

Exercice sur table : réaction aux incidents



Temps total
2 heures



Nombre maximum de
participants
30

🎯 Public visé

Employés participant au plan de réaction aux incidents de leur organisation, quel que soit leur niveau technique ou de formation.

👁️ Présentation

Un exercice sur table est une simulation guidée dans laquelle les participants endossent des rôles selon différents scénarios. Il permet d'identifier les failles de cohésion au sein de l'équipe et les points faibles pendant les périodes calmes, afin de renforcer la résilience en cas de véritables crises nécessitant une coordination en temps réel. L'objectif n'est pas de tout réussir parfaitement, mais de se préparer grâce à des scénarios pratiques.

👤 Objectifs d'apprentissage

À l'issue de cet exercice, les participants sauront :

- expliquer l'importance d'un plan de réaction aux incidents dans un environnement professionnel ;
- identifier les rôles et les responsabilités lors d'un incident de sécurité ;
- faire preuve de réactivité et prendre des décisions efficaces lors de scénarios d'incidents.

✂️ Matériel

- Supports de liste de contrôle de réaction aux incidents
- Minuteur ou chronomètre
- Cartes des participants (responsable de la sécurité informatique, responsable des incidents, responsable de la communication, conseiller juridique, représentant des RH et responsable de département)
- Cartes de scénario pour jeu de rôle
- Tableau blanc ou à feuilles
- Marqueurs
- Stylos et blocs-notes

👥 Rôles de l'exercice sur table

Animateur : il contrôle le rythme de l'exercice, guide les discussions, met à jour les scénarios, veille à ce que chacun participe et introduit des informations pour tester la concentration de l'équipe.

Participants : ils s'impliquent dans leur rôle lors de la simulation, discutent ouvertement de leur raisonnement, soutiennent leurs coéquipiers et réagissent aux scénarios selon leurs responsabilités respectives.

Évaluateur : il analyse les forces et les faiblesses, rédige des rapports post-incident et vérifie le respect des plans et procédures existants.

Observateur : il apporte son expertise sans participer directement à l'exercice et soutient les participants en posant des questions pertinentes et en prodiguant des conseils lorsque nécessaire.

Responsable de la prise de notes : il documente toutes les activités de l'exercice, les discussions, les lacunes identifiées, la conformité avec les procédures officielles de l'organisation et les améliorations suggérées.

Introduction

🕒 Durée : 10 minutes

Une réaction efficace aux incidents nécessite une communication claire, des rôles définis et une bonne capacité d'adaptation. Expliquez aux participants que les activités simuleront des scénarios et des difficultés réels, pour leur permettre d'acquérir les compétences requises en gestion des incidents de sécurité. Rappelez-leur qu'une réaction efficace aux incidents dépend à la fois de la **cohésion de l'équipe** et de la **vivacité d'esprit** de chacun.

Activité 1 : liste de contrôle de réaction aux incidents

 **Durée : 30 minutes**

Matériel

- Minuteur ou chronomètre
- Stylos et blocs-notes
- Supports de liste de contrôle de réaction aux incidents (voir l'annexe de l'activité 1)

Activité

Cette activité teste le plan de réaction aux incidents, la stratégie de communication et le processus de prise de décision des participants.

Présentez-leur le scénario suivant :

« Un rançongiciel a chiffré un serveur critique de votre organisation et les attaquants réclament une importante somme en cryptomonnaie en échange du déchiffrement des fichiers. »

Une fois le contexte établi :

1. Distribuez les supports de liste de contrôle de réaction aux incidents à chaque participant. La liste de contrôle contient des étapes courantes de réaction aux incidents, dans un ordre aléatoire.
2. Accordez aux participants 10 minutes pour classer individuellement les étapes de leur liste de contrôle dans l'ordre qu'ils estiment le plus approprié pour ce scénario de rançongiciel.
3. Demandez aux participants de former des petits groupes de 3 à 4 personnes et laissez-les discuter de leurs classements pendant 10 minutes, en veillant à ce que chaque personne remplisse sa propre liste de contrôle individuellement.
4. Consacrez les 10 dernières minutes à examiner ensemble l'ordre des étapes, en discutant des raisons pour lesquelles certaines doivent en précéder d'autres.

