THALES
Building a future we can all trust

DOSSIER DE PRESSE

THALES MEDIA DAY CYBERSÉCURITÉ

31 Mai 2022

Pour en savoir plus, clique ici

THALES MEDIA DAY 2022

Cybersécurité : nouvelles menaces, nouveaux enjeux

Le nombre de **cyberattaques et de rançongiciels** a explosé au cours des 12 derniers mois **(+ 150 %)** et les typologies de menaces évoluent constamment à mesure que la pandémie rend les outils numériques de plus en plus présents dans notre vie quotidienne.

Depuis **2019**, les coûts de la cybercriminalité sur l'économie mondiale ont plus que **doublé**.

[1] Source : Groupe IB www.group-ib.com

SOMMAIRE

A PROPOS DE THALES

Thales est un leader mondial des hautes technologies qui investit dans les innovations du numérique et de la « deep tech » – connectivité, big data, intelligence artificielle, cybersécurité et quantique – pour construire un avenir de confiance, essentiel au développement de nos sociétés. Le Groupe propose des solutions, services et produits qui aident ses clients – entreprises, organisations, Etats - dans les domaines de la défense, de l'aéronautique, de l'espace, du transport et de l'identité et sécurité numériques, à remplir leurs missions critiques en plaçant l'humain au cœur des décisions.

Thales compte **81 000 collaborateurs** dans **68 pays**. En 2021, le Groupe a réalisé un chiffre d'affaires de **16,2 milliards d'euros**.

EDITO DE PATRICE CAINE

Les nouveaux visages de la menace cyber

Le risque cyber n'a jamais été aussi élevé qu'aujourd'hui. La crise sanitaire et la situation en Ukraine ont encore intensifié le rythme, l'ampleur et le nombre des attaques. Or, cette dynamique qui constitue un danger grandissant pour nos économies, notre vie démocratique et notre vie quotidienne, n'est hélas pas prête de s'interrompre. Au contraire, la vigueur de la menace cyber est soutenue par plusieurs raisons de fond.

D'abord, la menace croît de façon presque mécanique à mesure que la transformation numérique poursuit son déploiement. Télétravail, diffusion du Cloud, multiplication des objets connectés… plus le monde est en réseau, plus la surface attaquable est grande.

La menace augmente également en raison de la très forte rentabilité de la cybercriminalité. Ces dernières années, le rapport coûts / bénéfices tend à être de plus en plus favorable pour les criminels. La dernière édition du ***Thales Data Threat Report***, publié en mars 2022 le confirme : une entreprise sur cinq est prête à payer en cas d'attaque par ransomware. Si bien que le cybercrime génère désormais 3 fois plus de revenus au niveau mondial que la drogue[1], alors même que cette activité est bien moins risquée et plus facile d'accès. Les enjeux sont colossaux, le coût global de la cybercriminalité entre 2020 et 2025 se calcule en milliers de milliards de dollars.

Un autre paramètre stimule la cybercriminalité : la montée de la conflictualité à l'échelle globale. Le domaine cyber constitue un domaine de confrontation entre puissances comme sur les théâtres d'opérations terrestres, navals ou aériens. Mais son fonctionnement est très spécifique.

Les nouveaux visages de la menace cyber

Comme nous le révèle le **Thales Cyber Threat Handbook**, les attaques y sont régulièrement conduites par des groupes privés agissant pour le compte d'acteurs étatiques, rendant encore plus floues les frontières entre opérations militaires et criminelles, entre état de paix et état de conflit. Les objectifs stratégiques comme le renseignement ou la déstabilisation vont ainsi de pair avec des objectifs de gains financiers pour les attaquants.
Enfin, la menace se renforce en raison de l'émergence de nouvelles technologies aux bénéfices multiples mais dont le potentiel est ou sera bientôt largement utilisé par les cybercriminels : c'est le cas de l'intelligence artificielle, de l'internet des objets, de l'industrie 4.0 ou encore des technologies quantiques par exemple.
Toutes ces évolutions géopolitiques, technologiques et économiques dessinent un paysage cyber très dynamique et dont les enjeux pour l'avenir de nos sociétés sont immenses. C'est ce qui nous a conduits à dédier à ce sujet la troisième édition des Thales Media Days.

Cet événement est l'occasion pour Thales de réaffirmer son ambition en matière de cybersécurité et de protection des données. Une ambition qui est au cœur de la raison d'être du Groupe car agir pour la cybersécurité, c'est contribuer de manière très directe à construire un avenir de confiance. C'est nous donner les moyens de tirer le meilleur parti des technologies pour créer un monde plus sûr, plus vert et plus inclusif.

Je vous souhaite un Thales Media Day riche en rencontres et découvertes.

