



# Accompagnement gestion de crise cyber

Proposition Commerciale

03 Juin 2024

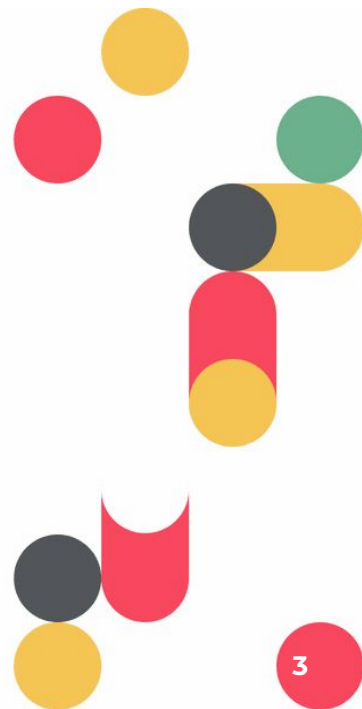


# agenda.

1. Contexte du projet
2. Méthodologie
3. Conduite du projet

# 1

## Contexte du projet.



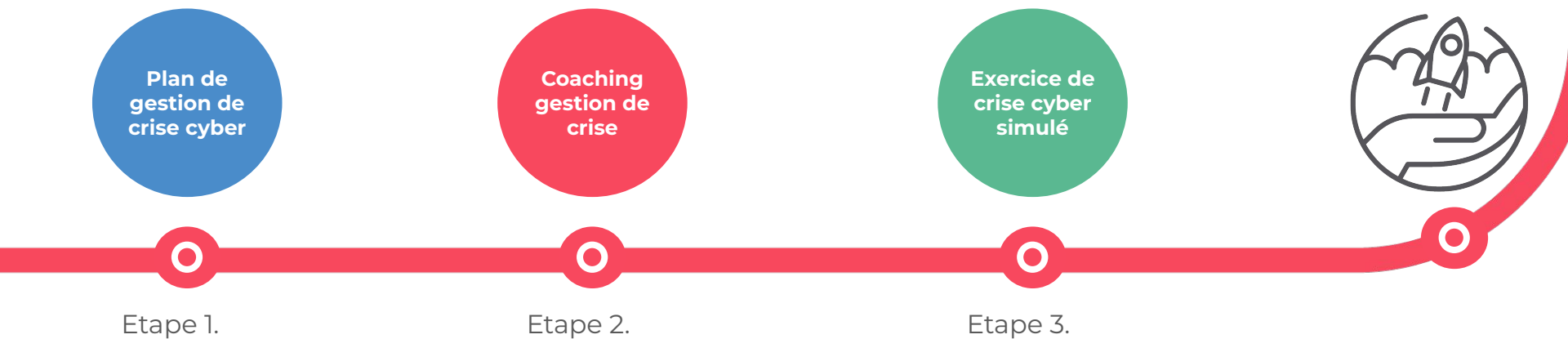
# Vos besoins.

## Rappel du contexte & objectifs

Dans la continuité de la précédente prestation, **la CNAM** souhaite être accompagné dans la mise en place de leur stratégie de gestion de crise cyber, comportant trois phases :

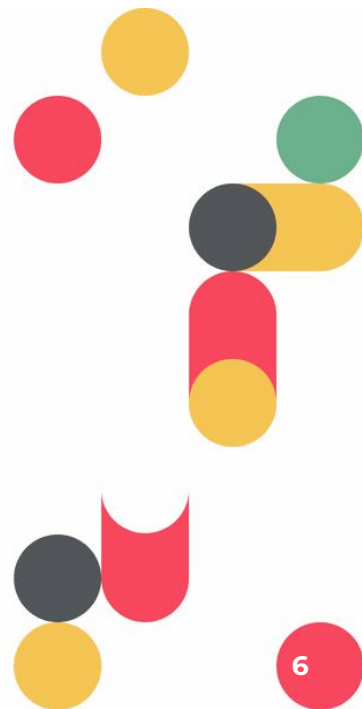
1. Rédaction de son **Plan de gestion de crise décisionnelle et opérationnelle** incluant les protocoles de déclenchement, et l'organisation de la cellule de crise, avec un mode d'utilisation aussi simple de déploiement que de mise en œuvre en cas de crise cyber, et **notamment un plan de confinement** .
2. La mise en place d'une **action de formation et de coaching dédiée à la gestion de crise cyber** ,
3. La conception et l'animation d'un **exercice simulé de crise cyber** (en option).

