# CYBERSECURITE POUR LES BIOLOGISTES

17.11.2023

Jerome Vetillard – Healthcare & Life Sciences Industry Advisor / Microsoft


You became victim of the PETYA RANSOMWARE!
PRESS ANY KEY_


# BIOGRAPHIE

- Conseiller Principal en Santé et Sciences de la Vie pour Microsoft EMEA+Americas, alliant expertise technique, compréhension métier et analyse stratégique.
- Spécialiste en Intelligence Artificielle et son application à l'industrie de la Santé et des Sciences de la vie.
- Expert en transformation numérique avec une solide expérience dans la recherche médicale académique et sa valorisation industrielle. Accompagnement des start-up et des grandes entreprises dans la gestion de leur innovation.
- Architecte d'Entreprise chez Microsoft, définissant et délivrant des programmes de transformation numérique pour des entreprises Fortune 100
- PhD Biotechnologie, Executive MBA, Ms.Sciences, Ms. Engineering, spécialisations médicales (DU/DIU) en hématologie, oncologie clinique, pionnier dans l'utilisation de la thérapie cellulaire pour traiter les cancers du sang (greffe autologue).

# AGENDA

- Introduction à la Cybersécurité en Milieu Hospitalier & laboratoires privés
- Panorama des Menaces et Vulnérabilités
- Hygiène Numérique et Prévention des Risques
- « Zero Trust » : Principe et Mise en Application
- Réponse aux Incidents et Continuité d'Activité
- Renforcement des Architectures LIMS et IAM
- Engagement des Professionnels de Santé dans la Cybersécurité
- Vers un Écosystème de Santé plus Sûr

# INTRODUCTION

## Le statut particulier des données de santé

La protection des données de santé est d'une importance capitale pour plusieurs raisons :

1. **Risques Cliniques**
   - Sécurité des Patients (Accès aux données, Intégrité des Données, Coordination transversale des Soins )
2. **Risques Opérationnels**
   - Continuité des Services de Santé / Coûts Financiers et Réputationnels / Conformité Réglementaire
3. **Menace des Ransomwares**
   - Blocage de l'Accès aux Données Vitales / Pression pour Payer la Rançon / Exposition au Risque de Répétition
   - Fuite de données et monétisation des données de santé
4. **Eléments économiques**
   - Coût annuel : 5000 Milliards de $ (Thalès 2020) -> 8000 Milliards (cybercrime 2023)
   - Ransomware as a Service : Pour une micro poignée de bitcoins
   - Coûts de XX$ à XXXXX$ pour des gains moyens de l’ordre de 6 Millions de $
   - Modèles économiques : location, royalties, partage des bénéfices, fremium (vous ne payez que si vous réussissez à extorquer), fourniture de support, etc..

# IAM & LIMS

## Gestion des identités et des accès


Les 4 As :

- Authentification
- Autorisations
- Administration
- Audit

What is Federated Identity Management (FIM)? How does it work? (techtarget.com)

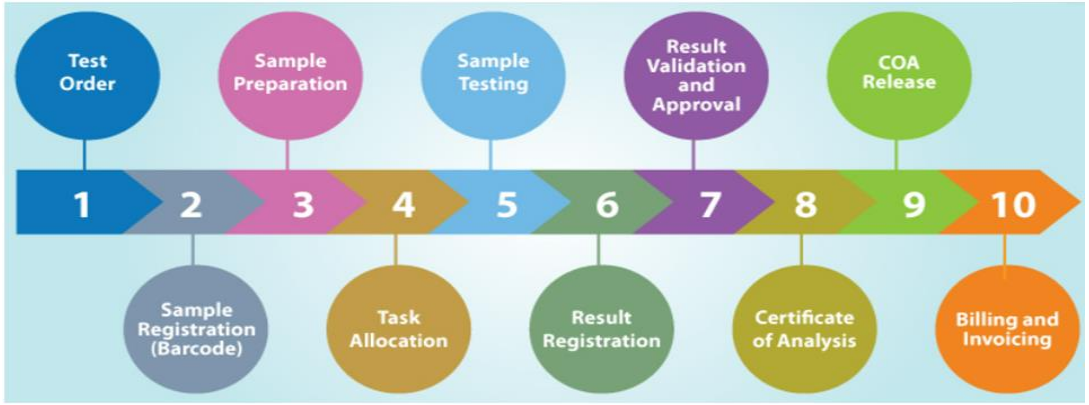
### Microsoft Active Directory

Une solution permettant de gérer les identités numériques et les accès aux systèmes informatiques dans l'hôpital (ou laboratoires privés)

Le « maître des clefs » : cible privilégiée des cyber attaques, car point focal de gestion des accès aux systèmes contenant les données (Base SQL)

C'est la colonne vertébrale de tout système d'information : Un annuaire d'entreprise qui référence tous les composants du SI, qui permet de s'authentifier, et qui permet de gérer les droits sur les applications.

