200 EXPOSANTS - CONFÉRENCES - DÉMONSTRATIONS - NETWORKING

DOSSIER DE PRESSE

CBC

CYBER SECURITY Business Convention

Le salon PRO de la Sécurité Numérique

JEUDI 28 NOVEMBRE 2024

TOULOUSE - MEETT

LE SALON INCONTOURNABLE POUR PROTÉGER
LES ENTREPRISES DES RISQUES CYBER

SOMMAIRE

L'ÉDITION 2024 DU CYBERSECURITY BUSINESS CONVENTION (CBC)

LE RENDEZ-VOUS CYBERSÉCURITÉ INCONTOURNABLE POUR TOUTE UNE FILIÈRE

6E ÉDITION - JEUDI 28 NOVEMBRE 2024 - MEETT DE TOULOUSE

À une époque où la sécurité numérique est vitale pour la résilience des entreprises, dirigeants et experts sont en quête de ressources fiables et de connaissances stratégiques pour mieux protéger leurs organisations. Mais dans cet écosystème complexe, comment identifier les solutions les plus adaptées à leurs besoins ? Quelles avancées façonnent le paysage de la cybersécurité ? Comment apprendre des expériences partagées par les pairs ?

Depuis 2019, pour répondre à ces enjeux, Dépêche Events organise à Toulouse le salon de la sécurité numérique, qui se tiendra cette année le jeudi 28 novembre au MEETT. Soutenu par des partenaires reconnus et engagés du secteur, ce rendez-vous s'est imposé au fil des éditions comme l'un des événements cybersécurité de référence en France, rassemblant un large éventail d'acteurs clés.

A l'occasion de cette 6ème édition, le salon prend une nouvelle ampleur avec un espace d'exposition doublé, atteignant plus de 5 000 m², et la présence de plus de 200 exposants et 50 intervenants de renom venus de toute la France mais aussi de l'Europe. Cette évolution souligne les ambitions du salon, qui propose cette année un programme encore plus complet et stimulant rythmé par des conférences, masterclass, remise de trophées, rendez-vous d'affaires ou encore animations de simulation de cellules de crise.

Cette année, une attention particulière est portée à l'Intelligence Artificielle, une thématique centrale qui sera explorée à travers diverses interventions et ateliers. Ce focus permettra d'apporter un éclairage novateur sur les nouveaux défis auxquels le secteur de la cybersécurité est confronté, ainsi que sur les solutions émergentes façonnées par l'IA.

Pour explorer pleinement la richesse du Cybersecurity Business Convention, rendez-vous le jeudi 28 novembre. Aux côtés de plus de 2 500 visiteurs, cet événement sera un véritable carrefour d'échanges, de découvertes et de networking, réunissant experts, entreprises et acteurs influents du secteur.

DÉROULÉ DE LA JOURNÉE MATIN

9h-9h15 Espace Conférences	Keynote d'ouverture - Les Nouvelles Règles du Jeu : Géopolitique du Numérique et de l'IA *Par Tariq Krim, Philosophe Tech*
9h-9h30 Espace Atelier 2	Piloter sa conformité NIS 2 : les erreurs à ne pas faire *Animé par Tenacy*
9h15-9h45 Espace Atelier 1	Anticiper, Réagir, Maîtriser : les enjeux de la visibilité réseau dans la cybersécurité d'aujourd'hui *Animé par Trend Micro*
9h15-10h Espace conférences	Confiance Numérique : Quand l'Intelligence Artificielle et la cybersécurité se renforcent mutuellement
9h35-10h05 Espace Atelier 2	Cyber-résilience : Assistez à une intrusion et gain de privilèges sur une architecture de sauvegarde *Animé par Protego et Fortalessa*
9h50-10h20 Espace Atelier 1	Démystification du 'Zéro Trust', où comment garantir un accès sécurisé à ses ressources informatiques dans tous contextes d'usage en environnements IT & OT *Animé par SFR Business*
10h-10h30 Espace Conférences	Keynote table ronde aéronautique : Les enjeux de sûreté dans le domaine aéronautique Par Pascal Andrei, Chief Security Officer, Airbus
10h10-10h40 Espace Atelier 2	Comment sécuriser votre supply chain face aux exigences de la Directive NIS2 ? *Animé par BeyondTrust*
10h30-11h15 Espace Conférences	Crises Cyber en Altitude : fédération des industriels de l'Aérospatial, de l'Aviation et de la Défense pour une seule excellence cyber de tous les fournisseurs
11h05-11h35 Espace Atelier 1	Comment gérer efficacement la sécurité des terminaux dans un environnement de travail hybride ? *Animé par ManageEngine*
11h30-12h30 Espace Atelier 2	IA de confiance : posez-vous les bonnes questions ! *Animé par Cyber'Occ et Ekitia*
11h30-12h Espace Conférences	Comment augmenter la résilience numérique grâce à la directive NIS2 : opportunités et menaces.
11h40-12h10 Espace Atelier 1	Performance ne signifie pas pertinence. Plongez dans un SOC et CERT MSSP et la stratégie mise en œuvre pour détecter les menaces dans un contexte en constante évolution. *Animé par Cheops*
12h-12h15 Espace Conférences	Keynote de clôture de la matinée : Transformation numérique : autonomie et sécurité dans un monde de plus en plus incertain. *Par Arnaud Coustillière, Vice-amiral d'escadre, Président du Pôle d'excellence cyber*

DÉROULÉ DE LA JOURNÉE

APRES-MIDI

13h30-14h15
Espace Conférences
L'Europe face aux cybermenaces : Renforcer la collaboration entre États membres