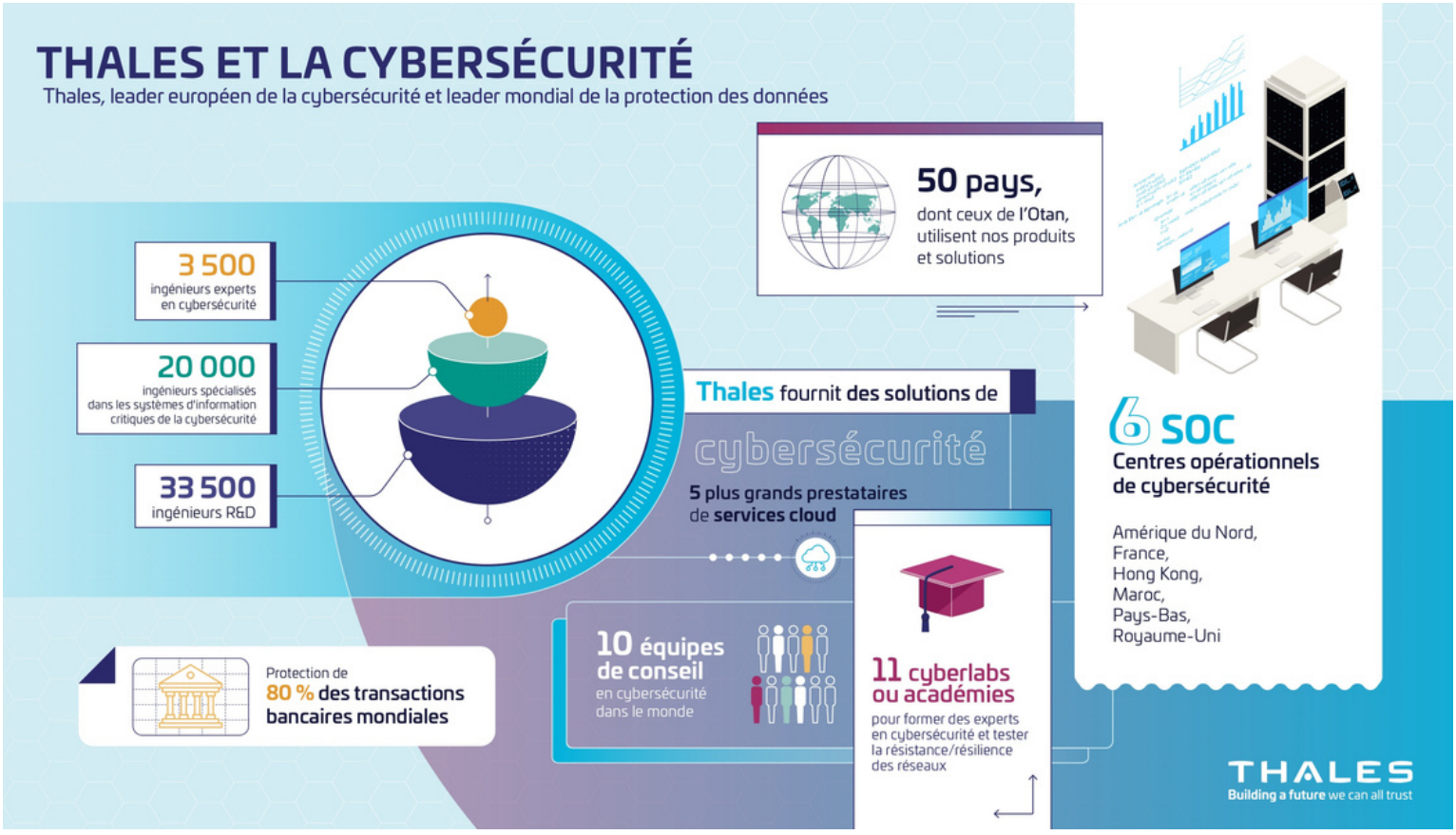
[1] Thales Cyber Threat Handbook 2020

PATRICE CAINE

THALES ET LA CYBERSÉCURITÉ

Thales dans le domaine de la cyber :

- Un portefeuille de solutions **Cybels** adressant les besoins d'évaluation des risques, d'entraînement et de simulation, de détection et de réponse aux attaques.
- Des produits dits de **souveraineté** comprenant l**e chiffrement et les sondes** pour protéger les systèmes d'information critiques.
- Une plateforme **CypherTrust** de protection des données, de sécurité du cloud et de gestion d'accès.



AGENDA

8:00 – 8:30

Accueil au Shack Paris Opéra

8:30 – 9:20 Session d'ouverture

Patrice Caine, Président - directeur général de Thales

Guillaume Poupard, Directeur général - ANSSI

9:20 – 9:30

Démonstration de l'Atlas des Cyber Attaquants

9:40 - 10:25

Première session de panels

10:35 - 11:20

Deuxième session de panels

11 :20 - 11 :30

Pause

11:30 – 11:55

Première session de démonstrations

12 :00 – 12 :25

Deuxième session de démonstrations

12:30 – 12:55

Troisième session de démonstrations

13 :00 – 13 :30 Clôture

Bernhard Quendt, Directeur technique de Thales

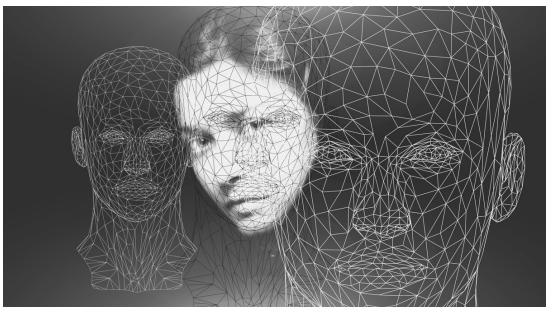
Marc Darmon, Directeur général adjoint, Systèmes d'Information et de Communication Sécurisés, Thales

13:30 – 14:30

Cocktail déjeunatoire

10 DÉMONSTRATIONS

organisées autour de 4 pôles



Identité

Infrastructures sensibles

Mobilité

Travail à domicile

PANELS DE DISCUSSION

De plus amples informations sont disponibles sur nos 5 tables rondes animées par nos experts Thales et des conférenciers extérieurs prestigieux, en lien avec les sujets cyber les plus brûlants du moment.

