SERMA
SAFETY & SECURITY

Nouvelles offres numériques et sécurité

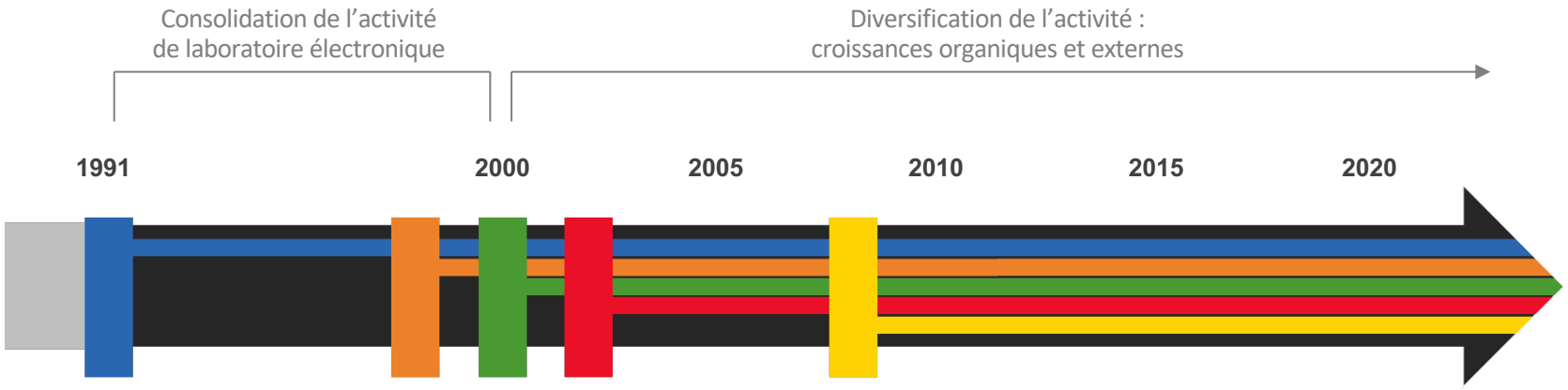
Club des ETI du 10 Mars 2021 – Lionel AGULHON

Le Groupe SERMA

En quelques slides…

SERMA
SAFETY & SECURITY

SERMA Group : 30 ans d'histoire, de croissance et de structuration



Structuration en 5 domaines d'activités stratégiques

Technologies de l'électronique

Sûreté et cybersécurité des systèmes

Ingénierie des systèmes embarqués

Micro-électronique

Énergie

Une offre complète - 5 domaines d'activité stratégiques

- Expertise
- Conseil & Audit
- Conception
- Assemblage
- Production
- Test et qualification
- Évaluation
- Build-to-spec/ Build-to-print
- MCO
- MCS
- R&D
- Formation

- **TECHNOLOGIES DE L'ÉLECTRONIQUE**
- **ÉNERGIE**
- **MICROÉLECTRONIQUE**
- **INGÉNIERIE DES SYSTÈMES EMBARQUÉS**
- **SÛRETÉ ET CYBERSÉCURITÉ DES SYSTÈMES**

Chiffres clés

1200
ingénieurs
et techniciens

20 sites
en France,
Allemagne et Tunisie

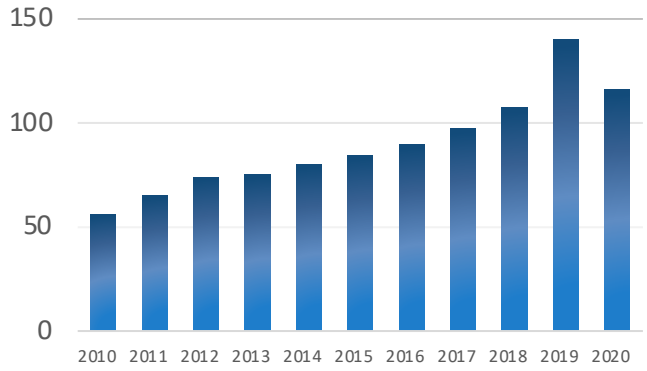
50 M€
moyens industriels

15 000 m² industriels
laboratoires, zone de
production, salle blanche,
plateaux d'essais