## Systèmes de Gestion de l'informatique du laboratoire




(Figure Courtesy CloudLIMS)

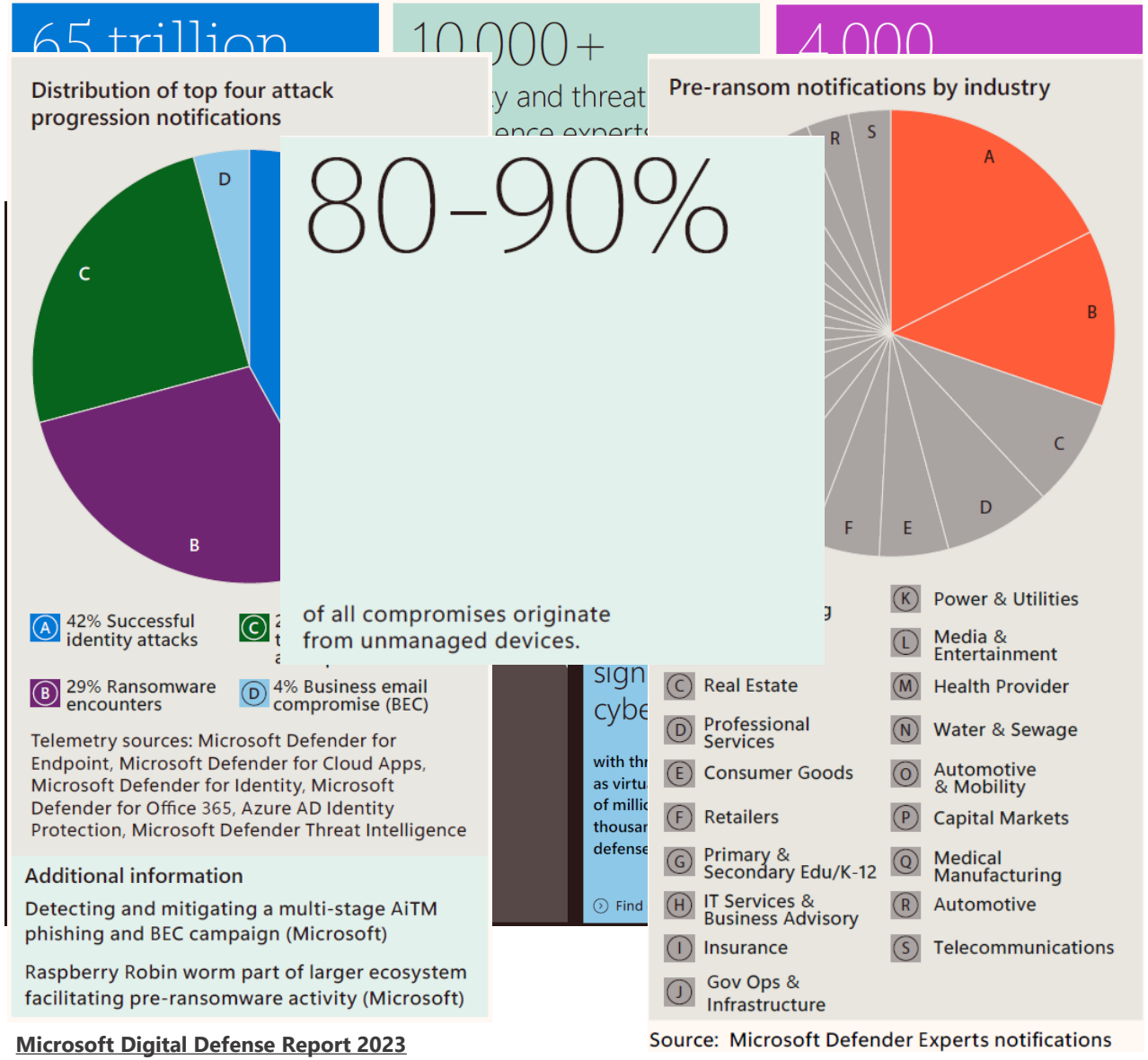
### Systèmes Propriétaires (Thermo, Abbott..)

