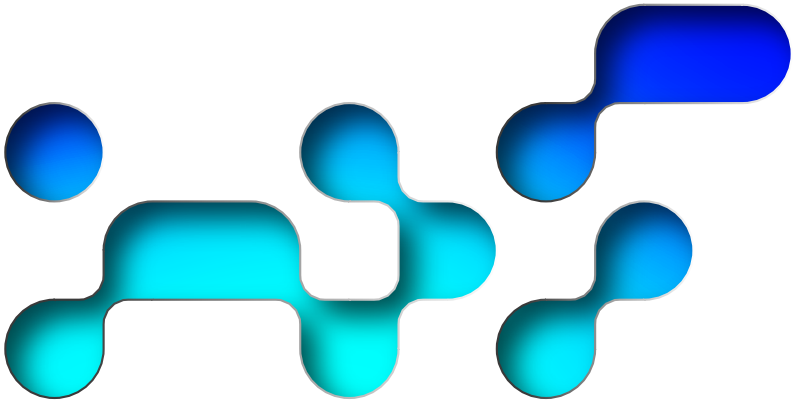
CAMPUS CYBER

METHODOLOGIE STRATEGIE D'ENTRAINEMENT CYBER

GROUPE DE TRAVAIL : GESTION DE CRISE CYBER ET ENTRAINEMENT



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

BANQUE DE FRANCE
EUROSYSTÈME

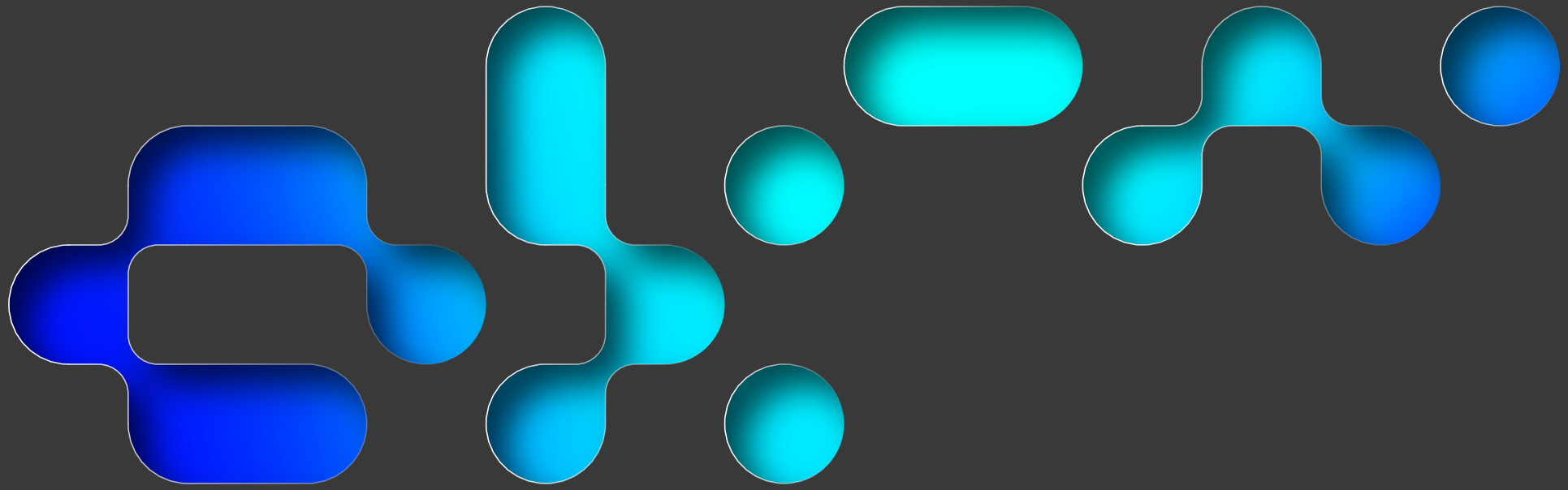
AMRAE
la Maison du risk management

CCA
Club de la Continuité d'Activité

CDSE
CLUB DES DIRECTEURS DE SÉCURITÉ DES ENTREPRISES

CESIN

CLUSIF



SOMMAIRE

Contributeurs : ANSSI, BNP Paribas, Bouygues, Ministère de l'Intérieur, Safran, Sanofi, Schneider Electric, SUEZ, Wavestone