13h45-14h15
Espace Atelier 1
Des hackers s'affrontent en direct et il n'en restera qu'un !
Animé par Vade

14h-14h30
Espace Atelier 2
Fence : l'outil d'analyse des risques cyber pour le spatial, l'aéro, l'IT, l'OT, les services essentiels (NIS 2)
Animé *par Airbus Protect*

14h15-15h
Espace Conférences
Quand l'Industrie Rencontre le Bureau : La Cybersécurité au Croisement de l'OT et de l'IT

14h20-14h50
Espace Atelier 1
Tir à blanc de Ransomware® : Retours d'expérience et anecdotes RSSI d'une solution inédite de simulation d'attaque en conditions réelles par ransomware
Animé par Holiseum

14h30-15h30
Espace Librairie
Séance de dédicaces
Auteur : Arnaud Coustillière - Livre : Soldat de la cyberguerre

14h35-15h05
Espace Atelier 2
Unified SASE/ Universal ZTNA : réseau sécurisé hybride basé sur l'IA pour travailler de n'importe où
Animé *par Fortinet*

15h-15h45
Espace Conférences
Données sensibles du citoyen et cybersécurité : quels enjeux pour nos administrations et nos établissements de santé ?

15h10-15h40
Espace Atelier 2
Visibilité, contrôle, protection : adaptez votre défense et sécuriser l'IA by design pour une protection temps réel
Animé *par Palo Alto*

15h30-16h
Espace Atelier 1
Comment intégrer une PKI aux processus de développement et de recette sans perturber la production ?
Animé *par OWN*

15h45-16h30
Espace Conférences
Gouvernance de la cybersécurité des programmes spatiaux

15h45-16h15
Espace Atelier 2
Technologies de détection et réponse : transformez votre approche de la cybersécurité !
Animé *par KASPERSKY*

16h30-18h
Espace Conférences
Cérémonie de remise de trophées Cyberstar
Animé *par Stéphane Descous, Chief Product Security Officer, Thales Alenia Space*

LES KEYNOTES

ESPACE CONFÉRENCES

LES EXPERTS CYBER AU RENDEZ-VOUS

Le CBC est fier d'accueillir un panel d'experts renommés pour des conférences clés sur les enjeux actuels de la cybersécurité. La participation de ces intervenants de haut niveau fait du salon un événement incontournable pour tous les acteurs du secteur, qu'ils soient décisionnaires, experts techniques ou porteurs de solutions innovantes.

9h-9h15 : **Keynote d'ouverture - Les Nouvelles Règles du Jeu : Géopolitique du Numérique et de l'IA**

Tariq KRIM, Entrepreneur, philosophe tech et ancien vice-président du conseil national du numérique

10h-10h30 **Keynote aéronautique : Les enjeux de sûreté dans le domaine aéronautique**

Pascal ANDREI, Chief Security Officer, Airbus

12h-12h15 : **Keynote de clôture de la matinée : Transformation numérique : autonomie et sécurité dans un monde de plus en plus incertain**

Arnaud COUSTILLIERE, Vice-amiral d'escadre, Président du Pôle d'excellence cyber

14h-15h : **Démonstration : OSINT et données personnelles un cocktail détonnant**

Julien METAYER, Pentaster, Red teamer, Osinter

TEMPS FORT
INTELLIGENCE ARTIFICIELLE

9H · KEYNOTE DE TARIQ KRIM

Les Nouvelles Règles du Jeu : Géopolitique du Numérique et de l'IA

9H15 · TABLE RONDE

Quand l'Intelligence Artificielle et la cybersécurité se renforcent mutuellement

11H30 · ATELIER ANIMÉ PAR CYBER'OCC ET EKITIA

IA de confiance : posez-vous les bonnes questions !

11H30 · CONSULTATION ORDRE DES AVOCATS

Comment évaluer la conformité de votre projet face à l'IA Act ?

LES TABLES RONDES

ESPACE CONFÉRENCES

Les tables rondes sont un moment privilégié pour anticiper les tendances futures et développer des stratégies adaptées aux nouvelles menaces qui pèsent sur les entreprises, les administrations et les infrastructures publiques.

9h15-10h : **Confiance Numérique : Quand l'Intelligence Artificielle et la cybersécurité se renforcent mutuellement**

Animé par Olivier AURADOU, Directeur Cyber'Occ

Alors que l'utilisation de l'intelligence artificielle connaît un bond sans précédent, dans le secteur public comme privé, nos intervenants feront le point sur la multiplication des menaces envers les SIA. Ils traiteront également de l'enjeu de la robustesse aux côtés des cadres légaux et éthiques pour renforcer la confiance dans ces systèmes d'IA. Enfin, cette table ronde sera l'occasion de s'interroger sur la nécessité de décloisonner le monde de l'IA et celui de la cyber l'un envers l'autre

Joséphine DELAS
Ingénieure en Intelligence Artificielle, Harfanglab et membre du CEFCYS

Selma SOUIHEL
Directrice du projet P16 - Programme IA, INRIA

Bertrand MONTHUBERT
Président d'Ekitia et co-président du GT "Data Governance" du Global Partnership on Artificial Intelligence

Marc SZTULMAN
Président de Cyber'Occ et Conseiller Régional Délégué au Numérique

10h30-11h15 : **Crises Cyber en Altitude : fédération des industriels de l'Aérospatial, de l'Aviation et de la Défense pour une seule excellence cyber de tous les fournisseurs**

Animée par Gil BOUSQUET, Rédacteur en chef de Dépêche Eco

Notre industrie s'y prépare depuis des années, mais difficile d'éviter la crise chez les fournisseurs. L'Europe et l'Etat Français passent à la vitesse supérieure avec de nouvelles réglementations imposées maintenant aux fournisseurs, fleurons de notre industrie mais pied d'argile d'une protection Cyber de toute la filière. Les attaquants n'ont pas changé de camp mais bien de cibles : la priorité est d'aider nos petites et moyennes entreprises à se protéger et se préparer au pire.

