AYI NEDJIMI Consultants

Exercice de Crise Cyber : Organiser un Tabletop Efficace

Catégorie : Forensics Lecture : 9 min Publié le : 08/03/2026 Auteur : Ayi NEDJIMI

Guide complet pour organiser un exercice de crise cyber : tabletop exercises, scénarios réalistes, implication de la direction, RETEX et amélioration.

Ce scenario simule une compromission via un fournisseur de logiciels. Une mise a jour routiniere d'un outil utilise quotidiennement contient un backdoor. L'attaquant utilise cette porte derobee pour se deplacer lateralement dans le reseau et acceder aux systemes critiques. Guide complet pour organiser un exercice de crise cyber : tabletop exercises, scénarios réalistes, implication de la direction, RETEX et amélioration. L'investigation numérique exige rigueur et méthodologie. Exercice de Crise Cyber : Organiser un Tabletop Efficace couvre les aspects pratiques que les analystes forensics rencontrent sur le terrain. Nous abordons notamment : cadre reglementaire, frequence et programme d'exercices par maturite et questions frequentes. Les professionnels y trouveront des recommandations actionnables, des commandes prêtes à l'emploi et des stratégies de mise en œuvre adaptées aux environnements d'entreprise.

Deroulement et injects

- **T+0** : Le CERT-FR publie une alerte concernant la compromission d'un editeur logiciel dont vous utilisez un produit deploye sur 500 postes. Une version trojanisee a ete distribuee il y a 2 semaines.
- **T+30min** : Inject 1 - L'analyse EDR revele des connexions C2 depuis 47 postes. Le malware utilise des techniques de post-exploitation et pivoting pour se deplacer dans le reseau.
- **T+1h** : Inject 2 - Trois de vos propres clients vous contactent : ils utilisent aussi votre produit et veulent savoir si vous etes impactes et si la compromission a pu se propager jusqu'a eux via vos systemes.
- **T+1h30** : Inject 3 - L'ANSSI vous contacte : vous etes identifie comme operateur d'importance vitale (OIV) potentiellement impacte. Un rapport d'incident est attendu sous 24h.
- **T+2h** : Inject 4 - Le conseil d'administration est informe. Le president demande un point de situation en 15 minutes avec un plan d'action clair et un calendrier de retour a la normale.

Scenario 4 : Menace interne (insider threat)

Ce scenario est souvent le plus delicat a gerer car il implique un collaborateur de l'entreprise. Un employe mecontent, en preavis, exfiltre des donnees confidentielles (plans strategiques, base clients, propriete intellectuelle) avant de quitter l'entreprise. La dimension RH, juridique et emotionnelle ajoute une complexite unique a ce type de crise.

Deroulement et injects

- **T+0** : Le DLP detecte un volume anormal de telechargements depuis SharePoint : 15 Go de documents classifies "Confidentiel" telecharges en 48h par un directeur technique en preavis de demission.
- **T+30min** : Inject 1 - L'analyse des logs montre que l'employe a egalement transfere des emails vers un compte Gmail personnel via une regle de transfert automatique creee il y a 3 mois.
- **T+1h** : Inject 2 - Le DRH signale que ce directeur technique rejoint un concurrent direct la semaine prochaine. Les documents exfiltres contiennent la roadmap produit et les algorithmes proprietaires.
- **T+1h30** : Inject 3 - Le service juridique du concurrent vous contacte : ils affirment que leur futur collaborateur n'a rien exfiltre et menacent de poursuites pour diffamation si l'affaire est rendue publique.
- **T+2h** : Inject 4 - Un collaborateur proche du directeur partant publie un message sur LinkedIn insinuant que l'entreprise "surveille illegalement ses employes". Le message commence a devenir viral.

Cas concret
L'analyse forensique de NotPetya (2017) a révélé que le malware utilisait le mécanisme de mise à jour du logiciel comptable ukrainien M.E.Doc comme vecteur de distribution initiale. La reconstruction de la timeline d'infection a montré que la propagation mondiale s'était faite en moins de 45 minutes via EternalBlue.

Disposez-vous d'un kit de forensique prêt à l'emploi en cas de compromission ?

