 2022, European companies in the sector raised a record 2.4 billion euros, reflecting growing maturity. Although this performance is noteworthy, it nevertheless highlights the gap that remains with American and Israeli investments. How can we close this gap? How do cultural, regulatory and investment differences between Europe and the United States impact the growth of the European cybersecurity ecosystem? How can innovation policies, incubators and gas pedals be optimized to foster the emergence of cutting-edge cybersecurity technologies in Europe?

What are the prospects for the AI market in cybersecurity up to 2030?

The market for artificial intelligence (AI) in cybersecurity offers promising quantitative prospects, illustrated by significant growth in investment. According to forecasts, the global cybersecurity market fuelled by AI is set to reach several tens of billions of dollars over the next few years. In 2022, global spending on AI-powered cybersecurity has already exceeded $15 billion, marking a substantial increase on previous years. While this market could exceed $30 billion by 2025, what are the emerging segments and associated opportunities? How will the AI for cybersecurity market be distributed by 2030 in terms of products, services, customers and geographies?

From start-up to scale-up: how to get through the critical stages?

Technology nuggets are here to stay, but many of them are struggling to make the grade. Having found their market with an innovative financing plan, not all of them are able to meet the challenges that follow: internationalization, the implementation of a long-term marketing strategy, or even the structuring of their internal leadership. There is no shortage of support mechanisms for innovation: public mechanisms (e.g. supported by the French Ministry of the Armed Forces, Bpifrance, cyber strategy supported by ANSSI and Campus Cyber, European Innovation Council), private funding and support (VCs, incubators, gas pedals)... But what about support for growth (notably through public procurement), often considered insufficient? What is needed to consolidate the momentum? Is Europe in a position to compete with the United States and Israel in this area?

OSINT
DAY

IN CYBER FORUM EUROPE

26–28 MARCH 2024

LILLE GRAND PALAIS

OSINT has become a practice in its own right. From the fight against crime (cyber, physical, financial, etc.) to crypto-currencies, via the security of goods and people in times of armed conflict, OSINT is now used in many fields.

OSINT DAY Round Tables

SESSION 1: 10AM – 11:30AM

OSINT and its French communities

From the FOX project to OSINT FR and the AEGE OSINT & Veille Club, the French OSINT movement boasts a number of particularly talented communities, each with its own specific characteristics. Finding a suspect on the run on the other side of the world, unmasking fraudsters, tracking the movements of armed troops... These French OSINT experts will explain it all to you, down to the smallest detail.

SESSION 2: 2:00 PM – 3:30 PM

Professional talk

Baptiste ROBERT, Camille DOLE, Oriana LABRUYERE, Dmytro BILASH, Daniel-Florin PITIȘ or Matthieu AMIOT and Frédéric LENFANT will share their experience by presenting the use they make of OSINT in their work: combating art counterfeiting, anti-fraud, cybersecurity, pentesting...

SESSION 3: 4:30 PM – 6 PM

Last but not least...

Forum InCyber's OSINT Day goes beyond borders and achieves the feat of bringing together, in the same session, Micah HOFFMAN (Webreacher), Steven HARRIS (Nixintel), Leone HADAVI (BBC/Bellingcat), Neil SMITH (UK OSINT), Craig SILVERMAN (ProPublica) and Ritu GILL (OSINT Techniques).

INCYBER FORUM

EUROPE

26-28 MARCH 2024

LILLE GRAND PALAIS

Contacts

partnerships

partenariat@forum-incyber.com

programme

programme@forum-incyber.com