ADN Ouest Vendée

# Cybersécurité : Comment se préparer et répondre aux nouvelles menaces ?

Mardi 04 avril 2023 de 8h30 à 12h
Loco numérique La Roche-sur-yon

Partagez votre expérience :
@adnouest

**Sophie MOUNIAU**

ADN Ouest

*Cheffe de projet*

# ADN Ouest : Agir pour le Développement du Numérique en Pays de la Loire et en Bretagne

## UN LARGE RÉSEAU

**+640** Structures adhérentes

**+3700** Membres

**100** Évènements

**2** Régions

## 4 ENJEUX MAJEURS

- Emploi et formation
- Transition Numérique
- RSE
- Innovation

## 7 COMMUNAUTÉS THÉMATIQUES

- Numérique Responsable
- Santé
- Infra & services
- Cybersécurité
- Stratégie Digitale
- Data
- Management

## DES PROGRAMMES AU SERVICE DE LA FILIÈRE

- 2 Observatoires : métiers et compétences numériques / économie et investissements
- 1 Fonds de Dotation : ADN Solidarity
- 1 accélérateur de projets innovants : ADN Booster
- 1 accélérateur de la transformation numérique des PME : ADN for Change

## DES PÔLES TERRITORIAUX

ADN 44
ADN 29
ADN 49
ADN 56
ADN 35
ADN 22
ADN 85

## DES CERCLES METIERS

- DPO
- DSI
- CMO

# ADN For Change : L'accélérateur d'ADN Ouest qui booste la transformation numérique des PME en Pays de la Loire !

UN PROGRAMME DE 12 MOIS
DISPENSÉ PAR UN COLLECTIF D'ENTREPRISES
EXPERTES DU NUMÉRIQUE.

**LES PARTENAIRES**

qui soutiennent notre démarche et apportent leur expertise pour être au plus près des besoins des PME.

optesysconseil
Avolaré
ODONATES GROUP
DIGITAL EASE & VOUS
VOTRE DIGITALISATION FACILITÉE
PrivacyImpact
CROSS DATA
croiser vos données avec le réel
VERY DIGITAL
e-commerce / génération de leads

4 champs d'expertises

- ORGANISATION
- BUDGET
- TECHNIQUE
- COMMERCE

- Un accompagnement à destination des PME des Pays de la Loire ayant pour objectif de se développer grâce au numérique.
- Un programme sur mesure avec un suivi individuel et des ateliers collectifs.
- Un coût pris en charge à 50% par nos partenaires privés/publics.

## ADN Ouest

ADN Ouest œuvre au quotidien pour représenter, développer et mettre en relation les professionnels de la filière numérique en Pays de la Loire et en Bretagne.

- 600 STRUCTURES ADHÉRENTES
- 100 ÉVÉNEMENTS PAR AN
- 4000 MEMBRES
- 2 RÉGIONS

Sophie MOUNIAU
sophie.mouniau@adnouest.fr
07 86 67 02 69

# Déroulé

1. **Accueil café : 8h30 à 9h**
2. **Contexte actuel et retour d'expérience clients : 9h à 9h45**
3. **Témoignages et Q&A : 9h45 à 10h30**
4. **Ateliers : 10h30 à 11h30**

# Contexte actuel et retours d'expériences clients

**François LEROY**

ENVOLiiS

*Directeur Général*

**Cédric GIRARD**

SIIUM & SHWETT

*CEO*

**Thomas SEEBURGER**

DIGITEMIS

*Manager Gouvernance Risques Conformité & Juridique*

**Thomas SEEBURGER**

DIGITEMIS

*Manager Gouvernance Risques Conformité & Juridique*

# Une expertise 360°

Une équipe d'experts pour vous accompagner.

- Consultants cyber en sécurité fonctionnelle
- Ingénieurs en test d'intrusion et sécurité des architectures
- Ingénieurs en organisation de la cybersécurité
- Juristes pour la protection des données personnelles
- Consultants chefs de projets

**403** projets livrés en 2022

**18%** de clients du CAC 40

DIGITEMIS
CYBERSECURITY & PRIVACY

**60** collaborateurs

**100%** de réussite au phishing

**71%** d'intrusions externes réussies

**94%** d'intrusions internes réussies

DIGITEMIS
CYBERSECURITY & PRIVACY

# Tendances cyber-sécurité

**54%** des entreprises déclarent avoir subi au moins une attaque en 2021

- **Généralisation** des cyberattaques sur **tout type d'entreprise**
- Une **menace qui s'industrialise** de plus en plus
- **Impunité** et profits importants
- **Divers vecteurs d'attaque** : phishing (73%), exploitation des failles (53%), supply chain (21%)

*Source : Baromètre de la cyber-sécurité des entreprises, CESIN (Club des Experts de la Sécurité de l'Information et du Numérique) Janvier 2022*

- Novembre 2022
  Le groupe Avril, connu pour ses marques Lesieur ou Puget, a fait face à une cyberattaque d'ampleur. Une semaine après l'ouverture du fichier corrompu, le **système informatique du groupe redémarre progressivement**.

- Août 2022
  *Continental :* Des **secrets commerciaux** de Volkswagen, BMW ou Mercedes ont été piratés sur les serveurs de l'équipementier allemand. Faute de réponse à une demande de rançon, **55 millions de fichiers** ont été publiés sur le darknet. Les **conversations du président du conseil de surveillance** seraient concernées.

- Août 2022
  L'Ehpad les Franches Terres à Beuzeville (Eure) a été confronté au **chiffrement de son fichier patients.**

- Avril 2022
  Le fabricant de cloisons amovibles pour l'aménagement d'espaces de bureau et de salles blanches, Clestra Hauserman a demandé sa **mise en redressement judiciaire**, suite à des événements impactant le Groupe dont une cyberattaque le 30 avril dernier.

DIGITEMIS
CYBERSECURITY & PRIVACY

# Exemple de mission du RSSI

Garant de la sécurité logique et physique de l'ensemble du système d'information

- Accompagnement d'une collectivité territoriale
- Survenance d'une crise cyber le 1er jour de notre intervention
- Participation à la gestion de la communication de crise et interview de la télévision locale

DIGITEMIS
CYBERSECURITY & PRIVACY

# RETEX sur l'intrusion d'un SI

Contrôle de la sécurité fonctionnelle, technique et physique

- Intrusion physique des locaux d'un groupe international
- Accès au système d'informations
- Destruction possible de l'ensemble du SI

DIGITEMIS
CYBERSECURITY & PRIVACY

# Perspectives et réflexions pour les années à venir

Face aux cyberattaques toujours plus complexes et nombreuses, l'IA peut nous accompagner dans un contexte de manque de ressources