I. PRÉSENTATION DE LA MÉTHODOLOGIE DE DÉVELOPPEMENT D'UNE STRATÉGIE D'ENTRAÎNEMENT

Cette méthodologie vise à préparer, au mieux, les organisations à **réagir aux crises d'origine cyber,** en leur proposant un ensemble d'**éléments de compréhension et de bonnes pratiques** afin de faciliter la conduite d'exercices de gestion de crise. Elle doit maximiser la plus-value des exercices, qui s'inscrivent dans une stratégie globale et nécessitent donc une certaine synchronisation.

Le but est de **structurer un programme d'entraînemen**t en cohérence avec les objectifs à long terme préalablement définis, visant à renforcer les capacités de réponse à la crise.

L'approche détaillée ci-dessous recommande de mettre en place **une stratégie d'entraînement pluriannuelle, nivelée par niveau de maturité** et qui doit d'être mise à jour annuellement pour prendre en compte les enseignements tirés des retours d'expériences (RETEX) ainsi que les priorités de l'organisation.

A QUI S'ADRESSE LA MÉTHODOLOGIE ?

Cette méthodologie est destinée à des **entités privées et publiques de tout secteur**. Elle n'est pas dédiée à des fonctions spécifiques mais complémentaires dans le processus de la gestion d'une crise cyber et doit permettre de servir à **développer la collaboration avec l'écosystème de l'organisation**. Ainsi, il s'agit de mobiliser l'ensemble des parties prenantes nécessaires à la résolution de la crise, que ces parties prenantes soient internes (métiers, équipes cyber, équipes IT, responsable communication, responsable juridique, financier etc.) ou externes (clients, partenaires, prestataires, autorités).

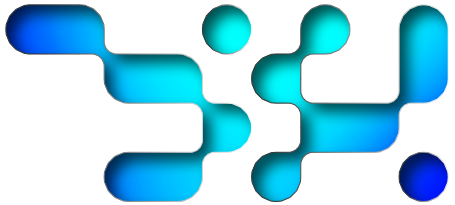
En effet, une bonne coordination de ces parties prenantes est essentielle et les exercices de crise doivent permettre de s'assurer de leur capacité à faire face à une gestion de crise d'origine cyber. Enfin, cette méthodologie s'adresse à **tous niveaux hiérarchiques de toute entité.**

Par ailleurs, **toute organisation**, dotée ou non d'un dispositif global de maîtrise du risque numérique ou d'un dispositif général de gestion de crise et des outils dédiés à la gestion des impacts (moyens d'alerte, salle de crise, dispositif opérationnel et décisionnel, outils de conduite, plan de continuité et de reprise d'activité, etc.), **peut appliquer cette méthodologie**. Ainsi, ce guide s'adresse à des organisations aux niveaux de maturité hétérogènes.

II. CONSTRUIRE UNE STRATÉGIE D'ENTRAÎNEMENT ADAPTÉE À CHAQUE ORGANISATION

A) ÉVALUER LA MATURITÉ « GESTION DE CRISE ET EXERCICES » DE L'ORGANISATION

Afin de construire une stratégie d'entraînement adaptée aux besoins de l'organisation, il est nécessaire d'**évaluer l'expérience de son organisation** tant sur le volet gestion de crise que sur le volet cyber. C'est donc autour de plusieurs niveaux de maturité, regroupés dans une matrice de maturité, que les recommandations de cette méthodologie ont été structurées, afin de définir une stratégie adaptée à chaque organisation.



Aussi, pour évaluer son niveau de maturité autour de plusieurs thématiques (gouvernance, processus/outillage, communication de crise, détection et réponse à incident et continuité d'activité/reconstruction), il est possible de s'appuyer sur l'**outil d'auto-évaluation mis à disposition sur le site web de l'ANSSI**.