#1 Comment l'Europe fera-t-elle respecter sa souveraineté en matière de cybersécurité ?

présenté par Pierre-Yves Jolivet, (VP Cyber Defence Solutions, Thales), Pierre Jeanne, (VP, Cybersécurité Technologies et Solutions CTS, Thales), Marie-Liane Lekpeli, (Digital Economy Project Manager, Direction Générale des Entreprises), Luigi Rebuffi (Secretary General and founder of ECSO (European Cyber Security Organisation)

Depuis quelques années, et dans la continuité du nouveau plan Européen pour le numérique, **le positionnement de l'Europe a évolué en matière d'autonomie stratégique dans le domaine de la protection des données et de la cybersécurité**. Passant désormais à un concept assumé de souveraineté européenne en matière de cybersécurité. **Centres Européens de Cybersécurité**, directive NIS v2, développement des capacités de cyberdéfense et de renseignement sur les cybermenaces, stratégie de cybersécurité industrielle… De nombreuses initiatives sont aujourd'hui lancées ou à l'étude.

DGE DIRECTION GÉNÉRALE DES ENTREPRISES ECS EUROPEAN CYBER SECURITY ORGANISATION

#2 Disposons-nous aujourd'hui de la bonne technologie pour protéger les systèmes spatiaux ?

présenté par Massimo Mercati (Head of European Space Agency Security office), Silvia Diana (Bid Manager, Thales Cyber Defence Solutions) Sylvain Barbier (Cybersecurity product manager, Thales Cyber Defence Solutions) & Franck Perrin (Head of discipline Cybersecurity, Platform and Infrastructure, Thales Alenia Space)

Le domaine spatial se transforme. Dans ce panel, nous aborderons **la cybersécurité spatiale.** Nous verrons comment protéger les systèmes spatiaux des principales **vulnérabilités**, quelles sont les principales **menaces** pour les infrastructures spatiales et comment prévenir **les cyberattaques terroristes**.

esa European Space Agency ThalesAlenia Space

#3 Comment la cybersécurité permet-elle aux citoyens d'agir en toute sécurité dans leur vie quotidienne ?

présenté par Raphaël De Cormis, (VP, de l'innovation et de la transformation numérique et PDG de Thales Digital Factory), Claire Godron, (Directeur Transformation, Identity & Verification Solutions, Thales), Beatriz Matesanz, (Directeur de l'Innovation, Microwave & Imaging Sub-Systems, Thales), et témoignage de Phil Sealy (Research Director ABI Research)

L'une des conséquences de la crise sanitaire est **une numérisation accrue de la société et le changement de nos modes de vie**. Avec des solutions hautement protégées et cryptées, Thales accompagne ses clients dans **l'accélération de leur transformation numérique**. Cette révolution offre notamment des possibilités de croissance et de nouveaux services dans de nombreux secteurs. Les solutions de Thales peuvent vous simplifier la vie quotidienne, par exemple dans le domaine de la santé et des services d'identité numérique, tout en garantissant un haut niveau de sécurité.

#4 Comment les entreprises peuvent-elles protéger les données de leurs clients et de leurs employés ?

présenté par Thiebaut Meyer (CISO Director, Google Cloud) & Stéphane Lenco (VP Information Systems Security, Thales)

Nous évoluons aujourd'hui dans un monde où les données sont de plus en plus sensibles, où de nouveaux modes de collaboration sont apparus, et par association de nouveaux besoins en sécurité.
Le chiffrement devient une nécessité. Nous devons passer du risque - perte de données, hacking des données - à la sécurité. Les entreprises doivent disposer d'une infrastructure nécessairement sécurisée et résiliente. Le cloud est donc devenu un outil incontournable.

#5 Comment la cybersécurité peut-elle façonner mobilité durable et de confiance ?

présenté par Sébastien Gueremy, (Directeur Stratégie), Pierre Gachon (IT security Director, Renault) Christine Caviglioli (VP Automotive business, Thales)

Avec le développement des voitures connectées, des véhicules électriques et des aides à la conduite, **la cybersécurité est devenue une priorité pour l'ensemble de l'écosystème « mobilité »** ; appelant les constructeurs automobiles, leurs partenaires et les gouvernements à plus d'intégration de la chaine de confiance pour une meilleure résilience. La cybersécurité est donc intrinsèquement liée à la sécurité du véhicule, à la protection des actifs, des données, des utilisateurs, et, in fine à la confiance des gens dans les voitures connectées.