# Vue d'ensemble de la démarche.



# 2

## Méthodologie.



# Plan de gestion de crise cyber et plan de confinement.

## Entretiens

Quand : à effectuer au plus tôt  
Entretiens : ~6

## Workshop

- Thème : préparation des stratégies de gestion de crise, de confinement et des modes opératoires  
Durée : 1h30 par workshop  
Workshops : ~6

## Livraison Finale

Après validation

- DSI
- Périmètre Infrastructures, réseaux et Production
- Périmètre Architecture
- Périmètre Patrimoines applicatifs métiers
- RSSI / RPCA

- Analyse des impacts d'arrêt des activités
- Définition, échange sur le contenu de la matrice de seuil de crise selon les impacts
- Identification des rôles et responsabilités des acteurs de réponse à incidents cyber
- Arbre de décision et processus d'escalade en fonction de la gravité de l'incident cyber
- Organisation de crise et de réponse à incidents cyber
- Stratégie de communication de crise
- Définition des stratégies de mise en sécurité
- Préparation des modes opératoires (fiche réflexes)

- Organisation de crise et de réponse à incidents
- Plan de confinement et de mise en sécurité
- Plan de communication de crise

# Plan de gestion de crise cyber et plan de confinement.

Livrable et RACI



## Livrables Devoteam

### Procédure V1

### Workshop

### Procédures finales

## Livrables CNAM

#### Procédure

- ❑ Organisation des cellules de crise
- ❑ Matrice de seuils de crise/impacts
- ❑ Alerte, qualification, mobilisation, gestion de la crise, démobilisation et post-crise
- ❑ Stratégie de confinement technique
- ❑ Plan de remédiation opérationnel / cyberdéfense

#### Annexes opérationnelles

- ❑ Annuaires, check-list des actions, rôles et responsabilités, communication de crise...

#### En distanciel

- ❑ Equipes techniques
- ❑ RSSI / RPCA
- ❑ Equipe projet Devoteam

#### Durée

- ❑ Environ 1h30 / workshop

- ❑ Organisation du dispositif de gestion de crise (RACI, etc) et de réponse à incidents cyber

- ❑ Plan stratégique de mise en sécurité

- ❑ PV des modes opératoires

#### Prérequis

- ❑ BIA (s'il existe)
- ❑ Documentation de crise
- ❑ Documentation d'architecture technique (applicative, infra,...)
- ❑ Rapport d'audit

#### Validation

- ❑ Organisation du dispositif de gestion de crise (RACI, etc.) et de réponse à incidents cyber
- ❑ Plan de confinement
- ❑ Modes opératoires



# Coaching gestion de crise.

## Thèmes et organisation

### Pilotage de crise

Durée : 1 jour

- Alerte, mobilisation
- Animation des points de situation
- Communiquer aux métiers

### Gestion opérationnelle de la crise cyber

Durée : ½ jour

- Analyser & qualifier
- Prioriser les informations reçues et à traiter
- Gérer les intervenants extérieurs : prestataires, CNIL, ANSSI...

### Cas pratiques

- Exemples: site, activation des prestataires, RGPD...




**Livrable & validation requis**

- Liste des participants
- Fonctionnement validé : ½ jour Pilotage de crise, ½ jour Communication de crise, ½ jour cyber (opérationnel)

# Préparation et animation d'un exercice de crise cyber simulé.


## Formation

Durée : 1 journée

- 
- Pilotage de la crise (alerte, mobilisation, animation des points de situation, communication,...)
  - Gestion opérationnelle de la crise (analyse, qualification, mise en œuvre de réponses,...)