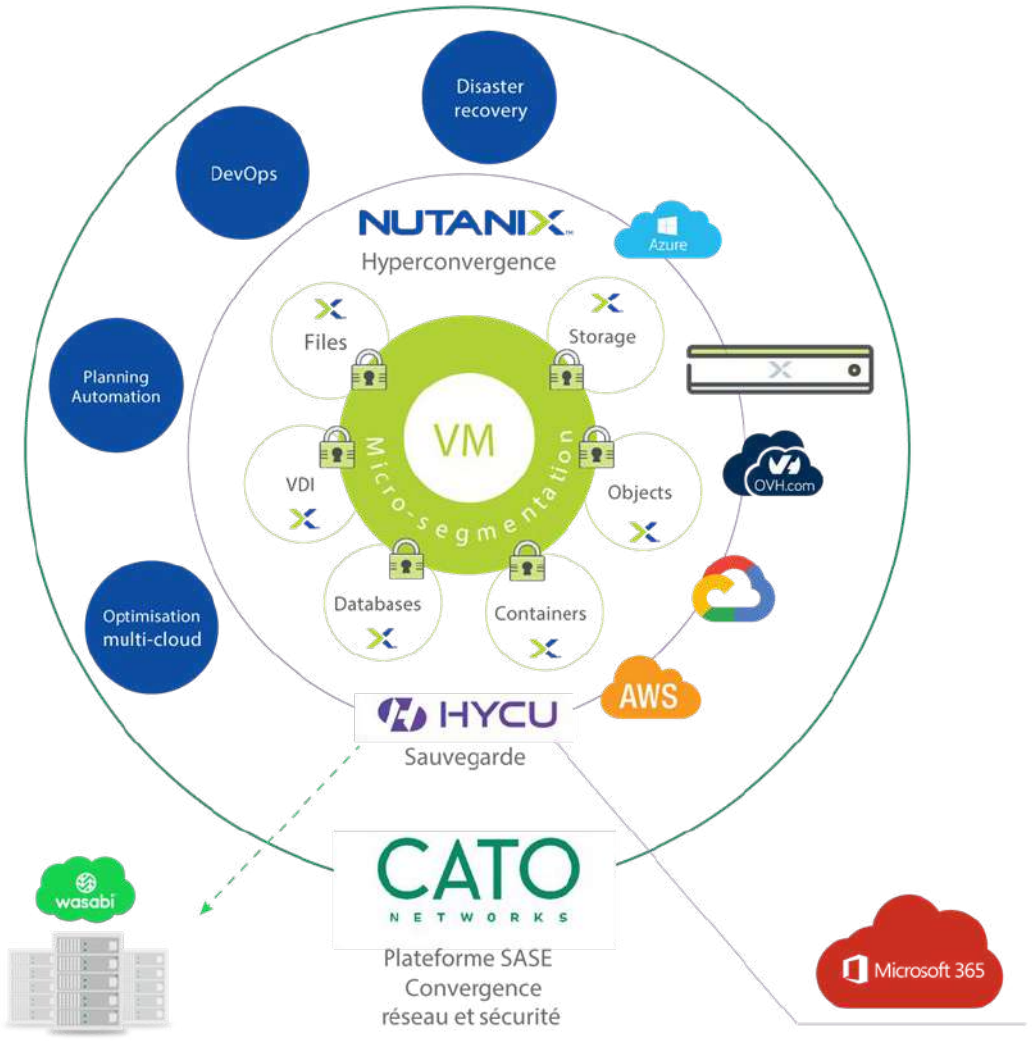
- L'IA apprend en permanence
- Le raisonnement de l'IA identifie rapidement les menaces
- L'IA supprime des tâches chronophages