Les qualites essentielles d'un bon facilitateur : connaissance du domaine cyber et de la gestion de crise, capacite a poser des questions ouvertes ("Et si...", "Que se passe-t-il si...", "Qui est responsable de..."), neutralite et absence de jugement, gestion du temps rigoureuse, capacite a gerer les personnalites dominantes et a faire participer les silencieux.

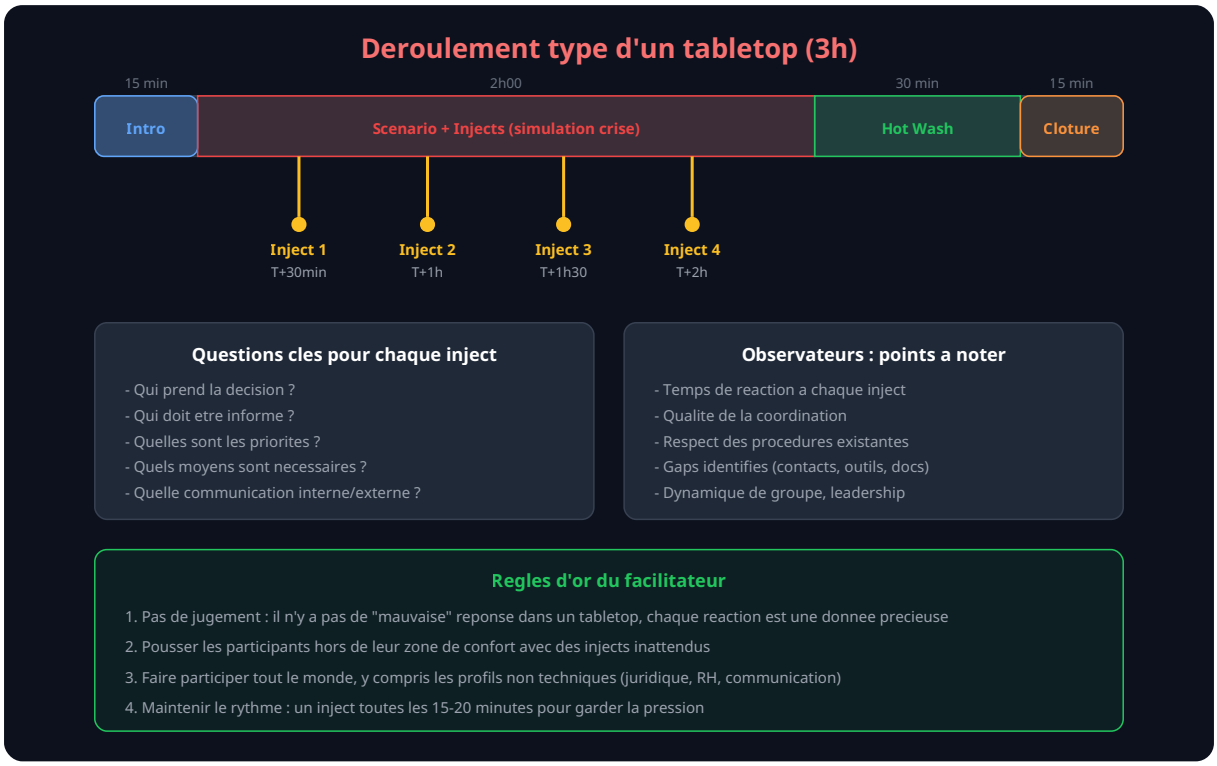
Gestion des injects et timeline

Les injects sont des evenements nouveaux introduits au cours de l'exercice pour forcer les participants a adapter leurs decisions. Ils simulent l'evolution d'une crise reelle, ou la situation change constamment et ou de nouvelles informations (parfois contradictoires) arrivent en permanence. Chaque inject doit etre soigneusement calibre pour augmenter progressivement la pression sur les participants.

La regle d'or : ne jamais injecter un nouvel evenement avant que le groupe ait eu le temps de reagir au precedent. Un inject toutes les 15 a 20 minutes est un bon rythme. Le facilitateur adapte le timing en fonction de la dynamique du groupe : si la discussion est riche, il peut retarder un inject ; si le groupe stagne, il peut accelerer.

