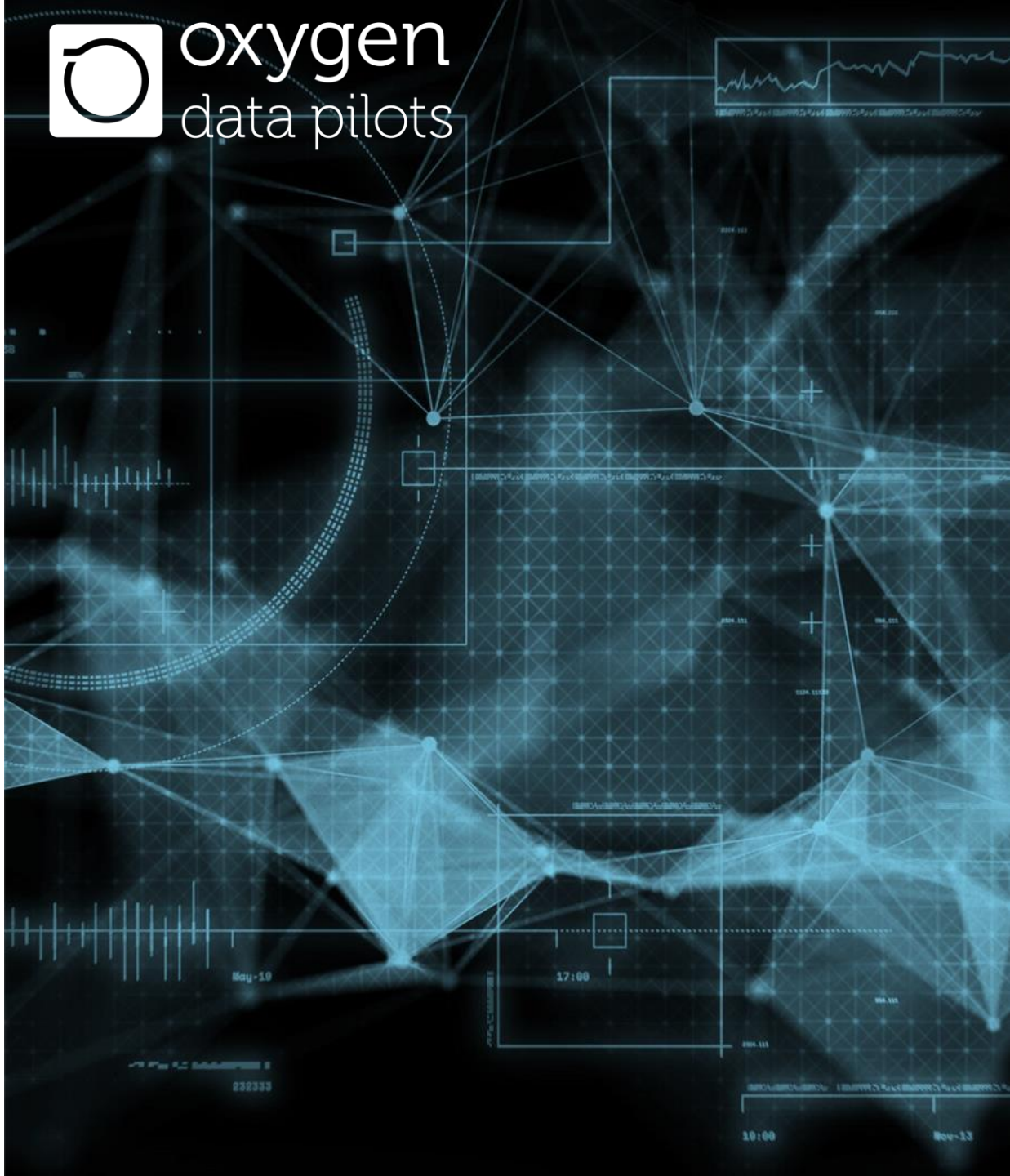
ARL Association des Responsables de Laboratoire de Suisse romande

JOURNÉE SCIENTIFIQUE D'AUTOMNE

JEUDI

10 OCTOBRE 2024

EN COLLABORATION AVEC OXYGEN DATA PILOTS



Ordre du jour

1) Les intervenants
2) Qui est Oxygen Data Pilots?
3) **Les cybermenaces dans le domaine médical**
4) **Les mesures de protection essentielles**
5) **La gestion des incidents de sécurité**
6) Cas pratique
7) Tour de table (Q&A)

oxygen
data pilots

/ CHAPITRE 1 /

Les intervenants

Vos orateurs

TOBIAS KULL

Directeur BU Cyber Sécurité

OLIVIER BUCHS

Directeur Opérationnel

oxygen
data pilots

/ CHAPITRE 2 /

Qui est Oxygen Data Pilots?

