L'USINEDIGITALE EVENTS

CONFÉRENCE CYBERSÉCURITÉ

Comment protéger concrètement son entreprise en 2019-2020

25/06/2019 - PARIS

Pourquoi participer à cet événement

- Identifier et mettre en oeuvre les bonnes pratiques au service de la cyber résilience de votre entreprise
- Intelligence artificielle : comment discerner les vrais usages des discours marketing ?
- La cybersécurité à l'heure du digital : comment laisser vos équipes innover sans se mettre en danger ?
- Smart building, industrie 4.0... Pourquoi l'IoT est le grand défi cybersécurité des 20 prochaines années
- Bug bounty, red team, forensics : des approches concrètes pour la cyber protection de votre entreprise

Avec la présence exceptionnelle de

- CAPARROS Fabien
  Chef de la Division Méthodes de management de la sécurité numérique
  ANSSI
- GUILLOT Christophe
  Directeur Digital
  LABORATOIRES PIERRE FABRE
- LIGNEUL Olivier
  Directeur Cybersécurité du Groupe - Administrateur
  EDF - CESIN

Accueil des participants

ALLOCUTION D'OUVERTURE

Gérer le risque numérique en entreprise : anticiper pour ne plus subir !

Keynote – Les défis du RSSI multicloud

Développer les bonnes pratiques et les bons outils au service de la cyber résilience

TABLE RONDE

Pour protéger votre entreprise, commencez par appliquer les règles de base

- Appliquez les correctifs de sécurité pour déjouer les attaques les plus fréquentes
- Pourquoi il est essentiel de cartographier votre réseau
- Comment bien évaluer la menace touchant votre entreprise
- Comment identifier et réduire les risques liés à un environnement en évolution permanente

MOUAKHER Abir
RSSI
ENGIE DIGITAL

THOMAZEAU Laurence
Group Chief Information Security Officer - Group Data Protection Officer
AIR LIQUIDE

Qui participe à cet événement

- Directeurs stratégie, Directeurs Sécurité, DSI, RSSI, CDO, Data Protection Officers, CISO, Directeurs R&D, Directeurs Innovation, Directeurs de la technologie, Directeurs Technique... de PME, ETI et grands groupes

Tarifs

Tarif général	995,00 €HT

Profitez du meilleur des technologies pour votre SOC (Security Operation Center)

- L'intérêt du déploiement d'un SOC
- L'apport de l'Intelligence Artificielle et du Machine Learning
- Exploration d'un cas concret de déploiement client

Bug bounty et read team : des approches innovantes pour se préparer concrètement aux cyber-attaques

- Bug bounty, un levier de sécurisation des services ouverts vers l'extérieur : comment le mettre en œuvre concrètement dans son organisation
- Red team : pourquoi il faut penser comme l'attaquant pour mieux le contrer
- Comment réussir des exercices qui exigent la mobilisation de tous les niveaux de l'organisation

Forensics : comprendre ce qu'il s'est passé pour se rétablir plus vite et éviter les rechutes

- Les erreurs à éviter après une attaque pour ne pas perturber l'enquête
- Objectifs et moyens d'un foresincs interne/externe/ou à l'initiative des autorités
- Analyser les traces et conséquences d'une attaque pour réduire sa vulnérabilité

Pause

Surveillez et corrigez vos vulnérabilités dans les meilleurs délais

- Pourquoi faire une veille sur les vulnérabilités ?
- Cas de la vulnérabilité CVE-2019-0708 "BlueKeep"
- Mettre en place un processus complet de gestion des vulnérabilités avec Cyberwatch

---

LA CYBERSÉCURITÉ À L'HEURE DU DIGITAL : COMMENT LAISSER LES ÉQUIPES INNOVER SANS SE METTRE EN DANGER

TABLE RONDE

Comment concilier cybersécurité et innovation technologique ?

- Modèle américain, chinois, européen : que nous apprennent-ils ?
- RSSI, DSI, CDO... Qui gère quoi et comment ne pas se marcher sur les pieds ?
- SAFE-UX : réussir concrètement le couplage cybersécurité/nouveaux usages digitaux
- Open data, ouverture du SI vers l'extérieur : les pièges à éviter

---

Keynote - Cybersécurité : levier de valeur stratégique pour les COMEX

- Les cybermenaces ont pris une telle ampleur que leurs conséquences peuvent avoir un impact significatif sur la valorisation d'une entreprise
- Comment projeter les dirigeants dans la prise de conscience des enjeux et des impacts des risques ?

Déjeuner

SMART BUILDING, INDUSTRIE 4.0… POURQUOI L'IoT EST LE GRAND DÉFI CYBERSÉCURITÉ DES 20 PROCHAINES ANNÉES

Keynote : Threat Intelligence et géopolitique : comment anticiper le risque cyber ?

- Comment identifier les menaces les plus crédibles pour votre entreprise ? Comment évaluer les fréquences et impacts associés ?
- Comment simuler l'impact d'une solution de sécurité, et ainsi créer un programme d'investissement optimisé ?

Retour d'expérience : comment protéger efficacement les données dans le déploiement d'objets et solutions connectées pour le grand public

- Quels sont les enjeux de sécurité liés au cloud, à l'IoT, à la data ?
- Quels sont les vecteurs d'intrusions potentiels via ces objets et solutions ?
- Pourquoi il faut s'en préoccuper dès aujourd'hui ?

Industrie 4.0 : pourquoi la cyber protection est un prérequis indispensable ?

- Équipement industriel historique ou moderne, lequel est le plus vulnérable ?
- De l'approvisionnement à la distribution, pourquoi la cyber protection doit être globale ?

Retour d'expérience : Comment assurer la cybersécurité des véhicules connectés et autonomes ?

- Agir efficacement sur deux volets complémentaires pour assurer la sécurité des véhicules :
- Réduire les risques d'injection de malware lors de la mise à jour logicielle à distance
- Accompagner le développement des véhicules autonomes par une approche cybersécurité adaptée

Security by design : une approche difficile mais impérative

- Prendre en compte les impératifs de sécurité dès la conception d'un produit/application
- Enjeux et solutions réglementaires, technologiques et business

INTELLIGENCE ARTIFICIELLE, BLOCKCHAIN... SIMPLES BUZZWORDS OU VRAIS LEVIERS DE PROTECTION ?

Keynote - Intelligence artificielle : comment discerner les vrais usages des discours marketing ?

- Les apports de l'IA en matière de cybersécurité
- L'automatisation du point de vue des attaquants
- Les risques introduits par l'intelligence artificielle

Conclusion de la journée par la rédaction de l'Usine Digitale

Fin de journée