La matrice ci-dessous doit faciliter le développement d'une stratégie d'entraînement en fonction du niveau de maturité de chaque organisation. Ainsi, les quatre niveaux de maturité proposés (identiques à l'outil d'auto-évaluation de l'ANSSI) représentent une progression dans les types exercices, leurs périmètres et acteurs impliqués pour répondre aux différents objectifs d'entraînement :

- **En termes d'objectifs visés** :
  - Sensibiliser : exercices de sensibilisation du personnel à la cybersécurité à travers différentes activités : conférences, stands d'information, activités interactives type Serious Game etc. ;
  - Construire : exercices ou ateliers-exercices permettant lors de leur exécution de construire des éléments de procédures ou d'identifier des premiers éléments de réponse à certaines questions liées à la gestion de crise cyber ;
  - S'entrainer : exercices de simulation pour acquérir ou entretenir des réflexes et bonnes pratiques utiles en tant de crise cyber ;
  - Tester : exercices pour s'assurer de la validité des procédures et des capacités existantes.
- **En termes de périmètre** :
  - Sur le plan technique : exercices de crise qui permettent de tester les capacités techniques tels que l'investigation numérique ou la restauration de sauvegarde ;
  - Sur le plan opérationnel : exercices de crise qui permettent de tester les capacités opérationnelles tels que la coordination des équipes, la consolidation de la situation ou encore la gestion de la reconstruction ;
  - Sur le plan organisationnel : exercices de crise de grande ampleur, au niveau de la durée et des parties prenantes impliquées :
    - Exercice complet sur plusieurs journées ;
    - Exercice complet sur au plus 1 journée ;
    - Exercice opérationnel : implication des équipes techniques et métiers ;
    - Exercice stratégique : implication du COMEX et des équipes de direction
    - Exercice sur table (ou Table top): implication du COMEX ;
- **En termes de thématiques abordées (quelques exemples non exhaustifs)** :
  - Détection et de réponse à incident cyber : entraînement de détection et réponse par simulation technique d'attaque (exercice red team). L'objectif est de tester à la fois l'aspect organisationnel mais aussi technique (temps de réponse, pertinence, capacité à stopper l'attaque etc.) ;
  - Communication de crise : entrainement par simulation visant à acculturer les équipes de communication aux spécificités des crises cyber. Ces exercices peuvent s'appuyer sur des outils de pression médiatique simulée (PMS) pour se rapprocher du réalisme d'une vrai crise, notamment sur les réseaux sociaux ;
  - Continuité d'activité : ateliers, exercices de simulation de crise ou exercice majeur visant à étudier la pertinence des procédures de continuité d'activité face à une menace cyber. Cette thématique s'intéresse notamment à la capacité à maintenir une activité sans moyens informatiques et à reconstruire rapidement et de manière sécurisée les infrastructures essentielles à l'activité ;
  - Coordination/prise de décision : ateliers, simulation de crise visant à tester la circulation de l'information, la coordination entre les différentes cellules de crise et la prise de décision.

Ces différents types d'exercices permettent donc de solliciter plusieurs cellules de crise :

- Stratégique : dirigeants, décideurs, COMEX, Conseil d'administration ;
- Opérationnelle : conduit des actions propres à son cœur de métiers et apporte la visibilité terrain aux cellules tactiques et stratégiques – implication des équipes métiers, fonctions supports, techniques, experts faiseurs, N-1 ;
- Tactique : suit le déroulement de la crise sur le périmètre de la fonction et décline et conduit les directives données au niveau stratégique - implication des équipes métiers, fonctions supports, techniques, coordonnateurs cadres.

