

Communication de crise 2.0 – Deepfakes, viralité algorithmiques et IA / Le programme Déroulé opérationnel sur 3 jours

Jour 1 : Alignement doctrinal, nouveaux périls et détection (8 heures)

Horaires	Module & Contenu opérationnel
09:00 – 11:00 (2h00)	PARTIE 1 : Préquelle — Fondamentaux & Résilience institutionnelle • Diagnostic d'entrée : alignement du vocabulaire de crise et benchmarking des réflexes. • Audit d'identité, socle de valeurs et cartographie critique des parties prenantes. • Définition des messages clés d'autorité : ce qui doit rester lisible sous l'opacité.
11:00 – 11:15	<i>Pause pédagogique</i>
11:15 – 13:00 (1h45)	PARTIE 2 (Début) : Le basculement 2.0 & L'illusion de la preuve • Les trois basculements : compression du temps (< 60 mn), inversion de la preuve et obsolescence des réponses classiques. • La mécanique des réseaux : pourquoi la viralité ne récompense pas la vérité mais l'amplitude. • Typologie des menaces : faux audios, deepfakes vidéo et documents falsifiés.
13:00 – 14:00	<i>Pause déjeuner</i>
14:00 – 16:00 (2h00)	PARTIE 2 (Suite) : Détection technique & Protocole « Doubt by Default » • Méthodologie d'investigation : outils d'authentification des contenus audio et vidéo manipulés. • Mise en œuvre du protocole de doute systématique avant toute qualification publique. • Analyse des flux et identification des signaux faibles sur les canaux émergents.
16:00 – 16:15	<i>Pause pédagogique</i>

16:15 – 18:15 (2h00)	PARTIE 2 (Fin) : Arènes numériques & Surveillance des interfaces • Les algorithmes de recommandation face à la parole publique. • Exercices sur répliques d'interfaces de réseaux sociaux : simulation de flux hostiles sur répliques de X, TikTok et LinkedIn.
--------------------------------	---

Jour 2 : Riposte d'autorité, simulations chronométrées et IA en cellule de crise (8 heures)

Horaires	Module & Contenu opérationnel
09:00 – 11:00 (2h00)	PARTIE 3 (Début) : L'architecture de la riposte sous 60 minutes • La chute du temps de réponse utile : pourquoi et comment tenir sous l'heure. • Élaboration des déclarations d'attente conservatoires (<i>holding statements</i>). • L'arbitrage psychologique : calibrer l'empathie institutionnelle face à la posture défensive/légaliste.
11:00 – 11:15	<i>Pause pédagogique</i>
11:15 – 13:00 (1h45)	PARTIE 3 (Suite) : Simulations chronométrées d'urgence • Exercice sous stress : rédaction et validation d'un <i>holding statement</i> en moins de huit (8) minutes. • Débriefing à chaud : identification des failles syntaxiques, des hésitations et du risque juridique.
13:00 – 14:00	<i>Pause déjeuner</i>
14:00 – 16:00 (2h00)	PARTIE 3 (Suite) : Intégration de l'IA générative en cellule de crise • Rédaction assistée par IA : stress-tester des scénarios et simuler les angles d'attaque de la presse. • Intégration des bibliothèques de prompts dédiés à la gestion de crise dans la chaîne de commandement.
16:00 – 16:15	<i>Pause pédagogique</i>

16:15 – 18:15 (2h15)	PARTIE 3 (Fin) : La bataille narrative & Transparence radicale • Riposte face à un deepfake en 4 étapes : activation de la doctrine <i>Starve the Beast</i>, riposte multicanale et contre-récit. • Simulation générale : gestion d'une fuite de document stratégique falsifié.
-------------------------	---

Jour 3 : Reconstruction, immunité institutionnelle & Outillage (4 heures – Matin)

Horaires 09:00 – 10:45 (1h45)	Module & Contenu opérationnel PARTIE 4 (Début) : Sortie de crise et reconstruction réputationnelle • La crise finit, la confiance se reconstruit : consolider la confiance publique après la déflagration. • Restaurer durablement l'image auprès des partenaires stratégiques et des tutelles. • Le front interne : remobiliser les équipes après l'épreuve de l'invective.
---	---

10:45 – 11:00 *Pause pédagogique*

11:00 – 12:15 (1h15)	PARTIE 4 (Suite) : Capitalisation & Check-list d'activation immédiate • Mise en route d'une cellule de crise pas à pas : les 5 premières décisions à acter. • Rédaction des protocoles d'immunité permanente au sein de vos organisations.
12:15 – 13:00 (0h45)	Clôture et remise du Kit opérationnel • Remise du Guide Méthodologique 2026 au format PDF interactif. • Transmission de la bibliothèque de scénarios types et de la base de prompts IA. • Délivrance des Attestations officielles de formation par SINE QUA NON conseil.

13:00 – 14:00 *Pause déjeuner*

APRÈS-MIDI OUVERTE Grande simulation collective et réseautage

14:00 – 16:00	La simulation inter-organisations Mise en situation réelle où participants et invités extérieurs jouent une séquence d'attaque informationnelle collective pour tester les réflexes sous un regard neuf.
16 : 00 ...	Débriefing & Réseautage Échanges informels autour d'un cocktail pour débriefer l'exercice, confronter les pratiques et tisser des liens entre décideurs et communicants.