Marc LEYMONERIE
Président
CERT Aviation France

Didier COLLET
Adjoint Industrie et International au chef du service de la sécurité de défense et des systèmes d'information
Direction Générale de l'Armement

Romain BOTTAN
CISO BoostAerospace & AirCyber Director

LES TABLES RONDES

ESPACE CONFÉRENCES

11h15-12h : **Comment augmenter la résilience numérique grâce à la directive NIS2 : opportunités et menaces.**

Animé par Sébastien GARNAULT, Fondateur, Paris Cyber Summit

Face à la menace numérique toujours plus intense, l'Union européenne a pris plusieurs décisions d'importance afin d'augmenter la cybersécurité des organisations et des États-membres. Parmi les nombreux textes adoptés, la Directive NIS2 est l'un des plus importants. Si NIS1 imposait aux organisations les plus stratégiques de sécuriser leurs systèmes d'informations, NIS2 est une révolution tant l'élargissement du périmètre des secteurs critiques concernés est important, d'un point de vue technique comme humain. Elle vise aussi et surtout à accroître la résilience des services essentiels face aux cyberattaques et aux menaces numériques croissantes en imposant aux organisations de toutes tailles -collectivités, PME, grands groupes- des exigences accrues en matière de gestion des risques et de signalement des incidents. La Directive NIS2 s'intéresse également aux collaborateurs et leurs compétences, aux sous-traitants, aux établissements de santé, etc. En un mot, à l'ensemble de la société. Pourtant, la France est en retard. La date limite de transposition du 17 octobre n'est pas tenue et aucune loi française n'aura été adoptée depuis 2022. Alors où en sommes-nous ? Quel est le nouveau périmètre de ces obligations de cybersécurité et quelles seront les organisations concernées ? Quelle responsabilité auront les dirigeants et les équipes en cas de cyberattaque réussie ? Comment l'État va-t-il accompagner les entreprises, quel sera son contrôle et quelles seront les sanctions ? Tout reste à définir.

Philippe LATOMBE
Député et membre de la Commission des Lois
Assemblée Nationale

Arnaud COUSTILLIERE
Vice-amiral d'escadre, Président
Pôle d'excellence cyber

Anne TRICAUD
Head of Airbus Corporate Security Office

Erwan BROUDER
Directeur adjoint Cybersécurité
SOPRA STERIA

13h30-14h15 : **Europe Facing Cyber Threats : Strengthening Collaboration Between Member States**

Moderated by Sébastien GARNAULT, Founder, Paris Cyber Summit *Conférence en anglais

Raimond KALJULAID
Member of the Estonian Parliament and Chairman of the Estonian Delegation to the NATO Parliamentary Assembly

Peter SUND
CEO
FISC (Finnish Information Security Cluster)

14h15-15h : **Quand l'Industrie Rencontre le Bureau : La Cybersécurité au Croisement de l'OT et de l'IT**

Animée par Alain BOUILLE, Délégué Général, CESIN

La cybersécurité sécurité industrielle n'est plus la chasse gardée des automaticiens et a fait une entrée presque obligée dans l'agenda de la plupart des RSSI désormais. Mais comment concilier une cyber « traditionnelle » du monde IT très mature avec une cyber du monde industrielle souvent « empêchée » par des systèmes d'exploitation incompatibles avec les dernières innovations en matière de protection cyber ? Cette table ronde réunissant des acteurs très impliqués dans ce domaine abordera les différents aspects à considérer en matière de démarche, de gouvernance mais aussi de solutions.

LES TABLES RONDES

ESPACE CONFÉRENCES

Stéphane NAPPO
Vice President, Cybersecurity Director & Global Chief Information Security Officer
Groupe SEB

Véronique BARDET
CISO
Groupe Pierre Fabre

Sabri KHEMISSA
Consultant Expert en Cybersécurité des Installations Industrielles
Fortress Cybersecurity

15h-15h45 : **Données sensibles du citoyen et cybersécurité : quels enjeux pour nos administrations et nos établissements de santé ?**

A l'ère du numérique, la protection des données personnelles est devenue une priorité absolue, en particulier dans le secteur de la santé. En effet, les informations de santé des concitoyens, telles que les dossiers médicaux et les données administratives, constituent des ressources clés pour les administrations publiques et les établissements de santé. Bien que indispensables pour la qualité des soins et la gestion des services, ces données sensibles représentent des cibles de choix pour les cyberattaques. Quelles sont les conséquences de ces menaces pour les patients, les professionnels de la santé, et les institutions ? Comment les administrations publiques et les établissements de santé peuvent-ils renforcer la sécurité de leurs systèmes d'information tout en protégeant efficacement les citoyens ?