Corrigé

Conformément aux bonnes pratiques du secteur, voici les éléments clés à inclure dans la liste de contrôle :

1. Signaler immédiatement l'incident selon la politique de l'organisation
2. Mobiliser l'équipe de réaction aux incidents
3. Isoler les systèmes compromis
4. Documenter la chronologie de l'incident
5. Évaluer l'état des sauvegardes de données
6. Activer le plan de communication de l'organisation pour les parties prenantes
7. Suivre les procédures de notification établies pour les obligations réglementaires
8. Consulter le conseiller juridique
9. Mettre en œuvre la politique de l'organisation concernant les demandes de rançon
10. Contacter les autorités judiciaires conformément à la politique de l'organisation

Activité 2 : simulation de réaction aux incidents

 **Durée : 35 à 60 minutes**

Matériel

- Cartes de rôles des participants de l'organisation (voir l'annexe de l'activité 2)
- Cartes de scénario avec complications (voir l'annexe de l'activité 2)
- Minuteur ou chronomètre
- Tableau blanc ou à feuilles
- Marqueurs
- Stylos et blocs-notes
- Plan de réaction aux incidents de l'organisation

Activité

Cette activité teste la coordination transversale des participants en s'appuyant sur leurs rôles réels au sein de l'organisation, leurs stratégies de communication internes et externes, ainsi que leurs processus décisionnels en cas d'incidents avec complications.

Répartissez les participants en groupes représentant les véritables équipes de réaction aux incidents de l'organisation. Chaque participant assume son rôle réel dans la réaction aux incidents ou l'équivalent le plus proche indiqué sur les cartes de rôle fournies.

Instructions :

1. Distribuez à chaque groupe une carte de scénario décrivant un incident de sécurité avec complications.
2. Accordez aux groupes 20 minutes pour discuter et élaborer une stratégie de réaction en s'appuyant sur leurs rôles respectifs et les procédures de l'organisation.
3. Chaque groupe présente son plan (5 minutes par groupe).
4. Introduisez une complication supplémentaire dans chaque scénario (par exemple, « Les médias ont appris l'incident suite à une fuite »).
5. Accordez aux groupes 10 minutes pour ajuster leurs plans en fonction des nouvelles informations, en s'appuyant sur les procédures établies.
6. Les groupes présentent leurs plans ajustés et expliquent comment ils se sont adaptés aux procédures de l'organisation.

Instructions supplémentaires pour les groupes :

- Reportez-vous au plan de réaction aux incidents de votre organisation lors des discussions.
- « Pensez à voix haute » pour partager votre cheminement de pensée.
- Veillez à ce que tous les participants contribuent en fonction de leurs responsabilités réelles.
- Concentrez-vous sur les mesures concrètes que vous prendriez réellement dans le cadre de vos fonctions.

Discussion

 **Durée : 15 minutes**

Questions

- En quoi l'exercice de classement de l'activité 1 vous a-t-il préparé à la simulation de rôle ?
- Quelles difficultés avez-vous éprouvées en appliquant les procédures établies de votre organisation ?
- Quelles lacunes avez-vous identifiées dans vos procédures actuelles de réaction aux incidents ?
- Dans quelle mesure la communication interservices s'est-elle avérée efficace pendant les exercices ?
- De quelles formations ou ressources auriez-vous besoin pour renforcer votre préparation face à de tels incidents dans votre quotidien professionnel ?