**Cédric GIRARD**

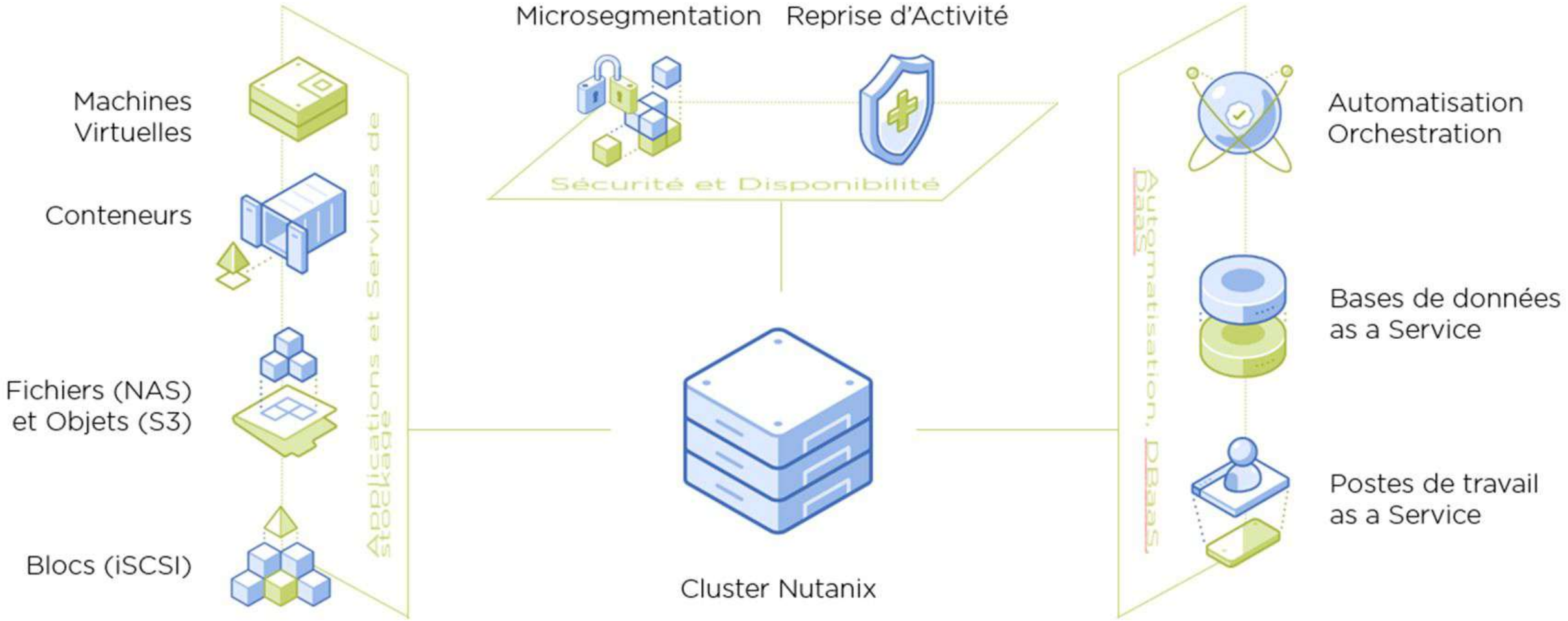
SIIUM &
SHWETT

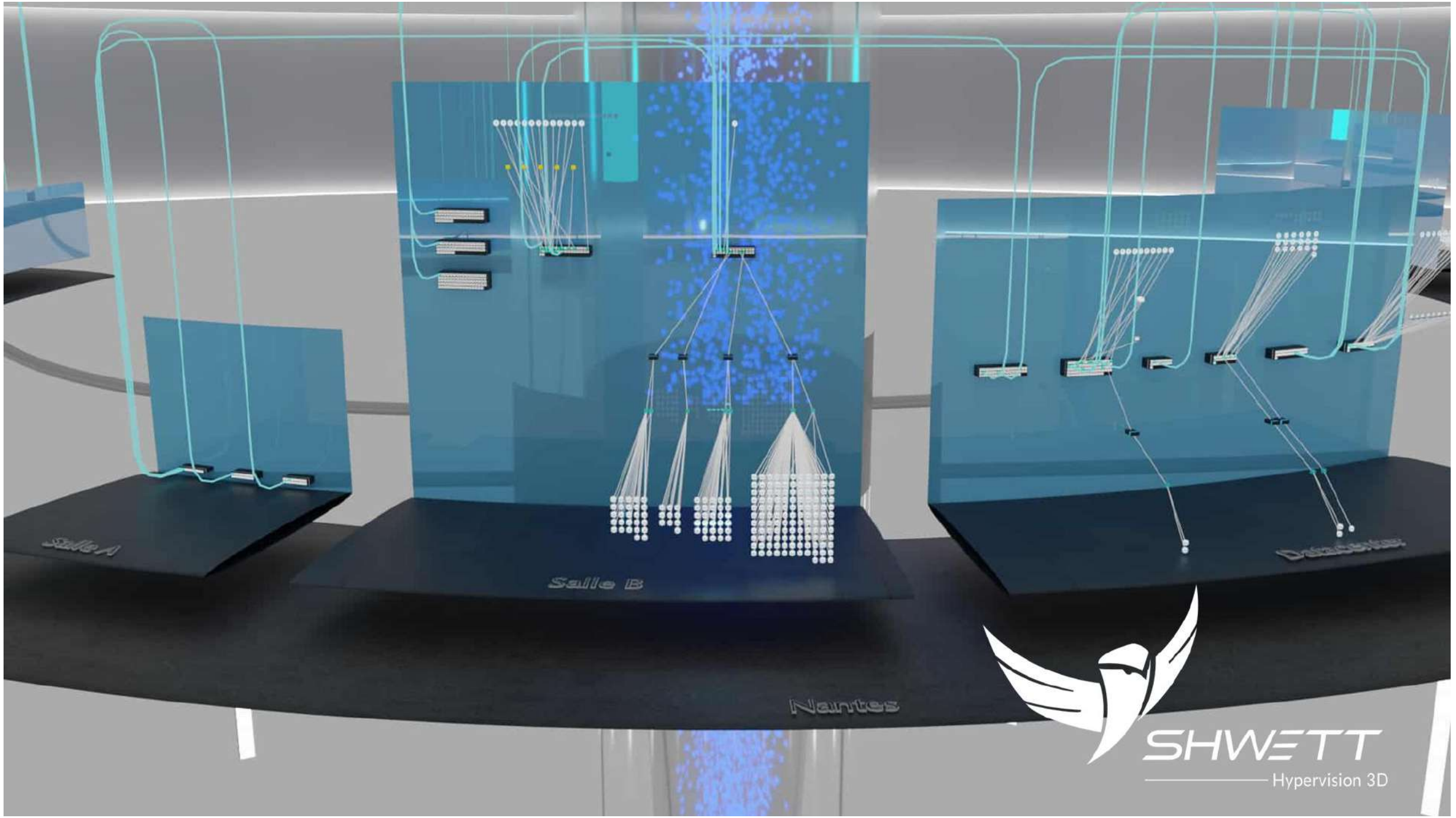
*CEO*

# Notre vision



# La valeur ajoutée



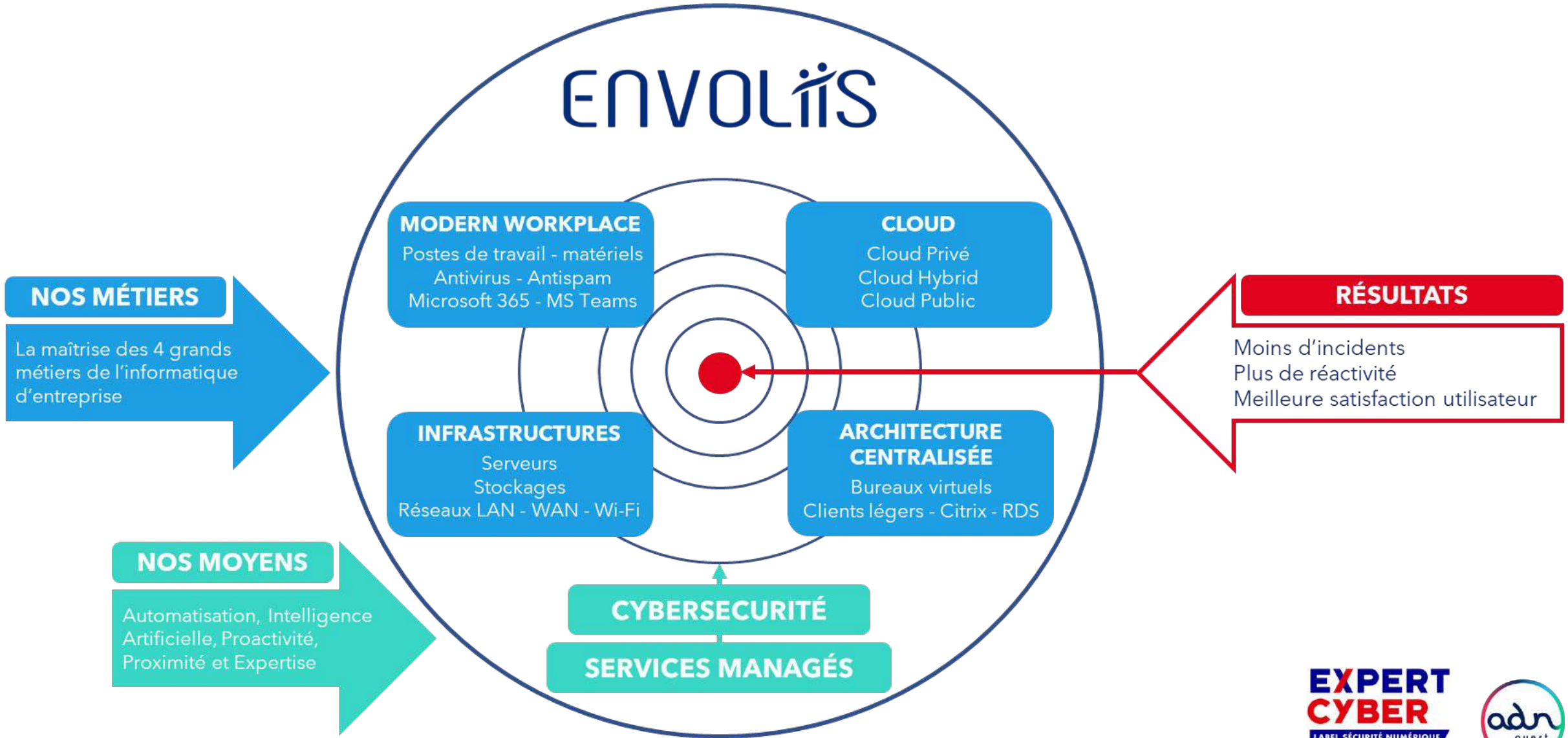

Salle A
Salle B
Nantes
SHWETT
Hypervision 3D

**François LEROY**

ENVOLiiS

*Directeur Général*

# La Cybersécurité et les Services Managés à 360°




EXPERT CYBER
LABEL SÉCURITÉ NUMÉRIQUE
Cybermalveillance.gouv.fr
RÉPUBLIQUE FRANÇAISE

adn ouest

# Quelques indicateurs clés

**750**

Serveurs managés

**850**

Périphériques réseaux managés

**1 600**

Postes de travail télé administrés

**3 500**

Incidents gérés par an dont 70% résolus dès le 1er appel

**10 000**

Tickets traités par an grâce à nos outils de Services Managés

**+ DE 20 000**

Points de contrôle analysés chaque minute

# RETEX : rapport d'étonnement

Plus on est petit et moins on se sent en danger. Plus on est petit et plus on fait confiance.
Ne pas oublier les KPIs… et les financer