Simulation media

L'un des aspects les plus sous-estimes des exercices de crise est la pression mediatique. En simulant des appels de journalistes, des tweets viraux ou des publications sur LinkedIn, l'exercice teste la capacite de l'organisation a communiquer sous pression. Preparez a l'avance de faux tweets, de faux articles de presse et de faux messages sur les reseaux sociaux pour les projeter au moment opportun. La reaction des participants a cette pression externe est souvent revelatrice des failles dans le dispositif de communication de crise.



Le rapport d'exercice est le livrable principal. Il doit etre produit dans les deux semaines suivant l'exercice et distribue a tous les participants et a la direction. Sa structure type comprend :

- **Resume executif** : objectifs, scenario, participants, principales conclusions (1 page)
- **Chronologie de l'exercice** : deroulement inject par inject, decisions prises, actions engagees
- **Points forts identifies** : ce qui a bien fonctionne, les bonnes pratiques observees
- **Lacunes et axes d'amelioration** : classe par criticite (critique, majeur, mineur)
- **Plan d'action** : pour chaque lacune, une action corrective avec un responsable, un delai et un indicateur de suivi
- **Recommandations strategiques** : investissements necessaires, formations, recrutements, outils

Plan d'action et suivi

Le plan d'action est l'element le plus important du RETEX. Sans actions concretes et suivies, l'exercice n'est qu'un evenement ponctuel sans impact durable. Chaque action doit etre SMART (Specifique, Mesurable, Atteignable, Realiste, Temporelle). Le suivi du plan d'action est assure par le RSSI ou le responsable de la gestion de crise, avec un point d'avancement mensuel presente en comite de direction.

Lacune identifiee	Action corrective	Responsable	Echeance	Priorite
Absence de liste de contacts d'astreinte a jour	Creer et maintenir un annuaire de crise avec contacts personnels	RSSI	J+15	Critique
Delai de notification CNIL non maitrise	Rediger une procedure de notification avec templates pre-remplis	DPO	J+30	Critique
Communication de crise non testee	Rediger des templates de communiques (interne, presse, clients)	Dir. Com	J+30	Majeur
Sauvegardes non testees en restauration	Planifier un test de restauration complete trimestriel	DSI	J+60	Majeur
MFA contourne par attaque AiTM	Deployer le MFA resistant au phishing (FIDO2)	RSSI	J+90	Majeur
Pas de prestataire IR sous contrat	Signer un contrat de retainer avec un CERT prive	RSSI/Achats	J+45	Majeur

Metriques d'evaluation

Pour mesurer l'efficacite de l'exercice et suivre la progression au fil du temps, definissez des metriques quantifiables :

- **Temps de detection** : combien de temps entre le premier signe d'incident et la detection par le SOC ?
- **Temps d'escalade** : combien de temps entre la detection et l'activation de la cellule de crise ?
- **Temps de decision** : combien de temps pour prendre les premieres decisions critiques (isolation, communication) ?
- **Completude de la notification** : les obligations reglementaires (RGPD, NIS2) ont-elles ete respectees dans les delais ?
- **Taux de participation** : pourcentage de participants actifs vs passifs pendant l'exercice
- **Nombre de lacunes identifiees** : et leur classification par criticite
- **Taux de realisation du plan d'action** : pourcentage d'actions correctives realisees dans les delais

Cadre reglementaire

NIS 2 (article 21)

La directive NIS 2, transposee en droit francais en 2024, impose aux entites essentielles et importantes des obligations de gestion des risques cyber. L'article 21 exige explicitement des mesures de gestion des incidents, de continuite d'activite et de gestion de crise. Les exercices reguliers de simulation d'incidents sont une composante essentielle de cette conformite. Les entites doivent pouvoir demontrer qu'elles testent leurs dispositifs de reponse.

DORA (article 25)

Le reglement DORA, applicable depuis janvier 2025, impose aux entites financieres un cadre strict de resilience operationnelle numerique. L'article 25 exige des tests de resilience operationnelle numerique, incluant des evaluations de vulnerabilites, des analyses de sources ouvertes, des evaluations de la securite du reseau, des analyses de lacunes, des examens de la securite physique, des questionnaires et des solutions logicielles d'analyse, et des tests avances par le biais de tests de penetration fondes sur la menace (TLPT). Les exercices de crise tabletop s'inscrivent naturellement dans ce cadre.