A noter que **la stratégie d'entrainement doit être en cohérence avec les menaces les plus probables pour l'organisation**, ses risques ainsi que sa chaine de valeur métiers. Aussi, les exercices réalisés doivent s'appuyer sur des scénarios adaptés à la menace actuelle (des livrables relatifs aux différents types de scénarios sont en cours de production). Il s'agit notamment de scénarios relatifs aux menaces suivantes :

- **Rançongiciel** : chiffrement du parc informatique bloquant l'activité de l'organisation, avec en option exfiltration de données ou gestion de la rançon ;
- **Attaque supply chain** : compromission d'un partenaire ou d'un service numérique présent sur le SI ;
- **Attaque sur systèmes industriels** (dont sabotage) : compromission d'équipements industriels conduisant à l'arrêt de l'activité de production ;
- **DDoS** : attaque par déni de service distribué contre des sites web exposés sur internet ;
- **Exfiltration de données** (dont espionnage) : fuite de données sensibles (personnelles, stratégiques secrets industriels, etc.) ;
- **Défacement** (dont hacktivisme) : compromission d'un site vitrine/ institutionnel ;
- **Atteinte à l'intégrité des données** : modification de données au sein d'un SI de manière furtive (ex : à des fins de fraude).

Concernant la matrice de maturité, il convient de noter que les objectifs de sensibilisation du niveau 0 jusqu'au niveau 3 de maturité restent les mêmes mais que les exercices, les thématiques abordées et les cibles visées évoluent en fonction des spécificités et du niveau de maturité de chaque organisation. Cet outil n'est qu'une suggestion de progression logique en fonction des objectifs d'entraînement à atteindre et de l'expérience de chaque organisation.

METHODOLOGIE STRATEGIE D'ENTRAINEMENT CYBER

Objectifs d'entraînement		Niveau de maturité			
		Niveau 0	**Niveau 1**	**Niveau 2**	**Niveau 3**
Objectif visé	**Sensibiliser**	**Objectif :** sensibiliser à la gestion de crise cyber interne, sensibiliser à des scénarios thématiques (ex : rançongiciel), etc.	**Objectif** : idem niveau précédent	**Objectif :** idem niveau précédent	**Objectif :** idem niveau précédent
		Type : e-learning et/ou présentation descendante, RETEX, bonnes pratiques et des réflexes à adopter	**Type :** table-top éducatif standard (Cf 6.2), Serious Game, RETEX sur mesure, etc.	**Type :** table-top adapté au contexte de l'entreprise (Cf 6.2)	**Type :** table-top adapté au contexte de la relation avec le partenaire (Cf 6.2)
		Cible/Population : équipes informatiques	**Cible/Population :** équipes informatiques et équipes métiers	**Cible/Population :** équipes informatiques et équipes métiers, Direction Générale	**Cible/Population :** clients, fournisseurs, partenaires
	Construire	**Objectif** : construire son dispositif de crise	**Objectif** : construire des procédures opérationnelles utilisables en temps de de crise	**Objectif** : idem niveau précédent + outiller la gestion de crise au travers de playbooks utilisables et tester la continuité d'activité	**Objectif** : idem niveau précédent + traiter les problématiques relatives à la supply chain : solutions, fournisseurs, etc. et mettre sous tension la chaine d'approvisionnement métiers (type production).
		Type : table-top, ateliers	**Type :** table-top, ateliers	**Type :** table-top, ateliers, simulation	**Type :** table-top, ateliers, simulation
		Cible/Population : équipes informatiques et équipes métiers, Direction Générale	**Cible/Population :** équipes informatiques	**Cible/Population :** équipes informatiques, équipes métiers	**Cible/Population :** équipes informatiques, équipes métiers
	S'entrainer	Pas d'entraînement de gestion de crise cyber	Pas d'entraînement de gestion de crise cyber	**Objectif** : maintenir des connaissances, capacités et bonnes pratiques établis dans le passé au travers d'incidents, de crise ou d'exercices	**Objectif** : idem précédent
				Type : simulations, exercices majeurs	**Type :** simulations, exercices majeurs
				Cible/Population : toute population impliquée dans la gestion d'une crise cyber, en interne	**Cible/Population :** toute population impliquée dans la gestion d'une crise cyber, en interne et avec implication des parties prenantes externes
	Tester	Pas d'entraînement de gestion de crise cyber	Pas d'entraînement de gestion de crise cyber	**Objectif** : tester des hypothèses internes (de maturité, de réactions du personnel, de compatibilité de la documentation, etc.) à des fins d'amélioration continue	**Objectif** : tester des hypothèses impliquant une réaction des parties prenantes externes.
				Type : ateliers, simulation, exercice majeurs	**Type :** ateliers, simulation, exercice majeur
				Cible/Population : toute population impliquée dans la gestion d'une crise cyber	**Cible/Population :** toute population impliquée dans la gestion d'une crise cyber