Xavier ALACOQUE
Directeur des DATA et de l' IA et RSSI
Oncopole Claudius Régaud

Vincent TEMPLIER
Responsable de la Sécurité des Systèmes d'information,
Centre hospitalier Princesse Grace - Monaco

Erik BOUCHER
Ingénieur expert en technologies de l'information, Référent santé
CNIL - Commission Nationale de l'Informatique et des Libertés

15h45-16h30 : **Gouvernance de la cybersécurité des programmes spatiaux**

Animée par Florent RIZZO, Founder & CEO, CyberInflight

Le domaine spatial, ainsi que le domaine cyber, sont désormais considérés comme des nouveaux champs de conflictualité. La dépendance de plus en plus forte aux services spatiaux demande à l'ensemble de la chaine de valeur du spatial de mettre en place des mesures de sécurité pour protéger cet écosystème. L'approche par la sécurité et la résilience doit être mise en place tout au long du cycle de vie de la chaine opérationnelle et de la chaine d'approvisionnement. Sécuriser un système spatial et ses services ne demande pas seulement des connaissances ou implémentations techniques, mais également une gouvernance forte et cohérente, alliant une connaissance des enjeux géopolitiques, économiques, industriels, réglementaires, opérationnels ou technologiques.
Cette table ronde traitera des principaux enjeux de gouvernance observés par différents experts reconnus dans ce domaine.

Contre-amiral Christophe MERIEULT
Officier Général adjoint,
Commandement de l'Espace

Stéphane LENCO
Vice Président
Group CISO, Thales

Julien AIRAUD
Expert Sénior Cybersécurité Spatiale
CNES

Clémence POIRIER
Senior Cyberdefense Researcher
The Center for Security Studies

LES ATELIERS EXPOSANTS

ESPACES ATELIERS 1 & 2

Animés par des experts du secteur, les ateliers du CBC offrent aux participants l'opportunité d'échanger directement avec les acteurs clés pour mieux comprendre les enjeux spécifiques de chaque domaine et de découvrir des solutions pratiques pour renforcer la sécurité au sein des organisations.

Espace Atelier 1
9h15-9h45

Anticiper, Réagir, Maîtriser : les enjeux de la visibilité réseau dans la cybersécurité d'aujourd'hui

Dans le contexte d'un réseau d'entreprise qui a profondément muté au cours des dernières années, les bonnes pratiques et les technologies qui permettent aux équipes de sécurité de juguler les risques de cybersécurité sont essentielles. Ce réseau, autrefois clairement identifié, car consolidé au sein d'un périmètre connu, s'est étendu vers de multiples Edges (environnements cloud, télétravailleurs, sites distants, infrastructures industrielles OT, etc.), chacun constituant de possibles passerelles d'intrusion vers le SI. La gestion des risques porte désormais sur un environnement large et diversifié tandis que les équipes de sécurité sont tenues de protéger des ressources disséminées, que celles-ci soient gérées par une politique de sécurité ou inconnues. Dans ce contexte, une visibilité consolidée et temps-réel sur la myriade de composants constituant le réseau devient critique.
Découvrez les principes d'une visibilité globale, fournie par une plateforme de cybersécurité unifiée, et qui offre aux équipes de sécurité une information en temps réel sur leur posture de sécurité et sur les risques liés à la surface d'attaque de leur entreprise.
Animé par Trend Micro

Espace Atelier 2
9h-9h30

Piloter sa conformité NIS 2 : les erreurs à ne pas faire

NIS 2 est entrée en vigueur en France il y a un mois, et pose déjà un réel challenge aux 20 000 entreprises concernées par cette nouvelle directive. Car ce n'est pas tout de se mettre en conformité : il faut ensuite la maintenir, et s'assurer de rester du bon côté de la barrière. Reporting, tâches récurrentes, gestion des tiers... jongler entre toutes ces responsabilités implique un pilotage cyber impeccable. Et c'est ce dont Baptiste David, Head of Market Strategy chez Tenacy, vous parlera durant cet atelier.
Animé par Tenacy

Espace Atelier 2
9h35-10h05

Cyber-résilience : Assistez à une intrusion et gain de privilèges sur une architecture de sauvegarde

A travers un scénario technique de test d'intrusion déroulé sur un périmètre de sauvegarde de données, Fortalessa exploitera des vulnérabilités présentes et effectuera une intrusion sur la cible. Une méthodologie d'escalade de privilèges sera ensuite déroulée afin d'obtenir des permissions sans restrictions mettant en danger l'architecture. Cette présentation technique sera accompagnée d'une approche de gouvernance SSI portant sur la segmentation, le principe de moindre privilège ou encore la ségrégation des tâches. Ces remédiations seront rapprochées des référentiels de conformité SSI du marché.
Animé par Protego et Fortalessa

LES ATELIERS EXPOSANTS

ESPACES ATELIERS 1 & 2

Espace Atelier 1
9h50-10h20

Démystification du 'Zéro Trust', où comment garantir un accès sécurisé à ses ressources informatiques dans tous contextes d'usage en environnements IT & OT

Est-ce que le paradigme historique du « Zéro Trust » uniquement périmétrique se doit d'évoluer suite à la transformation digitale et la dispersion des usages informatiques (travail hybride, BYOD, industrie 4.0, multi cloud, ...) pour assurer une vraie défense en profondeur ?
Lors de cet atelier, après avoir revu cette évolution du concept, nous verrons sur quels nouveaux périmètres il devient pertinent de l'appliquer (Utilisateurs, Sites distants, Datacenter Privé/Public, Environnements IT/OT/IoT...) ainsi que sur quels modèles, illustrés par des architectures types, ce Zéro Trust étendu peut se déployer et s'administrer de manière progressive, simplifiée et maîtrisée.
Animé par SFR Business

Espace Atelier 2
10h10-10h40

Comment sécuriser votre supply chain face aux exigences de la Directive NIS2 ?

