Afterwork juillet 2022

Sommaire

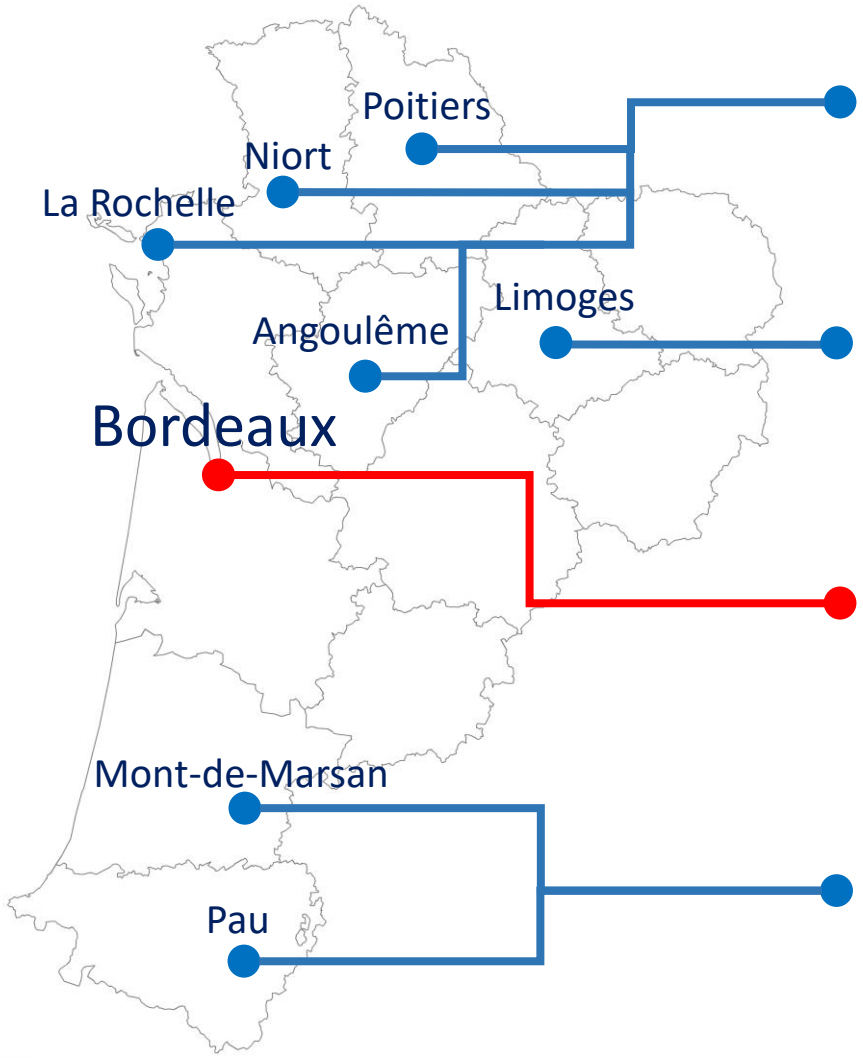
ACTU CNA

AFTERWORK: Comment Solidnames a initialisé une démarche d'amélioration continue de la SSI en s'appuyant sur une appréciation des risques, les difficultés rencontrées, les chantiers entrepris et notamment l'audit d'architecture AWS.

Anthony Don, Directeur associé chez Solidnames

Thierry Meyer, expert cyber
Cabinet Thierry Meyer Consultants

ACTU CNA: Antennes en région Nouvelle Aquitaine



Antenne Poitou-Charentes Responsable **Didier SPELLA**

Antenne.poitou-charentes@clusir-aquitaine.fr

Antenne Limoges Responsable **Pierre VENOT**

Antenne.limoges@clusir-aquitaine.fr

Bureau CNA Président **Gurvan QUENET**

Bureau@clusir-aquitaine.fr

Antenne 6440 Responsable **Christophe MARNAT & Nicolas Terrade**

antenne.6440@clusir-aquitaine.fr

Actus CLUSIR NA

Campus Cyber de Bordeaux :

- Guy Flament, nommé Directeur du Campus depuis le 1er juillet.
- Ouverture prévue en octobre 2022
- Le premier projet est l'ouverture du CSIRT [Computer Security Incident Response Team] est un centre de réponse aux incidents cyber au profit des entités implantées sur le territoire régional

CLUSIF / CLUSIR :

- Convention à venir pour « décloisonner » les entités

La vie du CLUB:

- Organisation des antennes CNA avec les responsables pour assurer un maillage régional
- Visite Datacenter **EQUINIX planifiée pour le 12 juillet 15h**
- AG en cours de planification pour la fin de l'année

