PLONGEZ AU COEUR DE LA RÉALITÉ D'UNE CRISE CYBER

Testez la résilience de vos équipes dans un cadre unique
Une expérience immersive et cognitive qui défie les conventions

SALLE DE SIMULATION IMMERSIVE ET COGNITIVE

ifpass GROUPE

Galileo Global Education™

CYBER EXPERIENCE by Galileo Global Education

PRÉPAREZ VOTRE ORGANISATION À GÉRER UNE CRISE D'ORIGINE CYBER

Être prêt n'est plus une option, mais une nécessité.

Dans un monde où la volatilité, l'incertitude, la complexité et l'ambiguïté redéfinissent les règles du jeu, maîtriser l'art de la gestion de crise – notamment en cas d'attaque cyber – est désormais une compétence incontournable.

Depuis 2020, les cyberattaques en France ont explosé de plus de 400 %, exposant chaque organisation non préparée à des risques majeurs. Être prêt n'est plus une option, mais une nécessité.

L'Ifpass, en partenariat avec Cyber Experience by Galileo Global Education, vous offre une opportunité unique de prendre siège dans la première salle de simulation de crise cyber au monde.

Développer la résilience de vos équipes et renforcer la sécurité de votre organisation : avec cet outil immersif et innovant, vous transformez l'imprévu en opportunité de démontrer votre maîtrise et votre capacité à anticiper et gérer les crises cyber avec proactivité.

Investissez dès aujourd'hui dans l'avenir numérique de votre entreprise !

Plongez au coeur de la crise pour renforcer vos capacités cyber

Découvrez une expérience immersive exceptionnelle au sein du Campus Cyber National, véritable vitrine de l'excellence en cybersécurité française. Notre solution vous place au centre de scénarii de crise cyber inédits, combinant technologies de pointe et analyse comportementale approfondie.

Avec ses 18 sièges et une flexibilité d'organisation unique, la salle Cyber Experience s'adapte à vos besoins :

- Exercices COMEX/CODIR et managers dirigeants : simulez des crises stratégiques à haut niveau.
- Scénarii individuels SOC/CSIRT : mettez vos cyber défenseurs et vos équipes DSI à l'épreuve en salle de réponse à incidents.
- Tests pour hauts potentiels et recrutements stratégiques : grâce à des mises en situation immersives et exigeantes, révélez leurs compétences clés face à des enjeux de leadership et de résilience.

GESTION D'UNE CRISE D'ORIGINE CYBER DANS UN CENTRE DE CRISE OPÉRATIONNEL (CCO)

Formation-action des équipes dirigeantes (COMEX / CODIR) Agir face à la crise

Préparez votre équipe à gérer une cybercrise avec efficacité et assurance.
Plongez au cœur d'une simulation immersive et collaborative pour affronter les enjeux critiques d'une cyberattaque. Organisés en équipes de 6 fonctions ou en 6 équipes de 3 fonctions, vos dirigeants seront formés à comprendre les impacts stratégiques d'une attaque, à développer les réflexes indispensables pour réagir avec confiance et à maîtriser la coordination, la prise de décision rapide et l'action collective face à des situations d'urgence. Ce programme unique transforme les défis en opportunités, en renforçant les compétences essentielles pour gérer avec succès un enchaînement d'événements critiques et faire de chaque crise une occasion de progrès pour votre entreprise.

Une formation indispensable pour anticiper et gérer les crises cyber
Dans un contexte où les menaces numériques évoluent sans relâche, préparer le Top Management à faire face à une crise cyber n'est plus une option, mais une nécessité stratégique et réglementaire. La question n'est pas de savoir si une attaque surviendra, mais quand.
Notre formation immersive et innovante vous donne les clés pour anticiper les enjeux critiques, réagir avec efficacité et limiter les impacts sur votre organisation. En plongeant au cœur des répercussions d'une attaque sur toutes les fonctions de l'entreprise, elle transforme chaque participant en un acteur clé de la résilience collective. Soyez prêt à agir, à protéger et à guider votre entreprise.

À travers des scénarios immersifs dans notre Centre de Crise Opérationnel (CCO), les participants découvriront comment :

- Développer les soft skills nécessaires pour réagir en temps de crise
- Travailler efficacement en équipe dans des conditions de haute pression
- Améliorer leur propre performance face au stress et à la surinformation
- Coordonner la réponse à un incident critique en collaboration avec les autres dirigeants

FORMATION EN ÉQUIPE

GESTION D'UNE CRISE D'ORIGINE CYBER DANS UN CENTRE DE CRISE OPÉRATIONNEL (CCO)

PROGRAMME

Briefing sur l'exercice CCO

- Introduction au contexte de l'entreprise (fictive) au centre du scénario + contexte géopolitique de l'exercice de simulation
- Accès et prise en compte des documents supports de l'exercice
- Explication sur les critères d'évaluation de l'exercice
- Fonctionnement de l'interface technique pour l'exercice et prise en main

10h00
Début de l'exercice de simulation CCO (par équipe de 3 ou 6 personnes)