Qui sommes-nous ?

Oxygen – Data Pilots est une société technologique qui a très tôt identifié la convergence entre la cybersécurité et les métiers de l'infrastructure, du cloud avec pour objectif la gestion, la sécurisation et la récupération de vos données!

Nos valeurs depuis plus de 30 ans:

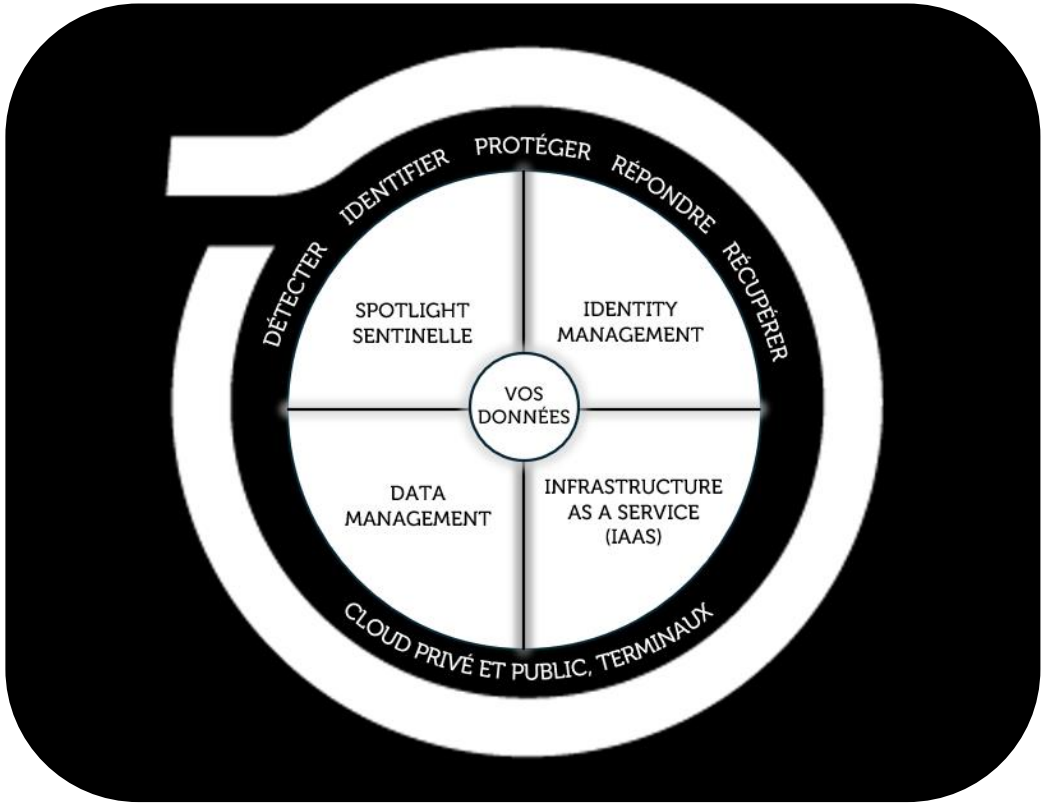
- Excellence
- Expertise métier et technologique
- Ecoute & satisfaction client
- Accompagnement client
- Innovation
- Capital humain

Notre métier? Protéger le vôtre!

Chez **Oxygen – Data Pilots** nous offrons des services informatiques spécialisés en Cybersécurité sur 4 axes:

- Identity Management
- Infrastructure as a service
- Data Management
- Spotlight Sentinelle

Développons ensemble un processus solide pour guider et mesurer vos progrès!