Le LIMS est un outil essentiel dans les laboratoires modernes, aidant à gérer efficacement les informations et les processus liés aux échantillons et aux tests.

- **Base de Données Centrale** : Cœur du LIMS, où toutes les informations sont stockées de manière sécurisée.
- **Interface Utilisateur** : Permet aux utilisateurs du laboratoire d'interagir avec le système
- **Modules Fonctionnels** : Différentes sections du logiciel dédiées à des tâches spécifiques (gestion des échantillons, planification des tests, etc.).
- **Intégration avec d'Autres Systèmes** : Souvent, les LIMS sont conçus pour s'intégrer avec d'autres systèmes utilisés dans les hôpitaux ou les laboratoires.

# PANORAMA DES MENACES & VULNÉRABILITES

## Menaces




Microsoft Digital Defense Report 2023

## Vulnérabilités

**Vulnérabilités IAM :**

- Défaut de mise à jour des serveurs d'infrastructure
- Politique de mot de passe faible / Absence de MFA
- Pas de station « bastion » de gestion des systèmes IAM / pas de gestion séparée des comptes à hauts privilèges
- Pas de « Tiering » (segmentation) des ressources et des utilisateurs / Pas de politique du moindre privilège

**Vulnérabilités LIMS :**

- Retard dans la mise à jour des composants du LIMS (défaut éditeur) / Absence de livraison de patchs de sécurité
- Problème de gestion de la sécurité des OS « embarqués » dans des dispositifs médicaux / robots d'analyse
- Interfaces externes mal sécurisées (favoriser les API)
- Systèmes obsolètes / Absence de planification des feuilles de route d'évolution des systèmes
- Pas de « Role Based Access Control » / Moindre privilège

**Vulnérabilités opérationnelles :**

- Pas de zonage réseau / Pas de sécurité réseau (802.1X)
- Absence d'une politique de sauvegarde / Restauration robuste
- Plan de Reprise d'Activité « perfectible »
- Culture Cybersécurité lacunaire

# HYGIÈNE NUMÉRIQUE & PRÉVENTION DES RISQUES

## AUGMENTER LA SECURITE

- **Politique de mots de passe / Authentification forte**
- **Sensibilisation culturelle /éducation risque cyber** (*campagnes de tests*)
- **Mise à jour immédiate de tous les systèmes / traitement de la dette technologique**
- **Politique d'achat / Cybersécurité by design**(*réduction du risque à la source*)


## PLAN DE REPRISE (Informatique)

- **Politique de sauvegarde/ restauration avec SLA** (RTO/RPO) **systématiquement testée**(serveurs + données)
- **Mise en place d'un SOC** (Security Operations Center)
- **Mise en place d'un SIEM**(Security Information & Event Management)
- **Mise en place d'une segmentation + règle du privilège minimal**
- **Supervision de la Gestion de Configurations** (analyse d'impact)

## PLAN DE CONTINUITE (Organisation)

- **La cybersécurité est l'affaire de tous**
- **Le Plan de Continuité d'Activités (PCA)** doit assurer la continuité des soins dans les services (il va au-delà de l'IT)
- **Le PCA doit impliquer toutes les directions** (IT, juridique, communication, centrale…) et être documenté et évalué et testé régulièrement
- **Des approches « *Pre Mortem* » peuvent être réalisées** (en sus des retours d'expérience)

**1. Absence de confiance implicite**

Chaque interaction est considérée comme potentiellement non sécurisée, quelle que soit la position de l'entité dans le réseau

**2. Vérification de l’identité**

L'identité doit être vérifiée de manière continue pour s'assurer qu'elle est légitime.

**3. Principe de Moindre Privilège :** Chaque entité ne reçoit que les privilèges d'accès nécessaires pour accomplir ses tâches, réduisant ainsi la surface d'attaque potentielle.

- **4. Segmentation**

Le réseau est divisé en segments isolés, et les flux de communication entre ces segments sont strictement contrôlés.

**5. Surveillance et Détection Continuelles :** Toutes les activités du réseau, y compris le trafic interne, sont surveillées en permanence. Les comportements et les activités anormaux sont détectés en temps réel à l'aide d'analyses comportementales

**6. Réponse Rapide et Automatisée :** En cas de détection d'une menace, une réponse automatisée est privilégiée pour isoler la menace, révoquer les privilèges d'accès et minimiser l'impact de l'attaque.

