RÉPUBLIQUE FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

Ne pas diffuser
aux joueurs en amont
de l'exercice

# EXERCICE DE CRISE CYBER JOP 2024

## Présentation du scénario

# SOMMAIRE


1 Présentation du scénario

2 Schéma d’attaque C1

3 Schéma d’attaque C2

4 Schéma d’attaque C3

# 1. PRÉSENTATION DU SCENARIO

***En amont de l'évènement sportif :***

La méthode utilisée pour permettre une introduction sur le système d'information se fera par le biais de 4 possibilités différentes :
**Hameçonnage** d'un salarié, **Clé USB** piégée, exploitation d'une **vulnérabilité « 0-jour », corruption d'un prestataire**

Nous sommes le **jour** d'un **grand évènement sportif** dans le cadre des **JOP2024**. Votre organisation **accueille** et participe à cet **évènement** de **grande ampleur** et se retrouve sous le feu des projecteurs : la compétition est retransmise en direct à la télévision.

## 01

**Dysfonctionnements applicatifs**

Des utilisateurs constatent des **dysfonctionnements** sur les applications permettant d'assurer le bon déroulé de l'évènement. *Exemple* : Accessibilité aux caméras, accès à de la documentation, site web inaccessible.

## 02

**Soupçons de cyber attaque et demandes d'investigations de la part du management**

Après de nombreuses **plaintes utilisateurs**, le management décide **d'investiguer** sur les **raisons** des **indisponibilités** constatées.

## 03

**Impacts "en cascade" liés à la cyber attaque**

Les gestionnaires de la crise reçoivent des **demandes** de la part des **collaborateurs** sur la résolution des **impacts** et les **contournements** à mettre en place.

## 04

**Fuite de données et enjeux de communication**

**Publication** sur le **dark web** de données confidentielles issues des applications critiques. **Réaction** en **chaîne** des **médias** pour obtenir des informations sur la crise en cours. Les **autorités publiques** souhaitent avoir **l'assurance** que la situation est maîtrisée.

## 05

**Définition d'une stratégie de continuité et de reprise d'activité**

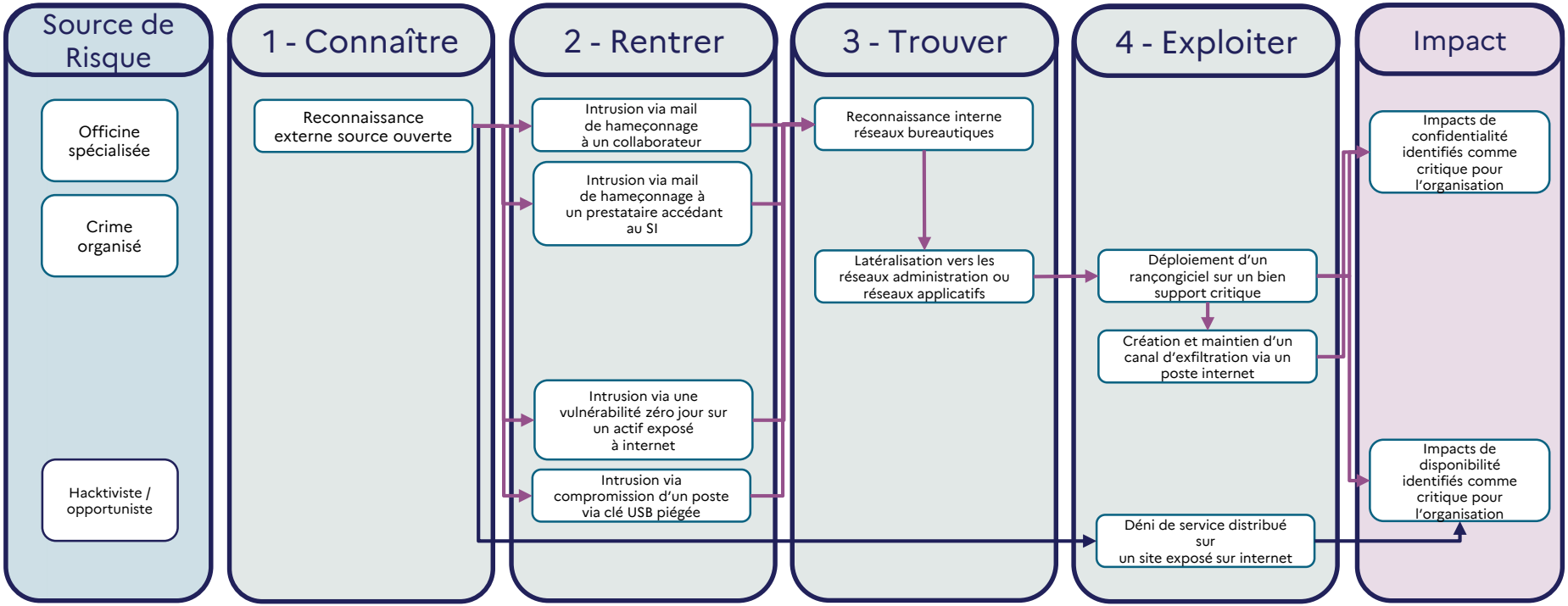
Elaboration d'une **stratégie de continuité / reprise d'activité** par les gestionnaires de crise.