METHODOLOGIE STRATEGIE D'ENTRAINEMENT CYBER

Périmètre	Niveau de maturité			
	Niveau 0	**Niveau 1**	**Niveau 2**	**Niveau 3**
Plan technique	**Objectif :** sensibiliser les équipes techniques aux activités techniques nécessaire en temps de crise (investigation, reconstruction, etc.)	**Objectif :** effectuer les actions techniques nécessaires en tant de crise, notamment la restauration de services vitaux (par application unitaire), la mise en place d'action de contournement ou l'investigation numérique	**Objectif :** idem niveau précédent + nouveau périmètre d'actions technique : isolation réseau/partenaire, restauration de chaine applicative informatique, restauration d'infrastructure	**Objectif :** idem niveau précédent + nouveau périmètre d'actions techniques ; restauration de chaine de valeur métier, automatisation de la reconstruction
	Type : table-top, ateliers	**Type- :** atelier, simulation, capture-the-flag	**Type :** atelier, simulation, capture-the-flag, exercices majeurs	**Type :** atelier, simulation, capture-the-flag, cyber-range, exercices majeurs
	Cible/Population : équipes informatiques	**Cible/Population :** équipes informatiques et métier	**Cible/Population :** idem niveau précédent	**Cible/Population :** idem niveau précédent
Plan opérationnel	**Objectif :** sensibiliser les équipes de gestion de crise aux spécificités des crises cyber	**Objectif :** entrainer le niveau opérationnel aux activités la gestion de crise cyber (communication de crise, qualification d'une alerte, travail juridique)	**Objectif :** idem niveau précédent + construire des éléments de réponse rapide (kits, modèles, valise de crise) + travailler à la priorisation des actions et des chantiers en temps de crise	**Objectif :** idem niveau précédent + travailler sur de nouvelles dimensions (anticipation de crise, participation médiatique, etc.)
	Type : table-top, ateliers	**Type :** atelier, simulation	**Type :** atelier, simulation (appuyé d'un outil de pression médiatique simulée), exercice de mobilisation	**Type :** atelier, simulation, média-training, exercices majeurs
	Cible/Population : équipes de gestion de crise et de continuité	**Cible/Population :** équipes informatiques et métier	**Cible/Population :** idem niveau précédent	**Cible/Population :** idem niveau précédent
Plan organisationnel	Pas d'entraînement de gestion de crise cyber	Objectif : tester l'organisation générale de la gestion de Crise Cyber. Les participants reçoivent les stimuli (emails, appels, messages) et doivent proposer une réaction immédiate : définition de stratégie de défense, coordination des groupes IT (CSIRTs, CTO, RSSI ...)	**Objectif :** idem niveau précédent, + : coordination avec les équipes métiers et fonctions, intégrant l'activation des PCA. Mobilisation et activation des cellules de crise	**Objectif :** idem niveau précédent, + : intégration des éléments techniques (isolation, forensic, connaissance de la menace et reconstruction des services vitaux)
			Type : table-top avec mobilisation (aucune action dans IT production) (Cf 6.2)	**Type :** table-top (Cf 6.2), (quelques actions dans IT Production peuvent être réalisées)
			Cible/Population : idem niveau précédent, + : équipes métiers et fonctions	**Cible/Population :** idem niveau maturité, + : Direction Générale, Partenaires externes