ISO 22301 et ISO 27001

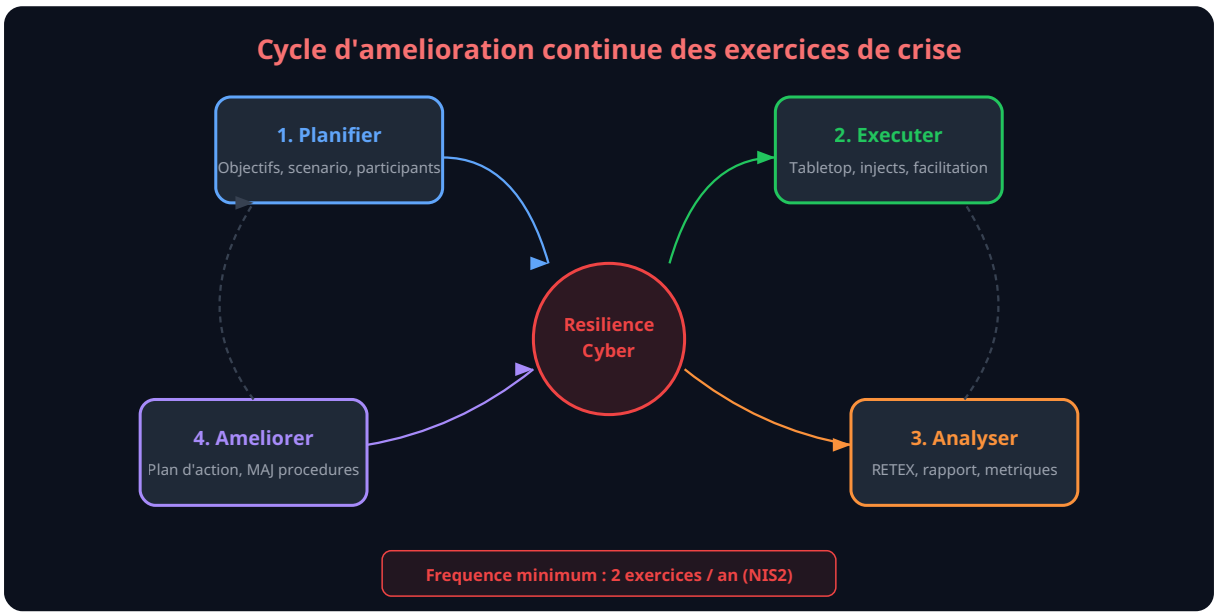
L'ISO 22301 (continuite d'activite) et l'ISO 27001 (securite de l'information) fournissent un cadre de reference pour les exercices de crise. L'ISO 22301 exige des exercices et des tests reguliers pour valider l'efficacite des plans de continuite. L'ISO 27001:2022, dans son annexe A (controle A.5.24 a A.5.28), impose la planification et la preparation de la gestion des incidents, incluant l'apprentissage tire des incidents et la collecte de preuves.

Frequence et programme d'exercices par maturite

Un exercice unique ne suffit pas. La resilience se construit dans la duree, par la repetition et l'amelioration continue. Le programme d'exercices doit etre adapte au niveau de maturite de l'organisation et integre dans le calendrier annuel de securite.

Niveau de maturite	Frequence recommandee	Types d'exercices
Initial	1 tabletop par an	Tabletop basique avec scenario generique (ransomware)
Defini	2 tabletops par an	Tabletops thematiques (ransomware, data breach) + revue procedures
Gere	2 tabletops + 1 fonctionnel par an	Scenarios adaptes au secteur, exercice fonctionnel avec SOC reel
Optimise	2 tabletops + 1 fonctionnel + 1 full-scale par an	Programme complet, Purple Team, simulation media, test de PCA/PRA
Excellence	Trimestriel (mix formats)	Exercices surprises, scenarios combines (cyber + physique), exercices multi-sites

Recommendation : Varier les scenarios
Ne repetez jamais le meme scenario deux fois de suite. Alternez entre ransomware, data breach, supply chain, insider threat, attaque DDoS, compromission cloud, etc. Chaque scenario teste des competences et des procedures differentes. La variete empeche les participants de developper de faux reflexes et garantit une couverture large des risques.