ARL Association des Responsables de Laboratoire de Suisse romande

/ CHAPITRE 3 /

Les cybermenaces dans le domaine médical

Panorama des cyberattaques ciblant le secteur médical

73%

des cyberattaques **réussissent** et ciblent particulièrement les données de l'organisation

Coût moyen d'une attaque

11Mio*

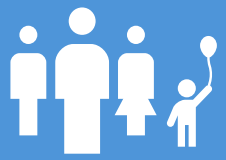
*le plus élevé des secteurs

60%

des cyberattaques utilisent des logiciels de **rançons**

55%

des violations impliquent des **informations personnelles de santé** (PHI)



171 Mio

de patients affectés

Motivations des attaquants (Quiz)

D’après vous, quels sont les principales motivations des attaquants ?

Rendez-vous sur Wooclap pour partager vos hypothèses

- wooclap.com
- Code d’accès : ARL101024

wooclap

Motivations des attaquants (Réponses)

Gains financiers

Les informations de santé personnelles (PHI) se vendent cher sur le marché noir généralement entre 100 et 250 dollars par dossier médical, car elles contiennent des informations détaillées (identité, historique médical, assurances, etc.).

Espionnage

Certaines attaques sont motivées par l'espionnage industriel ou l'accès à des informations sur des technologies médicales avancées, des traitements expérimentaux ou des recherches pharmaceutiques

Hacktivisme

Dans certains cas, les hacktivistes s'en prennent à des organisations médicales pour faire valoir des causes politiques ou éthiques.

Des attaques peuvent viser des cliniques pratiquant des avortements ou des entreprises impliquées dans des recherches controversées.

Sabotage

Les risques internes sont également une cause fréquente, qu'il s'agisse de vol de données par des employés mécontents ou d'erreurs internes.

En exemple, des accès non autorisés attribués par négligence ou par un processus de gestion des accès dysfonctionnel.

ARL Association des Responsables de Laboratoire de Suisse romande

/ CHAPITRE 4 /

Les mesures de protection essentielles

Mesures de protection essentielles

Gestion des identités

- Identification des comptes internes vs externes
- Politique d'accès (RBA) et mots de passe
- Mise en place des authentifications à 2 facteurs

Gestion des équipements (actifs)

- Identification des actifs internes, externes et laboratoires
- Sécurisation des postes de travail
- Cycle de vie des mises à jour

Protection des données

- Sensibilisation des utilisateurs aux données patients
- Portail d'échange sécurisé avec les partenaires
- Chiffrement des données en transit et à froid
- Politique de moindre privilège pour les applications sensibles et/ou systèmes critiques pour l'entreprise
- Cycle de vie de la donnée (patients)

ARL Association des Responsables de Laboratoire de Suisse romande

/ CHAPITRE 5 /

La gestion des incidents de sécurité

Quel est votre posture face aux situations de crise ? (Quiz)