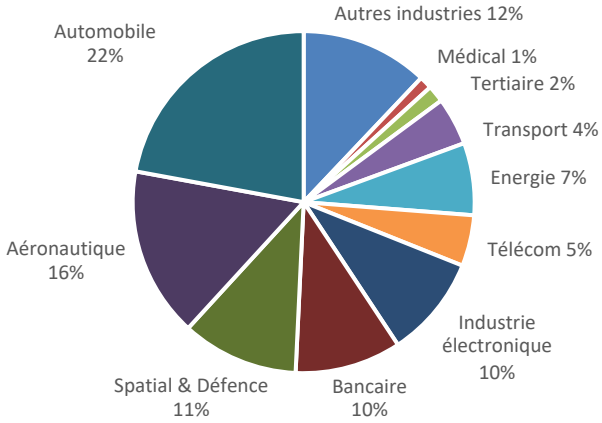
> 4 M€/an
Investissements R&D

Certifications,
qualifications
et agréments
qualité, sécurité et environnement

Un groupe en forte croissance (M€)



Un positionnement multisectoriel (% CA)



Serma Safety & Security (S3) : Cyber-sécurité et sureté des systèmes

Interlocuteur unique pour la sécurité des produits et systèmes

- Cybersécurité
- Laboratoire de sécurité (accrédité CESTI, FIPS, PCI et schéma privés)
- Sûreté de fonctionnement (système, matériel et logiciel)

Systèmes d'information | **Systèmes industriels** | **Systèmes IoT** | **Systèmes embarqués**

Conseil

- **Études** prospectives et cadrage
- **Schémas directeurs**, conformités, PSSI, PCA/PRA
- **Analyses de risques** et **audit** de maturité
- Intégration de la **sécurité dans tout le cycle de développement**
- **Accompagnement sûreté de fonctionnement**
- **Préparation à la certification**
- Conseil en **design sécurisé** (hard, soft, crypto)

Expertise

- Identification des **cibles de sécurité**
- Intégration de **solutions de sécurité**
- Étude de **sûreté de fonctionnement**
- Analyse de modules **cryptographiques**
- **Infogérance** des équipements de sécurité
- **Reverse engineering**
- **Formations** et **sensibilisation**

Évaluation

- **Audits :** Tests intrusion, audits archi/conf/code, PASSI, Redteam
- **Détection des alertes de sécurité** (SOC)
- **Audit du code** logiciel (qualité/sécurité)
- **Audit et évaluation** sûreté de fonctionnement
- **Évaluations sécuritaires** (nombreux schémas publics et privés)
- Outils de **test IoT** (Hardsploit)