## Préparation

Durée : ½ journée

- 
- 3 synopsis avec 1 synopsis validé
  - 1 scénario avec phases clés
  - Chronogramme et *inputs* réalistes : périmètre IT à valider avec le SPOC

## Exercice

Durée : ½ journée

- 
- Animation de l'exercice sur table
  - Observation de l'exercice
  - Retour à chaud

## Bilan

1 à 3 semaines après l'exercice  
Durée : 2 heures

- 
- Retour à froid
  - Axes d'amélioration

# Préparation et animation d'un exercice de crise cyber

## Phase 1 Formation



- Planning de formation
- Support de formation
- Liste des participants
- Fonctionnement validé

## Phase 2 Préparation



- Scénario
- Chronogramme
- Inputs
- Objectifs de l'exercice
- SPOC
- Liste des cellules joueuses
- Annuaire participants
- Documentation de crise
- Documentation IT (serveur, IP, app...)
- Description des outils : BAL, whatsapp, n° audio...
- Validation des inputs techniques notamment

## Phase 3 Exercice



- Support d'animation/brief des joueurs
- Grille d'évaluation
- Débriefing à chaud
- Logistique : salles par cellules et animation
- Ressources : un a deux animateurs (et observateurs si requis)

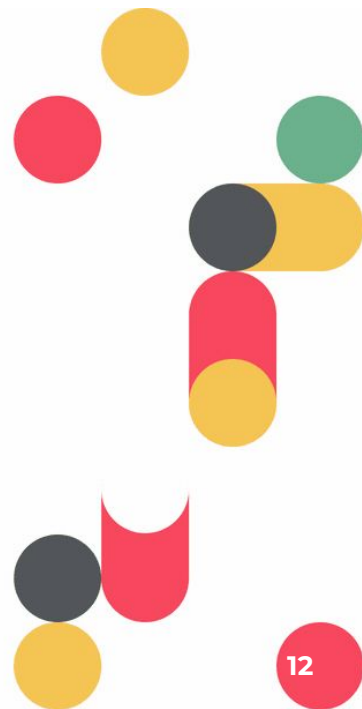
## Phase 4 Bilan



- Retour à froid: bilan et axes d'amélioration
- Support de restitution
- Réunion de restitution avec parties prenantes nécessaires

# 3

## Conduite du projet.



# Suivi du projet.



## Kick-off

### Modalités

Démarrage du projet 1h (visio)

### Participants

- SPOC CNAM
- RSSI CNAM
- Chef de projet Devoteam

### Sujets

- Déroulement de la mission
- Planning des interventions
- Pré-requis : documentation, logistiques...



## Points de suivi opérationnels

### Modalités

30min/semaine

### Participants

- SPOC CNAM
- Chef de projet Devoteam
- Membres additionnels si requis : MLA, experts Devoteam...

