

In Cloud
we trust ?



Forum International
de la Cybersécurité

5, 6 et 7 avril 2023
Lille Grand Palais

20 000 participants dont :

Plus de **16 000**
participants physiques
uniques (+ 10,7%)

4 000
participants en ligne

2 700
internationaux

650
partenaires
privés et publics

530
intervenants

+ de **1 800**
rendez-vous d'affaires
via la plateforme de networking

82
pays représentés

11 minutes : durée
moyenne de visionnage
en ligne (+ 22%)

+ de **700 000**
vues sur les réseaux sociaux
et **50 millions** d'impressions
sur le sujet

Chiffres-clés

Tendances

Menaces

- 13 fuites de données par jour (source : Baromètre 2023 des fuites de données FIC / CNIL)
- 30% des collectivités locales ont déjà été victimes de ransomware (source : CLUSIF)
- 53% des organisations ont subi une attaque sur leur infrastructure cloud au cours de l'année écoulée (source : Netwrix)
- 79% des entreprises ont subi au moins une violation de données dans le cloud au cours des 18 derniers mois (source : CapGemini)
- 43% des entreprises françaises touchées en 2022 (contre 54% en 2021) (source : CESIN)
- 74% des flux financiers liés aux attaques par ransomware pointent vers la Russie (source : Chainalysis)
- 13 000 vulnérabilités signalées en 2022 (-30% par rapport à 2021) (source : NIST)
- 62% des organisations attaquées en 2022 par un ransomware payent la rançon (source : Hiscox)
- La France compte en moyenne **1 personne** chargée de la cybersécurité pour 1 500 salariés (source : Wavestone)

Réponses

- La directive NIS 2, entrée en vigueur en 2022, fixe de nombreuses exigences en matière de cybersécurité et sera transposée dans les États membres d'ici la fin de l'année 2024.
- Le nombre d'organisations concernées par NIS 2 sera multiplié par dix.
- La Commission européenne a proposé en septembre 2022 une première version de la loi sur la cyber-résilience qui s'appliquera à tous les produits et services contenant du contenu numérique.
- 81% des entreprises ont déployé des systèmes EDR (Endpoint Detection & Response) (source : CESIN).
- 12 CSIRT régionaux sont en cours de création.
- 700 collectivités locales ont bénéficié d'une formation en cybersécurité.
- En 2022, les start-ups européennes ont levé 2,4 milliards d'euros (+20%), soit 16% des montants levés dans le monde en cybersécurité (source : Tikehau Capital / baromètre FIC).
- Lors du FIC 2023, le Commissaire européen Thierry Breton annonce la mise en place d'un «Cyber Solidarity Act» et d'un dôme cyber européen composé de plusieurs centres opérationnels de cybersécurité.

MARCHÉ

Un marché mondial
de **250 milliards €**
en 2022 :

- dont 34 milliards € pour l'Europe ;
- dont 3 milliards € pour la France.

« Il faut passer de la haute couture au prêt à porter pour élargir et massifier nos actions. »

Vincent STRUBEL
Directeur général de l'ANSSI
(Agence Nationale de la
Sécurité des Systèmes
d'Information),
FIC 2023

FIC

Temps forts

Intervention vidéo de Jean-Noël Barrot, Ministre délégué au Numérique

Nous assumons pleinement de défendre une logique de **souveraineté numérique** pour développer des **champions européens du cloud**.

Jean-Noël BARROT
Ministre délégué au numérique



Il est absolument indispensable de coordonner à un niveau européen la cybersécurité, vous pouvez compter sur moi pour le faire avec détermination et sans relâche.

Thierry BRETON
Commissaire Européen au marché Intérieur



Allocution d'ouverture de Thierry Breton, Commissaire européen au marché intérieur

Comment peut-on renforcer le continuum défense-sécurité ?

À l'OTAN, nous avons mis en place le projet DIANA : nous payons des start-ups pour travailler avec nous, ce qui leur permet de mettre un pied dans notre stratégie. Nous leur donnons accès à nos contrats, ce qui leur permet de travailler dans notre domaine. C'est une situation gagnant-gagnant : elles ont besoin de paix pour travailler, nous avons besoin d'elles pour la paix.

James APPATHURAI
Secrétaire général adjoint chargé de la politique de sécurité, OTAN



La force de la cybersécurité est l'union. L'Etat ne peut pas répondre seul aux attentes de la cybersécurité. Le FIC c'est le partenariat public-privé par excellence.

Jean-Noël DE GALZAIN
Président d'Hexatrust



Plénière d'ouverture

La préparation civile commence par la préparation personnelle. Chaque acteur doit assumer la responsabilité de sa cybersécurité. Les États ne peuvent pas assumer toutes les responsabilités. Chaque acteur doit faire son travail.

Carl-Oskar BOHLIN
Ministre de la Défense Civile, Suède



Merci au FIC, le plus grand salon de la cybersécurité d'Europe, de réunir tant de profils et de leur permettre de se rencontrer.

Ludivine DEDONDER
Ministre de la Défense, Belgique



Panel Ministériel - La résilience face au défi numérique

FIC

Temps forts

Cloud : Et si le ciel nous tombait sur la tête ?

La question ne se résume pas **au bon ou au mauvais cloud** : ce n'est pas une solution clé en main, cela ne dispense pas les entreprises de se préoccuper de leurs sauvegardes, leurs mises à jour...

Vincent STRUBEL
Directeur général de l'ANSSI



En ce qui concerne la responsabilité des États, nous disposons d'un cadre normatif pour prévenir les comportements non responsables. La boîte à outils de la diplomatie contient différents outils : le processus le plus direct consiste à tendre la main à un pays, mais nous pouvons aller jusqu'à demander à un pays de prendre des sanctions.

Nathalie JAARSMA
Dutch Ambassador at-Large
for Security Policy and Cyber



Agora - l'union fait la force : les citoyens et la cybersécurité

La confiance est-elle soluble dans le numérique ?

La difficulté avec les réseaux sociaux, c'est qu'ils génèrent des communautés qui sont **d'intérêt, pas de solidarité**. Nous sommes dans l'ère de la surveillance : n'importe qui peut diffuser n'importe quoi. Il y a tant d'information que nous sommes perdus. **On ne sait pas comment se repérer au sein de cet océan.**

Jean-Gabriel GANASCIA
Professeur d'université &
Président du comité d'éthique du CNRS



A ceux qui sont convaincus que la bataille n'est pas perdue, mettons nous ensemble, **rassemblons les acteurs pour concurrencer les GAFAM.**

Alain ISSARNI
PDG de Numspot



Cloud : L'Europe veut-elle faire sa révolution ?

Quel rôle pour l'Europe dans la reconstruction de l'Ukraine ?

Si des entreprises se proposent pour former des volontaires ukrainiens, nous bénéficierons de spécialistes en informatique. Nous espérons que des pays comme la France nous aideront à développer un véritable marché, afin que l'Ukraine puisse être un partenaire fiable et solide pour l'UE.

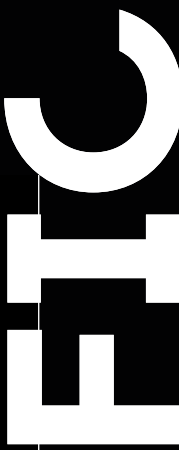
Yegor AUSHEV
Co-Fondateur de CyberUnit
& CyberSchool, Ukraine



Remise des prix de la Startup FIC 2023



Ce qu'ils disent du



Gérôme BILLOIS

Associé | WAVESTONE -

Lauréat du Prix du Livre FIC 2023

« Le FIC va rendre le livre encore plus visible et lui permettre d'atteindre le public visé, le grand public. Le FIC est depuis tant d'années le lieu où toute la communauté cybersécurité se retrouve, et le grand avantage est le mélange de communautés. On n'est plus juste sur des spécialistes techniques de la cybersécurité, mais sur une diversité de profils. Et le FIC catalyse tous les différents angles et permet les rencontres et les interactions pour développer un futur qui sera forcément meilleur. »

Félix BARRIO

Directeur Général | INCIBE (Centre national de cybersécurité de l'Espagne)

« Il est très important en ce moment de renforcer en Europe les projets communs qui sont le ciment de l'innovation. Nous devons travailler ensemble pour relever ces nouveaux défis cybernétiques. Nous sommes également tous d'accord pour dire que nous vivons le moment le plus passionnant des nouvelles directives sur la cybersécurité. Nous jetons les bases des nouvelles règles du marché pour la prochaine décennie. »

Carl-Oskar BOHLIN

Ministre suédois de la Défense Civile

« Je suis venu ici pour détailler le travail que nous faisons actuellement en Suède et pour faire gagner en résilience notre société et la base sur laquelle nous construisons nos capacités de défense. Et aujourd'hui au FIC, je vais pouvoir en discuter avec les gens, échanger des points de vue sur le travail mené sur la cybersécurité qui relève également de mon portefeuille. »

Dan LOHRMANN

Responsable de la Sécurité des Systèmes d'Information (CISO) | PRESIDIO

« Le FIC est un événement à portée mondiale qui suscite la réflexion et qui a un caractère européen marqué. C'est là que les professionnels de la cybersécurité et de la technologie en Europe se rendent pour trouver l'inspiration, apprendre et faire évoluer leur carrière. Il est également extrêmement bénéfique de discuter de sujets liés à la cybersécurité avec des personnes et des équipes issues de pays, de cultures, de situations différentes... Le FIC offre un événement unique et utile sur lequel on peut s'appuyer pour développer un dialogue international qui profiterait à tous. L'expertise, la coopération mondiale et le partage des meilleures pratiques étaient tout simplement incroyables, ce que je n'ai jamais vu à une telle échelle mondiale avec des perspectives diverses. »

Domitille DAÏEFF

Chargée de Communication et Marketing | EVIDEN, marque d'ATOS

« Nous avons profité du FIC pour présenter officiellement notre marque à nos partenaires, clients et candidats. Le FIC dans le monde de la cyber c'est un événement clé, un repère stratégique pour tous les acteurs du monde de la cybersécurité. Pour Eviden c'était important d'y être encore cette année. »

Séverine DEMARQUE

Chargée du mentorat | CFCYS

« Le FIC permet de rencontrer de nouveaux adhérents, rencontrer des partenaires et défendre notre cause.

Nous avons aussi la possibilité d'avoir des contacts de l'étranger. C'est un lieu privilégié, dû à la concentration d'acteurs de la cyber qui est extrêmement importante. Pour nous c'est un incontournable. »

Jean-Christophe LE TOQUIN

Co-Fondateur | FORUM TRUST&SAFETY

« Le Forum Trust & Safety voulait réunir en un seul lieu tous les acteurs liés à la régulation des contenus offensants et illégaux sur Internet, qu'ils viennent des plateformes, des hotlines, des ONG, des autorités, ou les victimes d'abus qui ont une voix à apporter. La FIC a toujours parlé de cybercriminalité, et là nous sommes sur des sujets connexes, très en amont, cette discipline, Trust & Safety n'a même pas encore de nom traduit en français. C'est un espace qui n'existait pas en Europe car nous sommes dans des domaines nouveaux. Le FIC nous offre cette voix. »

Ludivine DENDONDER

Ministre belge de la Défense

« Je pense que d'abord c'est important de pouvoir renforcer l'Europe de la Défense. Venir au FIC, autour de cet enjeu cyber qui est une de nos priorités à tout son sens. Nous avons récemment lancé le Cyber Command belge, et nous sommes occupés à monter en puissance au niveau des moyens technologiques et des moyens humains également. Nous avons au FIC toute une série d'entreprises et de personnalités belges présentes, qui rencontrent, collaborent, échangent avec leurs partenaires européens. C'est évidemment bénéfique pour notre pays, et pour l'Europe. »

Yegor AUSHEV

Co-Fondateur | CYBERUNIT.TECH et CYBERSCHOOL.TECH, Ukraine

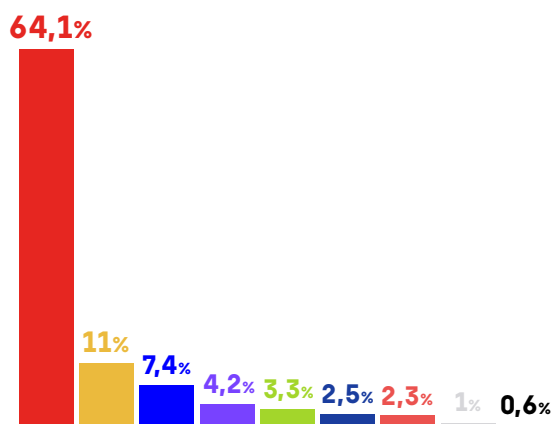
« Cette guerre se poursuit même lorsqu'elle s'est arrêtée sur le terrain. Nous devons partager notre expérience afin d'assurer une plus grande sécurité à notre gouvernement et à notre peuple. Nous espérons que les Européens nous aideront, nous les Ukrainiens, à fabriquer nos produits afin d'assurer notre souveraineté et notre sécurité. Le sujet le plus important pour moi est la chaîne d'approvisionnement. »

Étudiants en cybersécurité

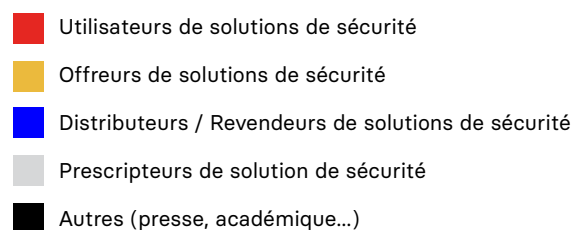
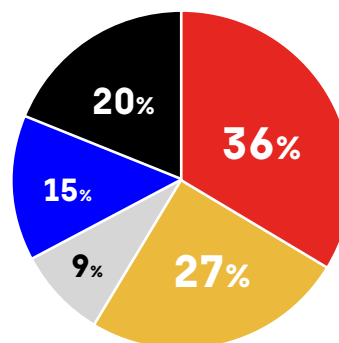
« Nous sommes là pour en apprendre plus sur les domaines de la cybersécurité, les différents métiers qui nous sont ouverts à l'avenir et trouver un peu notre chemin. Nous avons la possibilité d'accéder aux grandes entreprises pour identifier les acteurs dont on entend parler dans ce domaine. Et nous avons aussi accès à de plus petites sociétés qu'on ne connaît pas et qui ont des solutions innovantes qu'on ne soupçonne pas. Venir au FIC c'est aussi une super occasion d'agrandir son réseau et de rencontrer du monde. »

Un événement d'écosystème

Types d'organisations présentes au FIC 2023



Profils des participants présents au FIC 2023



Top 5 fonctions (en %) présentes au FIC 2023



Fonctions de
cybersécurité



Directeur /
Directeur des
ventes



Directeur
général / CEO



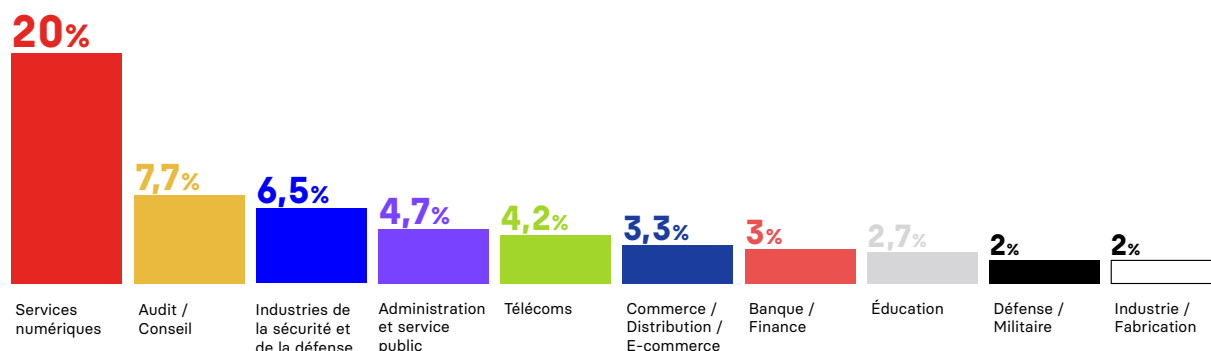
Fonctions
informatiques



Délégué à la
protection
des données

5850 décideurs sur des projets liés à la sécurité
ou la confiance numérique en 2023 (+72%)

Top 10 des secteurs d'activités des visiteurs présents au FIC 2023



Top 10 des centres d'intérêts des visiteurs présents au FIC 2023

1. Gouvernance de la cybersécurité / Politique de sécurité
2. Analyse de risques
3. Supervision de la sécurité / SOC / Services managés de sécurité
4. Sensibilisation à la cybersécurité
5. Détection des fuites de données
6. Gestion / Réponse à incidents
7. Renseignement sur la menace
8. Solutions automatisées de détection et de réaction (EDR, XDR...)
9. Chasse aux menaces
10. Gestion des vulnérabilités

Top 10 des pays les plus représentés sur un total de 2700 participants internationaux au FIC 2023

1. Belgique
2. Pays-Bas
3. Royaume-Uni
4. Luxembourg
5. Suisse
6. Canada
7. États-Unis
8. Allemagne
9. Italie
10. Japon

Un salon

- 650 partenaires exposants
- 20 000 m² d'exposition
- + de 84 200 scans de badges sur 3 jours
- 130 contacts qualifiés par exposant en moyenne
- En moyenne, **+160% de contacts qualifiés** pour les sociétés ayant au moins une intervention en plus de leur stand
- Un **village innovation** regroupant 32 startups et un espace de « pitch »
- Un **village « Cybersecurity For Industry »** regroupant 26 exposants et un espace de démonstrations
- Un **village « ID & KYC Forum »** regroupant 13 exposants et un espace de démonstrations
- Un **Hacking Lab** présentant des démonstrations d'attaques
- Deux **espaces de démonstrations** (FIC Talk et des démonstrations techniques)



Les contenus sont en français ou en anglais et sont pour la plupart traduits dans l'autre langue.

Un forum

- 530 intervenants
- 4 sessions plénières
- 1 Agora
- 51 tables rondes
- 29 conférences
- 58 FIC talks
- 51 démonstrations techniques
- 27 démonstrations d'attaques
- 31 masterclass
- 28 interventions sur l'espace Sécurité Intérieure et de la Défense
- 11 verticales sectorielles ou thématiques :
 - Cybersécurité industrielle
 - Identité numérique et KYC
 - Lutte contre la cybercriminalité
 - Gestion du risque cybernétique
 - OSINT
 - Sécurité des données et transformation numérique
 - Sécurité et stabilité du cyberspace
 - Sécurité opérationnelle
 - Souveraineté numérique
 - Confiance et sécurité
 - Sécurité intérieure et défense



1 visiteur sur 3
a assisté à au moins
une intervention

+ de 4000 participants
à distance en « live »

De nombreux contenus
en replay sur la chaîne
Youtube inCyber

Un lieu de networking

- o **68 400** messages échangés durant les 3 jours via la plateforme de networking
- o **1 800** réunions business sur 3 jours
- o **+ de 80** activités publiques ou privées organisées par les partenaires à l'occasion du FIC

De nombreux événements associés



+ 2200 participants (+175%)
Conférence sur la cybersécurité de l'OT et un village de 600m² sur le salon



+ 1500 participants (+87,5%)
Conférence sur l'identité numérique et la connaissance du client, et un village de 300 m² sur le salon



+ 400 participants
Conférence sur la réponse aux incidents et l'investigation numérique



+ 1400 participants (+366%)
Conférence sur l'OSINT et l'investigation



+ 720 participants (+380%)
Conférences sur la modération des contenus offensants et illégaux



+ 150 participants pour cette demi-journée (1^{er} année)
Conférences sur les investissements européens dans la cybersécurité
Pitch de startups européennes

Trois compétitions

- o **Prix de la Startup FIC**
- o **Prix du livre cyber**
- o **European Cyber Cup** : compétition de hacking éthique organisée autour de différentes épreuves (forensic, CTF, Speedrun, OSINT, hardware, bug bounty) destinée à valoriser les métiers et compétences liées à la cybersécurité
 - 2 jours de compétition
 - 6 épreuves
 - 25 équipes & 250 participants

Une forte visibilité

- o **+ de 100 journalistes accrédités**
- o Un média dédié à la communauté cyber internationale : **inCyber Media**
- o De nombreux contenus en replay sur la chaîne **Youtube inCyber**
- o **510 000 impressions** et **engagements** uniques du contenu posté par le FIC et ses événements associés sur ses propres comptes
- o **24 millions d'impressions** de contenus sur le FIC sur Twitter (événement + 2 semaines)
- o **21 millions d'impressions** de contenus sur le FIC sur LinkedIn (événement + 2 semaines)



Une communauté active toute l'année avec inCyber Media

inCyber Media est un média international
dédié aux enjeux de la cybersécurité.

- Un suivi permanent de l'actualité cyber
- De nombreux contenus écrits ou vidéo
- Une 50aine de RDV annuels (petits-déjeuners et webinars)
- La publication de plusieurs baromètres sectoriels

+88,5K abonnés

<https://www.incyber.org>

inCyber

Une contribution au débat public grâce à l'Agora

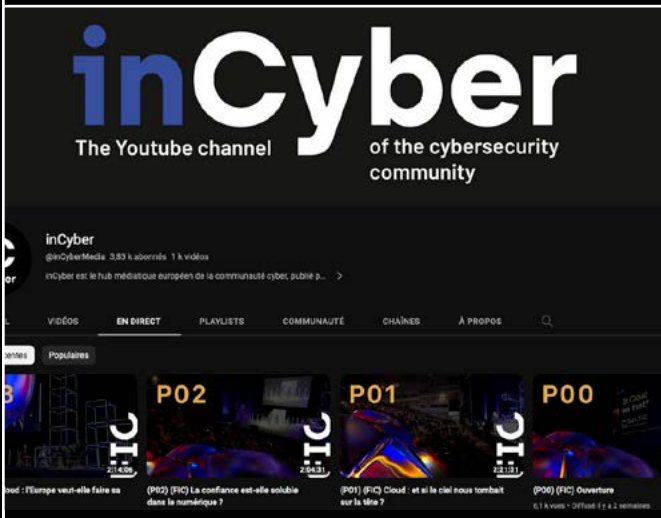
L'Agora est le think-tank européen
du FIC.

Elle réunit les décideurs publics et privés sur les enjeux stratégiques de la cybersécurité. Grâce à ses différents rendez-vous (clubs, rencontres...) et travaux, elle contribue à construire la cybersécurité de demain.

Lire le dernier livre blanc de l'Agora :
« *L'union fait la force. Les citoyens et la cybersécurité au 21e siècle* ».

<https://www.agora-fic.com/>

Agora



Le FIC devient

**IN CYBER
FORUM**

**AMÉRIQUE
DU NORD**

MONTRÉAL
CANADA

25 & 26 OCT. 2023

EUROPE

LILLE, FRANCE

**26, 27 & 28
MARS 2024**

AMERICAS

SAN ANTONIO
ÉTATS-UNIS

JUIN 2024