14h30
Fin de l'exercice de simulation et pause déjeuner

15h30 : Cours « Construction de la décision en gestion de crise »

- Introduction : les fondamentaux de la gestion de crise (10 min)
- Étape 1 : analyse rapide de la situation (15 min)
- Étape 2 : prise de décision sous pression (20 min)
- Étape 3 : communication et mise en oeuvre de la décision (20 min)
- Étape 4 : retour d'expérience et apprentissage post-crise (15 min)
- Conclusion et synthèse (10 min)

17h00 : Restitution des observations et résultats Crise Cyber Experience by GGE

- Restitution des analyses de performance des équipes (vitesse de traitement des informations, décisions et nombre d'actions)
- Restitution des analyses de comportements observés durant l'exercice (niveau de stress, concentration, implication)
- Restitution des analyses de contenus (réponses à la crise / production documentaire)
- Présentation des suites potentielles à l'exercice

18h30
Fin des opérations

DURÉE

9 heures de formation (8h30-18h30) sur une journée

ENCADREMENT

L'exercice et la formation à la gestion de Crise sont encadrés par 5 personnes.

- Un pilote de l'exercice (assurant le briefing de contexte, la conduite de l'exercice et le débriefing)
- Un pilote technique (assurant l'explication des outils et interfaces techniques pour la simulation, et assurant la gestion des opérations durant l'exercice)
- Un intervenant pour conduire le cours de construction de la décision en gestion de crise, et participant au RETEX de fin de journée.
- Un psychologue comporte-mental ou synergologue (diagnostic comportemental de l'équipe + RETEX de fin de journée)
- Un expert dans la gestion de crise (analyse des documents et contenus produits pendant l'exercice + RETEX en fin de journée).

PUBLIC VISÉ

Dirigeants, cadres dirigeants confrontés à des situations de crise ou devant prendre des décisions stratégiques sous pression. Administrateurs d'entreprise souhaitant renforcer leur capacité à gérer des crises, notamment d'origine cyber.

TARIFS

Sur demande

PRÉ-REQUIS

Pas de prérequis techniques. Expériences significatives pour la prise de décision.

DÉLAIS ET MODALITÉS D'ACCÈS

Après signature du devis, l'Ifpass vous fournira un formulaire pour inscrire les participants. Selon l'exercice, le nombre de participants doit être un multiple de 6 (3 équipes de 6) ou de 3 (6 équipes de 3), pour un total de 18 places. Les participants complètent leurs informations personnelles en ligne via un lien, avec un délai de 10 jours ouvrés pour finaliser les formalités. Une fois ces étapes terminées, un accusé de réception confirmant l'inscription et la réservation est envoyé par mail.

MODALITÉS PÉDAGOGIQUES

L'ensemble des moyens pédagogiques sont inclus et disponibles :

- matériel informatique et interfaces utilisateurs dans la salle
- capteurs et outils de mesures de performances
- systèmes de conduites de scénarii et d'envoi de stimuli
- documents ressources et modèles de documents (placés dans l'environnement de travail du participant).

MODALITÉS D'ÉVALUATION

Toutes les évaluations se font dans le cadre de l'exercice de simulation :

- vitesse de réaction et prise de décision
- qualité de la gestion opérationnelle
- analyse comportementale
- pertinence des réponses aux incidents et production de documents clés

Une attestation de formation sera remise à chaque participant. Ces attestations seront conformes aux directives NIS2 et DORA, accompagnées d'un rapport de performance individuelle et collective.

RÉPONSE À INCIDENT DANS UN SECURITY OPERATION CENTER (SOC) À DESTINATION DES CYBER DÉFENSEURS

Une expérience unique et individuelle

Renforcez vos capacités de réponse face aux incidents cyber. Notre formation immersive offre une expérience unique au cœur d'un SOC (Centre Opérationnel de Sécurité), spécialement conçue pour développer les compétences des cyber-défenseurs et optimiser leurs performances en situation d'attaque. Préparez vos équipes à anticiper, réagir et protéger avec expertise et assurance.

Une formation incontournable pour relever les défis de la cybersécurité moderne

Dans un environnement numérique de plus en plus complexe et exposé, les cyber-défenseurs doivent gérer un volume croissant d'événements de sécurité à travers des systèmes souvent hétérogènes et multipliant les points d'entrée (SCADA, IoT, Cloud).

Face à la rapidité des flux de données et à la prolifération des attaques, une réactivité exceptionnelle et une vigilance accrue sont indispensables pour garantir une défense efficace. Ces compétences ne s'improvisent pas : elles se développent et s'affinent grâce à un entraînement rigoureux dans un contexte collectif et immersif.

Notre formation vous permet non seulement de cultiver ces aptitudes essentielles, mais aussi de mesurer leur progression pour atteindre une performance durable et optimisée.

