Stratégies d'optimisation de la sécurité informatique

Construire une politique de cybersécurité adaptée aux menaces de demain

Hôtel Pullman Montparnasse, Paris, France

29 – 31 Mars 2017

> Il faut très **certainement repenser** Internet et les réseaux numériques de **communication** comme un véritable territoire à **sécuriser**.
>
> Eric Freyssinet

Atelier Interactif 31 Mars 2017

Gouvernance de la cybersécurité : Gérer la question de la quantification du risque cyber

Atelier animé par :

Benedicte Suzan
Senior Prospective Analyst
Airbus Defense and Space

Eric Savignac
Responsable IMSEC
Airbus Defense and Space

Philippe Cotelle
Head of Risk Management and Insurance
Airbus Defense and Space

Session Interactive

Faire collaborer les directions techniques et de sécurité informatique pour assurer la protection du patrimoine

Les Etudes de Cas Présentées vous Aideront à

- **Protéger** les données et les opérations de l'entreprise face aux risques informatiques
- **Evaluer et Quantifier** le niveau et l'impact des risques
- **Inclure** en amonts les problématiques de cyber sécurité
- **Sensibiliser** l'ensemble des parties prenantes de l'outil informatique sur les questions de sécurité
- **Gérer** le temps investi sur les maintenances et créer un cycle de vie sécurisé

Président de séance 1er jour

Jean Christophe Denis
Manager IT IOT Services Delivery Europe and West Africa
Rio Tinto

Président de séance 2eme jour

Yannick Fourastier
Industrial systems design & cybersecurity
Airbus Group

Panel d'Experts

Yannick Fourastier
Industrial systems design & cybersecurity
Airbus Group

Benedicte Suzan
Senior Prospective Analyst
Airbus Defense and Space

Jean Christophe Denis
Manager IT IOT Services Delivery Europe and West Africa
Rio Tinto

Julien Taste
Cloud architect and Data scientist: IOT, Scada
SNEF

Philippe Loudenot
Fonctionnaire de sécurité des systèmes d'information
Ministères chargés des affaires sociales

Jean Philippe Gaulier
Chief Information Security Officer
Orange Group

Fabrice Hatteville
Cybersecurity Evangelist
Thales

Florent Kirchner
Cybersecurity Program Director
CEA Tech

Eric Savignac
Responsable IMSEC
Airbus Defense and Space

Philippe Dewost
Directeur Adjoint, Mission « Programme d'Investissements d'Avenir »
Caisse des dépots **Pascal Tigreat**
Membre du CA
Smart Building Alliance for the Smart Cities

Philippe Cotelle
Head of Risk Management and Insurance
Airbus Defense and Space

Christophe Jouvray
Software Expertise Engineer - Cybersecurity
Valeo

Guillaume Rossignol
Head of CyberSOC Continental Europe
BT Security

Joaquin Garcia-Alfaro
Professeur
Télécom SudParis

Alain Bouillé
Président
CESIN

Pierre-alexis Saint-michel
Conférencier en cybersecurité

Benjamin Venelle
Cybersecurity Expertise Engineer
Valeo

marcusevans® conferences

Première Journée

Mercredi 29 Mars 2017

08.30 Accueil et Café

09.00 Discours du Président de Séance

Jean Christophe Denis
Manager IT IOT Services Delivery Europe and West Africa
Rio Tinto

LA SECURITE INFORMATIQUE DANS L'ENTREPRISE DYNAMIQUE

09.10 Étude de cas

Assurer la sécurité de la transformation digitale des infrastructures vers un modèle Smart Building

- Présentation des architectures pour rendre son bâtiment connecté en assurant sa cybersécurité
- Un bâtiment connecté pour quels services aux usagers et quel confort.
- Comment accéder aux DATAS et aux équipements
- Un bâtiment connecté source de valeurs

Pascal Tigreat
Membre du CA
Smart Building Alliance for the Smart Cities

09.50 Étude de cas

Mettre en place un SOC centralisé

- Approcher par l'étude des risques
- Centraliser les outils de suivi, de détection, de réponse, et de défense des incidents dans une même organisation
- Atteindre un équilibre entre la taille et l'agilité pour maximiser l'efficacité de la mission du SOC
- Implanter les systèmes de détections et de collection des données aux bons endroits

Guillaume Rossignol
Head of CyberSOC Continental Europe
BT Security

10.30 Refreshme

CONSTRUIRE UNE ARCHITECTURE "INDUSTRIAL INTERNET OF THINGS" SECURISE

10.50 Étude de cas

Sécuriser le cloud of things

- Répondre à la complexité de la sécurité des réseaux M2M
- Élaborer une approche cartographique de la sécurité de l'IIOT
- Contenir le risque grâce aux sandbox
- Sécuriser l'interconnexion avec les autres types de systèmes