Réponses ou suggestions possibles

- Difficultés : coordination entre départements, accès aux coordonnées réelles, clarification des autorités et pouvoir de décision effectif
- Lacunes : circuits de remontée d'information peu clairs, coordonnées obsolètes, autorités décisionnelles non définies, modèles de notification manquants
- Améliorations : formations croisées régulières, listes de coordonnées à jour, arbres de décision plus clairs, guides de référence rapide spécifiques aux rôles
- Ressources : cartes de réaction aux incidents selon les rôles, exercices réguliers avec les membres réels de l'équipe, formation sur le plan de réaction aux incidents mis à jour

Conclusion

 **Durée : 5 minutes**

Résumez les points clés des deux exercices :

- L'exercice de classement a permis de mieux comprendre les procédures de réaction aux incidents de l'organisation, tandis que la simulation de rôles a mis l'accent sur les difficultés de coordination dans des situations réelles.
- Une préparation individuelle et une réaction coordonnée en équipe, en s'appuyant sur les rôles réels de l'organisation, sont toutes deux essentielles pour une réaction efficace aux incidents.
- Des complications surviendront toujours. La réussite repose sur la capacité de s'adapter en respectant les procédures établies.

Étapes suivantes

- Mettez à jour le plan de réaction aux incidents de votre organisation en fonction des lacunes identifiées.
- Actualisez les listes de coordonnées et les protocoles de communication.
- Comblez les lacunes identifiées relatives à la définition des rôles ou de l'autorité décisionnelle.
- Planifiez régulièrement des exercices sur table avec les membres réels de l'équipe de réaction aux incidents de façon à assurer une amélioration continue.

Annexe de l'activité 1 – Supports de liste de contrôle de réaction aux incidents

Imprimez un exemplaire de cette page pour six participants. Découpez le long des traits pleins pour créer des cartes individuelles et remettez une carte à chaque participant. Pour davantage de résistance, imprimez sur du papier cartonné ou du papier épais.



Liste de contrôle : réaction aux incidents

- ☐ Isoler les systèmes compromis
- ☐ Signaler immédiatement l'incident selon la politique de l'organisation
- ☐ Évaluer l'état des sauvegardes de données
- ☐ Contacter les autorités judiciaires conformément à la politique de l'organisation
- ☐ Consulter le conseiller juridique
- ☐ Mettre en œuvre la politique de l'organisation concernant les demandes de rançon (consultation requise)
- ☐ Activer le plan de communication de l'organisation pour les parties prenantes
- ☐ Documenter la chronologie de l'incident
- ☐ Suivre les procédures de notification établies pour les obligations réglementaires
- ☐ Mobiliser l'équipe de réaction aux incidents

Liste de contrôle : réaction aux incidents

- ☐ Isoler les systèmes compromis
- ☐ Signaler immédiatement l'incident selon la politique de l'organisation
- ☐ Évaluer l'état des sauvegardes de données
- ☐ Contacter les autorités judiciaires conformément à la politique de l'organisation
- ☐ Consulter le conseiller juridique
- ☐ Mettre en œuvre la politique de l'organisation concernant les demandes de rançon (consultation requise)
- ☐ Activer le plan de communication de l'organisation pour les parties prenantes
- ☐ Documenter la chronologie de l'incident
- ☐ Suivre les procédures de notification établies pour les obligations réglementaires
- ☐ Mobiliser l'équipe de réaction aux incidents

Liste de contrôle : réaction aux incidents

- ☐ Isoler les systèmes compromis
- ☐ Signaler immédiatement l'incident selon la politique de l'organisation
- ☐ Évaluer l'état des sauvegardes de données
- ☐ Contacter les autorités judiciaires conformément à la politique de l'organisation
- ☐ Consulter le conseiller juridique
- ☐ Mettre en œuvre la politique de l'organisation concernant les demandes de rançon (consultation requise)
- ☐ Activer le plan de communication de l'organisation pour les parties prenantes
- ☐ Documenter la chronologie de l'incident
- ☐ Suivre les procédures de notification établies pour les obligations réglementaires
- ☐ Mobiliser l'équipe de réaction aux incidents

Liste de contrôle : réaction aux incidents

- ☐ Isoler les systèmes compromis
- ☐ Signaler immédiatement l'incident selon la politique de l'organisation
- ☐ Évaluer l'état des sauvegardes de données
- ☐ Contacter les autorités judiciaires conformément à la politique de l'organisation
- ☐ Consulter le conseiller juridique
- ☐ Mettre en œuvre la politique de l'organisation concernant les demandes de rançon (consultation requise)
- ☐ Activer le plan de communication de l'organisation pour les parties prenantes
- ☐ Documenter la chronologie de l'incident
- ☐ Suivre les procédures de notification établies pour les obligations réglementaires
- ☐ Mobiliser l'équipe de réaction aux incidents

Liste de contrôle : réaction aux incidents

- ☐ Isoler les systèmes compromis
- ☐ Signaler immédiatement l'incident selon la politique de l'organisation
- ☐ Évaluer l'état des sauvegardes de données
- ☐ Contacter les autorités judiciaires conformément à la politique de l'organisation
- ☐ Consulter le conseiller juridique
- ☐ Mettre en œuvre la politique de l'organisation concernant les demandes de rançon (consultation requise)
- ☐ Activer le plan de communication de l'organisation pour les parties prenantes
- ☐ Documenter la chronologie de l'incident
- ☐ Suivre les procédures de notification établies pour les obligations réglementaires
- ☐ Mobiliser l'équipe de réaction aux incidents

Liste de contrôle : réaction aux incidents

- ☐ Isoler les systèmes compromis
- ☐ Signaler immédiatement l'incident selon la politique de l'organisation
- ☐ Évaluer l'état des sauvegardes de données
- ☐ Contacter les autorités judiciaires conformément à la politique de l'organisation
- ☐ Consulter le conseiller juridique
- ☐ Mettre en œuvre la politique de l'organisation concernant les demandes de rançon (consultation requise)
- ☐ Activer le plan de communication de l'organisation pour les parties prenantes
- ☐ Documenter la chronologie de l'incident
- ☐ Suivre les procédures de notification établies pour les obligations réglementaires
- ☐ Mobiliser l'équipe de réaction aux incidents

Annexe de l'activité 2 – Cartes de rôle des participants de l'organisation et cartes de scénario

Imprimez cette annexe et découpez le long des traits pleins pour séparer les cartes figurant sur cette page.

Pour davantage de résistance, imprimez sur du papier cartonné ou du papier épais.



Carte du participant Responsable de la sécurité informatique

Responsable de l'analyse et du confinement technique des incidents
Évalue l'ampleur et la nature de la faille de sécurité
Met en œuvre des mesures de neutralisation immédiates
Dirige les activités d'analyse forensique
Gère la coordination avec les prestataires de sécurité externes



Carte du participant Responsable des incidents

Responsable global de la réaction à l'incident et décisionnaire
Coordonne toutes les activités de l'équipe de réaction
Prend les principales décisions stratégiques
Présente des comptes rendus à la direction
Alloue les ressources et fixe les priorités



Carte du participant Responsable de la communication

Gère l'ensemble des communications internes et externes
Met en œuvre les plans de communication existants
Rédige les notifications destinées aux parties prenantes
Gère la coordination avec les médias et l'équipe de relations publiques
Assure la veille sur les réseaux sociaux et dans les médias



Carte du participant Conseiller juridique

Conseille sur les implications juridiques et la conformité réglementaire
Assure le respect des lois sur la notification des failles
Conseille sur la conservation des preuves
Vérifie toutes les communications externes
Gère la coordination avec les forces de l'ordre, si nécessaire



Carte du participant Représentant des RH

Gère les aspects liés aux employés dans la réaction à l'incident
Gère les communications internes avec les employés
Gère les enquêtes sur les menaces internes
Coordonne les services de soutien aux employés
Gère les impératifs de continuité des effectifs