Cette formation vous permettra :

- d'améliorer votre vitesse de réponse et votre capacité d'analyse des incidents en temps réel
- de simuler des situations de crise cyber dans des conditions proches du réel
- de perfectionner votre intuition et vos soft skills dans un contexte émotionnel intense

FORMATION INDIVIDUELLE

RÉPONSE À INCIDENT DANS UN SECURITY OPERATION CENTER (SOC) À DESTINATION DES CYBER DÉFENSEURS

PROGRAMME

9h00 - Briefing sur l'exercice SOC/ CSIRT

- Présentation du contexte de l'entreprise fictive + contexte géopolitique de l'exercice de simulation
- Présentation des documents supports de l'exercice
- Présentation des critères d'évaluation de l'exercice

10h00

« Introduction à l'Analyse SOC / Gestion de Crise Cyber »
Présentation du fonctionnement de l'interface technique de l'exercice
+ prise en main des interfaces d'exercices.

11h00

Début de l'exercice de simulation SOC / CSIRT

14h00

Fin de l'exercice de simulation et pause déjeuner

15h00 - Formation « Retour sur la gestion des incidents et analyse SOC »

- Introduction à la gestion des incidents de sécurité (15 min)
- Détection et surveillance des menaces (20 min)
- Processus de réponse aux incidents (20 min)
- Analyse des logs et investigation (20 mn)
- Simulation d'incident et retour d'expérience (15 min)

16h30 - Restitution des observations et résultats concernant l'exercice

- Restitution des analyses de performance (vitesse de traitement des informations, nombre et qualité des réponses).
- Restitution des analyses de comportements observés durant l'exercice (niveau de stress, concentration, implication)
- Présentation des suites potentielles à l'exercice

17h30

Fin des opérations

DURÉE

7,5 heures de formation (9h-17h30) sur 1 journée

ENCADREMENT

L'exercice et la formation à la gestion de Crise sont encadrés par 5 personnes.

- Un pilote de l'exercice (assurant le briefing de contexte, la conduite de l'exercice et le débriefing)
- Un pilote technique (assurant l'explication des outils et interfaces techniques pour la simulation, et assurant la gestion des opérations durant l'exercice)
- Un intervenant pour conduire le cours de construction de la décision en gestion de crise, et participant au RETEX de fin de journée.
- Un psychologue comporte-mental ou synergologue (diagnostic comportemental de l'équipe + RETEX de fin de journée)
- Un expert dans la gestion de crise (analyse des documents et contenus produits pendant l'exercice + RETEX en fin de journée).

PUBLIC VISÉ

Chargés de cyberdéfense (SOC niveaux 1 et 2)
Cadres et équipes des centres opérationnels de sécurité (SOC)
Coordinateurs de réponse à incident dans des organisations privées et publiques
Équipes DSI
Hauts potentiels

TARIFS

Sur demande

PRÉ-REQUIS

Connaissances fondamentales en systèmes d'information, réseaux et sécurité informatiques

DÉLAIS ET MODALITÉS D'ACCÈS

Après signature du devis, l'Ifpass vous fournira un formulaire pour inscrire les participants. Selon l'exercice, le nombre de participants doit être un multiple de 6 (3 équipes de 6) ou de 3 (6 équipes de 3), pour un total de 18 places. Les participants complètent leurs informations personnelles en ligne via un lien, avec un délai de 10 jours ouvrés pour finaliser les formalités. Une fois ces étapes terminées, un accusé de réception confirmant l'inscription et la réservation est envoyé par mail.

MODALITÉS PÉDAGOGIQUES

L'ensemble des moyens pédagogiques sont inclus et disponibles :

- matériel informatique et interfaces utilisateurs dans la salle
- capteurs et outils de mesures de performances
- systèmes de conduites de scénarii et d'envoi de stimuli
- documents ressources et modèles de documents (placés dans l'environnement de travail du participant).

MODALITÉS D'ÉVALUATION

Toutes les évaluations se font dans le cadre de l'exercice de simulation :

- vitesse de réaction et prise de décision
- qualité de la gestion opérationnelle
- analyse comportementale
- pertinence des réponses aux incidents et production de documents clés

Une attestation de formation sera remise à chaque participant. Ces attestations seront conformes aux directives NIS2 et DORA, accompagnées d'un rapport de performance individuelle et collective.

Cette salle est dédiée à former chaque individu et chaque participant à mieux comprendre ses biais cognitifs, ainsi qu'à apprendre à se comporter, se gérer et analyser ses propres failles face à des attaques potentiellement liées à des machines. L'objectif est de travailler sur l'humain afin qu'il soit capable de se gérer efficacement lors de crises, qui, malheureusement, risquent de devenir de plus en plus fréquentes au fil des années.

Olivier FEIX - Directeur du projet Cyber Experience by GGE, Expert référent cybersécurité - Galileo Global Education

AU PLUS PRÈS DE VOUS

Proche Paris

IFPASS 01 47 76 58 52
172-174 rue de la République - 92800 Puteaux
informations@ifpass.fr

ACCESSIBILITÉ HANDICAP

Nos formations sont accessibles aux candidats en situation de handicap :
L'IFPASS met en place des aménagements techniques ainsi qu'un accompagnement humain adapté en fonction du besoin du candidat.