Toutes les sociétés que nous rencontrons ne testent pas leurs sauvegardes et n'externalisent pas leurs données

Investir de l'argent dans la Cyber sécurité
Sortir d'une vision techniques pour alimenter une vision direction. externe.
Pour l'investir au bon endroit on démarre par l'analyse des risques

Dernière attaque connues chez un de nos clients : décembre 2021

# Avez-vous des questions ?

# Témoignages et Q&A

**Lucie POIRAUD**

GROUPE ATLANTIC

*RSSI Responsable de la sécurité du Système d'information*


**Christophe BARTHEAU**

MONTS-FOURNIL
La Mie Câline

*Responsable systèmes d'information chez SAS MONTS-FOURNIL*

# REX ATTAQUE OCTOBRE 2012

## Contexte DSI

- Equipe de 4 personnes
- 2 métiers
  - Retail
  - Industriel

## Faits

- Modification de stocks sur tableaux de bord comptables d'un magasin (Marseille 2) sur 1er et 2ème trim 2012
- Modification de fichiers excel dans un dossier /gestion

## Analyse

- SI MOF
  - Relevés dates et heures modification fichiers excel
  - Relevés logs sur le FW (Juniper)
  - Relevés logs serveurs avec comptes admin ou users informatique
  - Relevés sources IP des connexions SSL
- SI Magasin
  - Récupération PC
  - Logiciels installés confirment les doutes
  - Faille dans plateforme collaborative de l'époque (Intraline)

## Réactions

- + Systématisation annuelle
  - Tests intrusion en décembre 2012
  - Renouvelée en 2019
    - Analyse de risques en 2013
    - Définition d'un plan d'actions sécurité
    - Rédaction PSSI
    - Sensibilisation depuis 2015
    - Prise de conscience du Codir (face aux attaques de sociétés vendéennes)
      - Depuis 2019
        - Jusqu'à 2022 avec rédaction périmètres et acteurs associés
        - Périmètres Offensif, défensif et réglementaire
        - Montée périodique du niveau de sécurité de MOF
        - Franchiseur
        - Industriel
          - Sensibilisation (sous diverses formes) pour tous les salariés du site de St Jean de Monts
        - Depuis 2013, alternance des rôles et des acteurs

## Actions à venir

- Franchiseur
- Industriel
- Retail
  - Systématisation de la sensibilisation pour tous les périmètres et publics du groupe
- Définition d'un RTO
- Partage / validation Codir
  - Tests tests tests PRA-PCA !
- Test cellule de crise
- Red team

# ATELIERS

**Jules AGOSTINI**

AUKFOOD

*Co-créateur et CTO*

*Responsable normalisation*

**Benjamin Piet**

AUKFOOD

*Consultant CyberSécurité*

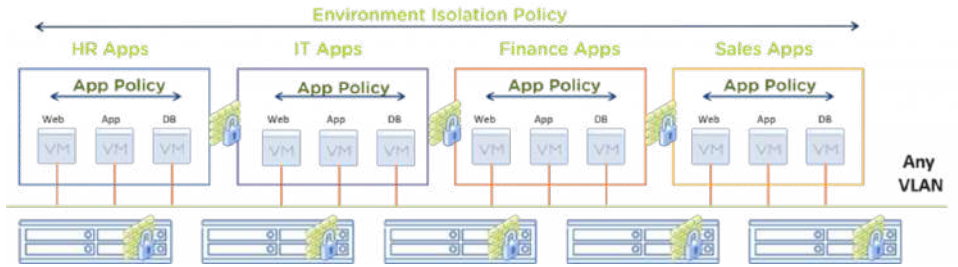
# Atelier 1 : CyberWargame cybersécurité. Comment sensibiliser les utilisateurs ?

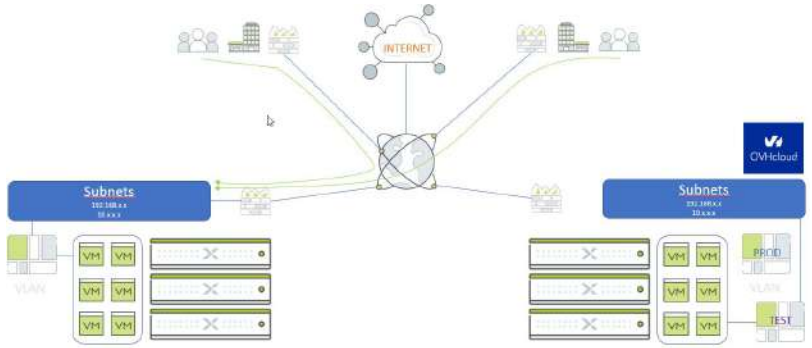
**Cédric GIRARD**

SIIUM & SHWETT

*CEO*

# Atelier 2 : Microsegmentation & PRA



**Thomas SEEBURGER**

DIGITEMIS

*Manager Gouvernance Risques Conformité & Juridique*

**François LEROY**

ENVOLiiS

*Directeur Général*

# Atelier 3 : Analyse de risques : quelle méthode pour les risques cyber ?

# ATELIER

## Identifiez vos risques pour vous protéger des cyberattaques

# Par où commencer ?

- Avoir une approche basée sur les risques
- Avoir une approche pragmatique
    - Exemple : Quel effort serait nécessaire pour patcher régulièrement les automates, et quel serait le gain sécurité ?
- Garder en tête ce qui est important pour le métier : être capable d'utiliser l'outil industriel
- Aucune technologie « magique » ne va venir sécuriser un SI industriel si les basiques (segmentation réseau, patching…) ne sont pas mis en œuvre

# AGENDA

1. PRÉSENTATION DU RISQUE CYBER
2. LES RISQUES POUR VOTRE ENTREPRISE
3. L'ÉTAT DE LA MENACE
4. LES VULNÉRABILITÉS SUR VOTRE SI
5. PLAN D'ACTION
6. BONNES PRATIQUES

# Atelier participatif avec 3 étapes :

# 1. PRÉSENTATION DU RISQUE CYBER

- **Définition** apportée par l'ISO 27005:2022 :

  Le risque de sécurité de l'information peut être associé à la possibilité que des menaces exploitent les vulnérabilités d'un bien informationnel ou d'un groupe de biens informationnels et portent ainsi un préjudice à un organisme.