Pour approfondir ce sujet, consultez notre outil open-source disk-forensics-analyzer qui facilite l'investigation forensique des disques.

Questions frequentes

Comment mettre en place Exercice de Crise Cyber dans un environnement de production ?

La mise en place de Exercice de Crise Cyber en production necessite une planification rigoureuse, incluant l'evaluation des prerequis techniques, la definition d'une architecture cible, des tests de validation approfondis et un plan de deploiement progressif avec des points de controle a chaque etape.

Pourquoi Exercice de Crise Cyber est-il essentiel pour la securite des systemes d'information ?

Exercice de Crise Cyber constitue un element fondamental de la securite des systemes d'information car il permet de reduire significativement la surface d'attaque, d'ameliorer la detection des menaces et de renforcer la posture globale de securite de l'organisation face aux cybermenaces actuelles.

Quels outils open source utiliser pour Exercice de Crise Cyber : Organiser un Tabletop Efficace ?

Les incontournables sont Autopsy, Volatility 3, Plaso/log2timeline et RegRipper. Ils couvrent l'analyse disque, mémoire, timeline et registre sans coût de licence.

Sources et références : SANS SIFT · MITRE ATT&CK

Conclusion

L'exercice de crise cyber n'est pas un evenement ponctuel destine a cocher une case de conformite. C'est un investissement strategique dans la resilience de l'organisation. Un tabletop bien concu, correctement facilite et rigoureusement debriefe produit des resultats concrets : des procedures corrigees, des reflexes acquis, une chaine de commandement clarifiee, et une direction sensibilisee aux enjeux cyber.

Les organisations qui s'exercent regulierement developpent une **culture de la resilience** qui se traduit par une detection plus rapide, une reponse plus coordonnee et un impact financier et reputationnel reduit lors d'incidents reels. Le cout d'un exercice tabletop est derisoire compare au cout d'un incident mal gere : quelques jours de preparation et 3 heures de session pour potentiellement economiser des millions d'euros et preserver la confiance des clients et des partenaires.

Commencez par un tabletop simple avec un scenario de ransomware. Impliquez la direction des le premier exercice. Documentez rigoureusement le RETEX et suivez le plan d'action. Puis augmentez progressivement la complexite : scenarios multiples, exercices fonctionnels, simulations grandeur nature. Chaque exercice est une brique supplementaire dans l'edifice de votre resilience cyber. La question n'est plus "serons-nous attaques ?" mais "serons-nous prets quand cela arrivera ?".

Enfin, n'oubliez pas que le principal objectif d'un exercice est l'apprentissage, pas la performance. Un exercice qui revele des failles est un exercice reussi. C'est dans les echecs simules que se forgent les reflexes qui sauveront l'organisation lors de la prochaine crise reelle.

Articles associes

- Ransomware : anatomie de la kill chain et contre-mesures -- Comprendre le deroulement d'une attaque ransomware pour creer des scenarios realistes
- Purple Team : methodologie et exercices -- Integrer les exercices techniques dans le programme de resilience
- NIS 2 : la directive europeenne expliquee -- Obligations reglementaires en matiere de gestion des incidents
- DORA 2026 : bilan de conformite -- Exigences de tests de resilience operationnelle pour le secteur financier
- ISO 27001 : guide complet -- Cadre de reference pour la gestion des incidents de securite
- Post-exploitation : pillage, pivoting et persistence -- Techniques d'attaquants a simuler dans les scenarios d'exercice

References et ressources externes

- ANSSI - Guide d'exercice de crise cyber -- Guide de reference de l'ANSSI pour organiser un exercice de crise
- ENISA - Cyber Exercises -- Ressources europeennes sur les exercices cyber
- NIST Cybersecurity Framework -- Cadre de reference pour la gestion des risques cyber
- MITRE ATT&CK -- Framework de reference pour construire des scenarios d'attaque realistes

- IBM Cost of a Data Breach 2025 -- Statistiques sur le cout des violations de donnees et l'impact des exercices

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr