IN CYBER FORUM

EUROPE

BROCHURE

Ready for AI ?

MARCH 26-28

LILLE GRAND PALAIS

Organized by

ceis Forward

With the support of

Région Hauts-de-France

europe.forum-incyber.com

Bienvenue

In Cloud We Trust ?

L'informatique dématérialisée est le moteur de la transformation numérique. Alors que le taux d'adoption en Europe n'est que de 40 %, le potentiel de marché pour les fournisseurs et les gains de productivité pour les clients finaux sont considérables. Pour autant, le choix d'une solution ne se résume pas à des critères fonctionnels et financiers, car il s'agit d'un engagement à long terme.

En clair, le cloud public revient à "utiliser l'ordinateur de quelqu'un d'autre", et les organisations lui confient non seulement leur patrimoine informationnel, mais aussi parfois leurs processus métiers les plus stratégiques. La cybersécurité et la confiance que nous pouvons - ou ne pouvons pas - accorder aux fournisseurs d'informatique dématérialisée sont donc cruciales. La cybersécurité peut être évaluée, mesurée et comparée, tandis que la confiance repose sur une appréciation beaucoup plus subjective qui peut rarement être garantie par des accords. Il en résulte que nous sommes souvent contraints de faire confiance "par défaut".

Ces deux aspects comportent de nombreux risques. Même si le partage des ressources, que facilite le Cloud computing, est un avantage en termes de cybersécurité, la concentration des données est aussi une faiblesse importante : une attaque sur un hyperviseur, par exemple, peut créer un risque systémique. D'un point de vue stratégique, la dépendance qu'elle crée, et même le verrouillage que certains accords de cloud computing impliquent, peuvent également affaiblir les organisations et même, à terme, perturber les chaînes de valeur traditionnelles. D'un point de vue opérationnel, le cryptage des données de bout en bout est bien sûr une solution technique efficace pour garantir la confidentialité des données, mais est-ce suffisant ? Faut-il également délocaliser nos données ? Comment s'assurer que les opérateurs de l'informatique en nuage disposent de contrôles efficaces ? La prolifération de lois dont la compétence dépasse les frontières nationales ou régionales a entamé la confiance, en particulier dans un climat géopolitique tendu. Avec 70 % des données européennes stockées et traitées en dehors du continent, principalement par des hyperscalers basés aux États-Unis, que se passerait-il si les données européennes étaient prises en otage ?

Pour relever ces défis et récolter à son tour les bénéfices de la révolution du cloud, l'Europe ne peut plus se reposer sur ses lauriers dans cet état de grande dépendance. D'autant plus que l'Europe possède de nombreux atouts : des entreprises performantes et innovantes, une industrie traditionnelle forte et un marché potentiel important, pour n'en citer que trois. Elle doit donc exploiter toutes ses prouesses en matière de politique industrielle et saisir les opportunités de la prochaine révolution de l'informatique dématérialisée - l'informatique dématérialisée en périphérie - déclenchée par l'explosion de l'internet des objets.

Général d'Armée (2S) Marc WATIN-AUGOUARD
Fondateur du Forum InCyber
Founder of the InCyber Forum

Welcome

In Cloud We Trust?

The public cloud is the driving force behind digital transformation. Given that the adoption rate in Europe is only 40%, the market potential for providers and the productivity gains for end customers are staggering. However, choosing a solution is not as straightforward as simply looking at functional and financial criteria, as this decision is a long-term commitment.

In simple terms, the public cloud is tantamount to "using someone else's computer", and organisations are entrusting it not only with their information assets, but also sometimes with their most strategic business processes. Cybersecurity and the trust we can – or cannot – place in cloud providers are therefore crucial. Cybersecurity can be evaluated, measured and compared, while trust is based on a much more subjective assessment that can rarely be guaranteed by agreements. The upshot is that we are often compelled to trust by "default".

There are many risks associated with both these aspects. Even though resource sharing, which Cloud computing facilitates, is an advantage in terms of cybersecurity, data concentration is also a serious weakness: an attack on a hypervisor, for example, can create a systemic risk. From a strategic point of view, the dependency it creates, and even the lock-in that some cloud agreements entail, can also weaken organisations and even ultimately disrupt traditional value chains. Operationally, end-to-end data encryption is of course an effective technical solution to ensure data confidentiality, but is it enough? Do we also need to relocate our data? How do we make sure that cloud operators have effective controls? The proliferation of laws that have jurisdiction beyond national or regional boundaries has dented trust, especially amid a tense geopolitical climate. With 70% of European data stored and processed outside the continent, mainly by US-based hyperscalers, what would happen if European data was taken hostage?

To square up to these challenges and in turn reap the benefits of the cloud revolution, Europe can no longer rest on its laurels in this state of high dependency. All the more so because Europe has many attractions: successful and innovative companies, strong traditional industry and a large potential market, to name just three. It must therefore harness all its industrial policy prowess and seize the opportunities of the next cloud revolution – the edge cloud – triggered by the explosion of the Internet of Things.

Guillaume TISSIER
Directeur du Forum InCyber Europe
Director of InCyber Forum Europe


SentinelOne®
Protect the Endpoint
Secure the Cloud
Unify Your Data
Learn How at SentinelOne.com

H E X A T R U S T

CLOUD CONFIDENCE & CYBERSECURITY

ÉQUIPE DE FRANCE DE LA CYBER & DU CLOUD DE CONFIANCE

WWW.HEXATRUST.COM

RETROUVEZ SUR LES PAVILLONS

HEXATRUST

AISI
ALGOSECURE
ARCAD SOFTWARE
ASTRAN
ATEMPO
AUCAE
AXIANS
BRAIN
CONSCIO TECHNOLOGIES
CRYPTONEXT SECURITY
CYBER-DETECT
CYBERWATCH
DASTRA
DEVENSYS CYBERSECURITY
EBRC
EVERTRUST
F24
FAIRTRUST
HOLISEUM
ILEX IAM PLATFORM
INQUEST
JALIOS
LAGERTHA
LOGIN SECURITE
MAILINBLACK
MAKE IT SAFE
NAMESHIELD
NEOTRUST
NUMSPOT
OODRIVE
OUTSCALE - Dassault Systèmes
PARSEC
PRIM'X
QONTROL
RETARUS
REVERSENSE
SMART GLOBAL GOVERNANCE
SNOWPACK
SYNETIS
TIXEO
TRANQUIL IT
TRUSTBUILDER
UBIKA
WALLIX
YOGOSHA

Table of contents
Sommaire

Notre engagement : vous garantir un numérique de confiance, sécurisé et souverain.

Nos solutions numériques, responsables et éthiques offrent **les plus hauts niveaux de sécurité** et s'adaptent à vos enjeux, quel que soit votre secteur.

Entreprises de toutes tailles, administrations, Docaposte et ses 6500 collaborateurs vous accompagnent dans votre transformation numérique en confiance.

Rencontrez-nous sur le **stand G24**
pour découvrir nos **solutions d'identités numériques et de cybersécurité.**

docaposte.com

DOCAPOSTE

Docaposte, filiale du groupe La Poste, société au capital de 90 000 000 €. Siège social : 45/47 bd Paul Vaillant Couturier 94200 IVRY-SUR-SEINE - AP - FIC 03/24

RÉGION Nouvelle-Aquitaine

TERRITOIRE DE CONFIANCE NUMÉRIQUE

Stand B12

ADACIS votre partenaire sécurité
AKTEA
escape
Game Partners
KNOCKKNOCK
VIGILAN SOLUTIONS
GOTTAPHISH
v6Protect Web Application Security
IS Decisions
sitincloud
NOVENCI Infrastructure. Infogérance & Sécurité

11 ENTREPRISES INNOVANTES à rencontrer sur notre espace

entreprises.nouvelle-aquitaine.fr

Highlights
Temps forts

26 March

Sommet d'ouverture
Opening summit

16H–19H
GRAND THÉÂTRE

Plénière d'ouverture
Opening Plenary

Web 3 Security Summit

9H30–16H
ROOM 0.5+0.6

Présentation des Forum InCyber Amérique du Nord 2024, Europe et Texas 2025
Presentation of the InCyber Forum North America 2024, Europe and Texas 2025

17H–18H
AMPHITHEATER MARIE CURIE

27 March

P1

8H45–11H15
GRAND THÉÂTRE

Réinventer la cybersécurité à l'ère de l'IA
Reinventing cybersecurity in the age of AI

Agora

15H15
SALLE 3.8 LOUNGE

P2

16H45–18H30
GRAND THÉÂTRE

Révolution numérique et bousculements géopolitiques : l'Europe est-elle toujours dans la course ?
Digital revolution and geopolitical upheaval: is Europe still in the race?

Lancement EC2
Launch EC2

9H
SALLE BEFFROIS

Début de l'European Cyber Cup, 20 équipes, 7 épreuves d'hacking ethique, 2 jours
Start of the European Cyber Cup, 20 teams, 7 ethical hacking challenges, 2 days

Remise Prix de la Startup

18H45
GRAND THÉÂTRE

Trophées
Trophies

20H45
CCI
Sur invitation

Remise Trophées CyberLeaders + Prix du livre
The CyberLeaders Trophies

Speakers Intervenants

Antoine BORDES
Vice President IA HELSING

Manfred BOUDREAUX-DEHMER
Responsable responsable de la sécurité de l'information – OTAN

Chief Information Security Officer – NATO

Thierry BRETON
Commissaire au marché intérieur Commission Européenne
European commissioner for Internal market

Marie-Laure DENIS
Présidente de la CNIL
Chairman of the CNIL

Raphaël ENTHOVEN
Professeur de philosophie, chroniqueur et auteur de nombreux ouvrages dont son nouvel essai « L'esprit artificiel »
Philosophy professor, columnist, and author of numerous works, including his new essay "The Artificial Mind"

Hugues FOULON
CEO Orange Cyberdéfense

Bernard GAVGANI
Group Chief Information Officer BNP PARIBAS

Juhan LEPASSAAR
Executive Director – ENISA

Vincent Strubel
Directeur général de l'ANSSI
Director General, ANSSI

Highlights

Temps forts

28 March

P3

9H–11H

GRAND THÉÂTRE

IA en quête de confiance

AI in a quest for trust

Remise des prix EC2

EC2 awards ceremony

16H30

SALLE BEFFROIS

Dévrouvrez le vainqueur de la compétition de l'European Cyber Cup

Discover the winner of the European Cyber Cup competition

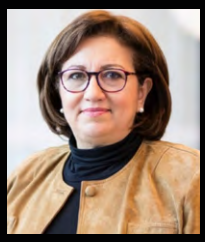
Intervenants

Olivier BABEAU

Président, Institut Sapiens

Françoise SOULIÉ-FOGELMAN

Conseiller Scientifique HUB FRANCE IA



Nozha BOUJEMAA

Vice-Présidente IA et Confiance DECATHLON DIGITAL

CMiB

"Cyber Made in Belgium"

A voice for the Belgian cyber security industry

Companies offering cyber security technologies in Belgium

Belgian Federal Public Cyber CMiB partners

CENTRE FOR CYBERSECURITY BELGIUM

DEFENSIE
LA DÉFENSE

CYBER SECURITY COALITION.be

CMiB Steering Committee

Cyberdefense

proximus NXT cybersecurity

Microsoft

TOREON
Business driven cyber consulting

APPROACH CYBER

cegeka
IN CLOSE COOPERATION

WAVESTONE

THE NRB GROUP

nviso

RHEA GROUP

NOKIA

Agoria Cybersecurity Services

Cyber attack Hotline	➪ Agoria REDline : tel: +32 2 706 88 77
Basic training	➪ Cyberstart.be : free e-tutorial
Advanced training	➪ · NIS 2.0 Academy · Cybersecurity in 30 steps

.AGORIA

Formats and New Features

Formats et nouveautés

Plénière
Plenary

26, 27 & 28 MARCH › 2H
GRAND THÉÂTRE

4 séances plénières accueillent les allocutions officielles, les keynotes, des fireset chats, et des débats en table-ronde.

4 Plenary sessions feature official addresses, keynotes, fireset chats and panel discussions.

Table Ronde
Round Tables

27 & 28 MARCH › 1H

Les tables-rondes font intervenir 4 à 5 intervenants sur un sujet précis.

Round tables bring together 4 to 5 speakers on a given topic.

Conférence
Conference

26, 27 & 28 MARCH › 30 min

Tribune libre donnant à un partenaire l'occasion de présenter un sujet technique, un retour d'expérience ou un témoignage client.

Talk by a Forum Incyber partner on technical topics, lessons learnt or client testimonials.

Démo. technique
Tehnical Demo.

26, 27 & 28 MARCH › 30 min
INCYBER DEMOS AREA

Présentations par les partenaires du Forum Incyber de projets R&D, solutions techniques, démonstrations d'attaques...

Presentations by Forum Incyber partners of R&D projects, technical solutions, attack demonstrations...

Masterclass

26, 27 & 28 MARCH › 30 min
VILLAGE RECHERCHE

Présentation de travaux de recherche, d'études et de projets de travail.

Presentation of research, studies and work projects.

Démo. d'attaque
Attack Demo.

26, 27 & 28 MARCH › 30 min
HACKING LAB

Présentations et demonstrations de Hacking éthique : projets R&D, solutions techniques, démonstrations d'attaques, recherches en vulnérabilités...

Presentations and demonstrations of ethical hacking: R&D projects, technical solutions, attack demonstrations, vulnerability research...

Startup Pitches

26, 27 & 28 MARCH
Innovation Village

Sessions thématiques de présentations de startups, animées par EVIDEN.

Startup pitches in thematic sessions, presented by EVIDEN.

InCyber Talk

26, 27 & 28 MARCH › 15 min
InCyber Talks Area

Intervention d'un partenaire sur le format TEDx.

TEDx-like keynote from a Forum Incyber partner.

ID&KYC Demo

26, 27 & 28 MARCH
ID & KYC Pavilion - G2

EU DEMOS

26, 27 & 28 MARCH
European Union Pavilion - E24

Forum InCyber Agora et PhilosoFIC

26, 27 & 28 MARCH › 1H30
Agora: 3.8 LOUNGE
PhilosoFIC: Théâtre Marie Curie

Des responsables d'entreprises, juristes, RSSI, chercheurs et parlementaires échangent au cours d'un atelier collaboratif.

Business managers, magistrates, lawyers, investigators, CISOs, academics and Congressmen work together on a given subject.

CFI Demo

26, 27 & 28 MARCH
CFI Pavilion E1

Retrouvez sur le village CFI des Talks et Démonstrations techniques présentant les meilleures solutions technologiques des systèmes d'information opérationnels, industriels ou embarqués

You will find talks and technical demonstrations on the CFI village presenting the best technological solutions for operational, industrial or embedded information systems.

TV SHOW

Media area - Coursive

En direct de notre plateau TV, RFI, Bsmart, S&D magazine, Capital, Alliancy, et SIH vous donnent rendez-vous pour décrypter l'actualité cyber au travers d'émissions et d'interviews d'experts et de décideurs. Les émissions seront diffusées en direct sur la page LinkedIn du Forum InCyber Europe !

Join us in the TV show area, where RFI, Bsmart, S&D magazine, Capital, Alliancy, and SIH will update you on the latest cyber news with many experts and cyber leaders! We will stream live on the LinkedIn page of the InCyber Europe Forum!

RH SHOW

Village Talents - G34

Le RH Show, votre rendez-vous sur le village Talents pour décrypter les enjeux RH dans la cyber ! Émissions, interviews, témoignages d'experts, retransmission EC2... Explorez les dernières tendances et meilleures pratiques RH dans un secteur en pleine expansion.

The RH Show: Joins us on the Talents Village to discuss HR challenges in the cyber world! Shows, interviews, expert testimonials, EC2 retransmission... Explore the latest trends and best HR practices in a booming sector.

Programme Overview

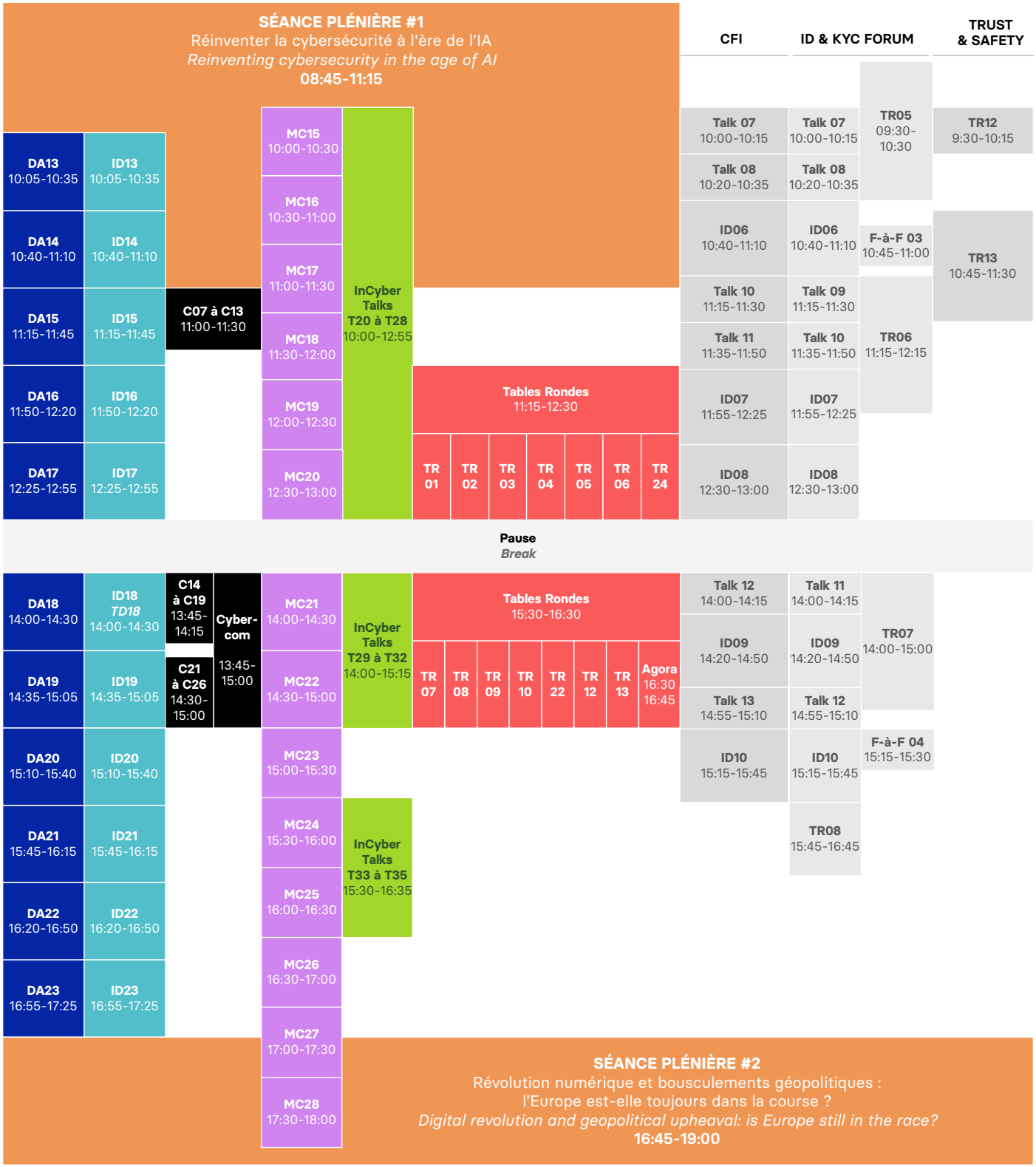
Grille programme

- P — Séance plénière / *Plenary session*
- TR — Table ronde / *Round table*
- C — Conférence / *Conference*
- FT — InCyber Talks
- MC — Masterclass
- ID — Incyber Demos
- DA — Démonstration d'attaque / *Attack demonstrations*
- Événements associés / *Associated events*
- P — Pause / *Break*

26 March

	CFI	ID & KYC FORUM	OSINT	TRUST & SAFETY	WEB 3	CYBER INVESTOR DAY
DA01 9:30-10:00	TR 01 9:20-10:20	Face à face 01 09:30-09:45	Discours d'intro. 09:30-10:00		Présentation 09:50-10:00	TR01 09:30-10:30
DA02 10:05-10:35		Talk 01 10:30-10:45	TR01 10:00-11:30	TR02 & TR05 10:00-10:45	TR1 & TR2 10:00-11:40	Pitch de startups 10:30-11:30
DA03 10:40-11:10		Talk 02 10:50-11:05				
DA04 11:15-11:45	TR 01 11:05-12:05	TR02 11:15-12:15	C01 11:40-12:10	TR03 11:15-12:00		Présentation baromètre Tikehau 10:30-11:40
DA05 11:50-12:20						TR02 11:40-12:30
DA06 12:25-12:55		ID02 12:25-12:55	C02 12:10-12:40			
ID01 09:30-10:00		TR01 09:45-11:00				
ID02 10:05-10:35		ID01 11:10-11:40				
ID03 10:40-11:10		Talk 03 11:45-12:00				
ID04 11:15-11:45		Talk 04 12:05-12:20				
ID05 11:50-12:20						
ID06 12:25-12:55						
MC01 10:00-10:30	InCyber Talks T01 à T11 09:20-12:55					
MC02 10:30-11:00						
MC03 11:00-11:30						
MC04 11:30-12:00						
MC05 12:00-12:30						
MC06 12:30-13:00						
Pause *Break*						
DA07 14:00-14:30	TR 03 14:10-15:10	TR03 14:00-15:15	TR02 14:00-15:30	TR01 & TR06 14:00-14:45	TR3 & TR4 14:00-15:45	Presentation Barometre Wavestone 14:00-14:10
DA08 14:35-15:05		Face à face 02 15:30-15:45	C03 15:30-16:00	TR04 & TR07 14:45-15:30		Pitch des startups 14:10-15:00
DA09 15:10-15:40		TR04 15:45-16:45	C04 16:00-16:15	TR11 16:00-16:30		TR3 15:00-16:00
DA10 15:45-16:15			TR03 16:30-18:00	TR09 16:30-17:15		
DA11 16:20-16:50				TR09 17:15-18:00		
DA12 16:55-17:25			Fermeture 18:00-18:30			
ID07 14:00-14:30		Talk 05 14:05-14:20				
ID08 14:35-15:05		ID03 14:20-14:50				
ID09 15:10-15:40		ID04 14:55-15:25				
ID10 15:45-16:15		Talk 06 15:30-15:45				
ID11 16:20-16:50		ID05 15:50-16:20				
ID12 16:55-17:25						
MC07 14:00-14:30	InCyber Talks T12 à T15 14:00-15:15					
MC08 14:30-15:00						
MC09 15:00-15:30						
MC10 15:30-16:00	InCyber Talks T16 à T19 15:30-16:45					
MC11 16:00-16:30						
MC012 16:30-17:00						
MC13 17:00-17:30						
MC14 17:30-18:00						
C01 à C03 15:30-16:00						
C04 à C06 16:30-17:00						
SOMMET D'OUVERTURE 16:00-19:00						
			Apér'OSINT 18:30-20:00			

27 March


SÉANCE PLÉNIÈRE #1
Réinventer la cybersécurité à l'ère de l'IA
Reinventing cybersecurity in the age of AI
08:45-11:15
CFI
ID & KYC FORUM
TRUST & SAFETY
DA13 10:05-10:35
ID13 10:05-10:35
DA14 10:40-11:10
ID14 10:40-11:10
DA15 11:15-11:45
ID15 11:15-11:45
DA16 11:50-12:20
ID16 11:50-12:20
DA17 12:25-12:55
ID17 12:25-12:55
C07 à C13 11:00-11:30
MC15 10:00-10:30
MC16 10:30-11:00
MC17 11:00-11:30
MC18 11:30-12:00
MC19 12:00-12:30
MC20 12:30-13:00
InCyber Talks T20 à T28 10:00-12:55
Tables Rondes 11:15-12:30
TR 01
TR 02
TR 03
TR 04
TR 05
TR 06
TR 24
Talk 07 10:00-10:15
Talk 08 10:20-10:35
ID06 10:40-11:10
Talk 10 11:15-11:30
Talk 11 11:35-11:50
ID07 11:55-12:25
ID08 12:30-13:00
Talk 07 10:00-10:15
Talk 08 10:20-10:35
ID06 10:40-11:10
Talk 09 11:15-11:30
Talk 10 11:35-11:50
ID07 11:55-12:25
ID08 12:30-13:00
TR05 09:30-10:30
F-à-F 03 10:45-11:00
TR06 11:15-12:15
TR12 9:30-10:15
TR13 10:45-11:30
Pause
Break
DA18 14:00-14:30
ID18 TD18 14:00-14:30
DA19 14:35-15:05
ID19 14:35-15:05
DA20 15:10-15:40
ID20 15:10-15:40
DA21 15:45-16:15
ID21 15:45-16:15
DA22 16:20-16:50
ID22 16:20-16:50
DA23 16:55-17:25
ID23 16:55-17:25
C14 à C19 13:45-14:15
C21 à C26 14:30-15:00
Cyber-com 13:45-15:00
MC21 14:00-14:30
MC22 14:30-15:00
MC23 15:00-15:30
MC24 15:30-16:00
MC25 16:00-16:30
MC26 16:30-17:00
MC27 17:00-17:30
MC28 17:30-18:00
InCyber Talks T29 à T32 14:00-15:15
InCyber Talks T33 à T35 15:30-16:35
Tables Rondes 15:30-16:30
TR 07
TR 08
TR 09
TR 10
TR 22
TR 12
TR 13
Agora 16:30 16:45
Talk 12 14:00-14:15
ID09 14:20-14:50
Talk 13 14:55-15:10
ID10 15:15-15:45
Talk 11 14:00-14:15
ID09 14:20-14:50
Talk 12 14:55-15:10
ID10 15:15-15:45
TR08 15:45-16:45
TR07 14:00-15:00
F-à-F 04 15:15-15:30
SÉANCE PLÉNIÈRE #2
Révolution numérique et bousculements géopolitiques : l'Europe est-elle toujours dans la course ?
Digital revolution and geopolitical upheaval: is Europe still in the race?
16:45-19:00

28 March

ID24 9:30-10:00

SÉANCE PLÉNIÈRE #3
l'IA en quête de confiance
AI in a quest for trust
09:00-11:00

DA24 10:05-10:35 | **ID25** 10:05-10:35

DA25 10:40-11:10 | **ID26** 10:40-11:10

DA26 11:15-11:45 | **ID27** 11:15-11:45

DA27 11:50-12:20 | **ID28** 11:50-12:20

DA28 12:25-12:55 | **ID29** 12:25-12:55

C28 à C34 11:30-12:00

MC29 10:00-10:30
MC30 10:30-11:00
MC31 11:00-11:30
MC32 11:30-12:00
MC33 12:00-12:30
MC34 12:30-13:00

InCyber Talks T36 à T39 11:00-12:15

Tables Rondes 11:15-12:15
TR 14 | **TR 15** | **TR 16** | **TR 17** | **TR 18** | **TR 19** | **Phi-loso-FIC** 11:00 12:30

CFI	ID & KYC FORUM
Talk 14 10:00-10:15	**Talk 13** 10:00-10:15
Talk 15 10:20-10:35	**Talk 14** 10:20-10:35
ID11 10:40-11:10	**ID11** 10:40-11:10
Talk 16 11:15-11:30	**Talk 15** 11:15-11:30
Talk 17 11:35-11:50	**Talk 16** 11:35-11:50
Talk 18 11:55-12:10	**ID07** 11:55-12:10

Pause
Break

DA29 14:00-14:30 | **ID30** 14:00-14:30

DA30 14:35-15:05 | **ID31** 14:35-15:05

DA31 15:10-15:40 | **ID32** 15:10-15:40

DA32 15:45-16:15 | **ID33** 15:45-16:15

DA33 16:20-16:50 | **ID34** 16:20-16:50

DA34 16:55-17:25

MC35 14:00-14:30
MC36 14:30-15:00
MC37 15:30-15:30
MC38 15:30-16:00
MC39 16:00-16:30
MC40 16:30-17:00

InCyber Talks T40 à T46 13:00-15:15

Tables Rondes 15:30-16:30
TR 20 | **TR 21** 13:30 14:45 | **TR 11** | **TR 23** | **TR 25** | **TR 26**

Round Tables
Tables rondes

↘ 27 March

11:15–12:15

Sécurité opérationnelle *Operational Security*

Des test d'intrusion à la vitesse de l'IA

Penetration testing at AI speed?

Sécurité opérationnelle *Operational Security*

L'IA réinvente les fondamentaux de la CTI

AI reinvents the foundations of CTI

Sécurité et stabilité du cyberespace *Security and Stability in Cyberspace*

Intelligence artificielle : la course à la régulation

Artificial intelligence: the race for regulation

Management des risques cyber *Cyber risk management*

Comment évaluer et valider en continu son niveau de sécurité ?

How do we continuously assess and validate your level of security?

Souveraineté numérique *Digital Sovereignty*

Comment évaluer et « normaliser » la sécurité des IA ?

How do we assess and "standardize" AI safety?

Souveraineté numérique *Digital Sovereignty*

Espace de données, la revanche européenne

Data spaces: European revenge?

Lutte anti-cybercriminalité *Fight Against Cybercrime*

Coopération internationale : clé d'un avenir numérique sécurisé face à la cybercriminalité ?

International cooperation: the key to a secure digital future in the fight against cybercrime?

15:30–16:30

Sécurité opérationnelle *Operational Security*

Automatisation du SOC : jusqu'où aller ?

SOC automation: how far do we go?

Sécurité opérationnelle *Operational Security*

Le défi de la complémentarité public-privé au niveau local

The challenge of public-private partnerships at local level

Sécurité et stabilité du cyberespace *Security and Stability in Cyberspace*

Armes autonomes : quelles perspectives en matière de régulation ?

Autonomous weapons: what are the regulatory implications?

Sécurité des données et transformation numérique *Security and Stability in Cyberspace*

Les sauvegardes immuables, une parade absolue ?

How do we manage NIS 2 compliance and maintain it over time?

Lutte anti-cybercriminalité *Fight Against Cybercrime*

Comment exploiter l'IA dans les investigations numériques ?

How to harness AI in digital investigations?

Lutte anti-cybercriminalité *Fight Against Cybercrime*

Les arnaques dopées à l'IA

AI-powered scams

Agora

Pour une IA responsable, condition de la cybersécurité

Responsible AI: a prerequisite for cybersecurity

28 March

11:15–12:15

PhilosoFIC

11:00-12h30

Pensée artificielle ou pensée humaine? Notre intelligence à l'épreuve de l'IA.

Artificial thinking or human thinking? Our intelligence put to the test by AI

Sécurité opérationnelle
Operational Security

IA, production et analyse du code : une révolution ?

AI-based code production and analysis: a revolution?

Sécurité et stabilité du cyberespace
Security and Stability in Cyberspace

Après la guerre, quelles conditions pour la paix dans le numérique ?

After war, what are the conditions for digital peace?

Management des risques cyber
Cyber risk management

De la haute couture au prêt-à-porter : quelle cybersécurité pour les PME ?

From haute couture to ready-to-wear: what kind of cybersecurity is right for SMEs?

Souveraineté numérique
Digital Sovereignty

IA et cybersécurité : comment développer et « hybrider » les compétences ?

AI and cybersecurity: how do we develop and "hybridize" skills?

Sécurité des données et transformation numérique
Security and Stability in Cyberspace

Les sauvegardes immuables, une parade absolue ?

Are EDR, XDR, and MDR miracle solutions for hospitals?

Lutte anti-cybercriminalité
Fight Against Cybercrime

Dispositifs de captation : quelle régulation pour une technologie d'enquête des plus intrusives ?

Capture devices: how do we regulate one of the most intrusive investigative technologies?

15:30–16:30

Management des risques cyber
Cyber risk management

Cherche IA résiliente pour systèmes critiques

Wanted: resilient AI for mission-critical systems

Sécurité opérationnelle
Operational Security

Quelles solutions techniques pour sécuriser les IA ?

What technical solutions do we need to secure AI?

Management des risques cyber
Cyber risk management

Vers une IA « super oracle en cybersécurité » : quel rôle pour le RSSI demain ?

Moving toward a "cybersecurity super oracle" AI: what role will CISOs play in the future?

Management des risques cyber
Cyber risk management

Préserver l'intégrité de vos chaînes d'approvisionnement à l'ère de NIS 2

Preserving the integrity of your supply chains in the era of NIS 2

Sécurité des données et transformation numérique
Security and Stability in Cyberspace

Responsabilité et légalité : comment composer avec les fuites de données ?

Responsibility and legality: how do you deal with data leaks?

Side Events

Événements associés

ID & KYC FORUM

26–28 March
Room 3.2

Pavillon ID & KYC
Forum G2

L'ID & KYC Forum revient pour sa 4ème édition sur le Forum International de la Cybersécurité avec un village de 270m2 comprenant un espace de démonstration ! Plateforme d'échange et de rencontre articulé autour d'un village et d'un forum, cet événement associé rassemble acteurs publics et privés autour de l'identité digitale et de la KYC en France comme en Europe. En 2022, l'ID & KYC Forum a rassemblé 50 partenaires et 40 experts intervenants en touchant 4 300 visiteurs uniques sur sa partie salon et 1 200 auditeurs sur sa partie forum.

The ID & KYC Forum returns for its 4th edition at the International Cybersecurity Forum with a 270m2 village including a demonstration area! A platform for exchange and meeting articulated around a village and a forum, this associated event brings together public and private actors around digital identity and KYC in France and Europe. In 2022, the ID & KYC Forum brought together 50 partners and 40 expert speakers, reaching 4,300 unique visitors at the exhibition and 1,200 listeners at the forum.

CFI CYBERSECURITY FOR INDUSTRY

26 March 9:00–16:30
Théâtre Marie Curie

26–28 March
Pavillon CFI E1

Cybersecurity For Industry, est l'événement associé du Forum InCyber dédié aux problématiques de cybersécurité du monde industriel. Unique en Europe, il est un carrefour d'échanges et de découverte des solutions de cybersécurité pour l'industrie, ainsi que des solutions industrielles sécurisées.

Les systèmes industriels (également appelés technologies opérationnelles ou « OT ») sont au cœur de nos vies. Ils sont utilisés pour créer les produits que nous consommons, les réseaux de transport que nous utilisons et les systèmes qui nous fournissent énergie, eau potable, nourriture, confort et protection.Ils participent à la conception et à la fabrication de tous les objets et équipements de notre quotidien, soutenant le développement d'un monde de plus en plus interconnecté. Ces technologies sont omniprésentes, mais cela ne les rend pas moins vulnérables. On voit de plus en plus d'exemples de prises de contrôle, d'altérations ou de destruction d'installations ainsi que d'innombrables démonstrations d'attaques contre des systèmes insuffisamment sécurisés.Plus un objet est connecté, plus il s'expose aux menaces. Quelle que soit la taille de l'entreprise concernée, les décideurs doivent évaluer ces risques et mettre en place les mesures de prévention, de détection et de réactivité nécessaires.

Pour profiter des bienfaits de cette révolution, chaque composante doit être sécurisée au bon niveau, pour assurer sûreté de fonctionnement, confiance et résilience à notre industrie.

"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.

Industrial systems (also known as operational technologies or "OT") are at the heart of our lives. They are used to create the products we consume, the transportation networks we use, and the systems that provide us with energy, drinking water, food, comfort and protection.They are involved in the design and manufacture of all our everyday objects and equipment, supporting the development of an increasingly interconnected world. These technologies are ubiquitous, but that doesn't make them any less vulnerable. There are more and more examples of systems being taken over, tampered with or destroyed, as well as countless demonstrations of attacks against insufficiently secure systems. The more connected an object is, the more exposed it is to threats. Whatever the size of the company concerned, decision-makers need to assess these risks and put in place the necessary prevention, detection and reactivity measures.

To reap the benefits of this revolution, every component needs to be secured at the right level, to ensure that our industry operates safely, with confidence and resilience.

EC2

Retransmission en direct sur le pavillon Talents

27 March 9:00 Salle Beffrois ou Pavillon Talents
28 March 16:30 Salle Beffrois

L'European Cyber Cup (EC2), 1ère compétition d'eSport dédiée au hacking éthique, revient pour sa 4ème édition avec :

- 36h de compétition non-stop
- 20 équipes étudiantes, professionnelles et institutionnelles
- 7 épreuves/challenges pendant 2 jours : Forensic, OSINT, CTF, Hardware, Speedrun, Bug Bounty
- 1 seule équipe vainqueur !

Dévrouvrez le vainqueur de la compétition de l'European Cyber Cup.

The European Cyber Cup (EC2), the 1st eSport competition dedicated to ethical hacking, is back for its 4th edition with:

- *36 hours of non-stop competition*
- *20 student, professional and institutional teams*
- *7 events/challenges over 2 days: Forensic, OSINT, CTF, Hardware, Speedrun, Bug Bounty*
- *1 single winning team!*

Unveil the winner of the European Cyber Cup competition.

JOURNÉE

OSINT

26 March 9:30–18:30
Salle 3.1.

L'OSINT est devenue une pratique à part entière. De la lutte anti-criminalité (cyber, physique, financière..) aux crypto-monnaies, en passant par la sécurité des biens et des personnes en période de conflits armés, l'OSINT est aujourd'hui utilisée dans de nombreux domaines.

La Journée OSINT du Forum InCyber a pour objectif de mettre en lumière des applications concrètes de cette pratique et de rassembler les professionnels, passionnés et curieux de l'OSINT à venir présenter leurs savoir-faire et assister aux RETEX présentés, autour des thématiques suivantes :

- Cybercriminalité
- Anti-terrorisme
- Criminalité financière
- Audits Red Team
- Tensions géopolitiques
- Fraudes
- Arnaques aux crypto-monnaies...

OSINT has become a practice in its own right. From the fight against crime (cyber, physical, financial, etc.) to crypto-currencies, not forgetting the security of goods and people during armed conflicts, OSINT is now used in a wide range of fields.

The aim of the InCyber Forum's OSINT Day is to highlight the practical applications of this practice and to bring together professionals, OSINT enthusiasts and the curious to come and present their know-how and attend the RETEX presented, around the following themes:

- *Cybercrime*
- *Anti-terrorism*
- *Financial crime*
- *Red Team fraud*
- *Geopolitical tensions*
- *Fraud*
- *Crypto-currency scams...*

TRUST & SAFETY FORUM

26 mars 9:30–18:00
Salle 3.7 et 3.8

27 mars 9:00–12:00
Salle 3.7

Depuis 2021, le Trust & Safety Forum (T&SF) offre un espace cohésif ouvert à toutes les parties prenantes, des plateformes aux régulateurs, en incluant les faggers de confiance et les fournisseurs de solutions, engagés en faveur d'un environnement numérique de confiance et plus sûr aujourd'hui et pour l'avenir. Le T&SF offre un lieu et un moment pour tisser des liens avec les différentes parties prenantes afin de discuter et de faire avancer les initiatives de collaboration, de développer des processus et des solutions innovantes en veillant à ce que l'environnement numérique reste un lieu de partage des connaissances, de construction de communautés, de développement d'opportunités et d'autonomisation des personnes.

Trust & Safety s'efforce de devenir une discipline standard au sein de la grande famille de la sécurité, mais elle ne doit pas être cloisonnée. Trust & Safety concerne l'identification et le traitement des contenus préjudiciables et illégaux, mais aussi les contenus inappropriés et tendancieux ("fake news"), la protection des contenus (IP), les cybermenaces (phishing et autres types d'abus), la fraude (fraude au paiement, vol d'identité, etc.). La plupart de ces dimensions ont été traitées au sein du FIC, la Conférence internationale sur la cybersécurité, au cours des quinzes dernières années. La T&SF est un nouveau aspect nécessaire qui contribue à la communauté de la sécurité.

La confiance et la sécurité sont un problème mondial qui nécessite des initiatives mondiales, mais les solutions sont également et essentiellement ancrées dans les écosystèmes locaux. C'est pourquoi la T&SF est associée au FIC, une conférence qui attire les écosystèmes nationaux de cybersécurité, car Trust & Safety est une question de synergies entre les disciplines.T&SF est cofondée par Jean-Christophe Le Toquin, Caroline Humer et Guillaume Tissier, qui apportent ensemble plus de 6 décennies d'expérience dans la mise en relation de personnes et d'organisations pour rendre notre monde numérique plus sûr et plus résilient.

Since 2021, the Trust & Safety Forum (T&SF) offers a cohesive space open to all stakeholders, from platforms to regulators, inclusive of trusted flaggers and solutions providers, committed to a trusted and safer digital environment today and for the future. The T&SF offers a place and time to connect with different stakeholders to discuss and advance collaborative initiatives, develop innovative processes and solutions ensuring that digital environment remains a place to share knowledge, to build communities, to develop opportunities and empower people.

Trust & Safety thrives to become a standard discipline within the broad family of security, but it should not be siloed. Trust & Safety is about identifying and treating harmful and illegal content, but also about inappropriate and biased content ("fake news"), protection of content (IP), cyber threats (phishing and other types of abuse), fraud (payment fraud, ID theft etc.). Most of these dimensions have been dealt with within FIC, the International Cybersecurity Conference, in the last fiffteen years. The T&SF is a new and necessary component in its own right, and a contributor to the security community.

Trust & Safety is a global problem which requires global initiatives, but the solutions are equally and essentially rooted in local ecosystems. This is why the T&SF is associated with FIC, a conference which attracts national cybersecurity ecosystems, because Trust & Safety is about synergies across disciplines.T&SF is cofounded by Jean-Christophe Le Toquin, Caroline Humer and Guillaume Tissier, who together bring more than 6 decades of experience in connecting people and organizations to make our digital word safer and more resilient.

Side Events

Événements associés

W3S

WEB3 SECURITY SUMMIT

26 March 8:30–19:00
Salle 0.4 à 0.6

En partenariat avec RAID SQUARE, le Web3 Security Summit rassemble les partenaires et intervenants sur la thématique Web3.
Nous sommes heureux de vous présenter les partenaires de cette première édition historique :
– ALLFEAT
– AMLBOT
– BUBBLEMAPS
– CHAINALYSIS
– FIREBLOCKS
– KALICERTIF
– SET IN STONE
– BLOBB_IO

Ils prendront la parole à l'occasion de cette journée :
– Fabien AUFRECHTER - VIVENDI
– Dominique PENIN - KRAMER LEVIN NAFTALIS & FRANKEL LLP
– Victor CHARPIAT - KRAMER LEVIN NAFTALIS & FRANKEL LLP
– Stanislas de QUERCIZE - MESSIKA
– Jean-Philippe AUMASSON - TAURUS
– Adrien LEMAIRE - SONEPAR
– Steve PEQUET - ALTEN
– Matthieu WORM - SIEMENS
– Guillaume LAMBOV - CHAINALYSIS
Nous vous attendons nombreux !

In partnership with RAID SQUARE, the Web3 Security Summit brings together partners and speakers on the Web3 theme. We are delighted to present the partners of this historic first edition:
– ALLFEAT
– AMLBOT
– BUBBLEMAPS
– CHAINALYSIS
– FIREBLOCKS
– KALICERTIF
– SET IN STONE
– BLOBB_IO

They will be speaking at the event:
– Fabien AUFRECHTER - VIVENDI
– Dominique PENIN - KRAMER LEVIN NAFTALIS & FRANKEL LLP
– Victor CHARPIAT - KRAMER LEVIN NAFTALIS & FRANKEL LLP
– Stanislas de QUERCIZE - MESSIKA
– Jean-Philippe AUMASSON - TAURUS
– Adrien LEMAIRE - SONEPAR
– Steve PEQUET - ALTEN
– Matthieu WORM - SIEMENS
– Guillaume LAMBOV - CHAINALYSIS
Nous vous attendons nombreux !

CORIIN

26 March 10:00–18:00
Louis Pasteur Theater

Inscriptions payantes

Conférence organisée par le CECyF, Centre Expert contre la Cybercriminalité Français, CoRIIN#9 est la 9e Conférence sur la réponse aux incidents & l'investigation numérique. Cette journée dédiée aux techniques de la réponse aux incidents et de l'investigation numérique, permettra aux enquêteurs spécialisés, experts judiciaires, chercheurs du monde académique ou industriel, juristes, spécialistes de la réponse aux incidents ou des CERTs de partager et échanger sur les techniques du moment. Thématiques attendues :
– Investigation numérique Techniques et outils d'analyse de supports numériques (forensic),
– Collecte et analyse de mémoire vive,
– Analyse d'artefacts d'applications, d'activités réseau,...
– Investigation sur Internet, sur les réseaux,
– Réponse aux incidents (outre les aspects forensiques évoqués ci-dessus appliqués à la réponse aux incidents),
– Détection des incidents, échange et traitement d'informations,
– Investigation dans des contextes professionnels (serveurs, postes de travail, appareils mobiles),
– En particulier dans le domaine des atteintes par virus informatiques,
– De la mitigation à la restauration d'un état normal de fonctionnement,
– Aspects juridiques.

Conference organised by the CECyF, French Expert Centre against Cybercrime, CoRIIN#9 is the 9th Conference on Incident Response & Digital Investigation. This day dedicated to the techniques of incident response and digital investigation will allow specialised investigators, forensic experts, researchers from the academic or industrial world, lawyers, incident response specialists or CERTs to share and exchange on the techniques of the moment. Expected themes :
– Digital investigation Digital media analysis techniques and tools (forensic),
– Collection and analysis of random access memory,
– Analysis of application artefacts, network activities,...
– Internet and network investigation,
– Incident response (in addition to the above-mentioned forensic aspects applied to incident response),
– Detection of incidents, exchange and processing of information,
– Investigation in professional contexts (servers, workstations, mobile devices),
– In particular in the field of computer virus attacks,
– From mitigation to restoration of normal operation,
– Legal aspects.

TREND MICRO™

Trend Vision One™

Unified Cybersecurity Platform

- To integrate Cloud Risk Management and XDR Across Customers' Entire Attack Surface
- To consolidate cybersecurity efforts
- To achieve a complete view of security risks across hybrid IT environments, both onprem & SaaS
- To benefit from a unified approach to **risk management, threat detection** and **incident response**—drawing on data from diverse sources, including **cloud metadata, containers, workloads, endpoints, identities, networks,** and **emails.**
- To support your IT teams

Stand B14

www.trendmicro.com

Cyber Solutions by Thales

- Detection and Response
- Risk evaluation
- Training and simulation
- Network, data and communications protection

11 CyberLabs & Academies
to train cybersecurity experts and test the resilience of networks

n°1 WORLDWIDE
in data protection

11 SOCs
Security Operation Centres

19 Consulting teams

THALES
Building a future we can all trust

Les temps forts des partenaires

ACCENTURE

Rencontrez SMESH, l'assistant dopé à l'IA qui révolutionne la cyber !

Venez découvrir notre dernier projet de R&D : un assistant cyber propulsé par l'IA. Assistez à une démonstration pour voir comment il accompagne les équipes cyber, facilite le travail de qualification du SOC, améliore le pilotage d'actions de remédiation et crée des scénarios de phishing adaptés en s'appuyant sur l'OSINT.

Meet SMESH, the AI-powered assistant that's revolutionizing cyber!

Come discover our latest R&D project: an AI-powered cyber assistant. Attend a demonstration to see how it supports cyber teams, facilitates the SOC's qualification work, improves the management of remediation actions, and creates tailored phishing scenarios by leveraging OSINT.

F4 - 26 March - 15:30

JO 2024 : Les enseignements de Tokyo

Nous vous proposons d'explorer les faits marquants des précédents Jeux Olympiques dont ceux de Tokyo, et de tester vos connaissances sur ce sujet. À seulement 4 mois des JO de Paris, abordons ensemble les actions essentielles pour renforcer la sécurité et garantir le succès de cet événement majeur. Rejoignez-nous pour une expérience interactive."

Olympic Games 2024: Lessons from Tokyo.

We invite you to explore the events that marked the previous Olympic Games, including those in Tokyo, and to test your knowledge on the subject. With only 4 months to go until the Paris Olympics, let's take a look at the essential actions needed to enhance safety and guarantee the success of this major event. Join us for an interactive experience.

F4 - 28 March - 10:30

Comment réaliser efficacement un exercice crise cyber ?

Préparez-vous à vous détacher des formats usuels ! Nous allons vous montrer comment réaliser un exercice de gestion de crise immersif, tout en évitant les pièges classiques les plus rencontrés et en étant le plus impactant possible au sein de votre organisation. Prêt pour l'exercice ? Rendez-vous sur notre stand F4."

How do you carry out an effective cyber crisis exercise?

Get ready to break away from the usual formats! We're going to show you how to carry out an immersive crisis management exercise, while avoiding the most common pitfalls and having the greatest possible impact on your organisation. Ready for the exercise? Come and see us on stand F4.

F4 - 27 March - 10h15

ADVENS

A la découverte de notre démo mySOC

Vous aurez l'occasion de découvrir en toute transparence comment les comportements malveillants sont détectés par notre plateforme SOC et comment nos analystes, augmentés d'IA et du nouveau portail mySOC, améliorent la posture sécurité de nos clients et remédient collaborativement à tous leurs incidents de sécurité.

Discovering our mySOC demo

You will have the opportunity to discover in complete transparency how malicious behavior is detected by our SOC platform and how our analysts, augmented with AI and the new mySOC portal, improve the security posture of our clients and collaboratively resolve all their security incidents.

C1 - 26, 27 & 28 March

Le tiering et la gestion du changement

Tiering and change management

C1 - 27 March - 10:30

Les exercices de crise, la meilleure préparation pour faire face aux menaces.

Crisis exercises, the best preparation to face threats

C1 - 27 March - 15h30

Un tour d'horizon des risques numériques sur les IA.

An overview of digital risks in AI.

C1 - 28 March - 10:30

AKERVA

TIBER-EU – Le Red Teaming sur mesure pour VOTRE structure !

Le Threat Intelligence Based Ethical Red Teaming rassemble les techniques de CTI pour identifier les menaces précises pesant sur votre structure et l'expertise d'une Red Team pour jouer des engagements réalistes et sur mesure issus directement des techniques des acteurs réels. Venez échanger avec Akerva sur cette nouvelle approche !

TIBER-EU – Red teaming made to measure for YOUR company!

Threat Intelligence Based Ethical Red Teaming brings together CTI techniques to identify precise threats on your perimeter and Red team expertise to simulate realistic and made to measure engagements directly from the real actors playbooks. Come and discuss this new approach with Akerva !

B7 - 26, 27 & 28 March- 10h30

DORA et les RTS de la Commission Européenne en cours !

Les exigences de DORA seront applicables au 17 Janvier 2025, en ce moment de nombreux travaux et discussions sont en cours avec la commission européenne sur les RTS nécessaires pour leur application. Akerva vous propose de venir échanger sur ce sujet !

DORA and the RTS of the European Commission in progress

The DORA requirements will come into force on January 17, 2025, and there is currently a great deal of work and discussion with the European Commission on the RTS expected for their application. Akerva invites you to discuss this subject with us!

B7 - 26, 27 & 28 March - 11:30

Red Team, comment un étranger s'invite dans vos locaux ?

L'intrusion physique est un scénario qui n'est plus réservé à Hollywood et les acteurs malveillants s'invitent dans vos locaux pour accéder à votre réseau, vos ordinateurs et vos documents papiers. Akerva vous propose un tour d'horizon des méthodes utilisées pour contourner votre sécurité et comment vous mieux protéger contre les intrus.

Red teaming, how a stranger gets into your offices?

Physical intrusion is no longer confined to Hollywood, and malicious actors invite themselves in your offices to access your network, your computers and your paper documents. Join Akerva for an overview on the techniques used to bypass your security, and how to better protect yourself against intruders.

B7 - 26 & 27 March - 14:30

SOC et réaction sur incident : ALERTE ROUGE et maintenant quoi ?

Votre SIEM est en place, vos règles sont configurées, tout est prêt. Et soudain, une alerte critique arrive. Que faire, comment réagir, quelles sont les bonnes actions pour qualifier et répondre aux alertes de votre supervision et protéger votre SI ? Akerva vous propose quelques réflexes et bonnes pratiques à garder en tête "au cas où".

SOC and incident response : RED ALERT, and now what ?

Your SIEM is deployed, your rules are tuned, everything is ready. And suddenly, the critical alert comes. What to do, how to react, what are the best actions to qualify and respond to your monitoring alerts and protect your network ? Akerva provides you with a few good practices and habits to keep in mind, "just in case".

B7 - 26 & 27 March - 15:30

NIS 2 et les travaux en cours entre prestataires PASSI/PACS et l'ANSSI

L'ANSSI crée l'exception à la Française et a proposé au cours de l'années 2023/2024 de nombreux échanges sur l'application de NIS 2 avec les prestataires PASSI/PACS, faisons le point !

NIS 2 and ongoing work between PASSI/PACS and ANSSI

ANSSI is creating a French-style exception, and has proposed a number of exchanges with PASSI/PACS providers over the course of 2023/2024 on the application of NIS 2.

B7 - 26 & 27 March - 16:30

ALTOSPAM

Protection de vos emails, la sensibilisation est-elle la seule arme ?

Pour protéger vos emails contre les attaques, la sensibilisation c'est bien mais chez Altospam, SaaS souverain, on pense que la protection c'est mieux ! On vous montre notre solution anti phishing, anti spam, anti virus 100% française, une forteresse sans compromis pour libérer vos emails. Simple, efficace et économique.

Email protection: is awareness training the only option ?

To protect your emails against attacks, awareness is good but at Altospam, we think protection is better! Come and see our SaaS cloud based anti-phishing, anti-spam, anti-virus solution, an uncompromising fortress to free your emails. Simple, effective and cost effective.

E1-3 - 27 March - 10:30

Armis & Aura iT

Comment faire face à la multiplication des vulnérabilités ?

La vulnérabilité « log4j » a montré la difficulté des entreprises à évaluer l'impact d'une CVE sur leur organisation. La gestion des vulnérabilités ne cesse de challenger les responsables sécurité, le nombre de vulnérabilités publiées croît chaque année, NIS2 et DORA se profilent... Quelles solutions pour faire face à ce problème universel ?

How to deal with the multiplication of vulnerabilities ?

The "Log4j" vulnerability showed how it's difficult for companies to assess the impact of a CVE on their organization. Vulnerability management continues to challenge security managers, the number of published vulnerabilities grows each year, NIS2 and DORA are coming... What solutions to deal with this universal problem ?

Espace Démo CFI E1 - 27 March - 15:15

Cocktail networking

Venez rencontrer les équipes Armis et Aura iT.

Networking cocktail

Come to meet Armis & Aura iT teams.

E1-7 - 27 March - 15:45

AUTONYM PTE LTD

Démonstration Cocktail Nevermind sur Stand

Nevermind est une solution innovante pour les entreprises qui propose une méthode de création, de contrôle et de partage des clés de chiffrement par l'utilisateur final. Nevermind introduit une connexion sans mot de passe qui reconnaît l'être humain et une rotation des clés à chaque session qui permet un chiffrement sans compromis. Notre Plateforme a été conçue pour garantir une sécurité et une confidentialité absolue mais aussi pour faciliter son utilisation et faciliter votre transformation numérique.

Demo Nevermind Happy Hours on Booth

Nevermind is an enterprise-grade solution that offers a new way of creating, controlling, and sharing keys to encrypt and store data, at the sole benefit of the end user. Nevermind introduces a password-less login that recognizes the human being, and a key rotation at every session to guarantee an uncompromised end-to-end encryption. Our Platform has been designed not only to guarantee absolute security and confidentiality, but also to make it easy to use and enable a stress-free digital transformation now.

Stand village innovation F18-28 - 28 March - 14:00-17:00

Bitdefender

Démo live XDR

Découvrez comment corréler et contextualiser facilement les données provenant des multiples sources réparties sur l'ensemble de votre infrastructure : endpoints, réseau, emails, identités et clouds. Vous serez ainsi en mesure d'unifier les alertes et de simplifier les investigations à l'échelle de votre organisation.

Live XDR demo

Discover how to easily correlate and contextualize data from multiple sources across your entire infrastructure: endpoints, network, emails, identities and clouds. You'll be able to unify alerts and simplify investigations across your organization.

B20 - 26 & 27 March - 10:00-17:00

BLANCCO

DÉMO : Découvrez l'Effacement Sécurisé Blancco

Blancco fournit aux organisations des solutions sécurisées, conformes et automatisées qui accélèrent la transition vers l'économie circulaire. Les effacements Blancco permettent aux organisations de protéger les données en fin de vie des accès non autorisés, redéployer en sécurité les supports de données et se conformer aux exigences liées au RGPD.

Live DEMO : Discover Blancco Secured Erasure

Blancco a carbon-neutral supplier provides organizations with secure, compliant and automated solutions that accelerate the transition to the circular economy. Each year 10 of millions of Blancco erasures allow organizations to protect end-of-life data against unauthorized access,safely redeploy data storage assets and firmly comply with GDPR.

D1 - 26, 27 & 28 March

BRADLEY & ROLLINS

VENEZ DÉCOUVRIR MAVGATE : VOTRE ANALYSE COMPLÈTE DE SURFACE D'ATTAQUE EN UN CLIC

Testez MavGate : notre nouvel outil d'analyse de surface d'attaque à 360 degrés, vous permettant d'obtenir en un rien de temps une analyse complète de la vue cybercriminelle sur votre infrastructure. L'outil passe au travers de plus de 250 sources pour vous fournir une analyse complète sous forme de dashboards. Venez tester gratuitement l'outil sur le booth de Bradley & Rollins qui se situe dans l'espace Opale et bénéficiez par la suite d'un coupon de réduction valable pour une durée de 30 jours suivant le salon afin de tester l'outil en interne.

DISCOVER MAVGATE: YOUR COMPLETE ATTACK SURFACE ANALYSIS IN JUST ONE CLICK

"Try out MAVGATE, our brand-new 360-degree attack surface analysis tool, giving you a complete analysis of the cybercriminal view of your infrastructure in the blink of an eye. The tool passes through over 250 sources to provide you with a complete analysis in dashboard form. Come

try out the tool for free at the Bradley & Rollins booth in the Opale area, and then benefit from a discount coupon valid for 30 days after the show to test it in-house."

Espace Opale - 26, 27 & 28 March

Centre pour la cybersécurité Belgique

Active Cyber Protection (ACP)

Au lieu de réagir de façon réactive aux menaces/incidents, l'ACP promeut une approche proactive, automatisée et participative pour renforcer la résilience du réseau d'une société. Elle vise à améliorer la prévention, la détection, la surveillance et la réduction des atteintes à la sécurité des réseaux face aux attaques malveillantes

Active Cyber Protection (ACP)

Rather than responding reactively to threats/incidents, ACP promotes a proactive, automated & participative approach to strengthen the resilience of a society's network infrastructure. It focusses on actively improving prevention, detection, monitoring & abating of network security breaches in the face of increasingly automated malicious techniques

E24/ European Pavillon - 26 March - 11:30

Cyber4Industry

Comment votre site de production va être mis à l'arrêt ?

En direct et sur place, notre démonstrateur montre l'attaque d'un réseau OT qui perturbe le système (votre outil de production) sans que l'opérateur ne s'en rendre compte. Dans un second temps, la démonstration montre la situation qui aurait permis de faire échouer l'attaque. Le tout est réalisé avec des équipements standards dans l'industrie.

How your production site will be disrupted?

Live and in situ, our demonstrator shows the attack on an OT network that disrupts the system (your production tool) without the operator realizing it. In a second step, the demonstration shows the situation that would have allowed the attack to fail. All this is achieved using industry-standard equipment.

H1-5 - 26,27 & 28 - 11:30-14:30

Cybersecurity Luxembourg

Happy Hour au Luxembourg !

N'hésitez pas à nous rejoindre sur le pavillon luxembourgeois (F9), pour une séance de networking en toute décontraction lors de notre traditionnel Happy Hour autour de délicieuses bières luxembourgeoises. Nous serons honorés de vous y retrouver et de partager ce moment mêlant, expertise, convivialité et bonne humeur.

Happy Hour in Luxembourg!

Do not hesitate to join us in the Luxembourg pavilion (F9), for a relaxed networking session during our traditional Happy Hour event, featuring delicious Luxembourg beers. We would be honoured to see you there and share this moment of expertise, conviviality and good vibes with you!

F9 - 26 March - 16:30-18:00

EGERIE

Démonstration : Pilotage dynamique du risque cyber : comment le mettre en œuvre ?

Exploiter la collaboration sur la plateforme EGERIE pour accélérer la construction de la vision 360°. Adapter la démarche en fonction des ressources et de l'échéancier Quels bénéfices pour le RSSI et la Direction Générale ?

Demonstration: Dynamic management of cyber risk: how to implement it?

Exploit collaboration on the EGERIE platform to accelerate the construction of the 360° view. Adapt the approach according to resources and schedule.What benefits for the CISO and C-Levels?

A8 - 26, 27 & 28 March

Démonstration : Quantification du risque cyber : comment prioriser vos investissements pour prendre les meilleures décisions ?

Pourquoi faut-il quantifier les risques cyber ? Comment définir les données entrantes de la quantification financière ? La quantification du risque cyber par EGERIE : processus et étapes. Comment utiliser les résultats de la quantification financière pour améliorer vos analyses de risques ?

Demonstration: Quantifying cyber risk: how to prioritize your investments to make the best decisions?

Why do we need to quantify cyber risks? How to define the incoming data for financial quantification? Quantification of cyber risk by EGERIE: processes and stages How to use the results of financial quantification to improve your risk analyses?

A8 en continu

Démonstration : Intégrer la sécurité dans les projets : comment impliquer les métiers ?

Exploiter la collaboration sur la plateforme EGERIE pour impliquer les métiers Utiliser les analyses de risques dans les projets pour construire une vision 360° Quels bénéfices pour le RSSI et la Direction Générale ?

Demonstration: Integrating security into projects: how to involve the professions?

Exploit collaboration on the EGERIE platform to involve the professions. Use risk analyzes in projects to build a 360° vision. What benefits for the CISO and General Management?

A8 - 26, 27 & 28 March

Enclaive

Making the cloud your Private Data Center: EMCP Product Launch, DEMO of software and FAQ

E8-4 - 27 March - 15:00-15:45

EUROPEAN CHAMPIONS ALLIANCE

Part 1: From defensive cybersecurity to resilience

E8 - 27 March - 14:00-14:45

Part 2: NIS2, constraints or business opportunity ?

E8 - 28 March 10:00-10:45

EXEO

Monitoring Cloud Security: Observability & Cyber Threat Intelligence

E8-5 - 28 March 11:30-12:15

FORTINET

Plateforme de Défense en Profondeur pour la Cybersécurité des Réseaux Industriels et OT

Démonstrations d'attaque et de défense cyber sur un environnement industriel comprenant un Robot, une IHM, un Panel, de la Safety et des protocoles Modbus, Profinet, OPC-UA. Firewalls industriels, Contrôles applicatifs OT et virtual patching des vulnérabilités. Segmentation et micro-segmentation. Système d'alarme OT avec le FortiDeceptor.

Industrial and OT Cybersecurity Platform covering the entire attack surface.

Cyber attack and defense demonstrations on an industrial environment including Robot, HMI, Panel, Safety with Modbus, Profinet and OPC-UA protocols. Industrial firewalls, OT application controls and virtual patching of vulnerabilities. Segmentation and micro-segmentation. OT alarm system with FortiDeceptor.

A14 - 26 March - 16:00

Accès évolutif, simple et sécurisé pour les utilisateurs en mobilité

Grâce à la convergence des services réseaux et sécurité, Fortinet garantit une sécurité maximale pour tous les utilisateurs et les terminaux, qu'ils accèdent au web, aux applications d'entreprise ou aux applications SaaS. Venez découvrir comment la solution FortiSASE offre une sécurité consistante et améliore l'expérience utilisateurs quel que soit leur localisation.

Scalable, Simple, and Secure Access for Remote Workforce

Fortinet SASE solution ensures the utmost security for all edges, devices, and users, whether they are accessing the web, corporate applications, or SaaS applications. Visit us to discover how Fortinet's unique security and networking convergence approach, offers organizations a consistent security posture and improved user experience.

A14 - 27 March - 11:00

FORTRA

Découvrez Fortra, votre allié en Cybersécurité

Fortra dessine un avenir à la fois plus solide et plus simple de la cybersécurité en proposant des solutions intégrées et évolutives. Découvrez nos suites de solutions de protection des données, de la messagerie ou encore de pentest. Des solutions qui incluent des marques telles que, Digital Guardian, Agari, Terranova Security et bien plus encore.

Discover Fortra, your Cybersecurity ally

Cybersecurity is constantly evolving... Just like us! Fortra is creating a stronger and more straightforward future for cybersecurity by offering integrated and scalable solutions. Discover our suite of Data Protection, Email Security and Offensive Security solutions, which include Agari, GoAnywhere, Digital Guardian, Terranova Security and more.

F1 - 26, 27 & 28 March - 10:30

Cas d'usage de Data Protection – Fortra's Digital Guardian et Data Classification live demo

Votre organisation doit protéger ses données sensibles tout au long de leur cycle de vie, de la création au partage, tout en garantissant leur conformité. Rejoignez-nous pour cette démo et découvrez comment la Data Classification et Digital Guardian de Fortra résolvent certains cas d'utilisation réels de protection des données.

Data Protection Common Use Cases – Fortra's Digital Guardian and Data Classification live demo

Your organisation needs to protect data across its entire lifecycle, from creation to sharing externally, while assuring compliance. Join us at this live demo to learn how Fortra's Data Classification and Digital Guardian solve common real data protection use cases.

F1 - 26 & 27 March - 16:00-17:00

La sensibilisation à la sécurité de l'information : Construire votre culture cyber –Fortra's Terranova Security live demo

La cybersécurité est l'affaire de tous. Vos employés doivent être une solide ligne de défense contre les cyberattaques. Dans notre démonstration en direct de Fortra's Terranova Security vous discuterez des meilleures pratiques pour mettre en œuvre des programmes de formation efficaces afin de créer votre propre culture de cybersécurité.

Security Awareness Matters: Building a Cyber-Aware Organisational Culture – Fortra's Terranova Security live demo

By engaging cyber security training, you can turn your employees into a strong line of defense against cyberattacks. Join our live demo to discover Fortra's Terranova Security in-depth training courses on phishing, ransomware and more. Learn best practices on implementing effective and scalable training programs to build a cyber-aware culture.

F1 - 26 & 27 March - 14:00-16:00

De l'importance d'interconnecter des solutions de sécurité offensives - Fortra's Offensive Security

La superposition de solutions de sécurité offensives comme la gestion des vulnérabilités, les tests d'intrusion et le red teaming permet à votre équipe de protéger efficacement vos actifs critiques. Découvrez comment la suite de sécurité offensive de Fortra, incluant Cobalt Strike et Core Security, aide à identifier et à hiérarchiser les risques.

The Importance of Layering Offensive Security Solutions - Fortra's Offensive Security

Layering offensive security solutions like vulnerability management, pen testing and red teaming can empower your team to identify threats and protect your critical assets more efficiently. Learn how Fortra's Offensive Security Suite -which includes Cobalt Strike and Core Security, among others- helps organisations to find and prioritise risks.

F1 - 26 & 27 March - 11:30-15:00

Sécurisez et rationalisez vos transferts de fichiers - Fortra's GoAnywhere MFT live demo

Modernisation de votre plateforme d'échanges de fichiers, remplacement de votre solution vieillissante? GoAnywhere est la réponse à votre besoin. Dans cette démo en direct, nous vous montrerons comment GoAnywhere MFT de Fortra gère et automatise en toute sécurité le transfert de vos fichiers, en interne ou avec vos partenaires.

Secure and Streamline your File Transfers - Fortra's GoAnywhere MFT live demo

Do you need to modernise your file exchange platform or replace your legacy solution? GoAnywhere is the answer to your needs. In this live demo, we'll show you how Fortra's GoAnywhere MFT securely manages and automates the transfer of your files, internally or with your partners.

F1 26 & 27 March - 15:00-16:30

Sécurité des emails - Fortra's Digital Risk and Email Protection Suite live demo

Les emails restent le principal vecteur de menace pour les attaques des entreprises. La suite Digital Risk and Email Protection de Fortra prévient les attaques de phishing, applique un DMARC solide et protège votre marque contre les abus de courrier électronique. Rejoignez-nous pour voir Agari, Clearswift, PhishLabs et Terranova Security en action.

Comprehensive Email Security - Fortra's Digital Risk and Email Protection Suite live demo

"Email remains the leading threat vector for business attacks, causing substantial financial losses and compromised accounts. Fortra's Digital Risk and Email Protection Suite prevents phishing attacks, enforces strong DMARC, and protects your brand from email abuse. Join us to see Agari, Clearswift, PhishLabs and Terranova Security in action.

F1 - 26 & 27 March - 16:30-11:30

Github

La sécurité applicative boostée par l'IA

Nous vous attendons sur le stand GitHub pour une démo de l'AppSec boosté par l'IA: Code scanning autofix qui rend accessible la remédiation en proposant une correction dès la detection des vulnérabilité dans le code. Améliorez votre recherche de secrets grâce à la detection des secrets générique par l'IA pour identifier les secrets non structurés.

Application Security powered by AI

Pass by GitHub booth for a demo about AI-powered AppSec, including Code scanning autofix that lowers the barrier of entry for developers to fix code vulnerabilities by combining best practices and a suggested fix using LLM. Learn how to enhance your secret detection with AI-powered generic secret detection to identify unstructured secrets.

C12 - 26, 27 & 28 March

INFOBLOX

Démonstation de techniques d'attaques au travers du DNS

Démonstation de techniques d'attaques au travers du DNS : Exfiltration de données et communication Command&Control

Demo of Attack Techniques Utilizing DNS

Demo of attack techniques utilizing DNS : Data Exfiltration and Command&Control (C2) communication

A12-2 - 26,27 & 28 March - 10:00

Le DNS Detection & Response au service du SOC/CSIRT et de l'anticipation et prévention des menaces

Démonstration de la puissance du DNS Detection & Response pour la prévention des menaces, d'une CTI spécialisée sur l'infrastructure des attaquants pour détection anticipée des signaux d'attaque, la puissance de l'AI appliquée au DNS pour démultiplier l'efficacité du SOC dans la

corrélation des événements de sécurité DNS, pour l'ensemble des machines connectées de l'entreprise. 92% des malwares requêtent le DNS, la puissance de la détection DNS Detection & Response sera illustrée lors de cette démonstration.

Leveraging DNS Detection & Response by SOC/CSIRT in anticipating and preventing threats

Demo Illustrating the effectiveness of DNS Detection & Response in preventing threats, utilizing specialized CTI to detect early attack signals from attacker infrastructure, leveraging AI in DNS to enhance SOC efficiency in correlating DNS security events across all enterprise-connected devices. This demonstration will highlight how 92% of malware queries the DNS, showcasing the robust detection capabilities of DNS Detection & Response

A12-2 - 26, 27 & 28 March - 15:00

Infodas

Proudly presenting the NEW SDoT Industry Gateway.

Military-grade experience at the service of industrial sector needs!"

E8-2 - 26 March - 15:00-15:45

ISL

La sécurité en tant que processus: comment le DTS Cockpit & le CONTINOUS ASSESSEMENT contribuent à améliorer votre sécurité informatique nonobstant votre infrastructure de sécurité.

27 March - 11:30-12:15

Kudelski Security

Apéritifs Kudelski Security

Rejoignons-nous pour un verre sur notre stand C19 à partir de 16h00 le 1er et 2nd jour du Forum InCyber, sans inscription !

Apéritifs Kudelski Security

Let's meet for a drink at our booth C19 on the 1st and 2nd day of the InCyber Forum from 4:00 PM, no registration required!

C19 - 26 & 27 March - 16:00

M.G.M. SOLUTIONS

Production et sécurisation : Comment trouver le bon équilibre ?

Notre BU Cyber élabore des stratégies pour renforcer votre maturité et votre niveau de sécurisation. Assistez à une démonstration d'exploitation de vulnérabilités sur une infrastructure standard vs sécurisée. Découvrez notre BU Santé afin de vous accompagner sur le programme Care. Sensibilisez vos interlocuteurs de façon ludique et pragmatique.

Production and Security : How to strike the right balance ?

Our Cyber Business Unit devises strategies to enhance your maturity and security levels. Witness a demonstration comparing vulnerability exploitation between standard and secure infrastructures. Explore our Health BU, designed to support you with the Care program. Engage your counterparts in an enjoyable and practical manner to raise awareness.

D14 - 26, 27 & 28 March - 11:00-15:00

Microsoft Security

Maitrisez l'IA avec Microsoft

Nous vous invitons à explorer nos nouveautés en matière de cybersécurité et d'IA ainsi qu'à apprendre comment contrôler les risques de l'IA générative. Vous aurez aussi la possibilité de découvrir nos solutions en action, comme Microsoft Copilot for Security pendant toute la durée du salon.

Master AI with Microsoft

We invite you to explore our latest developments in cybersecurity and AI, and learn how to control the risks of generative AI. You'll also have the chance to see our solutions in action, such as Microsoft Copilot for Security, throughout the show.

C12 - 26, 27 & 28 March

Mipih–SIB

Hébergement HDS et Résilience : Structure publique au cœur de la sécurité, la continuité et la reprise d'activités des établissements

Le Mipih-SIB, avec ses 4 datacenters HDS (Hébergement de Données de Santé), assure la sécurité et la continuité des services des établissements de santé et des collectivités. Il propose des solutions intégrables aux stratégies d'un Plan Blanc Numérique, avec des plans de reprise et de continuité, assurant ainsi une protection des données et le maintien des opérations critiques essentielles en toute situation.

HDS Hosting and Resilience: Public structure at the heart of security, continuity, and disaster recovery for institutions.

Mipih-SIB, with its 4 proprietary data centers certified for Health Data Hosting (HDS), ensures the security and continuity of services for healthcare institutions and local communities. It offers solutions that can be integrated into the strategies of a Digital White Plan, with recovery and continuity plans, thus ensuring data protection and the maintenance of essential critical operations in any situation.

F27 - 26 March - 11:30

Sécurité et Confiance : L'excellence d'un SOC public à votre service

Le MIPIH-SIB lance son SOC managé public. Basé sur des outils éprouvés d'EDR/XDR et CTI intégrée, il assure une surveillance continue pour détecter proactivement les menaces et réduire les délais de réponse. Découvrez lors de cet atelier comment notre offre peut vous aider à renforcer votre sécurité préventive et mieux protéger votre organisation.

Security and Trust: excellence of the public SOC offering

The MIPIH-SIB is launching its Managed SOC public offering. Based on state-of-the-art EDR/XDR tools with integrated CTI, it enables continuous monitoring to preemptively detect security incidents and reduce the response times. Join our workshop to learn how our offering can help improve your preventive security and protect your organization.

F27 - 27 March - 11:30

Mitigant

Cloud Attack Emulation: Enhancing Cloud Security Operations With Threat-Informed Defense

E8-3 - 27 March - 16:00-16:45

Nano Corp.

Technological announcement: First European multi-cloud NDR

E8-7 - 26 March - 16:00-16:45

ONETRUST

Construisez votre programme de gestion des risques des tiers avec OneTrust

Découvrez comment OneTrust vous accompagne dans la mise en place d'un programme de gestion des risques tiers lors d'une démonstration live sur notre stand

Building your third-party risk management program with OneTrust

Find out how OneTrust can help you set up a third-party risk management programme during a live demonstration on our stand.

H3 - 26 March - 16:00

Gouvernance de l'IA :La solution OneTrust pour la transparence et la conformité

L'Intelligence Artificielle s'immisce partout dans le paysage personnel et professionnel. Il est essentiel pour les organisations de mettre en place une gouvernance autour des initiatives d'IA. La solution OneTrust vous permet de garantir l'éthique, la transparence et la conformité réglementaire dans le déploiement de l'intelligence artificielle au sein de vos organisations

AI Governance: OneTrust's Solution for Transparency and Compliance

Artificial Intelligence is becoming an integral part of our personal and professional lives. It is essential for organisations to put in place governance around AI initiatives. The OneTrust solution enables you to guarantee ethics, transparency and regulatory compliance in the deployment of artificial

intelligence within your organisations.

H3 - 27 March - 16:00

Breaking Barriers: Relever les défis de la gouvernance, du risque et de la conformité avec OneTrust

Le lien entre la sécurité, le risque et la conformité peut s'avérer compliquer à gérer. Découvrez comment OneTrust peut vous accompagner.

Breaking Barriers: Addressing Challenges in Security, Risk, and Compliance with OneTrust

Bridging the gap between security, risk, and compliance doesn't come without its challenges. See the top-of-mind challenges and how OneTrust can help you succeed.

H3 - 28 March - 10:15

ONETRUST x DELOITTE

Client Success Story :Gestion des risques IT & liés aux tiers avec la solution GRC de OneTrust, démontrée par Deloitte

Découvrez comment notre solution GRC gère efficacement les risques tiers et IT pour garantir la conformité et la sécurité. Notre partenaire Deloitte présentera au travers d'un déploiement client la méthodologie employée et les bénéfices observés grâce à la plateforme OneTrust

Client Success Story: Managing Third-Party and IT Risks with OneTrust's GRC Solution, Demonstrated by Deloitte

Find out how our GRC solution effectively manages third-party and IT risks to ensure compliance and security. Our partner Deloitte will be demonstrating the methodology used and the benefits observed thanks to the OneTrust platform.

H3 - 27 March - 10:15

ORANGE CYBERDEFENSE

Malicious File Detection

Découvrez sur notre stand C09 une démonstration de Malicious File Detection ! Orange Cyberdefense vous présentera une solution innovante pour minimiser le risque d'introduction de malwares dans votre réseau interne : une occasion unique d'apprendre comment optimiser la sécurité de votre infrastructure. Notre équipe d'experts sera là pour répondre à toutes vos questions et vous fournir des conseils personnalisés. Rejoignez-nous pour une expérience enrichissante et proactive dans la protection de vos systèmes informatiques.

Malicious File Detection

DESCRIPTION EN ANGLAIS (max. 350 caractères, espaces compris) : On stand C09, Orange Cyberdefense will be presenting an innovative solution "Malicious File Detection" to minimize the risk of malware introducing your internal network: a unique opportunity to learn how to optimize the security of your infrastructure. Our team of experts will be there to answer all your questions and provide you with personalized advice. Join us for a successful and proactive experience in protecting your IT systems.

C09 - 26, 27 & 28 March

QEVLAR AI

Booth demo: analyste SOC avec et sans IA

Qevlar AI présente une démo qui met en évidence la richesse qu'une Intelligence Artificielle peut apporter à l'investigation d'une alerte, par rapport à l'investigation telle qu'elle se fait aujourd'hui.

booth demo: SOC analyst vs. SOC analyst with AI

Qevlar AI presents a demo that highlights the power that an Artificial Intelligence can bring to the investigation of an alert, compared to investigation as it's done today.

F18-10 - 26 March - 16:00

Success Story MSSP : comment l'IA a aidé U.Neat à fournir des services personnalisés à grande échelle

les équipes de Qevlar AI et de U.Neat vous présentent la façon dont leur collaboration a permis aux analystes de U.Neat de gagner 30% de temps. Du temps libéré pour mieux servir les clients du MSSP.

MSSP Success Story: How AI Helped U.Neat Provide Customization at Scale

the Qevlar AI and U.Neat teams present how their collaboration has enabled U.Neat's analysts to save 30% of their time - time that has been freed up to better serve the MSSP's customers.