Carte du participant Responsable de département

Représente les opérations de l'unité commerciale concernée
Évalue l'impact sur les activités du département
Met en œuvre des mesures de continuité des activités
Gère la coordination avec les autres responsables de départements
Rend compte de l'état des opérations au responsable des incidents



Scénario Attaque par rançongiciel avec vol de données

« Les serveurs de fichiers de votre organisation ont été chiffrés par rançongiciel. Les attaquants ont également volé des données financières de clients et menacent de les rendre publiques si la rançon n'est pas payée sous 24 heures. Complication : les systèmes de sauvegarde montrent des traces de compromission remontant à deux semaines. »



Scénario Compromission de la messagerie professionnelle

« La messagerie électronique du directeur financier a été compromise et utilisée pour autoriser un virement de 500 000 € vers un compte inconnu. Le virement a été exécuté ce matin. Complication : des e-mails frauduleux similaires ont été envoyés à trois clients importants pour leur demander de mettre à jour leurs informations de paiement. »



Scénario Vol de données interne

« Un employé quittant le service informatique a été surpris en train de copier des dossiers clients sensibles sur une clé USB personnelle. La sécurité l'a arrêté à la sortie, mais il affirme que les données sont simplement des fichiers de travail personnels. Complication : l'employé a auparavant publié des messages énigmatiques sur LinkedIn mentionnant qu'il emportait avec lui un précieux savoir-faire vers son nouveau poste. »

Annexe de l'activité 2 – Cartes de scénario et cartes de complications supplémentaires

Imprimez cette annexe et découpez le long des traits pleins pour séparer les cartes figurant sur cette page.
Pour davantage de résistance, imprimez sur du papier cartonné ou du papier épais.



Scénario

Compromission de la chaîne d'approvisionnement

« Le principal fournisseur de logiciels de votre organisation signale que des attaquants ont compromis son serveur de mises à jour et qu'ils auraient pu distribuer du code malveillant aux clients. Vos systèmes ont reçu des mises à jour hier. Complication : le fournisseur refuse de divulguer des détails techniques, invoquant sa propre enquête en cours. »



Scénario

Faible de sécurité physique

« Le personnel a découvert un intrus dans la salle des serveurs après les heures de fermeture, muni d'un ordinateur portable connecté au réseau. La sécurité l'a escorté dehors, mais cette personne a prétendu appartenir à "l'assistance informatique". Complication : plusieurs employés signalent des entrées suspectes enregistrées sur leurs badges en dehors des heures de travail qu'ils n'ont pas effectuées. »



Scénario

Compromission d'un service cloud

« Votre fournisseur de services de stockage cloud signale un accès non autorisé au référentiel de données de votre organisation, contenant des informations clients et des secrets commerciaux. L'incident pourrait avoir duré plusieurs semaines. Complication : la communication initiale du fournisseur cloud contient des informations contradictoires sur la chronologie et l'étendue de l'incident. »



Complications supplémentaires

« Alerte médias : un blog technologique a publié un article sur l'incident de sécurité de votre organisation, révélant des détails précis que vous n'aviez pas encore divulgués. »



Complications supplémentaires

« Notification réglementaire : votre régulateur sectoriel vous a sollicité pour obtenir rapidement des informations sur l'incident et votre plan d'action. »



Complications supplémentaires

« Crise avec un client : votre principal client a organisé une réunion d'urgence pour discuter de la sécurité de ses données et menace de mettre fin à son contrat. »



Complications supplémentaires

« Fuite interne : des employés discutent des détails de l'incident sur les systèmes de messagerie internes et certaines informations semblent inexacts. »



Complications supplémentaires

« Défaillance système : pendant la gestion de l'incident, un système essentiel a été mis hors ligne, potentiellement à cause de vos mesures de neutralisation. »



Complications supplémentaires

« Menace juridique : vous avez reçu une lettre d'un cabinet d'avocats représentant des clients concernés, qui exige des informations détaillées sur la faille et vos mesures de sécurité. »