Jean Christophe Denis
Manager IT IOT Services Delivery Europe and West Africa
Rio Tinto

11.30 Étude de cas

Détecter et sécuriser des attaques les IIOTs

- Développer des « Intrusion Detection Solutions » de sécurité adaptée à différent type d'IIOT
- Détecter et signaler le trafic anormal et les accès non autorisé
- S'adapter à l'évolution des attaques
- Surveiller et détecter les vulnérabilités

Julien Taste
Cloud architect and Data scientist :IOT, Scada
SNEF

12.10 Déjeuner

14.00 Étude de cas

Construire des systèmes de transports intelligents sécurisés

- Retours d'expériences du projet collaboratif CTI (Cybersécurité dans les Transports Intelligents)
- La cybersecurité dans trois domaines d'application que sont l'automobile, le transport ferroviaire et l'aéronautique
- Limiter l'impacte de la cybersecurité sur la sûreté de fonctionnement.

Christophe Jouvray
Software Expertise Engineer - Cybersecurity
Valeo

Benjamin Venelle
Cybersecurity Expertise Engineer
Valeo

GESTION DE LA GOUVERNANCE DES SYSTEMES D'INFORMATION ET DE LA CYBERSECURITE

14.40 Étude de cas

Flexibiliser les questions de cybersécurité dans le développement de projet

- Prendre en compte les besoins de sécurité en amont et tout au long du cycle projet
- Intégrer le « secure-by-design » dans le développement agile
- S'appuyer sur une analyse de risques s'inscrivant dans un processus standardisé et reproductible
- Quelles sont les pistes d'action pour obtenir une assurance sécurité intégrée, dite « built-in », alignée sur les objectifs stratégiques

Yannick Fourastier
Industrial systems design & cybersecurity
Airbus Group

15.20 Refreshme

SESSION INTERACTIVE

La salle sera divisée en quatre groupes, un leader désigné dans chaque table ménera les débats

15.40 **Faire collaborer les directions techniques et de sécurité informatique pour assurer la protection du patrimoine**

Table Un
Collaborer dans l'élaboration des politiques de sécurité

Table Deux
Développer les processus en commun pour assurer la maintenance de la sécurité du patrimoine

Table Trois
Rationaliser et coordonner les méthodes et mécanismes de reporting

Table Quatre
Expliquer les principes de l'hygiène informatique et les bonnes pratiques aux équipes industrielles

Yannick Fourastier
Industrial systems design & cybersecurity
Airbus Group

16.40 Fin du premier jour et commentaire du Président de Séance

Deuxième Journée

Jeudi 30 Mars 2017

08.30 Accueil et Café

09.00 Discours du Président de Séance

Yannick Fourastier
Industrial systems design & cybersecurity
Airbus Group

LA CYBERSECURITE : UN MONDE EN MOUVEMENT

09.10 Keynote

La souveraineté numérique : L'impact de la géopolitique sur la cybersécurité des entreprises

- Souveraineté numérique, enjeux de guerre économique
- Souveraineté 2.0
- Les paradoxes en jeu

Philippe Dewost
Directeur Adjoint, Mission « Programme d'Investissements d'Avenir »
Caisse des dépots

09.50 Étude de cas

Baromètre de la cyber-sécurité des entreprises

- La transformation numérique vient bouleverser les enjeux de la cyber-sécurité
- Face aux cyber-risques, des solutions techniques à l'efficacité relative
- Construire la gouvernance de la cyber-sécurité pour demain

Alain Bouillé
Président
CESIN

10.30 Refreshme

ACCOMPAGNIER L'INNOVATION PAR LA CYBERSECURITE

10.50 Étude de cas

Mathématiques et raisonnements automatisés : les stratégies d'innovation face aux verrous de la cybersécurité

- Utiliser les mathématiques comme un outil de raisonnement pour la cybersecurité
- Transformer les éléments de la cybersecurité en règles mathématiques
- Fournir des garanties pour la défense et l'attaque grâce à des fondements mathématiques

Florent Kirchner
Cybersecurity Program Director
CEA Tech

SECURISER LES INFRASTRUCTURES SMARTS

11.30 Étude de cas

Sécuriser l'architecture des Smart City : Enjeux et Défis

- Qu'est-ce qu'une Smart City? Quel est le marché ? Quels sont les exemples de projets en cours ?
- Quels sont les enjeux de cybersécurité pour les Smart Cities ?
- Quelles sont les particularités à prendre en compte pour cybersécuriser une Smart City ?
- Quelle approche de cybersécuriser pour un projet de Smart City ?