DÉMONSTRATIONS

Thales, au travers de ses solutions, démontre **comment la cybersécurité contribue positivement au quotidien des organisations et des entreprises**. Et surtout comment elle impacte la vie des citoyens, dans des domaines aussi variés que **l'identité numérique, les infrastructures critiques, la mobilité, la santé, l'espace, l'automobile, le travail à distance et la défense**.

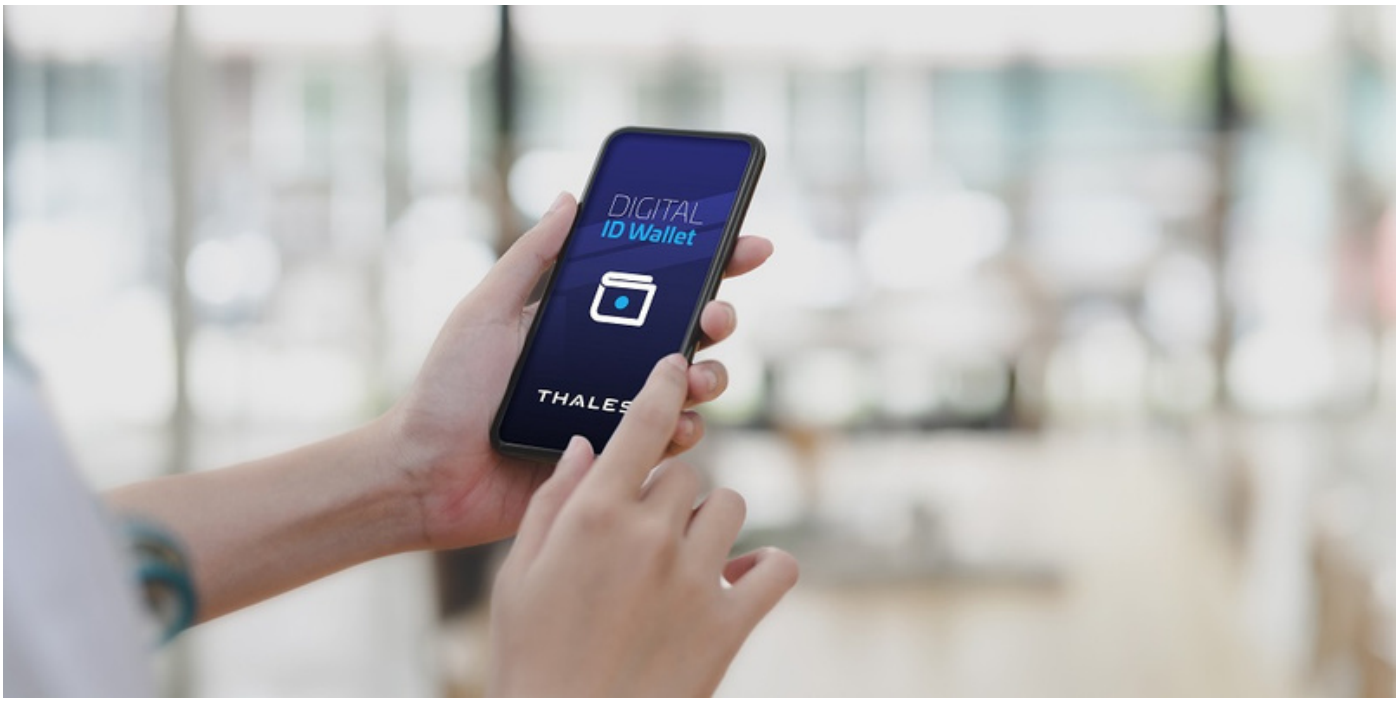
#1 Atlas Thales des Cyber Attaquants

présenté par Ivan Fontarensky (Technical Director Threat Intelligence, Thales) & Nicolas Quintin (Threat Analyst & Cert II, Thales)

Dans un monde ultra-connecté, on assiste à une augmentation considérable des **organisations cybercriminelles et des cyberattaques**.
En effet, la crise sanitaire a généré l'apparition de nouveaux vecteurs de **cybermenaces** : le recours accru au télétravail, l'augmentation des échanges à distance et la digitalisation de la plupart des secteurs d'activité.
Les conséquences sont sans précédent : **une augmentation de 37% des attaques a été observée entre 2020 et 2021 en Europe.**
Ainsi, nous observons une tendance constante à la sophistication croissante des cyberattaquants et une professionnalisation des modes opératoires à l'œuvre, motivée par la cupidité et les tensions internationales.

#2 Sécuriser mon identité numérique

présenté par Kristel Teyras (responsable marketing ligne de produits, Services d'identité numérique chez Thales)



Fournir à chacun **une identité numérique sécurisée** devient essentiel pour moderniser les États et dématérialiser les services publics (permis de conduire, immatriculation du véhicule, informations médicales, etc.).

Aujourd'hui, l'Australie et la Floride utilisent déjà ce type de solution. D'ici **septembre 2023**, tous les pays membres de l'UE devront procurer un **portefeuille d'identité numérique** à leurs ressortissants qui le souhaitent. Le portefeuille d'identité numérique Thales appartient à la nouvelle génération de l'ID mobile. Il héberge sur **smartphone**, en toute sécurité, l'ensemble des pièces d'identité numériques de son propriétaire.