Nouvelles offres numériques et sécurité

L’enjeux sur vos données

SERMA
SAFETY & SECURITY

Nouvelles offres numériques : De quoi parle t'on…

Les Services Hébergés

5G

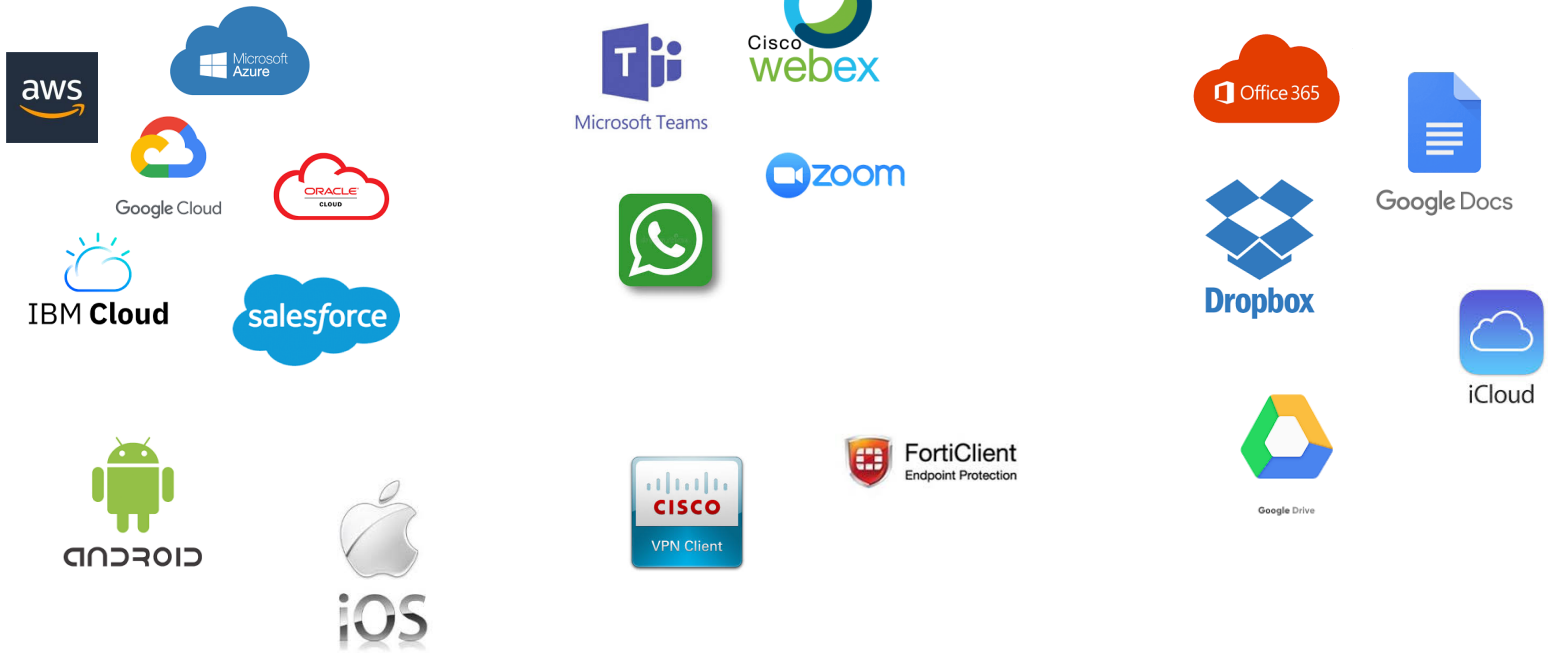
Le tout connecté

Les nouvelles sciences de la donnée

Intelligence Artificielle

La mobilité

Quelques exemples de produits et services



Point commun de tout ces services…

Ils sont américains

Petit rappel sur le cloud act

- Le Cloud Act est une loi fédérale promulguée le 23 Mars 2018 pour donner aux autorités américaines un accès aux données gérées par les sociétés Américaines de l'internet et du cloud, et ce même si elles sont stockées en dehors des USA.
- Une loi similaire existe depuis 2017 en Chine (Alibaba cloud)

- Ce contexte règlementaire ouvre la porte à des intrusions à des fins d'espionnage économique dans les données sensibles hébergées chez AWS, Google, Azure (Microsoft) qui dominent aujourd'hui le cloud public mondial. (exple the intercept)

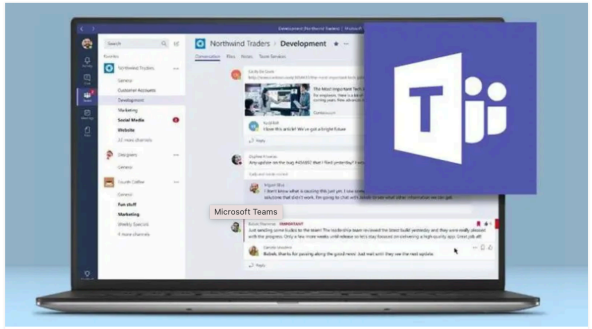
Health Data Hub : Les données sont désormais hébergées en région parisienne mais toujours par Microsoft

Le conseil de la Caisse nationale de l'assurance maladie maintient sa position réfractaire sur l'hébergement par Microsoft du Health Data Hub. Au coeur du problème : le Cloud Act, qui permet aux autorités américaines d'accéder à des données quelle que soit leur localisation. Mais pour Stéphanie Combes, à la tête du Heath Data Hub, il n'y a pas d'inquiétude à avoir étant donné que les données sont désormais stockées en "région parisienne".