F18-10 - 27 March - 11:00

petit déjeuner : pAIns au SOColat - regroupement des professionnels du SOC

Les personnes travaillant dans les Security Operations Centers sont invitées au stand de Qevlar AI pour discuter des défis, des innovations et des meilleures pratiques en matière de SecOps autour d'un petit déjeuner de qualité.

breakfast: pAIns au SOColat - SOC people gathering

people working in Security Operations Centers are invited to the Qevlar AI booth to discuss challenges, innovations and best practice in SecOps around a delicious breakfast.

F18-10 - 28 March - 09:00

Prix Qevlar AI : annonce des lauréats

venez continuellement participer à un concours sur le stand de Qevlar AI, avec un cadeau inédit à la clé. Le/la vainqueur sera récompensé.e sur notre stand dans les dernières heures du salon. #moneytime

Qevlar AI awards: prize winner announcement

come and take part in a competition on Qevlar AI, with a unique prize at stake. The winner will be rewarded at our booth in the final hours of the forum. #moneytime

F18-10 - 28 March - 15:00

Qorum SecurNum

DEMOS Open Sezam

Open Sezam vous présente sa solution AuthSezam® ! Découvrez la solution souveraine qui simplifie le déploiement et l'usage de la sécurité des accès. Simple à déployer et centrée sur l'expérience utilisateur, AuthSezam est un service d'authentification forte innovant, sans mot de passe et souverain.

DEMOS Open Sezam

Open Sezam presents its AuthSezam® solution ! Discover the sovereign solution that simplifies the deployment and use of access security. Plug-and-play and focused on the user experience AuthSezam is an innovative, passwordless and sovereign strong authentication service.

F43 - 26, 27 & 28 March

ID&KYC DEMO - par Emilie Bonnefoy (Open Sezam) et Xavier Domecq (ID-Logism)

Authentification et intelligence(s) artificielle(s) : association risquée ou maitrisée pour notre sécurité ? En partant de quelques cas d'usage, nos deux intervenants vous présenteront les opportunités mais aussi les risques liés à l'introduction d'intelligences artificielles dans les systèmes d'authentification.

ID&KYC DEMO - by Emilie Bonnefoy (Open Sezam) and Xavier Domecq (ID-Logism)

Authentication and artificial intelligence: a risky or controlled combination for our security? Based on a number of use cases, our two speakers will present the opportunities and risks associated with the introduction of artificial intelligence into authentication systems.

ID & KYC Forum G2 - 27 March - 10:00

Échange avec Véronique Torner - Présidente de Numeum

Échange avec Véronique Torner, Présidente de Numeum, pour son premier passage au Forum Incyber 2024. Adhérente de Numeum, Qorum SecurNum présentera la force collective de ses TPME innovantes dans le domaine de la cybersécurité.

Q&A with Véronique Torner, President of Numeum

Q&A with Véronique Torner, President of Numeum, on her first appearance at the Incyber 2024 Forum. Qorum SecurNum, a member of Numeum, will be showcasing the collective strength of its innovative SMEs in the field of cybersecurity.

F43 - 27 March - 14:15

QUEST SOFTWARE

Apple Watch SE et Casque VR Meta Quest 3 à gagner!

Rencontrez nos experts Cyber-Resilience et Protection des Données au stand F11 et glissez votre bulletin avant le tirage au sort prévu à 13h40 pour tenter de gagner: - Une Apple Watch SE GPS + cellular, le 26 mars - Un casque VR Meta Quest 3, le 27 mars.

Apple Watch SE and Meta Quest 3 VR headset to win!

Meet our Cyber-Resilience and Data Protection experts at stand F11 and swipe your ballot before the draw scheduled for 1:40 p.m. to try to win: - An Apple Watch SE GPS + cellular, March 26 - A Meta Quest 3 VR headset, March 27.

F11 - 26 & 27 March - 13:40

Rapid7

Threat Intelligence - Renseignement sur les menaces avec ThreatCommand :

Scruter en permanence le clear deep et dark web. Identifier les menaces ciblant votre entreprise. Procédez à de la remédiation pour neutraliser le risque et réduire votre exposition sur le Web.

Threat Intelligence - Threat collection with ThreatCommand

Continuously monitor the clear deep and dark web. Identify the threats targeting your business. Carry out remediation to neutralise the risk and reduce your exposure on the web.

C21 - 26, 27 & 28 March - 10:00

Test dynamique de sécurité de vos applications (DAST)

Avec Rapid7 InsightAppSec, vérifiez les vulnérabilités de vos applications en cours d'exécution afin de garantir un niveau maximal de protection de vos applications notamment Web

Dynamic application security testing (DAST)

With Rapid7 InsightAppSec, check your running applications for vulnerabilities to ensure the highest level of protection for your web applications.

C21 - 26, 27 & 28 March - 11:00

Un SOC managé par Rapid7 clés en mains

Découvrez la nouvelle offre MTC (Managed Threat Complete) Rapid7, l'offre de SOC managé la plus complète du marché.
Elle combine un MDR avec une phase "Avant" pour la détection des risques de vulnérabilités et la Threat Intelligence, ainsi qu'une phase "Apres" pour la remédiation et l'analyse Forensics avec le produit phare Velociraptor.

A turnkey Rapid7-managed SOC

Discover Rapid7's new MTC (Managed Threat Complete) offering, the most comprehensive managed SOC offering on the market. It combines an MDR with a 'Before' phase for vulnerability risk detection and Threat Intelligence, and an 'After' phase for remediation and Forensics analysis with the flagship product Velociraptor.

C21 - 26, 27 & 28 March - 11:30

Réduisez l'impact des failles et vos vulnérabilités IT

Avec Rapid7 InsightVM, scannez votre infrastructure IT pour réduire le risque avec un outil complet et leader du marché de la Gestion de Vulnérabilités

Reduce the impact of breaches and your IT vulnerabilities

With Rapid7 InsightVM, scan your IT infrastructure to reduce risk with a comprehensive, market-leading Vulnerability Management tool"

C21 - 26, 27 & 28 March - 15:00

Défendez-vous contre les menaces même les plus complexes

Avec Rapid7 InsightIDR, détectez et prenez les mesures défensives nécessaires contre les menaces sur votre infrastructure"

Defend yourself against even the most complex threats

With Rapid7 InsightIDR, detect and take the necessary defensive measures against threats to your infrastructure"

C21 - 26, 27 & 28 March - 16:00

RCDevs Security SA

YumiSign - E-signature

Découvrez la signature électronique avec RCDevs e-Signature : fluide, sécurisée et efficace qui révolutionne la façon dont vous signez vos documents. Avec un compte ou non, vous pouvez signer électroniquement où que vous soyez, à tout moment, sur n'importe quel appareil. - accélérez votre flux de travail dès aujourd'hui !

YumiSign - E-signature

Discover electronic signature with RCDevs e-Signature: a smooth, secure, and efficient process that revolutionizes how you sign your documents. With or without an account, you can electronically sign wherever you are, at any time, on any device. Accelerate your workflow today!

F9-8 - 26 March - 14:00

MFA-IAM avec OpenOTP Security Suite

Découvrez l'authentification multi-facteurs (MFA), la gestion des identités et des accès (IAM), le SSO et le contrôle d'accès réseau (NAC) avec RCDevs OpenOTP Security Suite. Notre solution garantit un accès sécurisé à votre réseau et à vos applications, offrant des options d'authentification flexibles et une gestion efficace des identités utilisateur.

MFA-IAM with OpenOTP Security Suite

Discover Multi-Factor Authentication (MFA), Identity and Access Management (IAM), Single Sign-On (SSO), and Network Access Control (NAC) with RCDevs OpenOTP Security Suite. Our solution guarantees secure access to your network and applications, offering flexible authentication options and efficient user identity management.

F9-8 - 27 March - 14:00

KYC avec YumiPass CheckID

Découvrez le KYC simplifié avec YumiPass CheckID. Notre solution garantit la conformité réglementaire (RGPD) tout en minimisant les frictions pour les utilisateurs. CheckID vérifie de manière sécurisée les identités, partageant uniquement les informations nécessaires pour renforcer la confiance et atténuer les risques.

KYC with YumiPass CheckID

Experience streamlined KYC compliance with YumiPass CheckID. Our solution simplifies identity verification, ensuring regulatory compliance (i.e. GDPR) while minimizing user friction. YumiPass CheckID securely verifies identities, requesting and sharing only necessary information to build trust and mitigate risk.

F9-8 - 28 March - 14:00

Red Alert Labs

CyberPass: Transforming Cybersecurity Compliance into Competitive Advantage for Product Manufacturers

E8-1 - 26 March - 14:00-14:45

Rsecure

DEMO : EGIDE, cybermonitoring simple et accessible

Venez découvrir la solution de cybermonitoring qui vous accompagne dans la surveillance de votre infrastructure informatique, et accessible à toutes entreprises ! Notre atout ? Une interface, un outil, un homme. Démonstration live sur demande.

Demo: EGIDE, simple and accessible cybermonitoring

Come and discover the cybermonitoring solution that helps you monitor your IT infrastructure, and is accessible to all businesses! Our advantage? One interface, one tool, one person. Live demonstration on request.

F09-11 - 26, 27 & 28 March - 9:00-18:30

Cyber-tombola !

RDV sur notre stand F9-11 pour tenter de remporter un laptop Microsoft, ou l'un de nos nombreux lots de consolation !

Cyber-tombola !

Visit us on stand F9-11 for your chance to win a Microsoft laptop, or one of our many consolation prizes!

F09-11 - 26, 27 & 28 March - 17:30

SECKIOT

Démonstration de cartographie & de détection d'intrusion des environnements industriels

De la cartographie cyber de vos systèmes d'information industriels à leur mise sous surveillance en temps réel, venez découvrir nos outils, nos méthodes et notre philosophie. Nous vous invitons à venir tester les capacités de notre solution française autour de cas d'usage représentatifs de vos environnements industriels.

Map and intrusion detection demonstration of industrial environments.

From Cyber Map of your industrial information systems to real-time monitoring, come and discover our tools, methods and philosophy. We invite you to come and test the capabilities of our French solution based on use cases representative of your industrial environments.

E1-9 - 26, 27 & 28 March

SecurityScorecard

Bien plus que du scoring : Gérer la surface d'attaque liée aux tiers

Souhaitez-vous optimiser et automatiser votre programme de gestion des risques pour l'ensemble de votre écosystème (tiers, partenaires, M&A...) ? Avec des cas d'usage à l'appui, découvrez une approche globale pour la cybersécurité : monitoring de vos tiers, analyse de votre propre surface d'attaque, et bien plus encore!

Beyond the Scoring: How to Manage Your Third- and Fourth-Party Attack Surface

Are you looking to mature your third-party risk management program? Find out how incorporating threat intelligence helps uncover true risk and threat across your vendor ecosystem. Through a customer use case, we will demonstrate how you can combine cybersecurity ratings and threat intelligence to prevent your business from harm.

D12 - 27 March - 15:15-15:45

SHIRUDO – SOKIEN

Shirudo – Conseil & solutions de sensibilisation cybersécurité

Venez tester nos solutions : Shirudo Serious Game : Alternative au e-learning, une approche 360° du risque cyber pour les utilisateurs non spécialistes Shirudo Phishing Simulation : Plateforme de faux phishing ergonomique incluant un catalogue de campagnes, un bouton de signalement et un suivi en temps réel des interactions

Shirudo - Consulting & cybersecurity awareness solutions

Visit us to try out our solutions: Shirudo Serious Game: 360° cyber-risk awareness for non-specialist users, as an alternative to e-learning. Shirudo Phishing Simulation: Ergonomic fake phishing platform with multilingual catalog, notification button and real-time dashboard.

G10 - 26, 27 & 28 March

SPIE ICS

Quelles sont les protections offertes par les architectures SASE ?

Les services cloud font désormais partie des infrastructures IT dans toutes les organisations. Ces changements ont augmenté de façon importante l'exposition aux cyberattaques, étant donné la possibilité d'accéder aux ressources cloud en toutes circonstances. Le modèle SASE offre plusieurs protections. Venez découvrir les éléments clés !

What protection is offered by SASE architectures?

Hybrid working combined with the use of Cloud is part of every day life for many organisations. This driver is added by regulatory requirements which are becoming more stringent with the arrival of NIS 2. This global situation requires us to consolidate our cybersecurity governance and to adopt an unified security approach with a SASE model. Visit us!

F15 - 26, 27 & 28 March

STORMSHIELD

Cocktail sur le stand

A13 - 27 March - 16:00

Attaque industrielle

Simulation des conséquences d'une télémaintenance non maîtrisée

Industrial attack

Simulation of the consequences of uncontrolled remote maintenance

A13 - 26, 27 & 28 March

Stormshield XDR

Mise en œuvre d'une infrastructure réseau plus opérationnelle et maîtrisée

Stormshield XDR

Implementation of an operational and controlled network infrastructure

A13 - 26, 27 & 28 March

SES Evolution

Techniques de protection et de remédiation face aux ransomwares

SES Evolution

Protection and remediation techniques against ransomware

A13 - 26, 27 & 28 March

SDS for Google Workspace et Office 365

Chiffrement intégré et transparent des données

SDS for Google Workspace and Office 365

Integrated and transparent data encryption

A13 - 26, 27 & 28 March

StrangeBee

TheHive 5, the Collaborative Case Management Platform

Découvrez TheHive, la plateforme de gestion collaborative des incidents pour les équipes SOC, CERT et CSIRT. Dans cette démo, apprenez à gagner une visibilité complète des incidents, ainsi qu'à automatiser les réponses, tout comme personnaliser sans limites vos process de travail ou encore collaborer efficacement avec d'autres équipes.

TheHive 5, the Collaborative Case Management Platform

Discover TheHive – the Collaborative Case Management Platform designed for SOC, CERT, and CSIRT teams worldwide. In this demo, you will learn how to customize it extensively, gain complete visibility of all incidents, automate responses, and collaborate efficiently for faster resolutions.

D47 - 27 March - 15:00

SUSE

Démo Sécurité Kubernetes - NeuVector

Découvrez la meilleure approche de sécurité pour votre Kubernetes et autres charges de travail conteneurisées. Le tout avec beaucoup moins de contraintes que vous ne l'imaginez !

Kubernetes Security Demo - NeuVector

Discover the best security approach for your Kubernetes and other containerized workloads. All with far less burden than you would imagine!

D42 - 26, 27 & 28 March

Démo SUSE Liberty Linux

Prolongez le support de vos distributions Linux d'entreprise sans migration, tout en maintenant les compatibilités et en simplifiant la gestion future.

Demo SUSE Liberty Linux

Extend support for your enterprise Linux distributions without migration, while maintaining compatibility and with simplified future management.

D42 - 26, 27 & 28 March

Démo SUSE Manager

Gérez, sécurisez et maintenez l'ensemble de vos distributions Linux à partir d'une seule console.

Demo SUSE Manager

Manage, secure and maintain your entire mixed Linux environment — at the core, on the edge or in the cloud - from a single console.

D42 - 26, 27 & 28 March

TRUSTFULL

Comment lutter contre les fraudes émergentes à l'ouverture de compte grace à l'OSINT ?

comment proteger la fraude à l'onboarding grace à l'osint et les signaux digitaux ?

How to fight emerging account opening fraud with OSINT?

How to use our digital risk intelligence platform with Osint to prevent fraud at onboarding?

G2-3 - ID & KYC forum - 26, 27 & 28 March - 10:00-16:00

UNIVERSITE DE LORRAINE

Des formations et une recherche de pointe en cybersécurité

- Formation pluridisciplinaire BAC+3 à BAC+8 (BUT, L, M, diplôme d'ingénieur...)
- 1 300 étudiant·es inscrit·es dans un parcours spécialisé ou non à la cybersécurité
- Potentiel de 60 000 étudiant·es grâce au module de sensibilisation à la cybersécurité
- Recherche, partenariats et projets collaboratifs (DefMal, Rewire...)
- Territoire engagé : exercice de cyber-guerre à grande échelle Cyber Humanum Est, et structuration en cours de l'écosystème cybersécurité (acteurs publics et privés)

Trainings and cutting-edge research in cybersecurity

- *Interdisciplinary learnings from BAC+3 to BAC+8 (B, M, engineering degree...)*
- *1,300 students trained in a specialized or non-specialized cybersecurity pathway*
- *Potential of 60,000 students thanks to cybersecurity awareness module*
- *Research, partnerships and collaborative projects (DefMal, Rewire...)*
- *An involved territory: large-scale cyber wargame Cyber Humanum Est, and ongoing structuring of the cybersecurity ecosystem (public and private players)*

D18 - 26 March - 14:15

VIRTUAL BROWSER

Comment protéger votre navigation internet grâce à la technologie RBI ?