#3 Renforcer la cyber-résilience des Technologies Opérationnelles (OT) telles que celles des usines

présenté par Dene Yandle (Automation Industrial Controls Engineer) & Adam Jefferies (Cyber & Network Technician, Thales)

Les cyberattaques contre les cibles du **secteur des services publics** et de **l'énergie ont augmenté de 32 % en 2021** et cette tendance devrait s'accentuer.

Thales, en partenariat avec le **National Digital Exploitation Centre (NDEC)** situé dans le Pays de Galles au sein du Thales Ebbw Vale, dispose d'un centre de formation dédié à la cybersécurité. Le NDEC permet de mettre en évidence la vulnérabilité des systèmes de contrôle industriels face aux cyberattaques, notamment au sein des infrastructures nationales critiques.
En plus de travailler avec de grands clients/partenaires mondiaux, le NDEC soutient les PME et la recherche universitaire galloises, ce qui permet à Thales de disposer d'un fort ancrage dans les « Tech Valleys » du sud du Pays de Galles.

National Digital Exploitation Centre
Canolfan Ecsbloetio Ddigidol Genedlaethol

#4 Simuler des cyber attaques sur des infrastructures majeures pour mieux comprendre les risques

présenté par Eric Weber, (Marketing Manager CTS, Thales), Guillaume Prigent (President and Co-founder, Diateam) & Nicolas Diaz (Communication & Cyber Projects, Diateam)

L**es cyber attaques ont pour cible privilégiées les infrastructures sensibles** : les utilisateurs ne peuvent plus accéder à leurs services numériques habituels et généralement, un paiement anonyme en ligne leur est demandé pour que l'accès soit rétabli.

Pour appuyer efficacement nos clients face à la menace cyber, nos experts Thales ont élaboré une offre de formation complète, **Thales Train & Experiment**, basée sur la pratique en immersion et en situation réelle. Dans ce cadre, Thales avec son partenaire **DIATEAM,** proposent un entrainement sur un jumeau numérique réaliste d'un port maritime, où les cybercriminels vont violer l'ensemble du système et causer des dommages et des pertes économiques. Les équipes Thales Train & Experiment **collaborent avec des cyberlaboratoires et des académies dans le monde entier**. Les cyber labs et académies capitalisent sur une **Cyber Range – Powered by DIATEAM** – un environnement virtuel qui permet aux organisations de simuler des cyber crises et des cyber attaques réalistes. Accessible partout dans le monde, elle est particulièrement adaptée pour les acteurs de **secteurs sensibles (gouvernements, défense, industries…**) mais aussi pour les scientifiques dans le cadre de leurs recherches.

#5 Détecter des attaques cyber sur des systèmes spatiaux

présenté par Silvia Diana (Bid Manager, Thales Cyber Defence Solutions) Sylvain Barbier (Cybersecurity product manager, Thales Cyber Defence Solutions) & Franck Perrin (Head of discipline Cybersecurity, Platform and Infrastructure, Thales Alenia Space)

Les activités humaines sur Terre sont de plus en plus dépendantes des systèmes spatiaux pour **les communications, la navigation, les prévisions météorologiques, la surveillance du climat, la gestion des pêches, la production agricole**... Les satellites sont des infrastructures critiques et l'analyse des cyberattaques récentes montre qu'elles ont **un impact direct sur la vie des citoyens et sur d'autres infrastructures critiques** - perte du signal GPS, perte des communications, etc. **Thales et Thales Alenia Space** proposent des solutions qui permettent de détecter des attaques cyber sur des systèmes spatiaux.

#6 Apporter la cyberfurtivité aux entreprises grâce à la technologie Darknet

présenté par Guillaume-Alexandre Chaizy-Gostovitch (CEO, Chimere by Thales), Gabriel Ladet (Chief Technical Officer, Chimere by Thales) & Marine Accart (Business Developer, Chimere by Thales)

L'exposition des services sur Internet est la cause de plus d'**1/3 des compromissions des systèmes d'information**. Avec les cyber-attaques et leurs problématiques, la **cyberfurtivité** est la clé pour sécuriser les applications des entreprises et des organisations, le tout avec une utilisation éthique de la technologie darknet. La startup interne **Chimere by Thales** a développé une solution de cybersécurité, en utilisant la **technologie darknet** dans le but de cacher les services et les applications aux yeux des hackers.

CHIMERE BY THALES

par la Digital Factory

Le Groupe Thales, acteur reconnu dans le secteur de la cybersécurité et à la pointe de l'innovation, soutient le développement de startups, incubées dans le programme Startup Studio de la Thales Digital Factory.

Lancé en Juillet 2017, **Thales Digital Factory** est le catalyseur d'innovation de Thales. Notre mission est d'accompagner le Groupe dans sa croissance à **l'ère du numérique à travers le développement de plateformes Cloud, la digitalisation de nos offres business, l'open innovation avec des startups** dans les domaines de la cybersécurité et de l'intelligence artificielle, et de la montée en compétence des **80 000 salariés du groupe** sur tous les sujets du numérique, qu'ils soient **technologiques, business ou culturels**. Nous employons 260 personnes répartis sur 3 sites : Montréal, Paris et Singapour.