La directive NIS2, évolution de la législation européenne en matière de cybersécurité, accorde une attention particulière à la sécurité de la supply chain. Dans un contexte où les cybermenaces se multiplient, il est crucial pour les entreprises de protéger non seulement leurs infrastructures mais également l'ensemble de leur supply chain, incluant les logiciels et les tiers mainteneurs ayant accès à leurs ressources. NIS2 impose ainsi de nouvelles responsabilités aux entreprises pour renforcer la sécurité à tous les niveaux.

Que va-t-on aborder dans cette session ?

- Comment NIS2 définit-elle la sécurité dans la supply chain ?
- Quels sont les différents éléments à sécuriser dans la supply chain ?
- Comment répondre aux exigences de NIS2 grâce à une gestion efficace des identités et des accès ?

Animé par BeyondTrust

Espace Atelier 1
11h05-11h35

Comment gérer efficacement la sécurité des terminaux dans un environnement de travail hybride ?

Participez à notre atelier dédié à la technologie ManageEngine Endpoint Central, un outil essentiel pour la gestion et la sécurité des terminaux dans votre organisation. Nous mettrons particulièrement en lumière ses modules de vulnérabilité, un enjeu majeur en cybersécurité, conçus pour détecter, évaluer et remédier aux failles de sécurité de manière proactive. Dans un contexte où vos utilisateurs travaillent aussi bien de la maison que depuis les bureaux, découvrez comment Endpoint Central peut renforcer votre cyberdéfense en automatisant la gestion des correctifs, en assurant une conformité continue et en fournissant des rapports détaillés sur l'état de sécurité de votre réseau. Rejoignez-nous pour une démonstration pratique et des échanges interactifs sur les meilleures pratiques en matière de cybersécurité.
Animé par ManageEngine

Espace Atelier 1
11h30-12h30

IA de confiance : posez-vous les bonnes questions !

Traiter les enjeux de cybersécurité et appliquer une approche éthique permet de renforcer la confiance dans l'utilisation de l'IA. Découvrez les points de convergence et les bonnes pratiques en la matière pour une application opérationnelle dans vos projets.
Animé par Cyber'Occ et Ekitia

LES ATELIERS EXPOSANTS

ESPACES ATELIERS 1 & 2

Espace Atelier 1
11h40-12h10

Performance ne signifie pas pertinence. Plongez dans un SOC et CERT MSSP et la stratégie mise en œuvre pour détecter les menaces dans un contexte en constante évolution.

Dans le monde d'aujourd'hui, marqué par une complexité croissante des menaces cyber, il est crucial de reconnaître que la performance d'un Security Operations Center (SOC) et d'une équipe de réponse aux incidents informatiques (CERT) ne se mesure pas uniquement par la quantité de menaces traitées, le nombre de cas d'utilisation en place, la couverture MITRE, etc. En effet, la pertinence est la pierre angulaire d'une stratégie de cybersécurité efficace.

Face à un volume incessant de menaces, il ne s'agit pas tant de couvrir intégralement chaque aspect du cadre MITRE, mais plutôt de cibler précisément les segments les plus pertinents pour chaque client. Prenons un exemple concret : si un SOC se concentre sur la couverture exhaustive des techniques de “persistance” et “élévation de privilèges” dans MITRE, cette approche peut sembler bonne en théorie. Cependant, si les acteurs de la menace ciblant spécifiquement notre client exploitent principalement des vecteurs liés à “Exfiltration” et “Persistance”, alors notre stratégie manque de pertinence. Nous consacrerions des ressources considérables à des domaines qui, bien que critiques en général, ne posent pas une menace immédiate au client en question.

Dans ce contexte, il est essentiel que notre approche évolue constamment pour s'aligner sur les tactiques, techniques et procédures spécifiques utilisées contre nos clients. Cela implique une veille technologique continue et une adaptation stratégique pour anticiper et contrer les menaces les plus critiques pour chaque industrie et chaque client. L'objectif est de passer d'une performance basée sur la quantité à une performance mesurée par sa pertinence, garantissant ainsi une protection efficace adaptée aux défis spécifiques auxquels chaque client est confronté.

Animé par Cheops

Espace Atelier 1
13h45-14h15

Des hackers s’affrontent en direct et il n’en restera qu’un !

Participez à cette session interactive en testant vos connaissances sur les thématiques du spear-phishing et de l'usurpation d'identité. Répondez correctement à chaque question pour passer au tour suivant, jusqu'à ce qu'il ne reste plus qu'un seul vainqueur parmi vous ! Révisez votre social engineering et affûtez vos techniques, car le gagnant remportera des Airpods !

Animé par Vade

Espace Atelier 2
14h-14h30

Fence : l'outil d'analyse des risques cyber pour le spatial, l'aéro, l'IT, l'OT, les services essentiels (NIS 2)

Fence est l'outil d'analyse de risques d'Airbus Protect, pour l'identification et la gestion des risques de cybersécurité. Intuitif et efficace, il est conçu aussi bien pour l'IT (EBIOS RM et ISO 27005), pour les opérateurs d'importance vitale ou essentiels (II 901, NIS 2...), que pour les systèmes industriels (IEC 62443) et les produits industriels de l'aviation, du spatial, du ferroviaire... Fort de l'expérience des consultants d'Airbus Protect, Fence permet également d'évaluer la conformité à plus d'une trentaine de standards, de suivre les plans d'actions et les risques résiduels, ou encore de générer rapports et tableaux de bord.