Fabrice Hatteville
Smart City Evangelist
Thales

LA CYBERSECURITE FACE AUX CHANGEMENTS DE L'ENVIRONNEMENT TECHNOLOGIQUE

12.10 Étude de cas

La question de la donnée personnelle dans l'entreprise moderne

- Définir la donnée personnelle
- Qu'est ce qu'on doit protéger
- Choisir la technologie de stockage approprié
- Gérer la cryptographie pour les données personelles

Jean Philippe Gaulier
Chief Information Security Officer
Orange

12.50 Déjeuner

14.00 Étude de cas

Développer la cyberdéfense contre les attaques de type « Advanced Persistant Threats » : Sécurité des systèmes cyber- physiques

- Développement des compétences et connaissances sur les systèmes de contrôle-commande
- Identifier leurs problématiques sécurité, sûreté, résistance ...
- Représentation d'un système dynamique et complexe avec modèles théoriques
- Banc de test pour mettre en place les modèles, expérimenter et vérifier les résultats

Joaquin Garcia-Alfaro
Professeur
Télécom SudParis

14.40 Étude de cas

Sécuriser l'environnement informatisé dans le domaine médical

- Assurer la gestion des données de manière sécurisée
- Inclure le risque des objets médicaux dans le réseau
- Gérer la sécurité de la logistique automatisée

Philippe Loudenot
Fonctionnaire de sécurité des systèmes d'information
Ministères chargés des affaires sociales

15.20 Refreshme

BUDGETISER ET GERER LE FINANCEMENT DE LA CYBERSECURITE

15.40 Etude de cas

Développer la cyberdéfense contre les attaques de type « Advanced Persistant Threats »

- Etat de la menace actuelle vs niveau de maturité des entités
- Phasage de l'APT
- Méthodologie permettant de restaurer la confiance dans le SI et chasser l'attaquant Approche proactive permettant de limiter le risque d'attaque

Pierre-alexis Saint-Michel
Conférencier en cybersecurité

16.20 Fin du deuxième jour et commentaire du Président de séance

Atelier Interactif Conférence

Gouvernance de la cybersécurité : Gérer la question de la quantification du risque cyber

Vendredi 31 Mars 2017

09.00 Présentation des animateurs

09.10 Introduction des participants

Avant le début de la conférence, chaque participant aura l'occasion de se présenter brièvement et de partager ce qu'il attend de l'atelier, afin de faciliter la prise de contact et les échanges pendant la session.

09.30 **Gouvernance de la cybersécurité : Gérer la question de la quantification du risque cyber**

Construire la gouvernance de la sécurité des systèmes d'information dans une grande organisation est un véritable défi. En effet, ce dernier est primordial pour instaurer une relation de confiance entre les différentes parties prenantes qui interagissent avec l'entrepris. Comment peut-on construire une gouvernance adaptée ? Quels sont les pré-requis à sa mise en œuvre ? Quel sont les éléments qui entre en jeux du coté technique ? Quelle implication le département risk doit avoir dans cette gouvernance ?

09.50 **Point de vue technique**

Le pilotage et la gouvernance de la sécurité au quotidienne inclus également une vision opérationnelle sur :

- Les quantités d'incidents et d'anomalies par type
- Les vulnérabilités exploitables et le déploiement des correctifs
- L'avancement des projets sécurité
- L'adoption et l'efficacité des processus sécurité

10.10 **Point de vue Risk Management**

- Gerer la relation Capex/Opex en cybersecurité
- Utiliser le ROCE (Return on Capital Employed) pour évaluer l'efficative des programmes de cybersecurité
- Evaluer le cout assuranciel et optimiser les dépenses

10.30 **Exercice interactif**

11.30 Commentaires de l'Animateur

12.00 Fin de la conférence

Atelier animé par :

Benedicte Suzan
Senior Prospective Analyst
Airbus Defense and Space

Philippe Cotelle
Head of Risk Management and Insurance
Airbus Defense and Space

Eric Savignac
Responsable IMSEC
Airbus Defense and Space

A qui s'adresse la conférence

- VP Digital Security
- CISO/RSSI
- CIO
- CTO
- IT Security Experts
- IoT Security Engineer
- Cybersecurity Architect
- Cybersecurity Operation Manager
- Information Security Manager
- IT Project Manager
- Group Digital Security Expert
- IT Security Audit Manager

Possibilités de Développement Commercial

Votre entreprise offre des solutions ou technologies susceptible d'intéresser les participants de l'évènement? Si tel est le cas, vous pourrez obtenir plus d'informations sur nos formules de partenariat en contactant:

Virginie Vetil, Sponsorship Manager, **marcus evans** Barcelona
Tel: **+34 (0) 933 934 600,** E-Mail: **VirginieV@marcusevanses.com**