THALES DIGITAL FACTORY

CHIMERE — PROTECT WITH HACKERS TECHNOLOGY

THALES
Building a future we can all trust

Mobilité

#7 Interagir avec votre voiture via une clé numérique installée sur un smartphone

présenté par Florent Abat (Product Solutions Marketing director, Digital Identity Services at Thales)

Les voitures sont plus connectées que jamais et **l'écosystème automobile** mondial évolue rapidement vers la **mobilité intelligente**. La **cybersécurité** et **la simplicité d'utilisation** sont donc toujours plus importantes.
C'est pourquoi Thales propose une **solution sécurisée** de bout en bout pour les acteurs du secteur automobile cherchant à mettre en œuvre la dernière spécification en matière de clés numériques du **Car Connectivity Consortium**. Grâce aux clés numériques Thales, on peut désormais verrouiller/déverrouiller son véhicule ou encore démarrer son moteur très facilement et de façon entièrement sécurisée **via son smartphone** ou tout autre appareil mobile.

#8 Connectivité cybersécurisée des aéronefs

présenté par Ludovic Simon (New business explorer & Flight Operations Services expert,Thales) & Nathalie Feyt (Cybersecurity Director for Avionics activities, Thales)

Les cyberattaques visant **les compagnies aériennes** sont de plus en plus nombreuses, **775 en 2020, contre 45 en 2019**. En parallèle, les avions sont de plus en plus connectés pour permettre de nouvelles fonctionnalités comme le téléchargement à distance.
Or, c'est aussi la porte ouverte aux **cybermenaces**. Le **cyberdétournement** d'avion est-il déjà une réalité, ou encore une fiction ? Face à ces menaces, les acteurs du secteur du transport aérien s'engagent dans une **révolution numérique** dont la cybersécurité est la clé de voûte. Thales place **la cybersécurité aéronautique** au cœur des réseaux et des applications de demain. Avec sa nouvelle solution **FlytLink Cyber Gateway**, bien plus qu'un produit pour les nouvelles opérations aériennes, Thales propose un service complet de maintien condition de cybersécurité des avions connectés.

#9 Nouvelle solution Thales de travail collaboratif dans le cloud, pour travailler sur des sujets « Diffusion Restreinte »

présenté par Romain Waller (Business Unit Director, Ercom Secure Digital Communications Thales / Ercom) & Laurent Theringaud (Head of Strategic alliances, Marketing & Communication, Thales / Ercom)

Avec la croissance des **besoins de travail collaboratif autour de données sensibles sur le cloud**, offrir les outils nécessaires avec le meilleur niveau de sécurité devient un enjeu majeur pour l'avenir **des entreprises et des collectivités**.

Avec **Thales Cybels Hub DR**, première plateforme collaborative homologuée pour traiter des informations de niveau « Diffusion Restreinte », vous aurez accès à de nouveaux modes de travail hybrides grâce aux services fournis par Cybels Hub DR : messagerie, visioconférences et audioconférences, partages et échanges autour de fichiers. Le travail collaboratif est désormais accessible aux utilisateurs les plus exigeants !

ERCOM
a Thales company

#10 Sécurisation du télétravail et chiffrement de la donnée : exemple appliqué à Google Workspace

présenté par Nicolas Aneas (Solution engineer manager, Thales) & Pierre-Yves Jolivet (VP Cyber Defence Solutions, Thales)

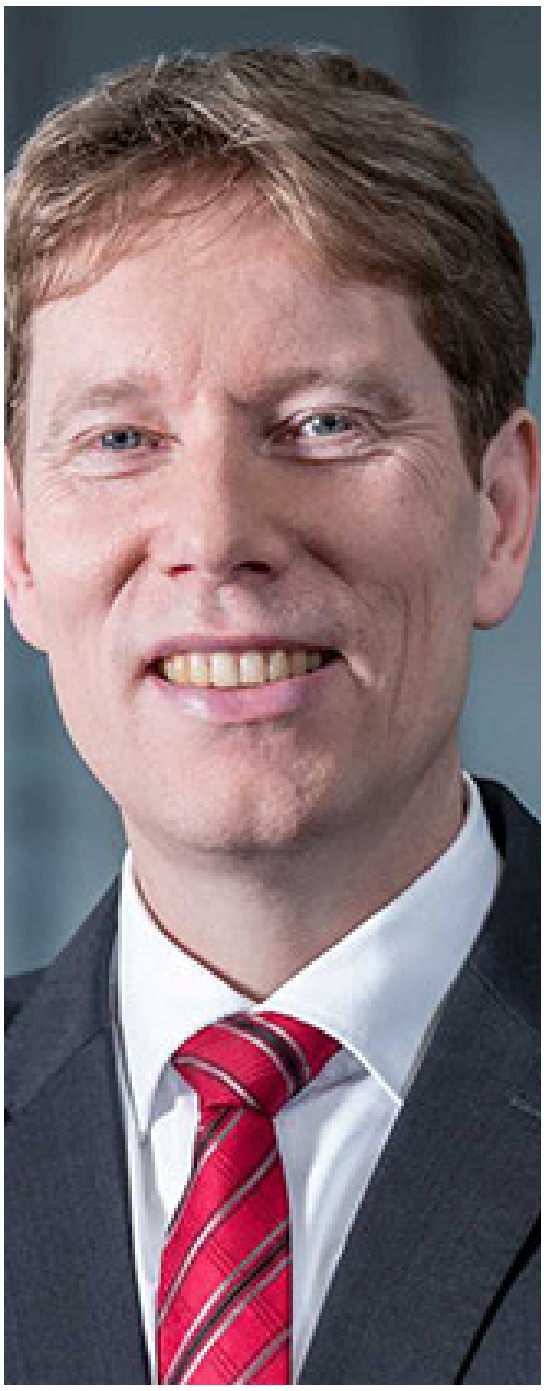
Les cyberattaques sont de plus en plus nombreuses et ont même augmenté pendant la pandémie. **Le travail à distance et la transformation cloud** ont déplacé les risques de sécurité au-delà du périmètre informatique d'une entreprise.