## 06

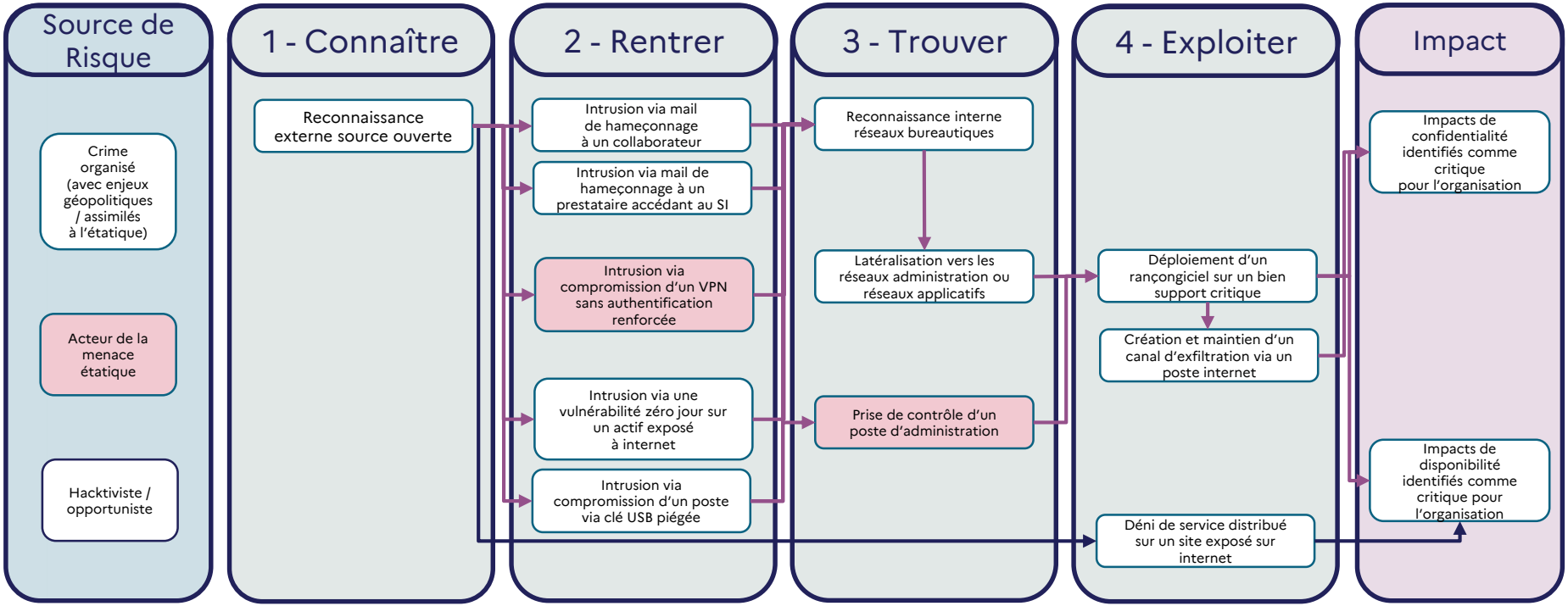
**Gestion juridique, résolution de la crise et plan d'action**

Organisation du **dépôt** de **plainte** auprès des **autorités compétentes**
Vérification des impacts sur l'évènement de la journée (*sécurité des participants, diffusion, etc.)*
Définition d'un **plan d'action** sur la supervision du SI.

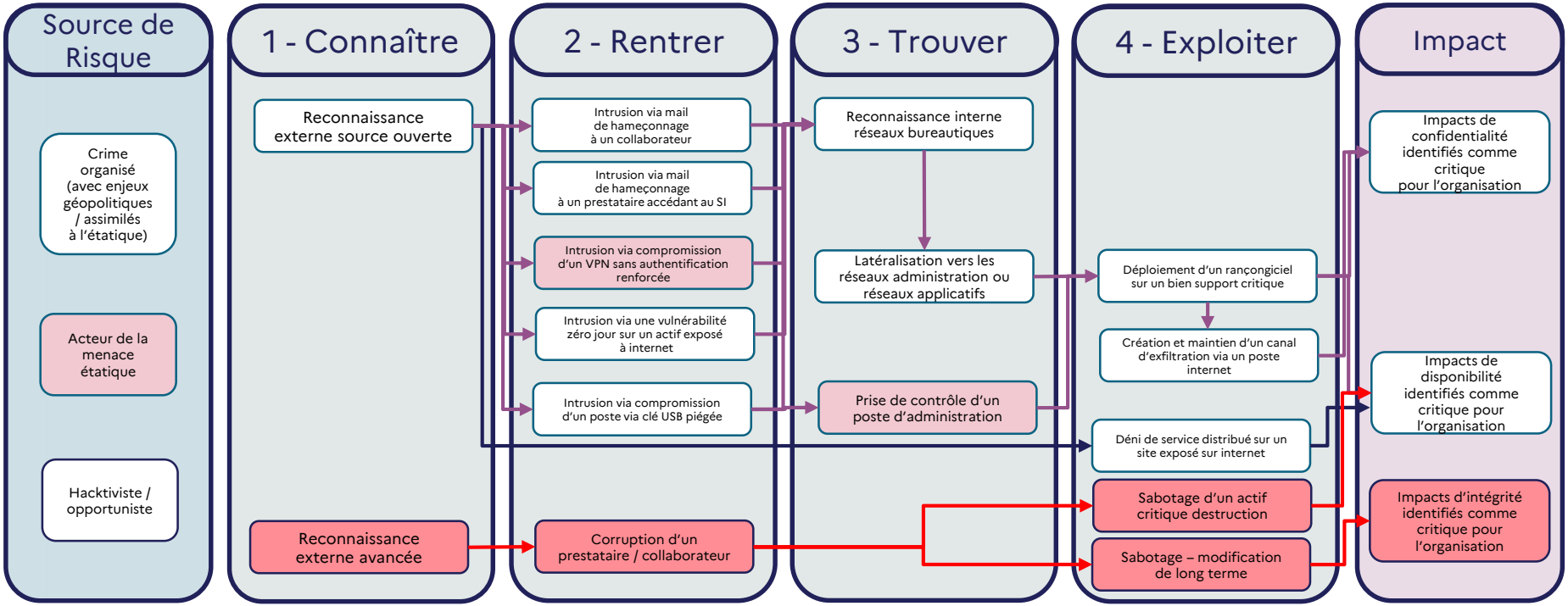
# 2. SCHÉMA D'ATTAQUE (COMPLEXITÉ 1)



# 3. SCHÉMA D'ATTAQUE (COMPLEXITÉ 2)



# 4. SCHÉMA D'ATTAQUE (COMPLEXITÉ 3)



RÉPUBLIQUE
FRANÇAISE

*Liberté*
*Égalité*
*Fraternité*