METHODOLOGIE STRATEGIE D'ENTRAINEMENT CYBER

		Niveau de maturité			
		Niveau 0	**Niveau 1**	**Niveau 2**	**Niveau 3**
Exercices thématiques (liste non exhaustive)	**Détection et de réponse à un incident cyber**	Si pas de capacités de détection, pas d'entraînement	**Objectif :** tester l'effectivité des fondamentaux de détection (logs, alertes, Faux positifs…), en particulier pour les processus vitaux. **Type :** exercices simples/ unitaires sur la détection - (Purple team) **Cible/Population :** SOC ou équipes informatiques	**Objectif :** tester des scénarios d'attaques (détection, réponse à incident) **Type :** exercices à partir de scénarios standards, ciblés (processus vitaux, Technologique…) sur la détection et réponse du SOC - (Purple team) **Cible/Population :** idem niveau précédent	**Objectif :** tester des scénarios d'attaques (détection, réponse à incident, forensic, connaissance de la menace (TI)) **Type :** exercices à partir de scénarios plus longs et complexes - et déroulement discret de la Purple team (équipe de supervision) **Cible/Population :** SOC, autres acteurs impliqués dans la réponse à incident, forensic et connaissance de la menace
	Communication de crise	**Objectif** : sensibiliser les équipes communication aux spécificités des crises cyber **Type :** table top, simulation **Cible/Population :** équipes communication		**Objectif** : faire réagir les équipes communication aux spécificités des crises cyber, en les faisant travailler au travers de la valise de communication de crise cyber **Type :** simulation, appuyé d'un outil de pression médiatique simulée **Cible/Population :** équipes communication et SSI	**Objectif** : idem niveau précédent, en ajoutant les éléments de coordination avec l'écosystème interne et externe **Type :** simulation ou exercice majeur, appuyé d'un outil de pression médiatique simulée **Cible/Population :** équipes communication et son écosystème (SSI, IT, équipes métiers, partenaires, COMEX, etc.)
	Continuité d'activité	**Objectif** : sensibiliser les équipes aux spécificités de la menace cyber dans le contexte de la continuité d'activité **Type :** table top **Cible/Population :** équipes métiers		**Objectif** : faire travailler les équipes sur la continuité de leurs activités respectives (PCA pour les équipes métiers, PRA pour les équipes informatique) dans le contexte d'une attaque cyber **Type :** simulation **Cible/Population :** équipes métiers et équipes informatiques	**Objectif** : idem précédent + travailler à la coordination interne et externe (avec les prestataires) sur la continuité d'activité **Type :** simulation ou exercice majeur **Cible/Population :** équipes métiers et équipes informatiques, prestataires et fournisseurs de service
	Coordination / prise de décision	**Objectif** : sensibiliser les équipes aux enjeux de circulation de l'information, coordination et prise de décision dans un contexte d'incertitude **Type :** table top **Cible/Population :** équipes métiers et COMEX		**Objectif** : faire travailler les équipes sur les modalités de circulation de l'information et de coordination entre les cellules **Type :** simulation **Cible/Population :** équipes métiers et COMEX	**Objectif** : idem précédent + mobiliser les filiales/partenaires, etc. **Type :** simulation **Cible/Population :** équipes métiers, COMEX et écosystème

B) DÉFINIR LES OBJECTIFS DES EXERCICES

Une fois le niveau de maturité définit, il convient d'établir les objectifs d'entraînement pour l'organisation.

Ainsi, **chaque exercice doit avoir ses propres objectifs** représentatifs de ce que l'organisation veut tester. Ces derniers doivent être **partagés avec les sponsors ou les représentants de "haut niveau"** de l'organisation participant à l'exercice. Leur support permet d'avoir l'attention requise sur l'exercice afin que les enseignements tirés soient bénéfiques pour l'organisation.

Voici ci-dessous une liste non exhaustive d'exemples d'objectifs d'exercice dont il est possible de s'inspirer :

- Vérifier le niveau de formation des employés et collaborateurs à être prêts à répondre à une cyberattaque majeure et à améliorer les capacités de gestion de crise cyber ;
- Tester la coordination des parties prenantes internes et le rôle qu'elles sont censées endosser en cas de crise ;
- Tester des manuels opérationnels de gestion de crise ;
- Tester la coordination entre les cellules de crises opérationnelles et stratégiques ;
- Tester la coordination avec l'écosystème de gestion de crise (clients, fournisseurs, prestataires, régulateurs, SOC externe, Autorités – ex : ANSSI, etc.) ;
- Tester et améliorer ses capacités techniques (détection, reconstruction, investigation numérique, isolation, etc.) ;
- Tester la communication durant la crise (interne, intra cellule de crise, extra cellule de crise, hors entreprise, média, …) ;
- Établir un point de situation régulier à destination des décideurs ;
- Analyser le comportement des participants face à une situation stressante ;
- Évaluer la compréhension des décisions et du rôle des différents acteurs