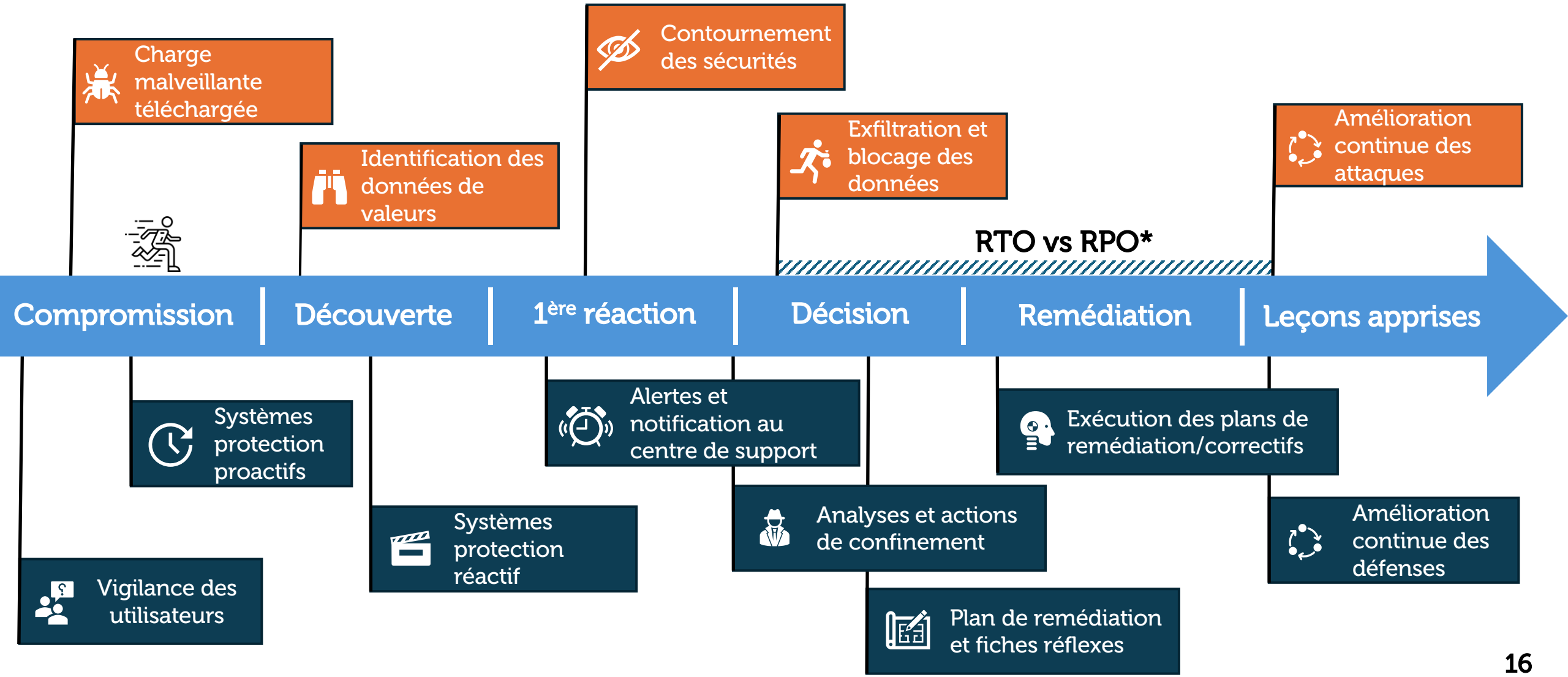
Quel est votre niveau d'expertise face à une situation de crise ?

Rendez-vous sur Wooclap pour partager vos expériences

- **wooclap.com**
- **Code d'accès : ARL101024**

wooclap

Cycle de vie d'un incident cyber



Gestion des incidents (incl. sécurité)

1. Planifier (PLAN)

- Identifier les systèmes critiques vs non-critiques
- Identifier les scénarios pouvant mener à un risque cyber (ou opérationnel)
- Déterminer les durées cible RPO/RTO
- Challenger la raison d'être des mesures proactives et réactives en place
- Développer les mesures additionnelles et/ou compensatoires
- Construire les plans de réponses (fiches réflexes) et communication
- Construire un agenda de mise en place réaliste et réalisable

2. Développer (DO)

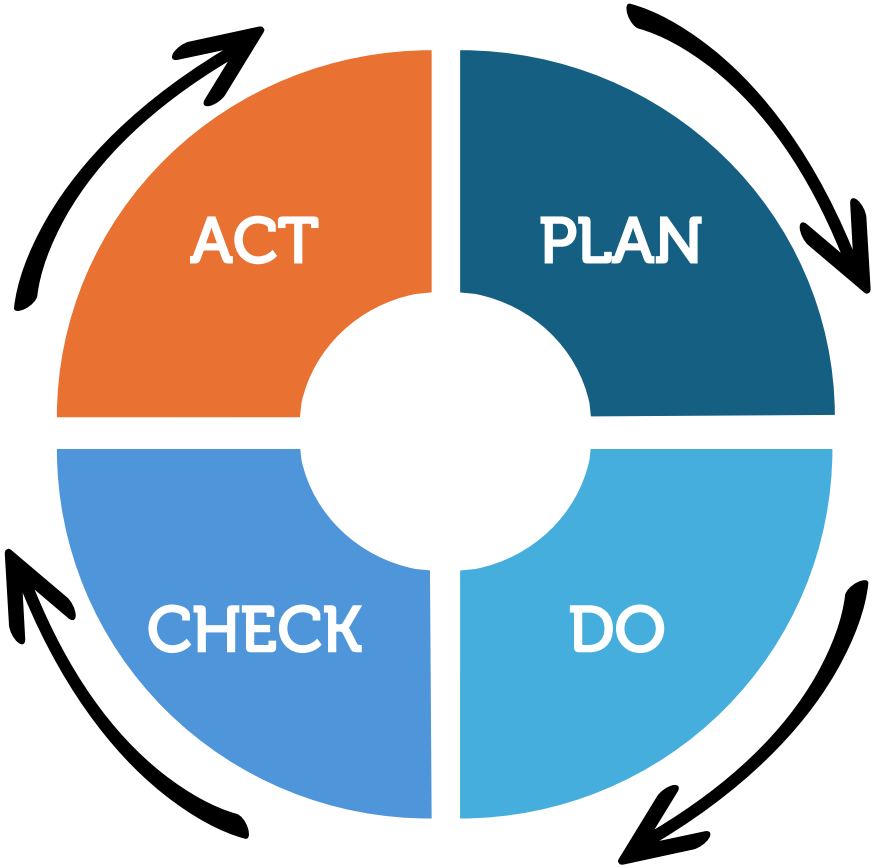
- Exécutez le plan d'action élaboré dans la phase précédente
- Arbitrage sur les priorités et ajustement du calendrier