Conséquence de ces offres sur la sécurité : la perte de contrôle

- **Services hébergés par un tiers**
  - Une perte de contrôle de la sécurité
  - Un transfert des responsabilités
- **Une expérience utilisateur enrichie**
  - Mais une surface d'attaques plus importantes
  - Une collecte des données personnelles (contenu, position, navigation…)
    - API google sur les terminaux android
    - Réseaux sociaux (modèle facebook : si c'est gratuit c'est vous le produit)
- **Externalisation des annuaires utilisateurs**
  - Criticité de la politique d'accès et de sa surveillance
- **Externalisation des données sensibles de l'entreprise**
  - Nécessité de cartographier et catégoriser les données
- **Services cible d'attaques « hors de contrôle »**
  - Obligation des hébergeurs / éditeurs de communiquer sur les attaques et vulnérabilités ?

Quelques exemples d’attaques sur les communications



Vulnérabilités

Microsoft Teams, un contournement de patch permet l’exécution de code à distance

11 août 2020 Aucun commentaire microsoft teams

Cisco webex

Vulnérabilités

Une faille de Webex permet d’espionner les réunions

25 novembre 2020 Aucun commentaire cisco, webex

Une vulnérabilité dans l’application de conférence Webex de Cisco pourrait permettre à un participant d’agir comme un «fantôme» lors de

Lire la suite

ESPIONNAGE

Une fausse appli WhatsApp mise au point pour les services secrets italiens

Le faux programme de WhatsApp permettait aux pirates d'obtenir l'UDID et IMEI des appareils infectés

06/02/21 1 42

Quelques exemples d’attaques sur les « objets » connectés

HACKERS

Des hackers piratent des Amazon Ring et harcèlent des familles

Quinze familles ont lancé des poursuites contre la filiale d’Amazon en raison d’une faille de sécurité

30/12/20 11 387

Vulnérabilités

Les appareils médicaux GE contiennent des failles critiques

14 décembre 2020 Aucun commentaire ge, hopitaux

Une paire de vulnérabilités critiques ont été découvertes dans des dizaines d’appareils radiologiques GE Healthcare dans les hôpitaux, ce qui

Lire la suite

Les failles TCP/IP Ripple20, un risque durable pour les dispositifs IoT Gratuit

le 25/06/2020, par Jon Gold / Network World (adaptation Jean Elyan), Sécurité, 805 mots

Un patch est disponible pour contrer Ripple20, mais la faille de sécurité affectant une bibliothèque TCP/IP utilisée par des millions de dispositifs IoT sera difficile à corriger.

Découverte la semaine dernière, la série de vulnérabilités critiques de sécurité réseau baptisée Ripple20 a secoué le monde de l'IoT. Si la faille de corruption de mémoire expose dangereusement les dispositifs IoT des entreprises équipées, elle est aussi difficile à résoudre. Découverte en septembre 2019 par l'entreprise de sécurité israélienne JSOF, la

L’espionnage industriel une réalité

DÉCRYPTAGES

L’affaire SolarWinds, une des opérations de cyberespionnage « les plus sophistiquées de la décennie »

Les contours de l’immense piratage commencent à peine à apparaître : les centres de pouvoir américains étaient le cœur de cible. La France ne déplore pas de victime à ce stade.

Publié le 27 janvier 2021 à 11h13 - Mis à jour le 27 janvier 2021 à 12h14 • Martin Untersinger

Piratage informatique : une faille chez Microsoft touche 30 000 organisations américaines

Selon un spécialiste de la cybersécurité, l’Etat chinois serait derrière cette attaque sur la messagerie Exchange du géant de l’informatique.

Publié le 06 mars 2021 à 03h51 - Mis à jour le 06 mars 2021 à 09h33 • Le Monde avec AFP

Quelques recommandations pour contrôler sa sécurité

- **Connaitre ses risques pour les maitriser**
  - Réaliser une/des analyses de risques
  - Ne pas hésiter à se faire accompagner
- **Identifier ses biens sensibles**
  - Les données
  - Les ressources critiques
  - Les points de faiblesses (SPOF)
- **Définir sa stratégie de sécurité**
  - La déployer
  - La « monitorer »
- **Penser aux plans de continuité**
  - Restaurations des moyens informatiques, données incluses
- **Faire évaluer sa sécurité régulièrement**
  - Audit
  - Pentest

Merci de votre attention !

Lionel AGULHON

Director of Serma Security Labs (SSL)

l.agulhon@serma.com

14 rue Galilée CS 10071 | 33608 Pessac Cedex, France

Mob :+33 6 68 36 94 32 | Tel : +33 5 57 26 08 64

http://www.serma-safety-security.com