

## RÉSUMÉ

Cette simulation immersive de demi-journée est conçue pour préparer les entreprises à faire face efficacement aux crises de cyber-sécurité. À travers un scénario réaliste et hautement interactif, les participants seront confrontés à une série d'événements critiques qui testeront leur capacité à réagir rapidement, à prendre des décisions éclairées et à communiquer efficacement sous pression. L'objectif est de renforcer la résilience de l'organisation face aux cyberattaques et d'améliorer la collaboration interne pour une gestion de crise optimisée.

Deux scénarios sont proposés :

- a. Un scénario sur catalogue prêt à l'emploi
- b. Un autre scénario sur mesure adapté au contexte de votre entreprise. Celui-ci nécessite en amont une phase d'ingénierie, la consultation des équipes et une étude de la documentation (PSSI, plan de reprise, ...)

## PUBLIC ET PRÉREQUIS

- Connaissance du fonctionnement interne et des processus de décision de l'entreprise.
- Aucune expertise technique approfondie en informatique n'est nécessaire.

## LES OBJECTIFS

À l'issue de cette simulation, les participants seront capables de :

- Comprendre l'importance d'une préparation et d'une réponse rapide et coordonnée en cas de cyberattaque
- Identifier les points faibles de leur organisation en matière de cyber-sécurité et de gestion de crise
- Améliorer la communication interne et avec les parties prenantes externes lors d'une crise
- Élaborer des stratégies pour renforcer la posture de sécurité de leur entreprise
- Instaurer une culture de la résilience au sein de leur organisation

## OUTILS PÉDAGOGIQUES

Formation en présentiel avec alternance d'apports théoriques et de mises en situation pratiques pour ancrer les apprentissages et/ou en distanciel pour certains modules.

Salles de Formation équipées pour utilisation de supports pédagogiques classiques et numériques. Plateaux techniques adaptés et aménagés d'équipements spécifiques.

CENTRES DE FORMATION

**Saint-Nazaire, Laval, La Roche-sur-Yon, Angers, Le Mans, Nantes**

DURÉE DE LA FORMATION

**0.5 jour / 4 heures**

ACCUEIL PSH

**Formation ouverte aux personnes en situation de handicap. Moyens de compensation à étudier avec le référent handicap du centre concerné.**

## Les + Fab'Academy

- + de 1400 Jeunes formés en apprentissage chaque année
- + de 5300 salariés accompagnés en formation continue
- + de 1720 entreprises nous font confiance (TPE, PME, groupes industriels)
- Diplômes reconnus par l'Etat
- Pédagogie innovante (par projets, en îlots, parcours individualisés...)
- Equipement en machines modernes qui préparent aux métiers de demain
- 7 implantations en Pays de la Loire avec des campus neufs et modernes
- 24000m<sup>2</sup> de plateaux techniques et performants (outils numériques, cellules robotisées...)

## MODALITÉ D'ÉVALUATION

Modalités d'évaluation des formations qualifiantes : Les connaissances et/ou capacités professionnelles de l'apprenant sont évaluées en cours et/ou en fin de formation par différents moyens : mises en situation, études de cas, QCM, ..

## MODALITÉS D'ACCÈS

Délais d'accès de 6 mois maximum après confirmation via le bulletin d'inscription, sous réserve d'un nombre suffisant d'inscrits et dans la limite des places disponibles et sous réserve d'étude du dossier d'admissibilité

## CONTENU DE LA FORMATION

- Introduction : Présentation des objectifs, du déroulé de la simulation et du contexte.
- Simulation : Les participants sont plongés dans un scénario de crise cybernétique évolutif, nécessitant des décisions rapides sur les actions à entreprendre pour limiter les dommages, communiquer avec les parties prenantes et planifier la reprise d'activité.
- Phase 1 : Détecter et évaluer la menace.
- Phase 2 : Réponse et confinement de l'incident.
- Phase 3 : Communication de crise et gestion des parties prenantes.
- Phase 4 : Récupération et leçons apprises.
- Débriefing et Retour d'expérience (REX) : Analyse des actions prises, évaluation de l'efficacité de la réponse à la crise, discussion sur les améliorations possibles et élaboration d'un plan d'action pour renforcer la cyber-résilience de l'entreprise.

## VALIDATION ET CERTIFICATION

Attestation de fin de formation

## DATE DE MISE À JOUR

23/02/2024

## VERSION DOCUMENTAIRE

V1