Les données sensibles sont désormais réparties dans des services et applications basés sur le cloud, auxquels les employés peuvent accéder de n'importe où.

Thales aide les entreprises à sécuriser et à contrôler l'accès aux données et aux applications, pour tout utilisateur et en tout lieu, via une bonne gestion de clés de chiffrement et une protection accrue de l'identité, permettant aux employés de travailler à distance et en toute sécurité avec une plateforme cloud de collaboration.

BERNARD QUENDT

IA et cybersécurité, deux technologies interdépendantes pour notre futur



DIRECTEUR TECHNIQUE DE THALES

Un invité surprise a décidé de s'inviter pour conclure cette troisième édition des Thales Media Days consacrée à la cybersécurité. Laissez-moi vous le présenter, c'est une vieille connaissance de Thales, il s'agit de l'intelligence artificielle (IA). Et puisqu'il m'appartient en tant que Chief Technology Officer de regarder l'horizon plutôt que nos côtes, si nous voulons savoir ce que le futur nous prépare, nous devons nous pencher sur cette technologie du futur. Il s'agit d'un futur déjà proche dans certains secteurs. En effet, nous constatons déjà les bienfaits de l'IA qui améliore considérablement la cybersécurité et j'ajouterais que la cybersécurité est essentielle pour protéger les systèmes basés sur l'IA. On peut ici véritablement parler d'interdépendance entre cyber et IA.

Pendant la dernière décennie, nous avons été les témoins de plusieurs succès de l'IA dans notre quotidien, pour activer nos smartphones, fournir une analyse des données du patient en soutien au corps médical, aider à la maintenance prédictive des équipements des armées, permettre l'avènement du véhicule autonome ou encore se mesurer aux capacités humaines dans des jeux de logique.

Derrière ces exemples très concrets se cache une évolution notable : **nous sommes passés de la révolution de l'automatisation à celle de l'autonomie**, des systèmes automatisés à qui l'on demandait des actions préalablement enregistrées (exemple : un métro automatique suivant une programmation) à des systèmes autonomes, capables d'apprendre, et d'établir leurs propres objectifs (une voiture autonome, capable de réagir elle- même à un événement comme un obstacle imprévu).

BERNARD QUENDT

IA et cybersécurité, deux technologies interdépendantes pour notre futur

A mesure que les systèmes deviendront de plus en plus autonomes, et que la puissance de la 5G accélérera leur développement, **la cybersécurité deviendra elle-aussi de plus en plus nécessaire et se devra d'être autonome à son tour. Il s'agit d'une cybersécurité se déclenchant de sa propre initiative lorsqu'une vulnérabilité est détectée.**

Pourquoi ? Du fait des multiples détournements qu'offre ce nouveau terrain de jeu pour les cyberattaquants. Un système de reconnaissance d'image peut être trompé. Un cyberattaquant peut entrer dans le système de reconnaissance d'incendie d'un drone empêchant l'intervention des pompiers, dans le système de reconnaissance de plaque d'un véhicule, engendrant un accident. Il peut même accéder à la formule algorithmique d'un système de sécurité d'une infrastructure sensible pour mieux déterminer le pourcentage de reconnaissance d'un type de drone par rapport à un autre et ainsi déterminer son mode opératoire et préparer son attaque. Une fois le système pénétré, le cyberattaquant peut aussi tout simplement remplacer l'IA en place par une version corrompue.
Dès lors, quelles solutions peuvent nous prémunir de telles attaques, souvent invisibles ? Il existe désormais des solutions de watermarking qui consistent à marquer les modèles d'apprentissage automatique pour les identifier, les tracer et vérifier leur intégrité avant utilisation.
Thales développe également sa **Battle Box**, un ensemble d'attaques et de contre-mesures adressant les menaces sur l'IA. Ce dispositif vise à renforcer la robustesse d'une IA pour préserver la confidentialité, l'intégrité et la disponibilité des systèmes intelligents. Chez Thales, nous partageons ces connaissances dans le cadre du programme national Confiance.ai, le collectif ayant pour objectif de concevoir et industrialiser des systèmes à base d'IA. C'est grâce à des connaissances et des bonnes pratiques partagées que nous constituerons un véritable écosystème en capacité de lutter contre les détournements de l'IA.