### Sujets

- Avancée opérationnelle
- Points bloquants
- Suivi des validations/livrables



## Réunion de bilan

### Modalités

Fin du projet  
2h présentiel ou visio

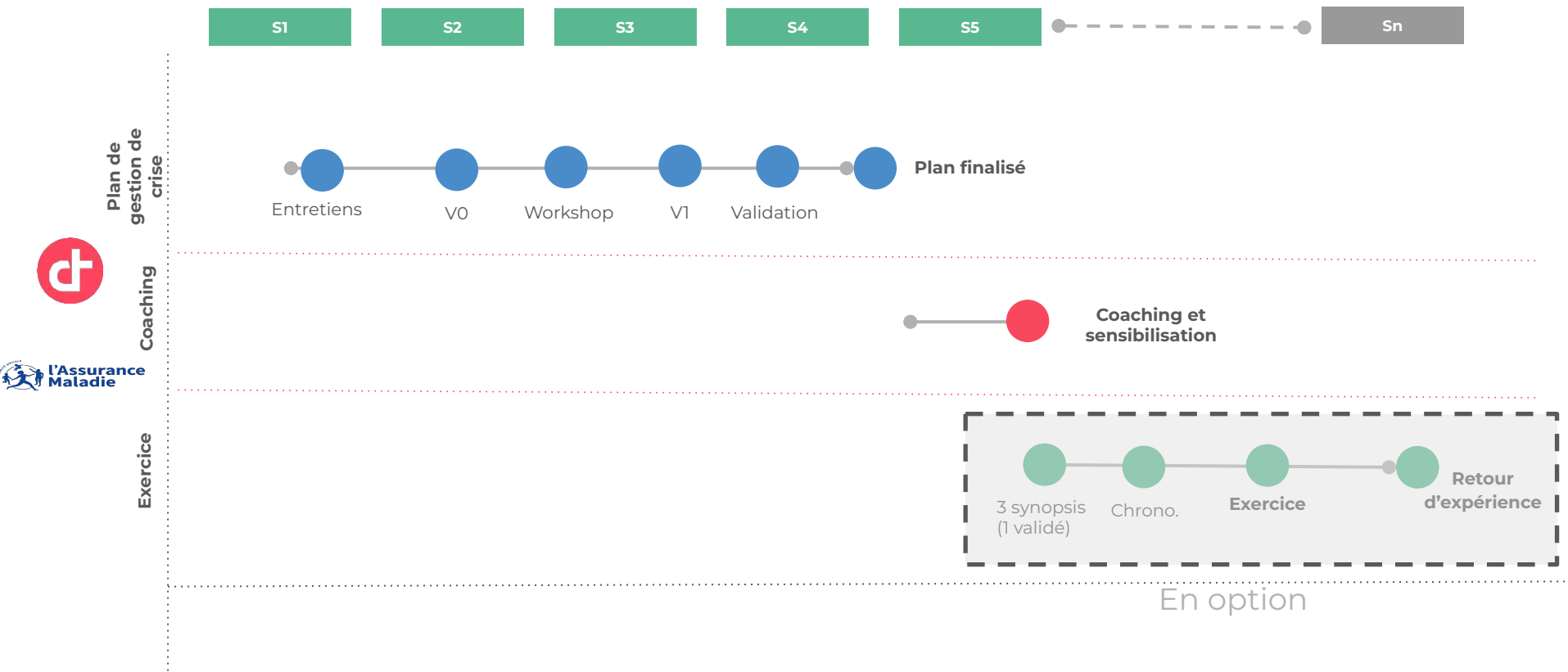
### Participants

- Equipe projet CNAM
- Equipe projet Devoteam

### Sujets

- Bilan de la mission
- Conclusions de la mission et du projet

# Planning prévisionnel



# Plan de charge

Total hors exercice	Experts crise Cyber J/H
<b>Plan de gestion de crise</b>	
Workshop et comité	6
Elaboration du plan de gestion de crise	7
Elaboaration du plan de confiement	6
<b>Coaching</b>	
Préparation des supports	3
Coaching "Pilotage de crise"	2
Coaching "Gestion opérationnelle de la Cyber crise"	1
<b>Total hors exercice</b>	<b>25</b>
<b>Exercice (en option)</b>	
Construction et préparation de l'exercice	6
Animation & observation	3
Retour d'expérience et amélioration	3
<b>Total</b>	<b>37</b>

# Equipe projet dédiée



**Kais STAMBOULI**  
**Expert PCA et gestion de crise**

**Garant :**

- De la réalisation de la mission et de la relation client
- Du respect des engagements et de la qualité des livrables
- De la définition du chronogramme et du synopsis volet cyber
- Expertise crise cyber

**En charge :**

- De la rédaction des livrables
- Du respect des engagements et de la qualité des livrables

**+10 ans : PCA, crise, cyber**



## Équipe d'experts en appui

**En charge :**

- De l'expertise technique
- De la revue de la documentation
- De l'animation des workshops avec les équipes techniques

**Profils:**

**Experts continuité d'activité & crise**