Animé par Airbus Protect

Espace Atelier 1
14h20-14h50

Tir à blanc de Ransomware® : Retours d'expérience et anecdotes RSSI d'une solution inédite de simulation d'attaque en conditions réelles par ransomware

La menace cyber n°1 rencontrée par les organisations à travers le monde est l'attaque par ransomware.
Une question cruciale se pose alors : comment mesurer le niveau de résilience de notre Système d’Information face au risque ransomware, sans attendre de subir une véritable attaque ?
A chaque problème sa solution ! Le Tir à Blanc de Ransomware® est une solution innovante et unique sur le marché simulant en conditions réelles une cyberattaque sophistiquée par ransomware.
Au cours de cet atelier, découvrez le retour d'expérience d'un RSSI sur la solution Tir à Blanc de Ransomware®, lauréate de plusieurs prix de l’innovation.

Animé par Holiseum

LES ATELIERS EXPOSANTS

ESPACES ATELIERS 1 & 2

Espace Atelier 2
14h35-15h05

Unified SASE/ Universal ZTNA : réseau sécurisé hybride basé sur l'IA pour travailler de n'importe où

La convergence du réseau et de la sécurité au travers du wifi, LAN, SD-WAN, ZTNA, SASE et le pare-feu réseau permet des accès prenant en compte la localisation, l'utilisateur, l'appareil, le contenu et les applications.Au travers de cet atelier, nous expliquerons pourquoi nous parlons d'accès sécurisé convergé. Nous évoquerons les composants du SASE unifié de Fortinet et les bénéfices pour vos enjeux métiers. Sans oublier la notion des services de sécurité fournis dans le Cloud grâce à FortiSASE. Venez échanger avec nos experts.

Animé par Fortinet

Espace Atelier 2
15h10-15h40

Visibilité, contrôle, protection : adaptez votre défense et sécuriser l'IA by design pour une protection temps réel

L'ère de l'IA a complètement bouleversé nos usages et fait partie prenante de notre vie. L'adoption inégalée de cette nouvelle technologie est immédiate et exponentielle.Cela engendre de nouveaux risques d'exposition des données mais également un manque de visibilité de l'utilisation des applications Gen AI sans parler de l'absence de politiques claires concernant l'utilisation de celles-ci. C'est pour cela que Palo Alto Networks en fait une de ses priorités. Venez découvrir comment notre plateforme Zero Trust intègre by design l'intelligence artificielle afin de répondre concrètement à ces nouveaux usages tout en simplifiant vos opérations au quotidien. Venez assister à la démonstration de notre plateforme Strata afin de renforcer votre sécurité tout en simplifiant vos opérations.

Animé par Palo Alto

Espace Atelier 1
15h30-16h

Comment intégrer une PKI aux processus de développement et de recette sans perturber la production ?

Ensemble de technologies, procédures et de logiciels, Les Public Key Infrastructure (PKI) ou infrastructure à clés publiques ont pour objectif de gérer de manière sécurisée le cycle de vie des certificats numériques. Cette technologie, basée sur les certificats, aide les organisations à établir une signature, un chiffrement et une identité fiable entre les personnes, les systèmes et les objets. Elle est un élément essentiel d'une stratégie informatique.

Animé par OWN

Espace Atelier 2
15h45-16h15

Technologies de détection et réponse : transformez votre approche de la cybersécurité !

En matière de cybersécurité des terminaux, l'importance croissante des systèmes EDR (Endpoint Detection and Response - qui intègrent le deep learning ou l'apprentissage automatique pour détecter les menaces - est toujours plus prégnante. Mais au-delà de la technologie EDR, les solutions MDR (Managed Detection and Response) - qui incluent une approche proactive de chasse aux menaces - contribuent à une protection informatique avancée. L'objectif de ce workshop est donc de vous offrir une compréhension globale de l'évolution et des avantages des technologies EDR et MDR, afin de renforcer la sécurité de vos systèmes. Découvrez comment ces outils essentiels peuvent transformer votre approche de la cybersécurité.

Animé par Kaspersky

Espace Atelier 1
16h - 16h30

Violations de données et incidents de sécurité : quelle responsabilité pour les dirigeants d'entreprise ?

Découvrez les bonnes pratiques juridiques et techniques de gestion des incidents de sécurité. Cet atelier abordera les démarches à suivre pour les déclarations et notifications en cas de violation de données, ainsi que les impacts des nouvelles régulations, comme la directive NIS2, DORA et la Loi de Programmation Militaire (LPM), sur la responsabilité des dirigeants d'entreprise.

Animé par La Commission Sécurité Economique : France Charruyer Avocat Associé Altij&Oratio et Frédéric Ollivier Tech lead auditor Totem Numérique

LES DÉMONSTRATIONS

ESPACE DÉMONSTRATIONS

9h30-10h15

IA & OSINT: Un cocktail révolutionnaire pour la cybersécurité ?

Découvrez comment l'intelligence artificielle (IA) transforme l'Open Source Intelligence (OSINT) en un outil puissant pour la cybersécurité. Cette conférence explore les potentiels, les limites et les implications de l'intégration IA-OSINT pour une veille proactive et une détection des menaces améliorée.

Animé par Baptiste ROBERT pour Predicta Lab

10h30 - 11h

Escales Numériques : Comment les Publications de nos données attirent les Hackers

Les informations partagées sur les réseaux sociaux, comme les photos, les lieux visités ou les détails personnels, peuvent être exploitées par des hackers pour mener des attaques ciblées. Ces données permettent de créer des phishing convaincants, voler des identités, ou surveiller les habitudes des victimes. Les conséquences peuvent être graves, allant du piratage de comptes à des vols financiers ou des attaques contre des entreprises via leurs employés, montrant l'importance de limiter l'exposition de ses données personnelles en ligne.