3. Contrôler (CHECK)

- Evaluer l'efficience des mesures
- Tester et valider les plans de réponses
- Reboucler pour arbitrage avec la phase No2 après les évaluations et tests

4. Agir (Act)

- Prenez des décisions en fonction des résultats obtenus dans la phase No3



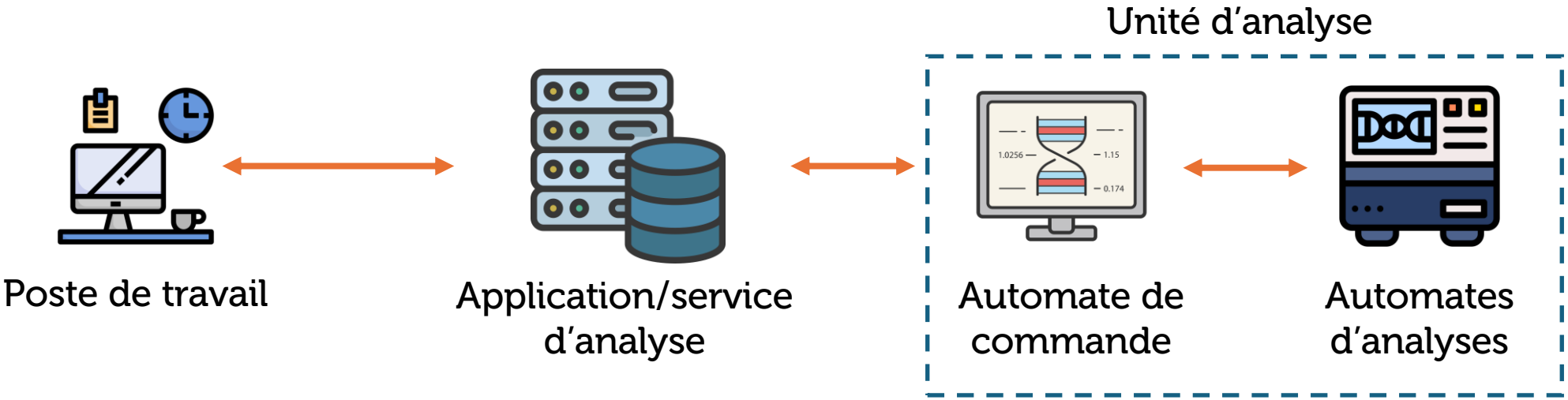
ARL Association des Responsables de Laboratoire de Suisse romande

/ CHAPITRE 6 /

Mise en situation

Cas pratique (1/4)
→ automates d'analyses connectés

Description fonctionnelle d'une solution d'analyse informatisée permettant le traitement automatisé de divers types d'analyses médicales en laboratoire.



Cas pratique (2/4)
→ automates d'analyses connectés

Impacts métier

- Identifier les processus métiers
- Garantir les engagements/partenariats
- Définir le RTO/RPO

Actifs

- Machine-outil connectée
- Système critique et sensible
- Machine non-gérée* par l'IT

Identités

- Identifier les comptes internes
- Identifier les comptes externes
- Identifier les comptes génériques

Accès

- Connectivités uniquement internes
- Dépendances aux serveurs d'analyses
- Maintenances annuelles

Cas pratique (3/4)
→ automates d'analyses connectés

Protections réactives et proactives

- Agent MDR sur la station d'analyse
- Filtrage Firewall interzones
- Bloquer les interfaces USB*
- Indépendance au réseau électrique
- Indépendance aux connexions Internet

Protections des données

- Chiffrement des données sensibles
- Protection des impressions (Watermark)
- Sécuriser la plateforme d'échange des rapports d'analyses
- Utilisation de données anonymisées/pseudonymisées
- Sauvegardes externalisées

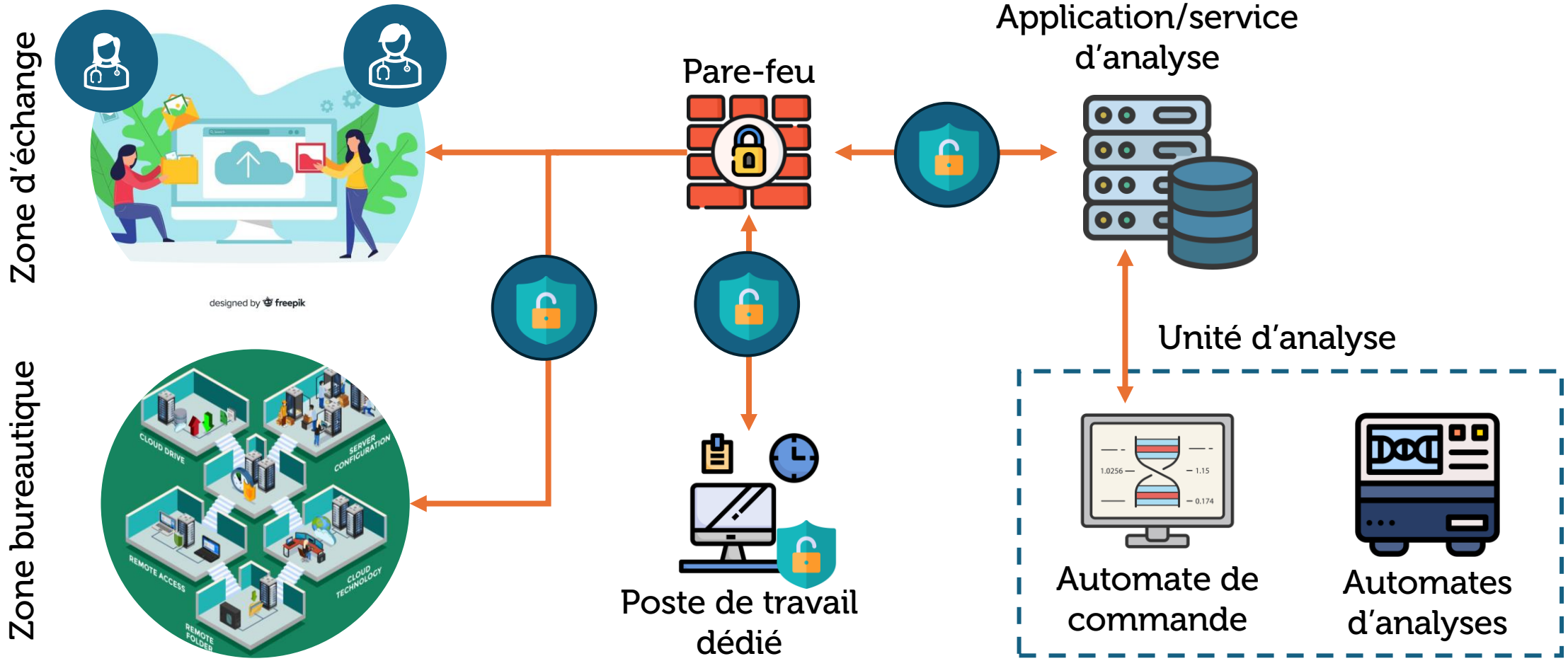
Gestion de crise

- Plan de communication interne et externe
- Exercice et simulation de crise
- Equipes et équipements dédiés à la crise
- Guide d'analyses manuels (Stockage, Papier)
- Guide d'extraction et transmission des rapports d'analyses

Accès

- Stations de travail dédiées aux analyses
- Réseau dédié aux machines critiques
- Réseau isolé de la bureautique
- Restriction d'accès aux serveurs d'analyse
- Limiter les accès utilisateurs/administrateurs
- Validation des accès de maintenance