III. METTRE EN PLACE LA STRATÉGIE D'ENTRAÎNEMENT

A) LES ÉTAPES DE LA MISE EN PLACE D'UNE STRATÉGIE

Plusieurs étapes sont nécessaires pour la bonne mise en œuvre de la stratégie d'entrainement :

- Définir les objectifs et le budget ;
- Définir les périmètres intégrés ;
- Définir l'équipe et le rôle de chacun ;
- Définir la maturité actuelle et la cible à atteindre ;
- Impliquer les périmètres concernés dans la définition de la stratégie ;
- Faire valider la stratégie par le sponsor ;
- Déployer la stratégie ;
- Piloter l'application de la stratégie ;
- Suivre l'avancement et réaliser un reporting ;
- Valoriser la stratégie de crise et promouvoir des actions d'amélioration ;
- Ajuster les objectifs ;
- Assurer un retour d'expérience continu sur l'approche.

B) CONSEILS

La réalisation d'une stratégie d'entraînement ne dépend pas uniquement de la maturité de l'organisation mais aussi de ses **ressources disponibles**. En effet, des éléments clés doivent être identifiés pour réussir à mettre en place la stratégie définie. Pour chaque l'exercice, il faut **notamment identifier** :

- Un ou plusieurs **coordinateurs** pour piloter la réalisation d'entraînements et assurer la gouvernance de la stratégie (indicateurs, reporting etc.) ;
- Un ou plusieurs **sponsors** d'exercice pour valider les cibles stratégiques et les livrables clés et suivre le déroulé de la stratégie d'entraînement ;
- Le **budget** nécessaire et qui l'alloue.

Par ailleurs, toutes les **ressources internes RH** doivent être identifiées au début du projet pour s'assurer de leur disponibilité. De plus, il est important de **planifier en amont les dates d'exercices** de crise afin de s'assurer de la mobilisation des bonnes parties prenantes.

Enfin, si l'organisation n'a pas d'équipe dédiée pour mettre en place la stratégie d'entraînement, il est possible de faire appel à des entreprises spécialisées dans l'accompagnement à la préparation à la gestion de crise cyber. À cette fin, l'ANSSI a élaboré un référentiel PACS (Prestataires d'Accompagnement et de Conseil en Sécurité des systèmes d'information), apportant aux organisations les garanties de la compétence et de la sécurisation des prestations fournies par les PACS.

IV. VALORISER ET PROMOUVOIR LA STRATÉGIE ET SA PROGRESSION

Le partage de la stratégie d'entraînement au **Comité exécutif** (COMEX) permet de valoriser plusieurs points, tant en interne qu'en externe :