Animé par Anozr Way - Nathalie GRANIER, Threat Intelligence & Human Behavior Specialist

11h15-11h45

Révolutionner la sécurité informatique : la psychologie au cœur du management des risques humains

Pour parvenir à une véritable réduction des risques et répondre aux exigences des responsables de la sécurité, les mesures de sensibilisation de base ne suffisent pas. L'évolution du paysage des menaces exige de passer à une gestion des risques humains centrée sur les personnes, qui donne la priorité aux résultats et aux moteurs du comportement. Avec l'intervention d'Arnaud Loubatière, nous explorerons le pouvoir de la gestion des risques humains pour une atténuation durable des risques cyber et fournirons des conseils pratiques sur la façon de favoriser une culture de sécurité robuste avec un changement de comportement durable grâce à la psychologie.

Animé par SoSafe - Jean-Baptiste ROUX, Vice-Président et Expert en sensibilisation à la cybersécurité

14h - 15h

Osint et données personnelles, un cocktail détonnant

Les données personnelles en open source sont devenues massives et très riches à qui sait les exploiter. Particuliers comme entreprises sont les cibles privilégiées des hackers, en particulier avec l'utilisation de ces données sociales qui fournissent à la cybermalveillance des outils tout à fait efficace de reconnaissance ou d'intrusion sur les systèmes d'information.

Animé par Julien METAYER – Pentaster, Red teamer, Osinter

15h15-15h45

Passez des campagnes de sensibilisation (à la cybersécurité) au risque humain réel pour l'entreprise

Mimecast révolutionne la sensibilisation à la cybersécurité des utilisateurs grâce à Mimecast Engage®, qui intègre les signaux réels des comportements utilisateurs en entreprise et permet d'appliquer des réponses ciblées et automatisée.

Animé par Mimecast

16h-16h30

Cyblex Consulting – De l'autre côté du miroir : Suivez toutes les étapes d'une attaque à travers les yeux du pirate

Un hacker éthique de Cyblex Consulting fera la démonstration de toutes les étapes d'un scénario de compromission mené dans un réseau d'entreprise depuis internet. Découvrez les tactiques, les techniques et les outils utilisés à la fois par les équipes « red team » et les pirates. De quoi vous donner des sueurs froides…

Animé par Cyblex Consulting

LES ANIMATIONS

Stand Great X
Toute la journée

SIMULATION DE CYBERATTAQUE - Animé par Thierry ROUX, Dirigeant de GREAT X

- Simulateur de crise cyber Open EX vous permet de tester une expérience réaliste durant laquelle les participants sont plongés en immersion au cœur d'une cyberattaque. Un entraînement unique et innovant !
-Serious game : Crisis Black out

Meeting Room 1
8h45-9h30

CAFE DEBAT - Organisé par AFCDP et la CNIL

Le DPO face au tsunami réglementaire : enjeux et évolutions du métier

Règlement sur l'IA, directive NIS 2, DSA, DMA… la réglementation européenne liée au numérique a connu une inflation forte ces dernières années. Dans ce contexte, bien que le RGPD, en application depuis plus de 6 ans, demeure le texte de référence pour la CNIL et les DPO, son articulation avec ces autres textes ouvre de nouvelles incertitudes et bouleverse parfois les organisations mises en place.
Lors de ce café-débat nous débattrons des défis pour les DPO et les RSSI, ainsi que des impacts sur leurs métiers dans les années à venir.

Espace Capture The Flag
10h-17h

CHALLENGE CAPTURE THE FLAG - Organisé par Devensys Cybersecurity en partenariat avec le Commandement de l'Espace et le ComCyber

Voyage Spatial en Informatique : édition numéro 2

Le challenge CTF consiste à résoudre des épreuves contenant des failles volontaires et à retrouver des informations appelées "flags", qui sont placées sur les serveurs de manière chiffrée, cachées ou à des endroits difficiles d'accès. Le challenge est ouvert à tous les étudiants et professionnels passionnés de sécurité informatique.
Préparez-vous à un voyage intergalactique unique dans le monde de la cybersécurité ! Devensys et sa Red Team vous proposent un CTF avec plus de 10 épreuves. Que vous soyez un expert en sécurité ou un passionné de technologie, cet événement vous emmènera dans une aventure où vous devrez découvrir et corriger des failles de sécurité sur un site de réservation de voyages spatiaux.
Attention, places limitées - Pour composer votre équipe veuillez contacter ethilie.fonroques@ladepeche.fr

Meeting Room 2
10h30-12h30

SIMULATION D'UNE CELLULE DE CRISE - Animé par EH&A Consulting

Venez gérer la crise !

Mise en situation, en équipes de 7 personnes vous serez confrontés à une cyber attaque.
Les écrans sont noirs, plus aucune donnée n'est accessible, plus de doute, il s'agit bien d'une cyber-attaque ! Vous êtes le comité de direction d'une entreprise sous-traitante d'un fleuron de l'aéronautique français. Plus aucun employé ne peut travailler normalement et des données stratégiques sont en danger ! À vous de gérer la crise ! Participez à une expérience immersive inédite dans une cellule de crise lors d'une cyberattaque et prenez les grandes décisions stratégiques.

LES ANIMATIONS

Meeting Room 2
11h30-12h30

CONSULTATION ORDRE DES AVOCATS

Consultation gratuites par l'Ordre des Avocats de Toulouse : Comment évaluer la conformité de votre projet face à l'IA Act ?