  En d'autres termes : Danger, inconvénient plus ou moins probable auquel on est exposé et qui porte un préjudice à une organisation

  *LE RISQUE EST INHÉRENT À TOUTE ACTIVITÉ HUMAINE*

- Les **objectifs** de l'identification du risque :
  - Déterminer les événements susceptibles de se produire causant une perte potentielle permettant de les anticiper et d'améliorer sa capacité de réaction
  - Responsabiliser les propriétaires des actifs
  - Et :

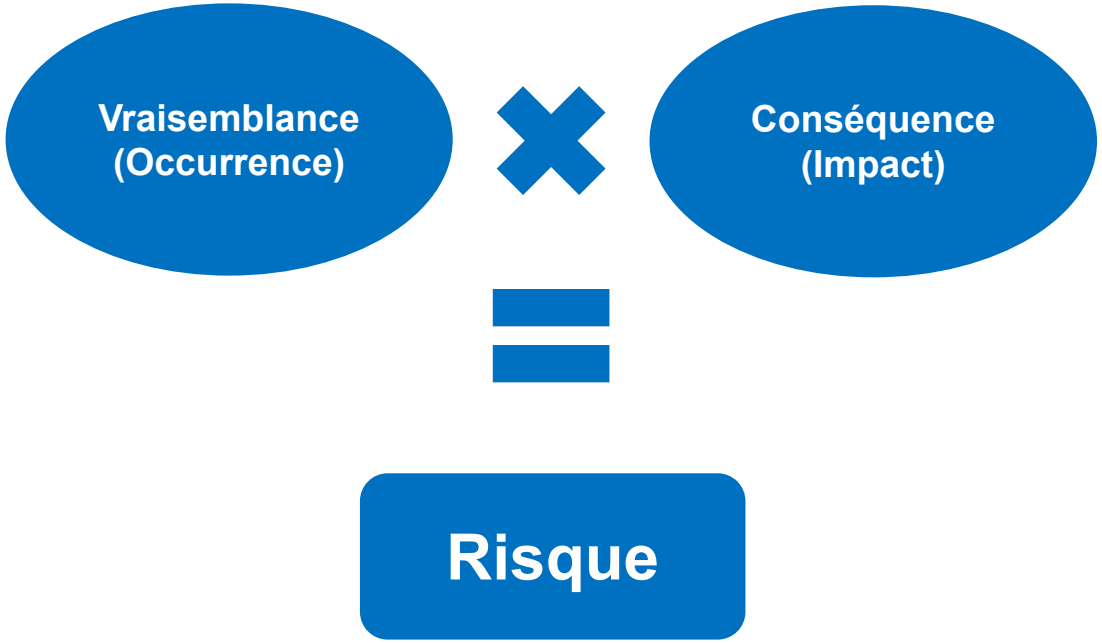
  *PRIORISER ET RENFORCER L'EFFICIENCE DES DÉPENSES*

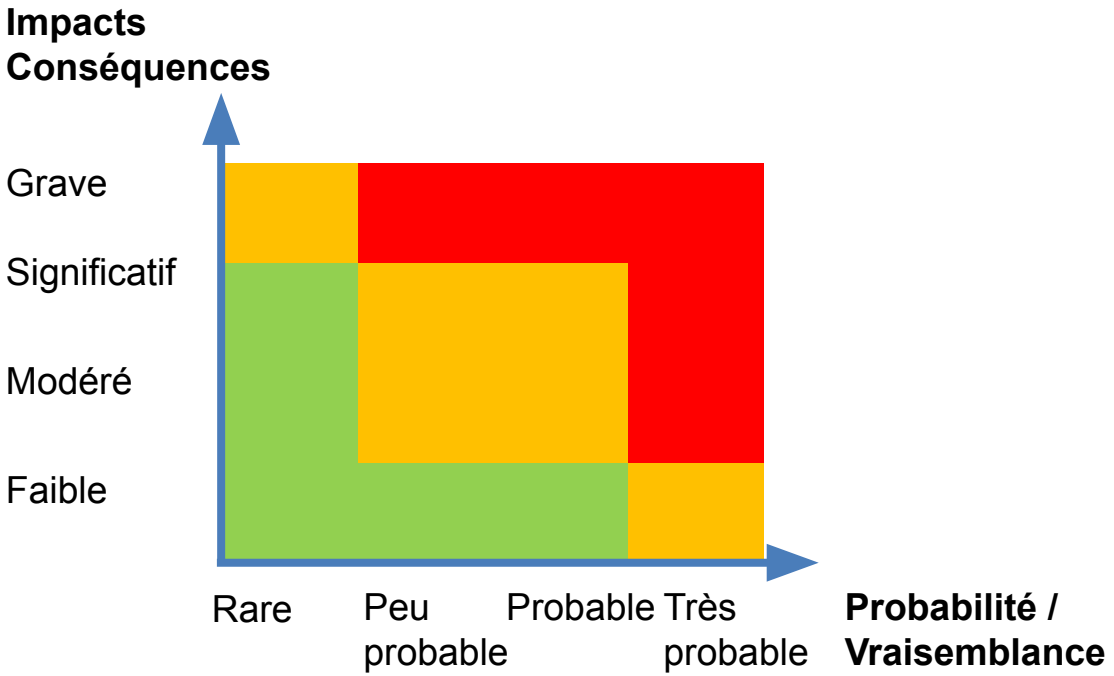
# CRITERES D'EVALUATION DU RISQUE EN SECURITE INFORMATIQUE

| CONFIDENTIALITE | INTEGRITE | DISPONIBILITE |
| --- | --- | --- |
| Propriété que l'information ne soit accessible qu'aux individus, entité, ou processus autorisés | Propriété de sauvegarder l'exactitude et la complétude des actifs | Propriété qu'une information soit accessible et utilisable au moment voulu par une entité autorisée |

Un risque en sécurité de l'information est :

- Exprimé en termes de combinaison des conséquences d'un événement en sécurité de l'information associés à la probabilité de survenue