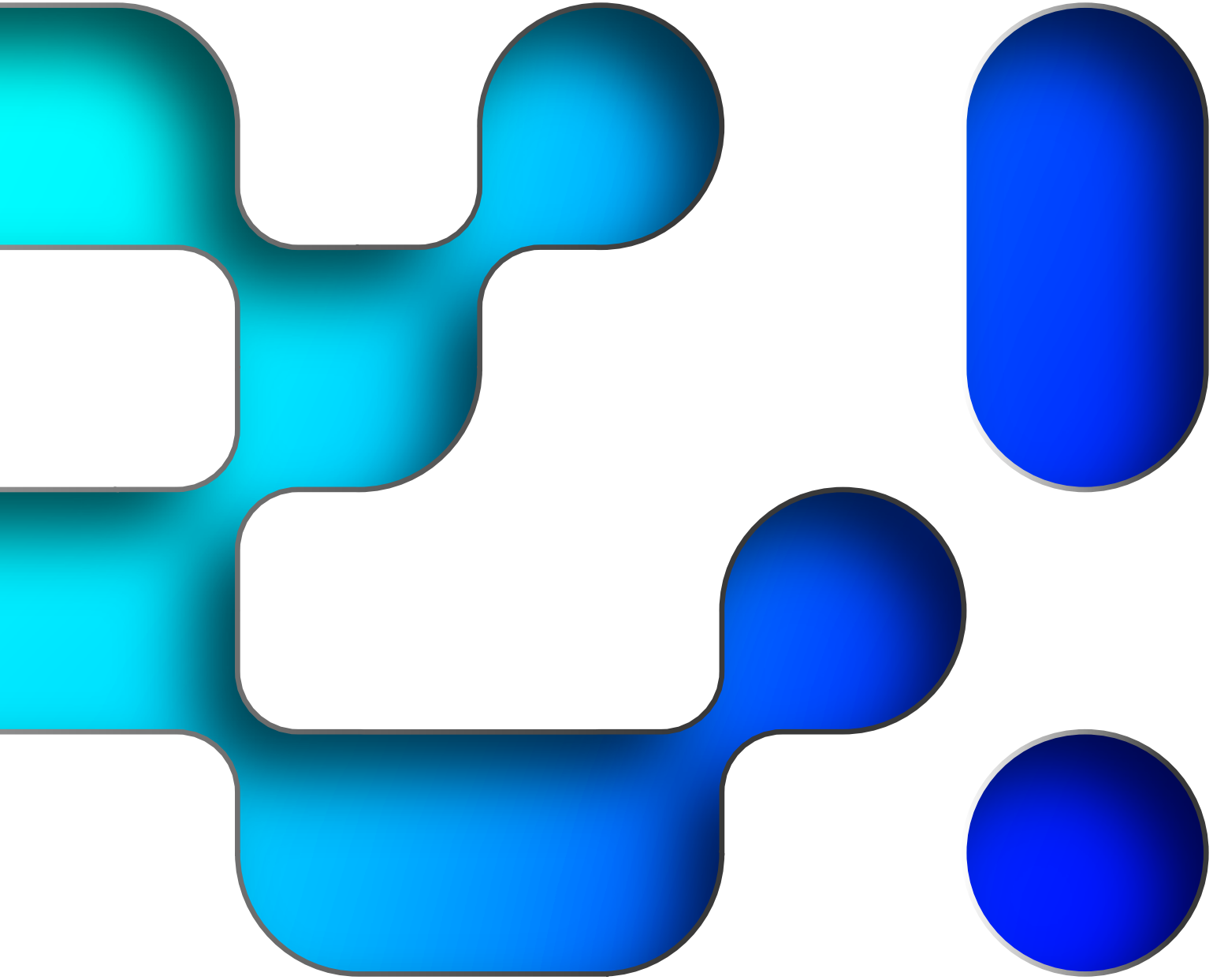
- Démontrer les progrès réalisés au moyen d'indicateurs de suivi (par exemple, nombre de personnes formées, nombre d'exercices réalisés, etc.) ;
- Démontrer le retour sur investissement des actions d'entrainement et obtenir les ressources nécessaires au bon déploiement de la stratégie ;
- Permettre une anticipation budgétaire au regard des objectifs fixés ;
- Communiquer en externe et valoriser les exercices de crise réalisés.

V. AMÉLIORER DE MANIÈRE CONTINUE SA STRATÉGIE

Il est nécessaire de rappeler que la force de toute stratégie d'entraînement réside dans sa **ritualisation**. La stratégie proposée doit en effet être l'objet d'un processus dédié et **révisé pluri annuellement**. Cette révision doit se construire au **regard des retours d'expérience** de crise réelle ou d'exercice.

Inscrire ce processus dans une démarche perpétuelle d'amélioration vise ainsi à assurer une réflexion stratégique globale de l'entité ou de son écosystème pour s'assurer de la pertinence de la stratégie et des exercices qui la composent.

Pendant le déploiement de la stratégie, il est donc important de **mettre à jour régulièrement la documentation et les livrables** afin d'améliorer la pertinence et l'adaptation de la stratégie d'entraînement.



CAMPUS CYBER
5 - 7 RUE BELLINI
92800
PUTEAUX

https://campuscyber.fr/