Afterwork juillet 2022

AFTERWORK JUILLET 2022

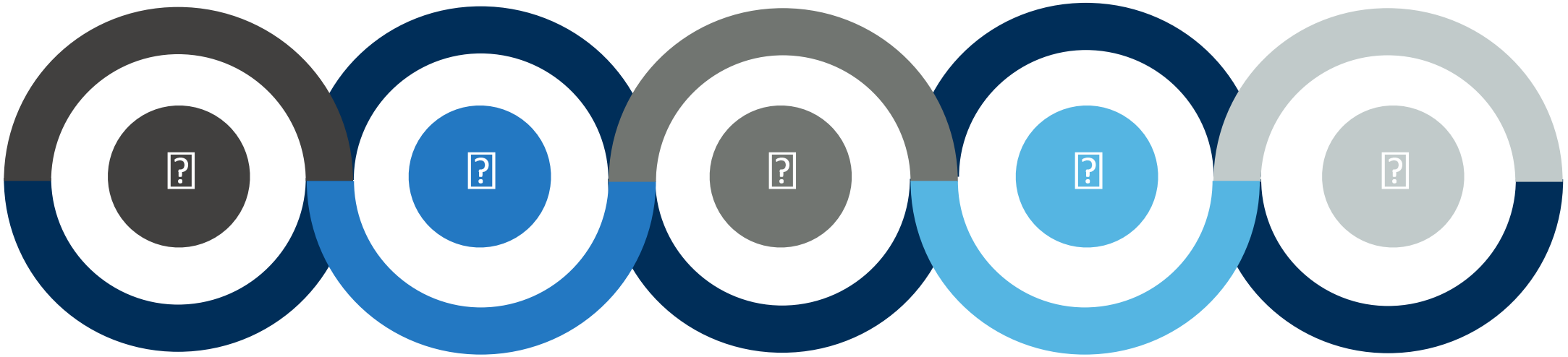
AFTERWORK: Comment Solidnames a initialisé une démarche d'amélioration continue de la SSI en s'appuyant sur une appréciation des risques, les difficultés rencontrées, les chantiers entrepris et notamment l'audit de son architecture AWS.

Cabinet Thierry MEYER Consultants

- Thierry MEYER - Trésorier CLUSIR NA
  - Certifié ISO27001 Provisionnel Auditor
  - Certifié ISO27005 Risk Manager
- Cabinet spécialisé en sécurité des systèmes d'information
  (17 années d'existence)
- Audit, Conseil, Expertise technique, gestion de crise SSI
- 3 consultants en SSI

Noms de domaine internet

Cœur d'expertise de SOLIDNAMES



Surveillance

- **Brand Alert** : Surveillance de marque parmi les nouveaux dépôts de noms de domaine
- **SecURL** : Monitoring quotidien d'un nom de domaine sensible
- **Investigation** (ex : Audit, Reverse Whois, Historique d'un nom de domaine, ect...)

Gestion

- **Dépôts, transferts, renouvellements** de noms de domaine dans plus d'un millier d'extensions internet
- **Hébergement** : Certificat SSL, Email, Site Web

Récupération

- **Rachat** de noms de domaine déjà pris
- **Backorder :** veille de retombée dans le domaine public de noms de domaine expirés

Valorisation

- **RefURL** : Diagnostic du référencement d'un site web
- **ValURL** : Evaluation financière d'un nom de domaine
- **MuscURL** : Vente et monétisation d'un nom de domaine dans un PBN

Consulting

- **Site Web** : Création et refonte de site internet
- **DRUIDE** : Sécurisation contre l'email spoofing
- **Formation** : Prestataire de formation déclaré
- **Cours**

Ils nous font confiance

Nos références

Motivation de la démarche …

… Gros à perdre en cas de crash sérieux

2016 - 2017

- Lancement activité
- Développements logiciels
  - Services principaux
  - Base de données
  - ERP
- 100% télétravail – 2 associés

2018

- Acquisition bureaux
- Développements
  - Sites web clients WP + hébergement
  - Extranet client
- Présentiel / Télétravail – 2 collaborateurs

2019

- **Analyse des risques 11/2019**
- Développements
  - Extranet client noms de domaine et DNS
  - Accréditation AFNIC

2020 – 2022

- Développements
  - Automatisation facturation
  - Surveillance Usernames réseaux sociaux
  - Surveillance NFT
- Covid
- Présentiel / Télétravail – 4 collaborateurs

Novembre 2019 : mission appréciation des risques avec Thierry Meyer

Motivations pour lancer la mission

1. Totale dépendance à l'IT
2. Enjeux grandissants pour SN et ses clients
3. Sensibilisé aux risques cyber

Motivations pour se faire accompagner

1. Démarche mentale dev + sécu difficile à concilier
2. Manque de connaissance des référentiels, outils, méthodes
3. TMC a su convaincre sur le coût et l'aspect utilisable d'un tel accompagnement

Actions réalisées

- **Prestations**
  - Missions de 3 à 4 jours / an
  - RDV Thierry Meyer et Anthony Don, chez Solidnames
  - Analyse et/ou restitution
  - Rédaction livrables

- **2019 - 2020 : analyse des risques**
  - Analyse des processus métiers
  - Identification des actifs supports
  - Estimation des risques et pondération

- **2021 : cartographie du SI**
  - Analyse de l'infra Solidnames et des services AWS
  - Recommandations