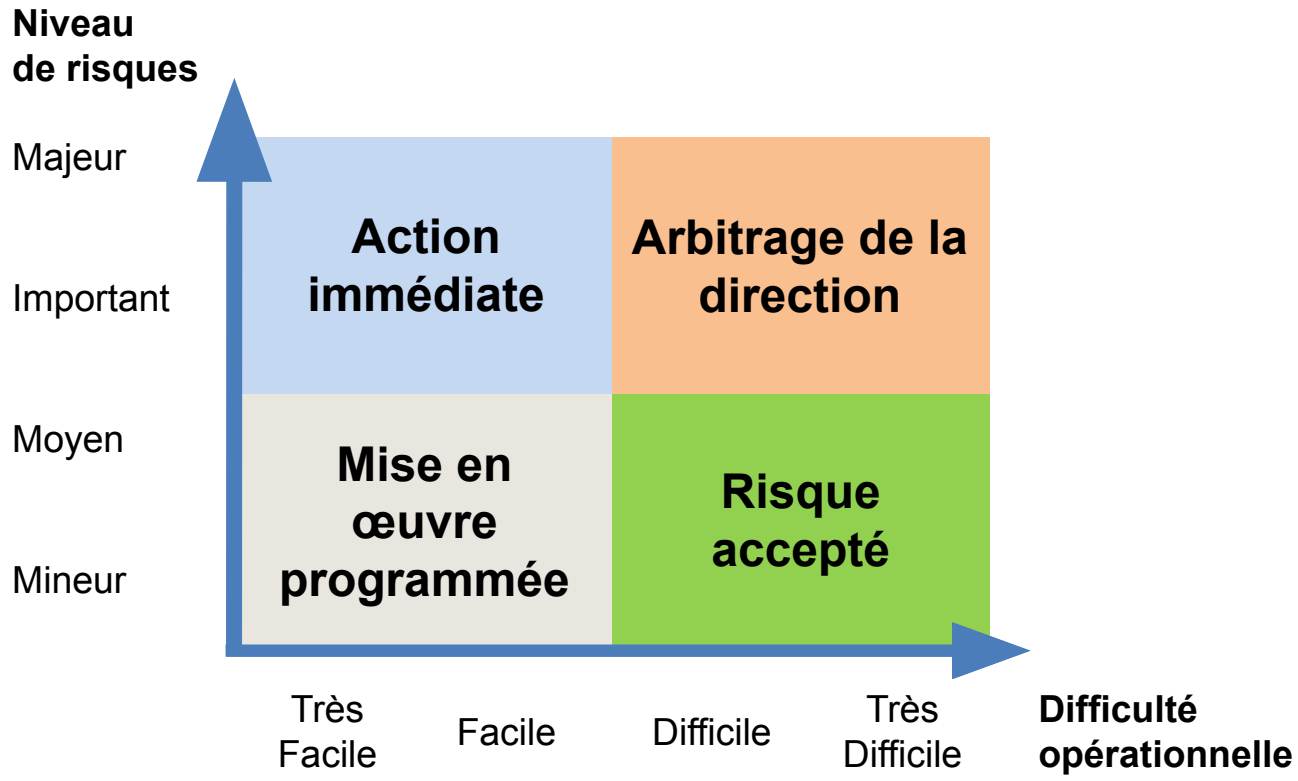



- Les impacts peuvent être d'ordres humains, opérationnels, financiers, d'image, règlementaires…

Consciemment ou inconsciemment, nous pratiquons à chaque instant, une gestion du risque en faisant des choix :

- prise de risque
- réduction du risque
- partage ou transfert du risques
- refus du risque



# QUESTIONS SUR LA NOTION DE RISQUES CYBER ?

# 2. LES RISQUES POUR VOTRE ENTREPRISE

# Quels sont les risques cyber identifiés pour votre entreprise ?

## Ex : Un pirate informatique accède à votre logiciel de programmation et modifie la configuration de vos machines


# 3. L'ÉTAT DE LA MENACE

## 1 Source & motivation

États et groupes associés (Géopolitique)

Cybercriminels (Financières)

Hacktivistes (Idéologique)

Terroristes (Violence idéologique)

Hackers amateurs (Challenge)

Employés, clients, fournisseurs, partenaires (mécontentement)

Concurrents

## 2 Points d'entrée

Hameçonnage (Phishing, SMiShing, Vishing..)

Exploitation de failles techniques sur services exposés (Local, Cloud, Objets connectés, Applicatifs)

Exploitation de mots de passe faibles/réutilisés

Installation d'applications compromises sur terminaux utilisateurs

Exploitation de failles techniques sur applications terminaux utilisateurs

Infection via supports amovibles (Clé USB…)

Accès physique au réseau ou à des machines

Réseaux sans-fil vulnérables (Wifi, Bluetooth…)

Porte dérobée matérielle/logicielle

Accès distant vulnérable

Supply chain attack

Fourniture volontaire d'accès

Shadow IT

## Faiblesses supplémentaires

Gestion des comptes d'administration locaux

Cloisonnement réseaux

Gestion des droits d'accès

Gestion des MAJ ou Obsolescence

Conception

Configuration

Failles techniques sur services internes

Gestion des comptes à privilèges

Gestion des mots de passe

Sauvegarde connectée

Trafic réseau et données non chiffrés

## 3 Malveillances

Rançongiciel (avec /sans exfiltration)

Envoi de spam

Intégration à un réseau de botnet

Espionnage / Exfiltration de données (identité, informations stratégiques, mots de passe…)