# ZERO TRUST : NEVER TRUST / ALWAYS VERIFY


https://www.strongdm.com/zero-trust

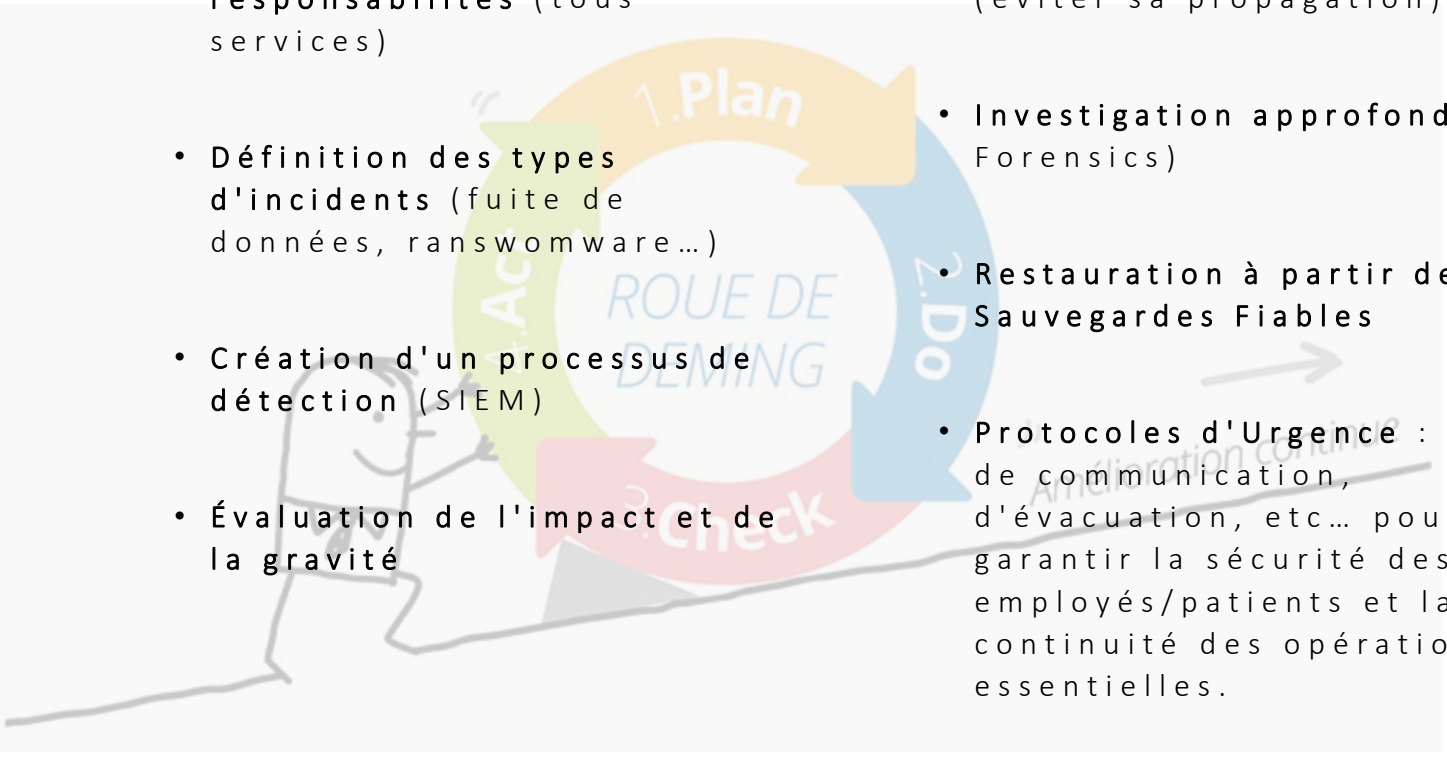
Le modèle Zero Trust est une approche de sécurité qui remet en question la notion traditionnelle de confiance implicite à l'intérieur du périmètre réseau.
Cela signifie que chaque utilisateur, appareil ou application, même s'ils se trouvent à l'intérieur du réseau, doit être constamment vérifié et authentifié pour accéder aux ressources sensibles.