Vous développez un projet utilisant l'intelligence artificielle et vous vous interrogez sur sa conformité avec la réglementation en vigueur ? Profitez de consultations exclusives d'une heure offertes lors de notre salon dédié à la cybersécurité. Nos experts vous guideront à travers les exigences de l'IA Act, en vous aidant à identifier les risques juridiques, à comprendre les obligations de transparence et à anticiper les mesures de conformité à mettre en place. C'est une occasion unique de bénéficier de conseils personnalisés pour sécuriser vos innovations tout en respectant les nouvelles législations européennes. Ne manquez pas cette opportunité de faire évaluer votre projet par des spécialistes du droit !

Espace Ateliers 1
12h15-12h45

REVERSE RECRUTING - Organisé par France Travail Pro

Les entreprises participantes : Sopra Steria et SNS-Security

Recrutement, et si on inversait les rôles ? Dans un contexte où trouver le profil idéal est devenu une problématique majeure, nos exposants vous proposent de participer à une expérience inédite : le reverse recruiting ! Pour la première fois, ce sont les exposants qui postuleront auprès des candidats. Ils auront 5 minutes pour vous convaincre de rejoindre leur team cybersécurité !

Espace Librairie
14h30-15h30

SEANCE DE DEDICACE LIVRE

Ouvrage : Soldat de la cyberguerre
Auteur : Arnaud COUSTILLIERE

LES PITCHS

SESSION 1 - 10h45 à 11h25

Espace Atelier 2

Sans NDR, votre sécurité est-elle aussi efficace ?
avec Cédric LEFEBVRE, Expert Cybersécurité
par *Custocy*

NEXT GEN SIEM : L'intensification d'un contexte cyber sous tension nécessite désormais une nouvelle approche du SIEM qui se veut plus intelligente et efficiente
avec Frédéric MASANA et Dao VO TRUNG
par CrowdStrike et Exaprobe

SOC managé 24/7 : la meilleure réponse au manque de temps, de personnel et/ou de compétences en cybersécurité
avec Antoine PITAUD, Sales Engineer
par Bitdefender

SESSION 2 - 14h55 à 15h25

Espace Atelier 1

SOFIE : La Réactivité Instantanée pour Protéger Votre Entreprise des Cybermenaces - Le copilote IA pour une Cybersécurité Sans Relâche
avec Arnaud LOUBATIERE, Expert en sensibilisation à la cybersécurité
par SoSafe

Immuable : la sauvegarde qui rend vos données intouchables
avec Thierry ROBERT et Steeve GHINTRAN
par OCI et VEAM

La cybersécurité, un enjeu pour toutes les entreprises : Comment les stagiaires de la formation et alternants jouent un rôle clé ?
avec Samira BARCHICHE et Peggy POLLAGBA
par ORT Toulouse

LA CEREMONIE DE REMISE DE TROPHÉES

ESPACE CONFÉRENCES 16h30 à 18h

REMISE DE TROPHÉES CBC

SPONSORISÉ PAR

xmco
We deliver cybersecurity expertise

Pour la première année, le CBC organise en partenariat avec la communauté Cyberstar, une remise de trophées qui récompense les personnalités qui dynamisent l'écosystème cyber. L'occasion unique de voter pour vos experts préférés et de prendre part à ce moment convivial. 4 experts seront récompensés dans chacune de ces catégories :

- Hackeur Ethique,
- Championne des Réseaux,
- Jeune Talent
- Cyber Contributeur

La remise des prix se tiendra le jeudi 28 novembre au CBC dès 16h30 dans l'espace conférences et sera suivie d'un afterwork dès 17h dans l'espace lounge.
Une cérémonie animée par Stéphane DESCOUS

Les votes sont ouverts et en ligne jusqu'au lundi 25 novembre : https://qlic.it/1499891

LES EXPOSANTS 2024

HALL D'EXPOSITION

Retrouvez pas moins de 200 exposants et partenaires, répartis dans les 5 000m² de salon du CBC. Offreurs de solutions, société de conseils, ESN, intégrateurs, opérateurs publics ou encore organismes de formation seront présents pour apporter toute leur expertise et présenter leurs innovations. Parmi lesquels : Airbus Protect, Sopra Steria, Capgemini, Fortinet, Vade, Cheops Technology, MailinBlack, Palo Alto ou encore BeyondTrust.

Retrouvez la liste des 200 exposants qui seront présents sur le salon sur le site internet du CBC :

https://cbc-convention.com/annuaire-exposant-cybersecurite/

LES RENDEZ-VOUS D'AFFAIRES

Les Rendez-vous d'affaires du CBC sont une opportunité unique pour les visiteurs présents et les exposants de se rencontrer et d'échanger sur des solutions concrètes face aux défis croissants de la sécurité numérique.

Ces sessions de networking sont conçues pour favoriser la recherche de prestataires, la construction de partenariats stratégiques ou encore renforcer les collaborations entre les acteurs.

Structurés en rendez-vous préprogrammés, ces moments de rencontre permettent d'établir des connexions de qualité et d'organiser en amont sa journée.

Pour réserver les RDV d'affaires : inscription gratuite ici

LES PARTENAIRES

Partenaires

Partenaires média

Organisateur

LES INFOS PRATIQUES

MEETT - Parc des Expositions
Centre de Conventions & Congrès
Concorde Avenue
31840 AUSSONNE

Le jeudi 28 novembre 2024
8h30-18h
Entrée gratuite
Restauration sur place

Inscription gratuite sur :
cbc-convention.com

LES CHIFFRES CLÉS

6ème édition

200 exposants

2 500 visiteurs attendus

+50 prises de parole

Contact presse :
Jeanne Bassinet - jeanne.bassinet@ladepeche.fr - 06 33 03 36 07