Extorsion de fonds / Arnaque au président / FOVI

Minage de cryptomonnaie

Déni de service / Sabotage logique ou physique

Défiguration sites

Déstabilisation / Chantage

**OPTIMISER SA ROBUSTESSE**
Capacité à limiter les points d'entrées et à combler ses principales faiblesses

## Se protéger des actes malveillants

**OPTIMISER SA RÉSILIENCE**
Capacité à se rétablir en cas d'incident (sauvegarde, reprise d'activité, gestion de crise)

# Capacité à faire face aux principales menaces

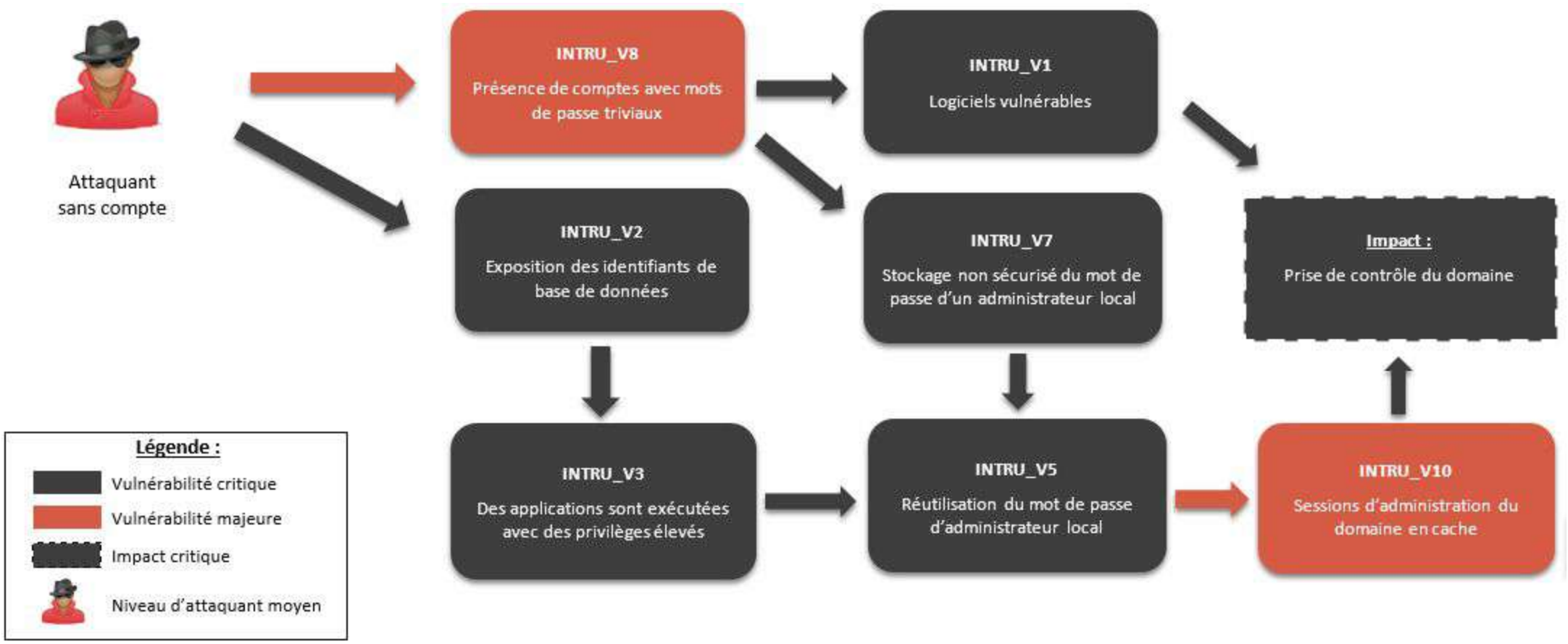
| Source de menace | Evènement redouté | Niveau d'exposition à la menace estimé | Principales vulnérabilités |
|---|---|---|---|
| Menace cybercriminelle<br>  <br>**Attaque opportuniste** | • **Perte de continuité de service public, notamment avec impact sur la santé, la vie humaine ou l'écologie** | **Très fort** | • Manque de sensibilisation des utilisateurs<br>• Niveau de sécurité de l'AD insuffisant<br>• Manque de cloisonnement réseau<br>• Systèmes obsolètes ou pas à jour<br>• Sauvegarde déconnectée peu fréquente<br>• Pas de Plan de Reprise d'Activité |
| Menace cybercriminelle<br>  <br>**Crime organisé** | • **Vol de données personnelles**<br>• **Vol de données politiques et contentieux**<br>• **Modification malveillante de RIB**<br>• **Perte de continuité de service, notamment avec impact sur la santé, la vie humaine ou l'écologie** | **Fort** | • Manque de sensibilisation des utilisateurs<br>• Niveau de sécurité de l'AD insuffisant<br>• Manque de cloisonnement réseau<br>• Systèmes obsolètes ou pas à jour<br>• Sauvegarde déconnectée peu fréquente<br>• Pas de Plan de Reprise d'Activité<br>• Pas de politique anti usurpation de la messagerie, ni chiffrement d'e-mails<br>• Pas de MFA sur la messagerie, ni sur les solutions SaaS |
| Menace étatique<br>  <br>**Étatique** | • **Indisponibilité de services fournis par l'Etat** | **Faible** | • Dépendance au bon fonctionnement des solutions de l'Etat et de leur accessibilité |
| Menace interne<br>  <br>**Vengeur ou interne malveillant** | • **Indisponibilité d'une application critique** | **Moyen** | • Manque de sensibilisation des utilisateurs<br>• Mouvements RH parfois non signalés<br>• Pas d'utilisation systématique de coffre-fort de mots de passe |

# 4. LES VULNÉRABILITÉS SUR VOTRE SI

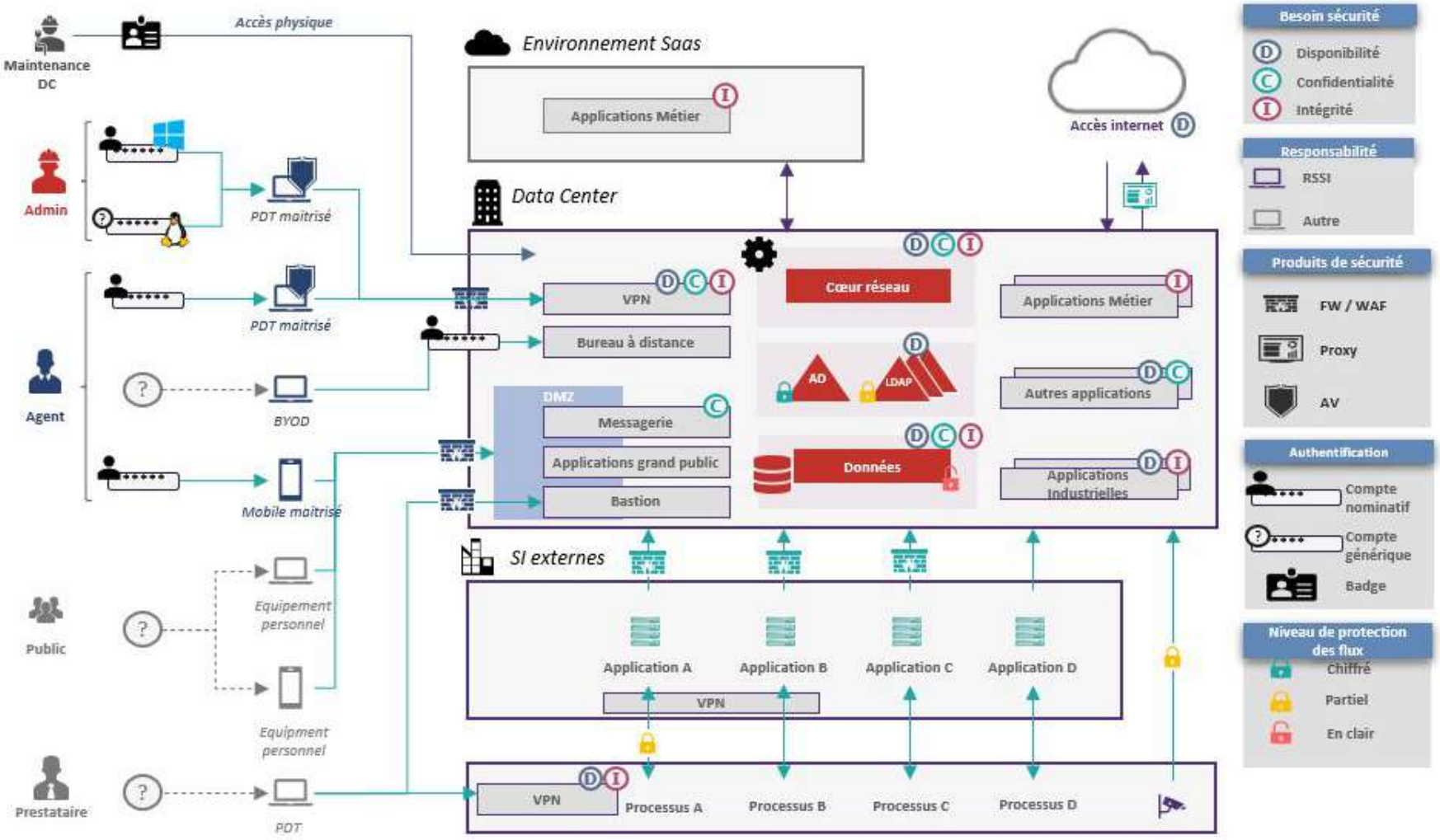
# Quels sont les vulnérabilités potentielles sur votre SI ? (vecteurs d'attaque)