# RÉPONSE AUX INCIDENTS & CONTINUITÉ D'ACTIVITÉ

## Élaboration d'un Plan de Réponse aux Incidents (PRI)

Un Plan de Réponse aux Incidents est un document essentiel qui prépare une organisation à faire face à des incidents de sécurité informatique. Voici les principales étapes pour élaborer un PRI :

- **Identification des responsabilités** (tous services)
- **Définition des types d'incidents** (fuite de données, ranswomware…)
- **Création d'un processus de détection** (SIEM)
- **Évaluation de l'impact et de la gravité**




## Stratégies pour la Récupération Post-Incident

Après la détection d'un incident, il est crucial de mettre en place des stratégies de récupération pour minimiser les perturbations et les dommages potentiels :

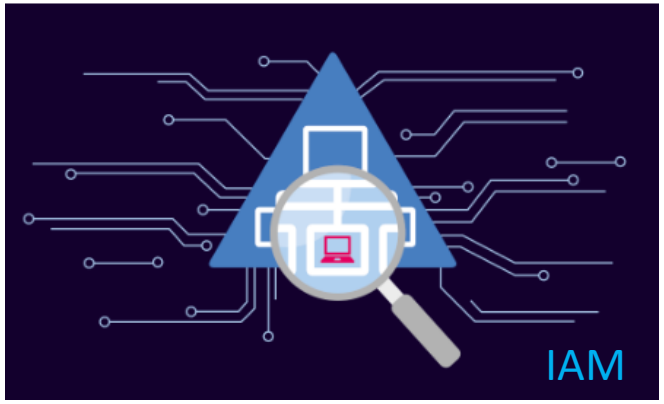
- **Isolation de l'incident** (éviter sa propagation)
- **Investigation approfondie** (IT Forensics)
- **Restauration à partir de Sauvegardes Fiables**
- **Protocoles d'Urgence** : Plans de communication, d'évacuation, etc… pour garantir la sécurité des employés/patients et la continuité des opérations essentielles.

## Mesures de Remédiation

Après la résolution d'un incident, des mesures de remédiation doivent être mises en place pour prévenir de futurs incidents similaires :

- **Analyse de l'incident :** Une analyse approfondie pour comprendre les failles de sécurité et corriger
- **Mises à jour de la Sécurité :** Les systèmes, les logiciels et les politiques de sécurité doivent être mis à jour en fonction des leçons apprises de l'incident.
- **Formation et Sensibilisation :** Les employés doivent être formés sur les meilleures pratiques de sécurité et sensibilisés aux risques potentiels.
- **Améliorations Continues :** La sécurité informatique est un processus continu. Les organisations doivent évaluer régulièrement leur PRI et leurs mesures de sécurité

# SÉCURISATION DES SYSTÈMES IAM & LIMS

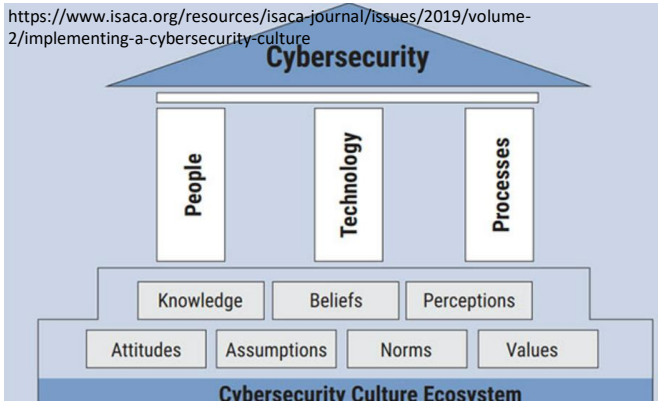



- Patcher régulièrement les contrôleurs de domaine systématiquement
- Segmentation et isolation réseau
- Fiches de poste opérationnelles et privilège minimal
- Révision des Politiques de groupes d'objets (GPO)
- PKI et gestion des certificats
- Journalisation et supervision temps réel
- Forêt Active Directory à Hauts Privilèges + Stations d'administration « bastion »


- Politique d'achat incluant des critères « cybersécurité »
- Le LIMS doit souscrire aux approches « Zero Trust »
- Authentification forte des utilisateurs (CPS),et des services applicatifs externes (Certificats)
- Implémentation native de RBAC « Role Based Access Control »
- Procédure de reprise sur incident majeur « scriptée » et automatisée (démarrage/arrêt « propres » des systèmes)
- Intégrer le LIMS au SIEM