Cas pratique (4/4)
→ automates d'analyses connectés

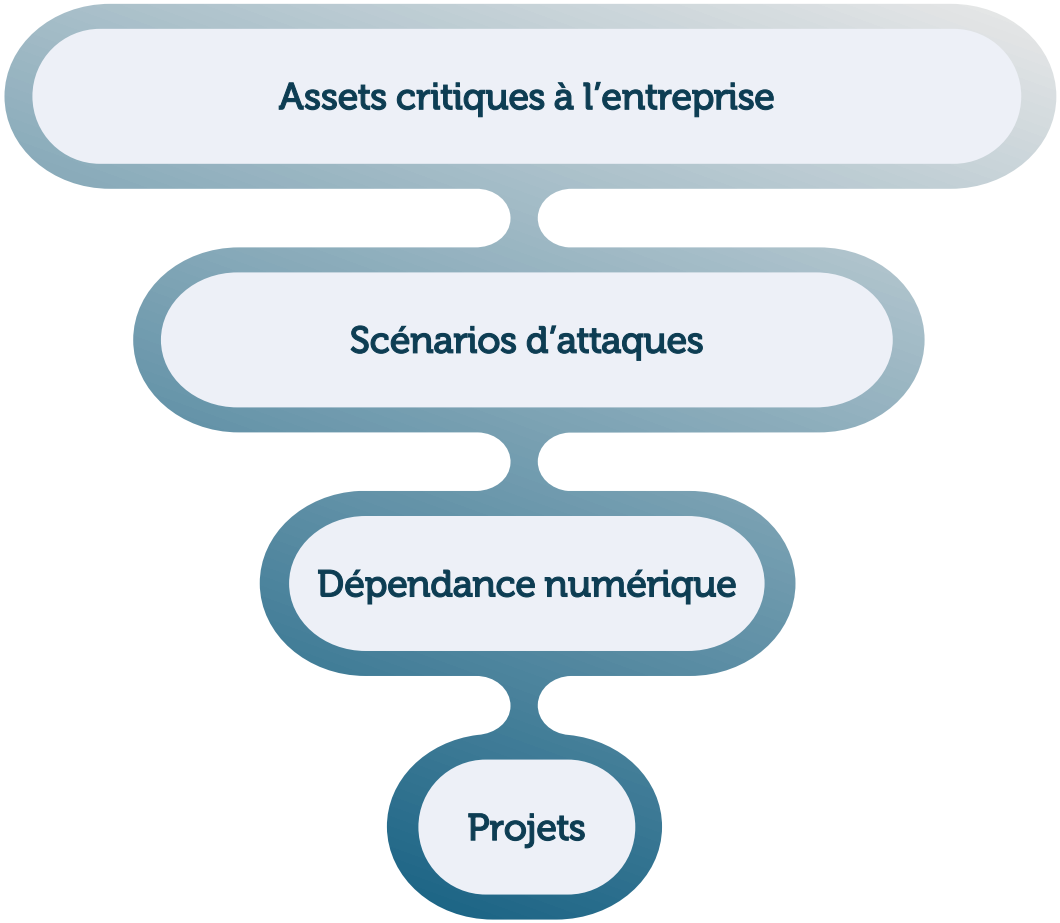


ARL Association des Responsables de Laboratoire de Suisse romande

/ CHAPITRE 7 /

Take away

Le résumé…



…à prendre avec vous

1) Gestion des actifs

- Identifier vos assets critiques à l'entreprise

2) Gestion du risque

- Modéliser les scénarios d'attaques impactant vos assets critiques et diminution de la matérialisation de vos cyber risques

3) Plan de continuité

- Diminution de la dépendance liée au numérique

4) Portefeuille de projets

- Piloter et prioriser vos chantiers cyber

ARL Association des Responsables de Laboratoire de Suisse romande

/ CHAPITRE 8 /

Tour de table (Q&A)

Merci pour votre attention!

Notre métier ? Protéger le vôtre !

Si vous souhaitez obtenir des informations supplémentaires

Jeff **Curcio**
Fondateur & Expert en Cyber Gouvernance et intégrité numérique

j.curcio@oxygen-it.ch

0848 848 989
+41 76 399 20 00

Olivier **Buchs**
Directeur Opérationnel

o.buchs@oxygen-it.ch

0848 848 989

Tobias **Kull**
Directeur BU Cybersecurity

t.kull@oxygen-it.ch

0848 848 989

oxygen
data pilots