Rappelons toutefois que l'IA n'est pas qu'une menace. Elle ouvre aussi d'immenses opportunités pour améliorer **nos vies quotidiennes** : mobilité, qualité de vie, accès aux soins, optimisation des ressources, concentration de l'humain sur des tâches à plus haute valeur ajoutée. Aujourd'hui, les décideurs politiques et les scientifiques font face à des menaces et à la désinformation qui se propagent si facilement sur le web et qui tentent parfois d'affaiblir l'action publique. La confiance en la science reste primordiale pour relever les défis de nos sociétés actuelles : la stabilité dans le monde, le réchauffement climatique, l'accès pour tous aux ressources fondamentales de manière durable.

L'IA et la cybersécurité font partie des solutions et nous sommes déterminés, chez Thales, à en exploiter le plein potentiel.

MARC DARMON

Cybersécurité : servir 130 grands clients dans le monde nous engage

DIRECTEUR GÉNÉRAL ADJOINT, SYSTÈMES D'INFORMATION ET DE COMMUNICATION SÉCURISÉS, THALES

« On ne progresse pas dans le domaine de la cybersécurité **sans partager en toute confiance et sécurité avec son écosystème** des données qui nous permettent à tous, collectivement, de renforcer notre capacité à maîtriser le risque numérique. C'est la raison pour laquelle nous avons rejoint une initiative fondamentale pour nourrir la synergie entre entreprises et acteurs publics, celle du Campus Cyber, situé à Paris La Défense. Ce lieu totem du savoir-faire international en matière cyber a été inauguré en février 2022 par le Ministre français de l'Economie et des Finances, et de la Souveraineté industrielle et numérique, Monsieur Bruno Le Maire. Nous sommes heureux d'y avoir installé une soixantaine de spécialistes cyber de Thales pour travailler sur des projets communs, avec l'ANSSI ou encore d'autres entreprises du secteur.

La cyber requiert une force de frappe pour pouvoir adresser l'ensemble des problématiques de détection, d'identification des menaces, de réponse et de résolution des incidents et de prévention. Aujourd'hui, la cyber est un domaine en constante évolution, où Thales souhaite se renforcer et asseoir son leadership en Europe. C'est dans cette perspective que s'inscrit l'acquisition de deux pépites européennes de la cyber, S21sec et Excellium, au sein de la famille Thales. Ce rachat a été annoncé il y a quelques semaines et s'inscrit dans la continuité d'une stratégie de long terme et il constitue notre sixième acquisition dans la sécurité numérique au cours des dernières années, en particulier après l'achat de Gemalto et de Vormetric.

A mesure que la surface de vulnérabilité croie, la menace croie et avec elle la prise de conscience des risques. A ce titre, nos équipes de Threat Intelligence ont pu élaborer et mettre à disposition du plus grand nombre un formidable **Atlas des cyberattaquants**. Cet atlas participe à la connaissance plus fine des menaces et du profil des attaquants, de leur origine, de leur organisation, de leur mode opératoire. A la lumière de ces études et du monitoring constant que nous effectuons pour nos clients, nous avons construit une offre de solutions robustes **autour de trois grandes familles de produits** :

MARC DARMON

Cybersécurité : servir 130 grands clients dans le monde nous engage

DIRECTEUR GÉNÉRAL ADJOINT, SYSTÈMES D'INFORMATION ET DE COMMUNICATION SÉCURISÉS, THALES

- **Un portefeuille complet de services**, Cybels, adressant les besoins d'évaluation des risques, d'entraînement et de simulation, de détection et de réponse aux attaques ;
- Des **produits dits de souveraineté** comprenant le chiffrement et les sondes pour protéger les systèmes d'information critiques ;
- **Une plateforme de protection des données**, de sécurité du cloud et de gestion d'accès.

Nous servons ainsi plus de 130 grands clients dans le monde, des gouvernements, des opérateurs d'importance vitale, des administrations, 19 des 20 plus grandes banques mondiales, 9 des 10 géants mondiaux de l'internet mais aussi plusieurs milliers d'entreprises.
Thales est aussi une entreprise de défense et nous assurons la cybersécurité des systèmes critiques de 50 pays et de leurs armées. Nous fournissons par exemple à l'OTAN un système cybersécurisé de tenue de situation opérationnelle. Dans le domaine spatial, nous sécurisons aussi les systèmes satellitaires de Galileo, le système européen de navigation par satellite, à l'importance stratégique.

La cybersécurité intègre chacun de ses trois piliers de croissance de Thales : l'aéronautique civile et l'espace, la défense et la sécurité, l'identité et la sécurité numérique. Nous opérons dans tous les milieux, air, terre, mer, espace et cloud. La cybersécurité est une activité au cœur de notre stratégie, la développer est engagement pour nos clients, pour un avenir en toute confiance.

MARC DARMON

Thales Media Day

Contacts

Chrystelle Dugimont (+33 6 25 15 72 93)

Anne-Sophie Malot (+596 696 02 71 26)

Marion Bonnet (+33 6 60 38 48 92)

Inès Samama (+33 7 8236 32 79)

THALES

Building a future we can all trust