## Ex : Ports USB non bloqués sur les postes de travail

# Exemple de scénario d'exploitation de vulnérabilités



# Exemple de cartographie des zones de vulnérabilité de l'infrastructure



# 5. PLAN D'ACTION

# ECHANGE SUR LES MESURES POTENTIELLES RESULTANT DES REPONSES DES PARTICIPANTS

## Exemple de thématiques à adresser


Gouvernance


Sensibilisation


Environnement utilisateur


Applications


Gestion des fournisseurs & partenaires


Administration


Protection des données


Gestion des identités et des accès


Réseau


Détection


Gestion des incidents et Résilience


Cloud


SI industriels / biomédicaux


Conformité et Audits

# 6. BONNES PRATIQUES

# A RETENIR

- **Aucun Système d'Information n'est sécurisé à 100%.** Et même si c'est le cas, ce ne sera que très temporaire et on ne pourra pas s'arrêter !
- La **sécurité informatique** est à comparer à un mur : **plus il est haut, plus il est dur à escalader et à passer.** Et on fait grandir le mur étape par étape
- La sécurité informatique, c'est **80% d'organisation (humain)** et 20% de technique
- La sécurité informatique, **c'est l'affaire de tous**, et vous êtes en 1ère ligne : **tout collaborateur** au sein d'une entreprise est impliqué et partie prenante dans la sécurité
- Les **règles de sécurité** sont les mêmes dans le milieu professionnel et le monde personnel. Elles sont généralement simples, de bon sens, mais on les oublie facilement


10
Points
à retenir


1. Choisir des **mots de passe adaptés** et les **modifier** périodiquement / utiliser un gestionnaire de mot de passe
2. Mettre en place de la **double authentification**
3. **Protéger** son poste de travail et **être prudent** avec son smartphone
4. Identifier le niveau de maturité de ses **sous-traitants** en **sécurité**
5. Vérifier ses **systèmes / logiciels** et les **mettre à jour**
6. **Tester** régulièrement ses **sauvegardes** et leur **restauration**
7. Documenter **en dehors du réseau de production** et **cloisonner**
8. **Protéger** ses données y compris en déplacement
9. Conserver une **maîtrise** raisonnable sur vos **activités** dans le **cloud**

Et surtout >>>

10. **Sensibiliser** et former les utilisateurs / maintenir en alerte ses collaborateurs

ENVOLIIS LA PERFORMANCE DE L'IT MANAGÉE

DIGITEMIS CYBERSECURITY & PRIVACY

# ANNEXES

# Les dirigeants, acteurs clés dans l'anticipation d'une cyberattaque

En cybersécurité, il vaut mieux **prévenir que guérir.** Votre rôle est ainsi **crucial** dans le cadre des actions qui permettront **d'empêcher les attaques, de les anticiper et d'en limiter les impacts**

## 1. Suivre et s'impliquer dans la gestion du risque cyber

- Se tenir informé de la cybermenace et de son niveau de sécurité (suivi d'indicateurs réguliers, participation à un comité de pilotage stratégique annuel, etc.)
- Participer à la démarche de priorisation des activités métiers devant faire l'objet de dispositifs de sécurisation ou de continuité. S'impliquer dans la politique de sécurité, avec la DSI, y compris pour les équipements connectés.

## 2. Donner les moyens (humains et financiers) nécessaires pour un bon niveau de sécurité

- Attribuer les budgets nécessaires à la mise en œuvre des démarches de sécurisation
- Prévoir le maintien en condition de sécurité de son SI dans les budgets

## 3. Être exemplaire

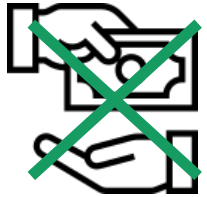
- Être exemplaire dans son rôle au quotidien (phishing, pièces jointes chiffrées, mots de passe utilisés….)
- Appliquer les bonnes pratiques pour permettre de maintenir un niveau d'hygiène numérique satisfaisant et de prévenir de nombreuses menaces, internes et externes, accidentelles et malveillantes

## 4. Relayer les bonnes pratiques

- Appuyer les démarches mises en œuvre par les équipes cybersécurité (sensibilisation, projets majeurs,…) voire y participer (exercice de crise cyber …)
- Relayer les bonnes pratiques de manière régulière et opportuniste, auprès de l'ensemble des utilisateurs des SI

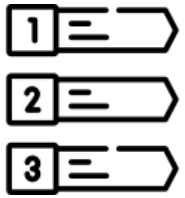
# Quel rôle pour les dirigeants en cas de cyberattaque ?

*Communiquer, organiser les équipes et rétablir le service*



## Ne pas payer la rançon !

*En cas d'attaque par rançongiciel, un paiement de la rançon n'accélère pas la gestion de crise et ne garantit ni la récupération des données ni l'effacement des données volées.*




## Savoir réagir et prioriser les services à rétablir

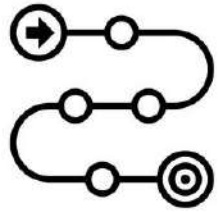
*Mettre en place une cellule de crise visant à prioriser le rétablissement du service selon les besoins métiers, en ayant au préalable anticipé et déterminé quels services sont les plus importants.*

## Communiquer sur l'incident et porter plainte

*Alerter immédiatement les régulateurs (ANSSI, CNIL…).*

*Communiquer de façon maîtrisée auprès des citoyens et des partenaires.*

*Porter plainte.*



## S'organiser pour tenir sur la durée

*En cas de cyber attaque, le retour à la normale peut être un très long chemin. La gestion de la crise n'est donc pas un sprint mais un marathon : il faut être prêt à tenir dans la durée, les équipes risquent de s'épuiser sinon.*

# Avez-vous des questions ?

# Vos prochains événements ADN Ouest

**AGENDA DES ÉVÉNEMENTS**



Après le succès de notre première édition, nous vous donnons rendez-vous le **jeudi 22 juin 2023 à Rennes pour la 2ème édition d'ADN Festival, le grand événement organisé par nos adhérents pour nos adhérents.**

Et comme chez ADN on aime voir les choses en grand, on vous a réservé le Stade Rennais Roazhon Park pour la journée !

Ce rendez-vous incontournable, sera l'occasion de partager :

- des conférences inspirantes sur l'engagement des hommes et des femmes dans le numérique
- un grand défi créatif pour réaliser une construction collective
- des remises de Trophées pour célébrer des projets engagés
- une Assemblée Générale
- du networking autour d'un verre
- des animations et des surprises
- et bien sûr du spectacle et du bon son pour finir la journée en beauté

# Votre avis compte !

*(un pseudo vous sera demandé)*

**Lien : https://app.klaxoon.com/join/M3TWPKG**

# Vous êtes au ♡ du numérique !

www.adnouest.org

Partagez votre expérience :

@adnouest