univlearn.
COACHING & FORMATIONS IT
REEL iT GROUPE

FORMATION EN PRESENTIEL ET/OU EN DISTANCIEL (SELON LE THEME)

EXERCICE DE GESTION DE CRISE CYBER

Dernière mise à jour le 10/02/2025.

OBJECTIF

Préparer et former vos équipes à réagir efficacement face à une situation de crise cyber à travers un exercice de simulation réaliste.
• Tester vos capacités de réponse face à une cyberattaque.
• Identifier les points d'amélioration dans votre procédure de gestion de crise.
• Renforcer la coordination et la prise de décision en équipe dans des contextes de gestion de crise.

Tarif	500 € HT par participant
Réf.	EXCRICYB
Contact	0465260114 contact@univlearn.fr https://univlearn.fr/

COMPÉTENCES DÉVELOPPÉES

Aucune compétence

PUBLIC CONCERNÉ

• Direction • Équipe IT / Technique • Équipe Sécurité (RSSI / DPO)
• Équipe Finance • Équipe Communication

PRÉ-REQUIS

Aucun

MODALITÉS ET DÉLAIS D'ACCÈS

Vous pouvez vous inscrire pour suivre une de nos formations jusqu'à la veille de la date de démarrage si la formation est financée directement par votre entreprise ET si le nombre maximum de participants n'est pas atteint. Si la formation est financée via un OPCO, vous devez au préalable avoir obtenu un accord de ce dernier.

MÉTHODES ET MOYENS MOBILISÉS

Déroulement de l'exercice : Mise en situation réaliste : Un scénario de cyberattaque adapté à votre contexte technique est déclenché pour simuler une crise cyber en temps réel. Activation de la cellule de crise : Chaque équipe mobilise ses compétences pour organiser la réponse, assurer la communication et prendre des décisions stratégiques afin de contenir l'incident. La direction joue un rôle central en coordonnant les efforts, en exerçant ses responsabilités dans la prise de décisions critiques et en s'engageant dans la communication interne, externe et la coordination des collaborateurs tout au long de l'exercice. Remédiation : Passez à l'action en identifiant la source de risque permettant de résoudre la crise et de restaurer les activités.

MODALITÉS DE DÉROULEMENT DE L'ACTION DE FORMATION

Plongez au cœur d'un exercice immersif de gestion de crise cyber ! À travers un scénario d'attaque réaliste et personnalisé selon votre secteur d'activité, testez vos capacités à détecter, organiser et remédier face à une cyberattaque. Une expérience engageante pour renforcer la prise de décision, la communication et la cohésion entre vos équipes IT, Direction, Finance et Communication.

Niveau	Modalité	Effectif par session	Durée
Autres formations professionnelles continues	**Présentiel**	**2 mini > 8 maxi**	**7 heures / 2 jour(s)**

PROGRAMME

Module 1 - Phase préparatoire en amont de l'exercice
Réunion technique avec les équipes DSI
Analyse du périmètre IT, des systèmes et de l'infrastructure existante
Compréhension des enjeux métiers
Élaboration d'un scénario réaliste en fonction du secteur d'activité, pouvant être décliné avec l'accompagnement du RSSI

Module 2 - Déclenchement de la crise et mise en situation
Simulation du début d'une cyberattaque en temps réel adapté au contexte initialement identifié
Déclenchement de la cellule de crise
Prise de décision sous un stress constant

Module 3 - Réponse opérationnelle à l'Incident
Identification des sources de l'attaque
Localisation des zones impactées
Isolation des systèmes compromis
Identification des procédures à appliquer (gestion de crise)

Module 4 - Communication de crise interne et externe
Communication en situation de crise
Diffusion de messages
Gestion de la pression médiatique
Préparation d'une déclaration publique.
Identification de potentielles fuites de données en collaboration avec la DPO

Module 5 - Restauration des systèmes critiques
Évaluation des impacts et priorisation des actions
Plan de remédiation et de reprise d'activités
Restauration des systèmes priorisée
Vérification de l'intégrité des données

Module 6 – Débriefing
Débriefing à chaud avec les équipes
Analyse des décisions prises
Points d'amélioration identifiés
Établissement d'un plan d'action
Question/réponse
Retex à froid et proposition d'un plan d'action

INTERVENANT(S)	ÉVALUATION	ATTRIBUTION FINALE
Aucun	Analyse post-crise pour l'amélioration continue des processus., Communication interne et externe adaptée à une crise cyber., Maîtrise des protocoles de gestion de crise cyber, Prise de décision rapide et structurée face à une cyberattaque., Renforcement de la coordination inter-équipes en situation de crise.	Attestation individuelle de formation