Venez tester VirtualBrowser, une solution pionnière de Remote Browser Isolation qui sécurise les postes et applications sensibles de vos utilisateurs en isolant physiquement les accès à risques de manière fluide et transparente, et ce depuis votre navigateur habituel.

How to protect your Internet browsing with RBI technology?

Come and test VirtualBrowser, a pioneering Remote Browser Isolation solution that secures your users' sensitive workstations and applications by physically isolating high-risk access in a seamless and transparent way, right from your usual browser.

D35 - 26, 27 &28 March - 11:00-16:00

Wavestone

Venez découvrir sur notre stand nos maquettes sur l'IA et la cybersécurité !

1/ Lassé de passer des heures à chercher dans vos politiques de sécurité ? Découvrez CISO GPT, le chatbot qui répond aux questions de sécurité à partir de votre corpus documentaire cyber !
2/ Comment attaquer une IA ? On vous montre comment détourner un algorithme de reconnaissance faciale, et comment vous protéger contre ce type d'attaque !

Come and see our AI and cybersecurity demonstrators on our stand!

*1/ Tired of spending hours searching through your security policies? Discover CISO GPT, the chatbot that answers security questions based on your security documentation!
2/ How to attack an AI? We can show you! In our demonstration, you hijack a facial recognition algorithm, and we explain how to protect yourself against this type of attack.*

A3 - 26, 27 & 28 March

YesWeHack

Live Bug Bounty

Rendez-vous sur le stand E12 pour le Live Bug Bounty organisé par YesWeHack : une occasion unique pour les passionnés de cybersécurité et les hackers éthiques de se réunir, d'apprendre, et de passer un excellent moment ! La cible (entreprise partenaire et périmètre) sera révélée en début d'événement. Tous les visiteurs du salon peuvent participer.

Live Bug Bounty

YesWeHack will hold a Live Bug Bounty event at booth E12: a unique opportunity for cybersecurity enthusiasts and ethical hackers to come together, learn, and have a great time! The target (partner company and scope) will be revealed at the beginning of the event. All InCyber Forum attendees can participate, so don't miss out!

E12 - 26, 27 March - 16:00

CYBER LEADERS

THE STRATEGIC CYBERSECURITY REVIEW

BUY YOUR MAGAZINE ON STAND N°B38

Partners

Partenaires

Major Partner

HEXATRUST

CLOUD CONFIDENCE & CYBERSECURITY

Diamond Partners

CMiB "Cyber Made in Belgium" — A voice for the Belgian cyber security industry

.AGORIA

Auvergne-Rhône-Alpes

Cyberdefense

SentinelOne

Platinum Partners

Avantdecliquer.com — L'humain au cœur de la cybersécurité

BRETAGNE — LA CYBERSÉCURITÉ A SON TERRITOIRE

CYBERSECURITY LUXEMBOURG

DOCAPOSTE

EGERIE — INTEGRATED CYBERRISK MANAGEMENT

EXCLUSIVE NETWORKS

GOBIERNO DE ESPAÑA — MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA

incibe_ — SPANISH NATIONAL CYBERSECURITY INSTITUTE

NCC-ES — SPAIN CYBERSECURITY COORDINATION CENTRE

TEHTRIS — FACE THE UNPREDICTABLE

THALES — Building a future we can all trust

TREND MICRO

Région Nouvelle-Aquitaine

Partenaires

Gold Partners

Partners

Partenaires

Silver Partners

accenture
ACKnowledge
afnor GROUPE
AKERVA
ALL4TEC SAFE & SECURE
allentis
almond
ANTEMETA
APPROACH CYBER
ASTRAN
Atheo
AURAIT
AXBX
axians
beys
BigID
Bitdefender
BITSIGHT
box
brain.
AGORIA BSDI
BUREAU VERITAS
CENTRE FOR CYBER SECURITY BELGIUM
CHECK POINT
CLOUDFLARE
conscio
Cresco. Cybersecurity
CSC
CybelAngel
CYBER SECURITY COALITION
CYBER 4 INDUSTRY
cybereason
cyberprotect
CYBER WALL
cyberwatch
DARKTRACE
dastra
Delinea
devensys CYBERSECURITY
DIATEAM
DIGITAL LEAGUE
elastic
EPIEOS
ERIUM
eset
ETN
European Commission
EVERTRUST
fair trust
FORTINET
FORTRA
framatome
GATEWATCHER
GICAT
GitGuardian
Hewlett Packard Enterprise
howest university of applied sciences
hp
HS2 Hervé Schauer Sécurité
Ilex. IAM Platform inetum.
INQUEST
Jalios
kaspersky
KEYFACTOR
LACEWORK
LOCKSELF
LOGPOINT
Lookout
MAKE IT SAFE
METSYS
Microsoft
nameshield
néowoft
NEOPRIME
netwrix
nomios être là
NOZOMI NETWORKS
THE NRB GROUP

Partenaires

Silver Partners


Partners

Partenaires

Bronze Partners

Partenaires

Bronze Partners

Partners

Partenaires

Bronze Partner

Partners

Partenaires

Bronze Partner



Partners

Partenaires

Innovation

ARSEN

Nevermind

Ballpoint

Chimere

Confidencial

Cyber Booster

Cybi

CYGO

Lailaps

EYAKO
SECURITY MADE SIMPLE

Giskard

Opera Cyber
Security Consulting

KERYS

P4S

Patrowl

Qevlar AI

CAPE

Scovery

SEMICUBE

soc partner

zygon

Opale

Bradley & Rollins

bsi.

Cogitanda
Cyber is us.

cyna

Portwell

InterCloud

ENEA
Qosmos

Partners

Partenaires

Hiring

BNP PARIBAS

MAIF

Academic and research

ASTON ECOLE IT

CESI ÉCOLE D'INGÉNIEURS

CSB School

diiage

DataScientest

esaip La Salle ÉCOLE D'INGÉNIEURS

quest EDUCATION GROUP

utt UNIVERSITÉ DE TECHNOLOGIE TROYES

ynov CAMPUS

cdefi Conférence des Directeurs des Écoles Françaises d'Ingénieurs

cea

cnrs

Inria

Institut Mines-Télécom Business School

PROGRAMME DE transfert AU campus cyber

Media

Alliancy LE MAG NUMÉRIQUE ET BUSINESS

Capital

ChannelNEWS

DÉCIDEURS MAGAZINE

archimag

Informatique News

IT for Business

REVUE POLITIQUE ET PARLEMENTAIRE

SMARTDSI

ANEWS SECURITE

Global Security Mag THE LOGICAL & PHYSICAL SECURITY MAGAZINE

iTPro.fr

L'INFORMATICIEN

B SMART

RÉGIONS MAGAZINE

S&D Sécurité & Défense MAGAZINE

Finyear

CYBERUN CYBERSECURITY STRATEGIES

Partners

Partenaires

CF CYBERSECURITY FOR INDUSTRY

txOne networks · Schneider Electric · ARMIS · AURA iT · NOZOMI NETWORKS

framatome · SECKIOT · NTT DATA · Rexel · DATIVE

DELL Technologies · Rockwell Automation · Altospam · MOXA

INEO UNE MARQUE DE EQUANS · Upstream · FORESCOUT · wallix · CYBER ICS

D&KYC FORUM

accenture · adneo · Archipels · beys The wise side of data

Certigna · FEITIAN WE BUILD SECURITY · keepit · DOCAPOSTE

okta · QORUM Secur'Num · RADIANT LOGIC · SECURE IDENTITY ALLIANCE

trustfull · Universign by Signaturit Group · yousign · WORLDLINE

W3S WEB3 SECURITY SUMMIT

Allfeat. · AMLBot · BLOBB.IO · bubblemaps

Chainalysis · Fireblocks · KALICERTIF BUILT ON KALICHAIN · SET IN STONE

Partners

Partenaires

TRUST & SAFETY FORUM

GIFCT Global Internet Forum to Counter Terrorism

yubo

aws

TREMAU

BLUEBEAR

WEBKONTROL You create it. We protect it.

Google

checkstep

sightengine

JOURNÉE OSINT

EPIEOS

BREACHUNT

InteLFe

ELEPHANTASTIC

trustfull

PREDICTA LAB

TOA OSINT ACADEMY

ANOZR WAY PEOPLE-CENTRIC CYBER PROTECTION

EC2

hello lille

LE FIGARO étudiant

Lexfo

MEL MÉTROPOLE EUROPÉENNE DE LILLE

MISC

RootMe PRO

runningman

zqsd /PROD

Exhibitors List

Liste des exposants

#IWAS D56-7
2SB D21
3M D51

A

AAIS F44-6
ACCEIS F25
ACCENTURE F4
ACCESS INFORMER SECURITY SOLUTIONS G3-5
ACELYS SERVICES NUMÉRIQUES C7-5
ACESI G13
ACG CYBERSECURITY D11-7
ACKNOWLEDGE A5
ACRONIS B33-3
ADACIS B12
ADAPTIVE SHIELD B36
ADUNEO G2-4
ADVENS C1
AFNOR B24
AGORIA H1
AIOTRUST F44-1
AIRBUS C10
AISI A4-1
AKERVA B7
AKTEA B12
ALCYCONIE F24
ALEPH NETWORKS D11-5
ALGOSECURE A4-27
ALIGNER E24-7
ALL4TEC D2
ALLENTIS D7
ALLFEAT LABS SALLE 0.4
ALLISTIC C8-23
ALMOND & AMOSSYS F38
ALSATIS C7-9
ALTIJ C7-10
ALTOSPAM E1-3
AMLBOT SALLE 0.4
ANOZR WAY F31
ANSSI D6-1
ANTEMETA B1
ANTICIPA TECHNOPOLE LANNION F23-14
APIXIT A20
APPROACH CYBER H1-1
AQUA RAY E10
AQUASTAR CONSULTING C8-5
ARAMYS C8-22
ARC DATA SHIELD F18-30
ARCAD SOFTWARE A4-29
ARCHIPELS A9-1
ARCSI D56-18
ARMIS & AURA-IT E1-7
ARROW B21
ARSEN F18-32
ASSOCIATION NATIONALE D'AIDE AUX CYBERVICTIMES D56-8
ASSOVICA D56-9
ASTON G34-4
ASTRAN F39-12
ATEMPO A4-20
ATHEO INGENIERIE F42
AUCAE F39-4
AUTONYM PTE LTD F18-28
AUVERGNE-RHÔNE-ALPES ENTREPRISES F44
AVANT DE CLIQUER D27
AXBX E17
AXIANS A4-6

B

BALLPOINT F18-29
BARRACUDA B33-2
BE YS G2-7
BEARINGPOINT H38
BELLEDONNE COMMUNICATIONS E19
BEYONDTRUST F30
BIGID E25
BITDEFENDER B20
BITSIGHT A12-1
BITSIGHT TECHNOLOGIES F14
BLACKBERRY CYBERSECURITY H30-1
BLANCCO D1
BLOBB.IO SALLE 0.4
BLUEBEAR LES SALLE 3.7
BLUEFINCH F19-1
BLUESECURE C25
BNP PARIBAS G34-12
BOARD OF CYBER B26
BOX FRANCE E26
BRADLEY & ROLLINS B30 - OPALE
BRAIN SECURITY F39-5
BREIZH CYBER F23-15
BREST METROPOLE F23-17
BRETAGNE DÉVELOPPEMENT INNOVATION (BDI) F23
BRIGHTWAY D49
BSDI - BELGIAN SECURITY DEFENCE INDUSTRY H1
BSI GROUP B30 - OPALE
BUBBLEMAPS SALLE 0.4
BUREAU VERITAS D17
BUSTER AI D23-3
BZHUNT EXPLOITATION F23-2

C

C-CURE SYSTEMS F44-2
CAMPUS CYBER D6-2
CAMPUS RÉGION DU NUMÉRIQUE F44
CAPE BY AQUITAINE SCIENCE TRANSFERT F18-16
CAPGEMINI C3
CCB - CENTER CYBERSECURITY BELGIUM H1-2
CCI SEINE-ET-MARNE D11-3
CDEFI-FU D57-2
CDFEQ D56-16
CEA D30
CEA D57-1
CEFCYS D56-10
CERT AVIATION FRANCE D56-4
CERTIGNA GROUPE TESSI G2-1
CESI G34-2
CHAINALYSIS SALLE 0.4
CHAPSVISION CYBERGOV D26
CHECK POINT D22
CHECKMARX E4
CHEOPS TECHNOLOGIE H31
CHIMÈRE F18-8
CISCO F21
CISCO H30-5
CITALID C18
CITC EURARFID C8-11
CLEAFY E21
CLESSE F44-4
CLEVER CLOUD G46
CLOUDFENCE F18-18
CLOUDFLARE G4
CLUB DE LA SÉCURITÉ NUMÉRIQUE DES COLLECTIVITÉS D56-19
CLUB EBIOS D56-17
CLUSIF D5
CLUSIR C8-19
CLUSTER EDEN F44
CNIL D3
CNPP F16
CNRS D57-3
COGITANDA B30 - OPALE
COMPUTACENTER F37
CONFIDENCIAL.IO F18-31
CONSCIO TECHNOLOGIES A4-13
CORELIGHT D21-1
CRESCO CYBERSECURITY H1-3
CRIS RESEAUX A10
CRISP THINKING GROUP LIMITED SALLE 3.7
CROWDSEC B18
CROWDSTRIKE G1
CRYPTOMATHIC G9
CRYPTONEXT A4-21
CSB SCHOOL G34-8
CSC A2
CSIRT C8-11
CSIRT BOURGOGNE-FRANCHE-COMTÉ D56-5
CUCDB/DIIAGE G34-9
CUSTOCY C7-4
CYBELANGEL A6
CYBER DETECT A4-22
CYBER GURU D53
CYBER ICS E1-11
CYBER SECURITY COALITION H1-4
CYBER4INDUSTRIES H1-5
CYBERBOOSTER F18-20
CYBERDISE G3-5
CYBEREASON B19
CYBERESPONSE F18-2
CYBERLIFT E18
CYBERMALVEILLANCE.GOUV.FR D6-3
CYBERPROTECT B13
CYBERSECURITY LUXEMBOURG F9
CYBERVADIS F34
CYBERWALL H1-6
CYBERWATCH A4-15
CYBI F18-21
CYBLEX CONSULTING F18-25
CYFERALL F9-9
CYGO-ENTREPRENEURS F18-19
CYLLENE H16
CYNA-IT B30 - OPALE

D

DARKOWL G41
DARKTRACE B16
DASPREN F23-9
DASTRA F39-6
DATABACK C11-2
DATADOME E6
DATAPROTECT H32
DATASCIENTEST G34-7
DEEPDEF F18-24
DEFANTS F23-4
DELETEC E23
DELINEA C23
DELL TECHNOLOGIES E1-18
DEVENSYS A4-9
DIATEAM F20
DIGITAL LEAGUE F44
DMARC ADVISOR F19-2
DNRED G21
DOCAPOSTE G24
DOMAINTOOLS G19
DUOKEY G2-9
DUST MOBILE B34
DYNATRUST C8-1

E

E-ENFANCE D56-11
EASYDESK D16
EBRAND F9-5
EBRC F39-2
EUROPEAN CHAMPIONS ALLIANCE E8
ECLECTIQ F19-3
ÉCOLE 2600 D50
ECSO E24-2
EDIH F23-3
EGERIE A8
EHO.LINK F32
ELASTIC SEARCH D25
ELYSIUM SECURITY F44-7
ENCLAIVE E8-4
ENI EDITIONS H28
EPITA G16
EPITECH C8-8
ERIUM D19
ESAIP G34-10
ESCAPE TECHNOLOGIES B12
ESET C6
ESIA F35
ESIEA D38
ETIX EVERYWHERE G14
ETN (BELDEN) D9
EU-LISA E24-4
EUROPEAN COMMISSION E24-1
EUROPEAN PORTWELL TECHNOLOGY B30 - OPALE
EUROPOL E24-5
EUROPOL INNOVATION LAB E24-10
EVERBRIDGE E3
EVERTRUST A4-16
EVIDEN INTERNATIONAL FRANCE B2
EWC E24-6
EXAION D58
EXALENS F19-4
EXAMIN F9-3
EXAPROBE B8
EXCELLIUM F9-6
EXCLUSIVE NETWORKS A12
EXELERYS F17-1
EXEO E8-5
EXER C8-4
EXOSCALE G3-6
EY D4
EYAKO F18-6

F

F24 A4-19
F5 H2
FAIRTRUST F39-11
FÉDÉRATION FRANÇAISE DE LA CYBERSÉCURITÉ D56-20
FEEDER D48
FEITIAN TECHNOLOGIES G2-12
FILIGRAN G6
FIREBLOCKS SALLE 0.4
FOLIATEAM F23-1
FORCEPOINT B21-1
FORECOMM D11-1
FORESCOUT E1-5
FORMIND G8
FORTINET A14
FORTRA F1
FRAMATOME E1-8
FRANCE CYBER MARITIME D56-21
FRANCE CYBER MARITIME (M-CERT) D56-6
FUZZINGLABS F18-3

G

GAME PARTNERS B12
GATEWATCHER C22
GICAT D23-1
GIGAMON A12-6
GISKARD.AI F18-9
GITGUARDIAN B28
GITHUB C12-2
GLIMPS A16
GLOOMY CLOUDS C8-18
GOOGLE CLOUD F5
GOTTAPHISH B12
GRT GAZ E1-21
GUARDICORE D21-2

H

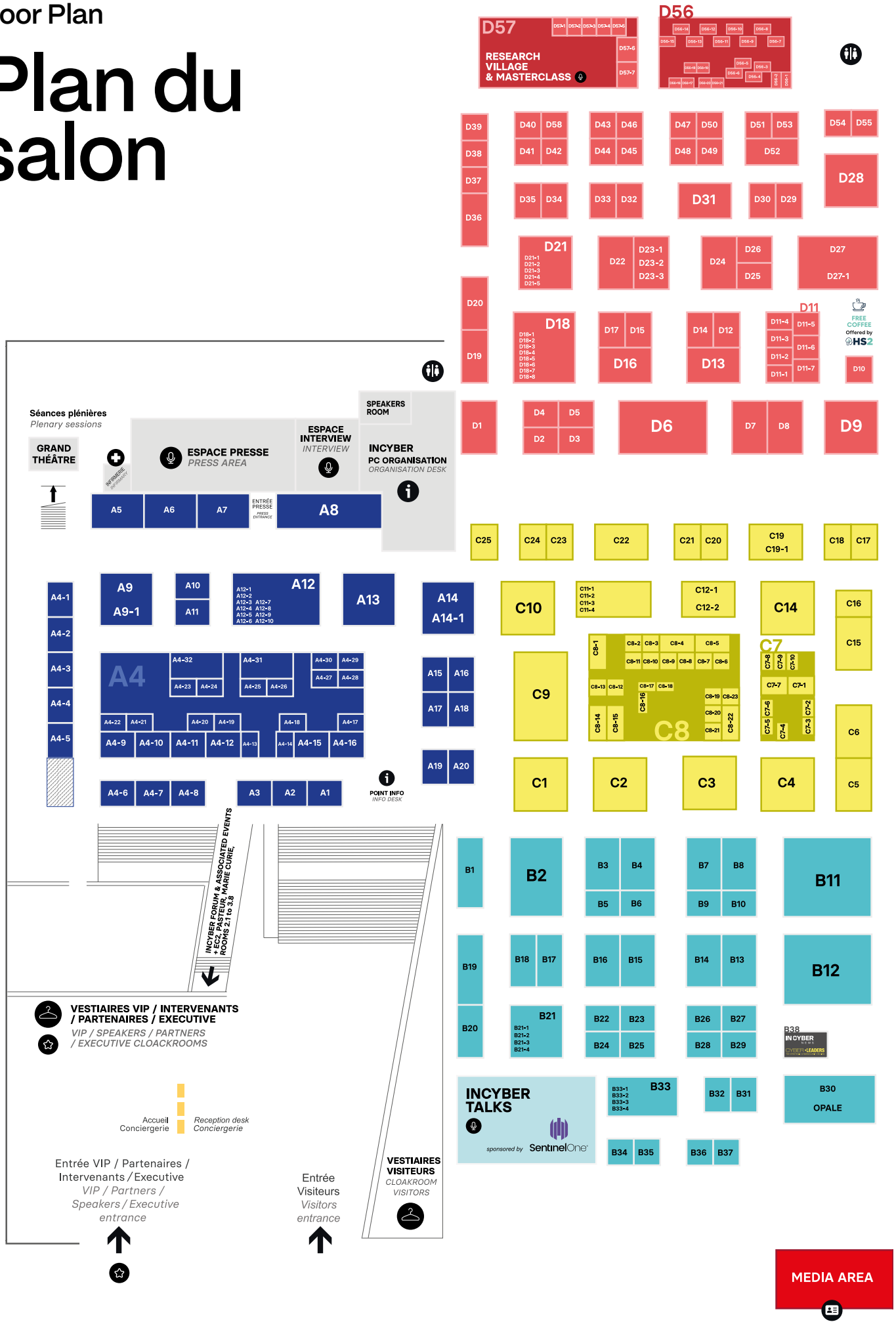
HADRIAN SECURITY F19-5
HAMYNA C8-21
HARFANGLAB A18
HEADMIND PARTNERS B27
HEXANET D18-1
HEXATRUST A4/F39
HID GLOBAL A12-10
HOGO H21
HOLISEUM A4-17
HOWEST H1-7
HP FRANCE F17
HEWLETT-PACKARD ENTERPRISE F3
HS2 D55
HUBITECH G7

I

I-TRACING F29
IBM H30-2
IC-CONSULT H11
ILEX IAM PLATFORM A4-23
IMT NORD EUROPE C8-9
IN GROUPE A9
INCIBE G23
INEO EQUANS E1-12
INFINIGATE B33
INFOBLOX A12-2
INFODAS E8-2
INQUEST F39-10
INRIA D57-5
INSTITUT MINES TELECOM D57-4
INTEL471 G11
INTERCERT FRANCE D56-1
INTERCLOUD B30 - OPALE
INTERSEC GROUP H7
INTUITEM H13
IONOS G40
IPARCUS C8-13
IRM360 F19-6
IS DECISIONS B12
ISIT C7-6
ISL E8-6
ISSA FRANCE D56-13

Floor Plan

Plan du salon




INCYBER DEMOS
sponsored by
TREND
E24
E24-1
EU PAVILION
EU DEMOS
E13
E14
E17
E25
E26
E18
E19
E20
E12
E9
E8
E8-1
E8-2
E7
E4
E2
CISO LOUNGE
by CESIN
SALON VIP
VIP LOUNGE
E1
E1-26
E1-22
E1-23
CFI DEMOS
E1-18
E1-19
MEETING AREA #3
CYBERSECURITY FOR INDUSTRY
E1-1
E1-2
E1-5
E1-6
E1-3
E1-4
E1-7
E1-9
E1-8
E1-11
E1-12
E1-14
F1
F4
F2
F3
F5
F8
F6
F7
F9-1
F9
F9-5
F9-6
F9-7
F9-8
F10
F13
F11
F12
F14
F15
F17
F16
H1
H2
H3
H4
MEETING AREA #1
H7
H8
F23
F23-1
F23-2
F23-3
F23-4
F20
F21
F19
F18
INNOVATION VILLAGE
STARTUP PITCHES
EVIDEN
H18
H15
H17
H16
H13
H12
H14
H11
MEETING AREA #2
hacking LAB
H19
H20
H21
H22
H23
H24
H28
H27
H29
H26
H25
F24
F27
F25
F26
F28
F31
F29
F30
F32
F35
F33
F34
F36
F37
F38
F44
F43
F42
F41
F40
F39
H30
H31
H34
H32
H33
H35
H38
H36
H37
MEETING AREA #3
H40
G1
G2-1
G2-3
G2-4
G2
ID& KYC FORUM
G2-12
G2-13
G2-11
G2-10
G3
G4
G5
G6
G7
G8
G9
G10
G13
G11
G12
G14
G45
G46
INCYBER BAR
G24
G2-6
G2-7
ID&KYC FORUM DEMOS
sponsored by
DOCAPOSTE
G2-9
MEETING AREA #4
G23
G22
G19
G21
G18
G15
G17
G16
G25
G26
G27
G28
Furet du nord
FURET DU NORD LIBRARY
G42
G41
G40
G39
G34
VILLAGE TALENTS
PLATEAU TV
EC2
W32
ROOMS
0.4 & 0.5+0.6
TERRASSE
TERRACE
TV SHOW
Executive Restaurant
sponsored by imperva
& FOODCOURT

INCYBER FORUM

NORTH AMERICA

29–30
OCT. 2024

MONTREAL
QC, CANADA

EUROPE

1–3
APRIL 2025

LILLE GRAND PALAIS
FRANCE

AMERICAS

17–18
JUNE 2025

SAN ANTONIO
TEXAS, USA

Where to eat?

Où déjeuner ?

TRICYCLES

NON-STOP
TRIPORTEURS ITINÉRANTS
ROVING TRICYCLE

Toutes les boissons offertes sur les triporteurs le sont en échange du scan de votre badge.

All drinks on the tricycles are offered in exchange for a scan of your badge.

FREE COFFEE

NON-STOP
STAND DE CAFÉ GRATUIT
FREE COFFEE BOOTH
D ZONE

Pause café offerte par HS2 (zone D) en échange du scan de votre badge.

Coffee break offered by HS2 (D Zone) and in exchange for a scan of your badge.

SNACKING

(D HALL & LEVEL 3)

Des produits de snacking et boissons sont également proposés sur l'espace BAR (hall G) et devant l'espace Le Square (niveau 3)

Snacks and drinks are available in the BAR area (hall G) and in front of Le Square (level 3)

CLICK & COLLECT

Un service de click & collect est à votre disposition pour commander votre repas à venir récupérer au niveau de l'espace restauration sur le Parvis à l'horaire que vous choisissez. **Renseignez-vous au point Info ou au PC orga InCyber.**

A click & collect service is at your disposal to order your meal and collect it from the catering area on the Parvis at a time of your choice. ***Find out more at the Info point or at the InCyber PC orga.***

FOOD

SUR LE PARVIS DU GRAND PALAIS
ON THE FORECOURT OF THE GRAND PALAIS

Un espace InCyber food court avec des corners et des food trucks proposant une offre de restauration rapide variée. Le restaurant Executive ouvert aux badges Executive de 12h00 à 14h30.

N'hésitez pas à venir déjeuner à des horaires décalés pour éviter l'attente !

An InCyber food court area with corners and food trucks offering a varied range of fast food. The Executive restaurant is open to Executive badges from 12:00 to 14:30.

Don't hesitate to come and have lunch at staggered times to avoid waiting!

Practical Infos

Infos Pratiques

IMPRIMEZ VOTRE BADGE ET N'OUBLIEZ PAS VOTRE CARTE D'IDENTITÉ.

Des pochettes et portes badges sont disponibles à l'entrée du salon.

PRINT YOUR BADGE AND DON'T FORGET YOUR IDENTITY CARD

Pockets and badge holders will be available at the entrance to the show.

UN VESTIAIRE ET UNE BAGAGERIE SÉCURISÉS SERONT À VOTRE DISPOSITION.

un service de livraison de votre bagage directement dans votre hôtel est disponible à l'entrée de Grand Palais près du vestiaire de 08h00 à 17h00.

A SECURE CLOAKROOM AND LUGGAGE ROOM WILL BE AT YOUR DISPOSAL

A bags delivery service directly to your hotel is available at the entrance to the Grand Palais near the cloakroom from 8 a.m. to 5 p.m.

VOUS POUVEZ PARTICIPER AUX SESSIONS QUE VOUS SOUHAITEZ SANS INSCRIPTION PRÉALABLE.

Nous vous conseillons de vous présenter 15 minutes avant le début devant la salle concernée.

YOU CAN PARTICIPATE IN THE SESSIONS YOU WANT WITHOUT PRIOR REGISTRATION

We advise you to arrive 15 minutes before the start in front of the room concerned.

PARTICIPEZ À LA INCYBER NIGHT !

Vous cherchez un endroit festif pour vous retrouver après votre dîner ? Ne cherchez plus ! Le Forum InCyber lance la 1ère InCyber Night, la soirée ouverte à tous les "couche-tard" du FIC le **Mercredi 27 mars** 2024 au Bazaar St So (292 Rue Camille Guérin, 59800 Lille - Métro Grand Palais / Mairie de Lille) **de 22H00 à 02H30.**

Tarif ? 30 euros - Entrée + 2 tickets boisson

Réservation obligatoire sur : https://europe.forum-incyber.com/incyber-night/

JOIN US FOR INCYBER NIGHT!

Looking for a festive place to meet up after dinner? Look no further! The InCyber Forum is launching the 1st InCyber Night, a party open to all FIC 'night owls' on Wednesday **27 March 2024** at the Bazaar St So (292 Rue Camille Guérin, 59800 Lille - Métro Grand Palais / Mairie de Lille) **from 10pm to 2.30am**.

Price? 30 euros - Admission + 2 drinks tickets

Booking required at: https://europe.forum-incyber.com/incyber-night/

UNE QUESTION ? CONTACTEZ L'ÉQUIPE ORGA INCYBER !

Pour toutes questions, n'hésitez pas à vous rendre au **Desk Organisation,** situé dans le Hall A à droite de l'entrée du Grand Théâtre.

A QUESTION? CONTACT THE ORGA INCYBER TEAM!

If you have any questions, don't hesitate to visit the Organisation Desk, located in Hall A to the right of the Grand Théâtre entrance.

ACCÈS AU RÉSEAU WIFI GRATUIT ET SÉCURISÉ "INCYBER2024PUBLIC"

Lille Grand Palais met à disposition des visiteurs un accès wifi en créant un compte temporaire.
N.B. : Nous vous rappelons qu'un point wifi public doit être utilisé avec précaution. Vérifiez que vous êtes bien redirigé vers le portail captif de Lille Grand-Palais.

FREE AND SECURE WIFI NETWORK "INCYBER2024PUBLIC"

Lille Grand Palais provides visitors with a wifi access by creating a temporary account.
***N.B.** : We remind you that a public Wi-Fi point should be used with care. Check that you are redirected to the Lille Grand-Palais captive portal.*

TÉLÉCHARGEZ L'APP FORUM INCYBER 2024

Disponible sur les stores d'applications Apple et Android, elle permet de planifier sa visite, d'interagir avec les partenaires, les conférenciers et les prospects, et de se repérer dans le salon.

DOWNLOAD THE INCYBER FORUM 2024 APP

Available on **Apple** and **Android** app stores, and to plan your visit, interact with partners, speakers and prospects, and find your way around the show.

GET IT ON Google Play

Download on the App Store

SUIVEZ NOTRE COMPTE LINKEDIN ET TWITTER @FIC_EU

Il vous permet d'être informé des temps forts de l'événement. De plus, retrouvez toutes les sessions sur la chaîne youtube de notre média inCyber News quelque temps après le Forum Incyber !

FOLLOW OUR LINKEDIN AND TWITTER ACCOUNT @FIC_EU

Allows you to be notified of show highlights. In addition, find all the sessions on the youtube channel of our inCyber media InCyber News some time after the InCyber Forum !

CYBERLEADERS

Ne quittez pas le Forum InCyber sans avoir acheté votre exemplaire du **3ème numéro de la revue stratégique Cyberleaders !**

Disponible sur le stand B38 au tarif de 29 euros.

Don't leave the InCyber Forum without buying your copy of the **3rd issue of the strategic review Cyberleaders!**

Available on stand B38 for 29 euros.