- **Livrables**
  - Analyse des risques et actions
  - Cartographie du SI et recommandations
  - Registre des incidents
  - Rapport d'audit

- **Actions réalisées**
  - Plan de comm. en cas d'incident : liste des contacts par service prêt à l'envoi
  - Alerte Log4Shell : upgrade des dépendances
  - Fichier des incidents
  - Installation armoire informatique
  - Acquisition Appliance pfSense : VPN, Firewall pour LAN
  - Acquisition NAS et mise en place backups + supervision : bdd, WP clients, GIT, documents Drive, zones DNS …

- **Actions identifiées / besoins**
  - Meilleur cloisonnement VPC
  - PRA : scripts Terraform
  - Formation CCNA (en cours 50%)
  - Formation docker / Inventaire des versions
  - Conformité RGPD
  - Rédiger une charte informatique
  - Procédure d'arrivée / départ d'un collaborateur

Focus sur l'audit d'architecture

- **Audit d'architecture :**
  - « L'audit d'architecture consiste en la vérification de la conformité des pratiques de sécurité relatives au choix, au positionnement et à la mise en œuvre des dispositifs matériels et logiciels déployés dans un système d'information à l'état de l'art et aux exigences et règles internes de l'audité. L'audit peut être étendu aux interconnexions avec des réseaux tiers, et notamment Internet. » *Définition du référentiel PASSI*
- **Méthodologie :**
  - Expérience;
  - Bonnes pratiques SSI
- **Les points de contrôle (à minima):**
  - positionnement des éléments,
  - segmentation,
  - cloisonnement,
  - la problématique du management,
  - la résilience (différentes régions).

Focus sur l'audit d'architecture chez AWS

- **Les technologies AWS :**
  - **Technologies d'interconnexion :**
    - VPC (Virtual Private Cloud) permet de regrouper les ressources dans une même « zone », (!= zone géographique) .
    - Sous-réseaux (subnet), permet de découper les VPC en différents sous-réseaux.
    - Filtrage des flux :
      - Groupes de sécurité (Security Groups).
      - ACLs permet d'appliquer des règles de filtrage de flux sur les objets et buckets.
      - …
  - **Actifs du « réseau » :**
    - EC2,
    - RDS,
    - Lambda,
    - …
- **…**
- **Avec tout ça on arrive à faire à peu près ce que l'on veut**

« Retex » sur l'audit d'architecture

- **Cartographie du périmètre de l'infrastructure**
  - Nécessité de disposer d'une cartographie globale de l'infrastructure,
  - Mais manque de visibilité sur la structure globale
    - Dashboard très complet et complexe
  - Nécessité de produire la cartographie
    - travail long (et fastidieux -> peu différent d'une infra physique (souvent pas de carto))
    - Existe des outils mais pas testés et nécessite une passe manuelle malgré tout
- **Analyse de la cartographie et des règles de filtrage**
  - Peu de changement par rapport à du « physique »
  - Cf points de contrôle
- **Conception de la nouvelle architecture**
  - Peu de changement par rapport à du « physique »
  - Mais très grand nombre de services offerts par AWS … on s'y perd un peu
  - Nécessité de consulter la documentation pour les subtilités sur les types d'objet
    - Documentation très complète, bien faite.

Le retour d'expérience sur la démarche…

- **Apports**
  - Permet de structurer la démarche de sécurisation,
  - Optimiser les coûts liés à la sécurisation
    - se focaliser sur les chantiers vraiment urgents et importants
  - Initier une démarche d'amélioration continue
  - Mettre en lumière des scénarios d'incident auxquels on n'aurait pas pensé
    - par ex : perte d'un Associé

- **Facteurs clefs de réussite :**
  - Implication de la Direction,
  - Bonne sensibilisation à la sécurité et aux enjeux,
  - Préexistence de la formalisation des processus (ISO9001),
    → actifs primordiaux
  - Suivi planifié pour maintenir un rythme,
  - Importance des outils
    - limites des fichiers excel, ….

- **Points de difficulté :**
  - Nécessite de se former
    - gouvernance et technique
  - Temps et objectivité
    - intérêt accompagnement

- **Perspectives à venir :**
  - Automatiser le PRA (Terraform, …)
  - Pousser plus loin la démarche
    - ISO27001 ? Secnumcloud ?

Merci de votre attention !

CLUSIR Nouvelle Aquitaine

Réseau des référents Cybermenaces - RCM

- Dispositif lancé le 09 Mars 2018
- Missions du RCM :
  - Sensibiliser le tissu économique local aux risques cyber et aux bonnes pratiques
  - Assister en cas d'atteinte : conservation des preuves et inciter au dépôt de plainte
- Composé d'enquêteurs de PJ et de réservistes du secteur privé ou public
- Dans le Sud-Ouest : 18 réservistes sous la supervision de la direction zonale de Police Judiciaire de Bordeaux
- Point de contact pour les entreprises en Nouvelle-Aquitaine :

cybermenaces-bordeaux@interieur.gouv.fr