- 1.Authentification moderne résistante au Phishing (MFA)
- 2.Moindre privilège appliqué à l'ensemble des services/systèmes
- 3. Environnements sécurisés par des solutions de type anti-malware/virus, endpoint detection& response, gestion des vulnérabilités, SOC, SIEM (zero trust)...
- 4. Implication du management (budget/investissement) pour la mise en conformité des systèmes et la promotion d'une culture de cybersécurité
- 5.Sauvegarde cloud automatique des systèmes et des données critiques

# LES PROFESSIONNELS DE SANTÉ & LA CYBERSÉCURITÉ





• **Sensibilisation aux Risques :** Il est essentiel de sensibiliser les biologistes médicaux aux risques liés à la cybersécurité

• **Formation en Cybersécurité :** Les biologistes médicaux doivent comprendre les meilleures pratiques en matière de protection des données, d'authentification, de gestion des mots de passe, et de détection des menaces.

• **Simulations d'Attaques :** Des exercices de simulation d'attaques, tels que des tests de phishing ou des exercices de réponse aux incidents pour s'aguerrir

• **Leadership et Engagement de la Direction :** L'engagement de la direction est essentiel pour créer une culture de la sécurité.

• **Communication et Sensibilisation Continue :** Les établissements de santé doivent régulièrement communiquer sur l'importance de la cybersécurité et encourager les professionnels de la santé à signaler les incidents et les comportements suspects.

• **Responsabilisation :** Intégrez la cybersécurité dans les objectifs de performance et les évaluations du personnel

• **Suivi des Tendances en Cybersécurité :** Les professionnels de la santé doivent rester informés des dernières tendances en cybersécurité(newsletter interne ?)

• **Mise à Jour des Systèmes et des Logiciels :** Développez une politique d'achat avec des critères « cyber »

• **Collaboration avec des Experts en Cybersécurité :** Le secteur de la santé peut collaborer avec des experts en cybersécurité pour évaluer la sécurité de ses systèmes et mettre en place des mesures de protection appropriées.

# VERS UN ECOSYSTÈME DE SANTÉ PLUS SÛR…

•**Collaboration Interdisciplinaire :** La cybersécurité dans le secteur de la santé nécessite une collaboration étroite entre les professionnels de la santé, les experts en cybersécurité, les responsables informatiques et les décideurs politiques. Cette collaboration est essentielle pour partager des connaissances et des meilleures pratiques.
•**Investissement Continu :** La cybersécurité doit être considérée comme un investissement continu dans le secteur de la santé. Les établissements de santé doivent allouer des ressources adéquates pour maintenir et améliorer la sécurité.
•**Surveillance Active :** La surveillance active des menaces et des vulnérabilités est essentielle pour détecter et contrer les cyberattaques avant qu'elles ne causent des dommages importants.

**1. Architectures « Zero Trust »**

Le modèle de cybersécurité « Carcassonne » (défense périmétrique) est obsolète !!!

Patchs de sécurité !!!

**2. Authentification renforcée**

Politique de mots de passe, MFA/ OTP, sécurisation de l'Active Directory (ou Annuaire d'Entreprise), Provisioning « self service » des identités

**3. Segmentation**

Des réseaux, des services/serveurs et des utilisateurs. Moindre privilège / Role Based Access Control (RBAC)

Contrôle des interfaces externes

**4. Politique d'Achats**

Il est essentiel que les impératifs de cybersécurité soient reflétés dans les politiques d'achat pour réduire la dette technologique et investir dans des éditeurs idoines

**5. Création d'une culture « cyber sécurité »**

C'est l'affaire des tous.

Sensibilisation et formation aux risques cyber (régulièrement mises à jour)

Veille technologique « cyber »

**6. PRI / PRA / PCA**

Élaborer des plans de réponse aux incidents pour réagir rapidement en cas de cyberattaque et assurer la continuité des activités critiques.

# RENFORCER VOTRE CYBERSECURITE

# DEVELOPPER UNE CULTURE « CYBER »

Quelques liens pour aller plus loin (en Anglais)

- Rapport de défense numérique Microsoft 2023 (MDDR) | Microsoft Security Insider
- Microsoft Cybersecurity Reference Architectures - Security documentation | Microsoft Learn
- Une infiltration d'un gang exploitant un RaaS
- Cours sur le cybersécurité (quelques videos de vulgarisation)

# MERCI POUR VOTRE ATTENTION


Jérôme Vétillard

HLS Industry Advisor

Microsoft

Jérôme Vetillard

Jerome.vetillard@microsoft.com