Exercice de crise cyber :
une formation immersive pour apprendre à décider sous pression lors d'une cyberattaque.

Les cyberattaques sont de plus en plus nombreuses et menacent toutes les entreprises. Le jour d'une cyberattaque, le plus important est de savoir prendre les bonnes décisions rapidement. Entraînez-vous pour protéger votre activité.

Afin de vous accompagner, Groupe Y vous propose une formation d'une demi-journée, animée par sa filiale spécialisée en cybersécurité, YPSI.

EN PRATIQUE

Durée :

1 demi-journée

- 30 minutes de briefing
- 2 heures d'exercice
- 1 heure de debriefing

Lieu : Niort, Poitiers, la Roche-sur-Yon, Paris (format inter-entreprises) ou au sein de vos locaux (format intra-entreprise).

Tarif :

500 € ht	3000 € ht
par participant (inter-entreprises)	par session (intra-entreprise)

Informations légales et prises en charge : la convention de formation sera établie via groupe y services, organisme de formation certifié qualiopi. Veuillez noter que seul le format inter-entreprises est éligible à une prise en charge par votre OPCO.

GroupeY

Qualiopi processus certifié
RÉPUBLIQUE FRANÇAISE
La certification qualité a été délivrée au titre des catégories d'actions suivantes : ACTIONS DE FORMATION

Public : dirigeants d'entreprise (DG, DAF, DRH, directeurs métier, membres de COMEX/CODIR) susceptibles d'être mobilisés en cellule de crise lors d'un incident cyber.

Modalités : présentiel, 6 à 10 participants.

Intervenants
Consultants expert ypsi.

Contact :

Yann Pilpré
06.11.07.27.32,
yann.pilpre@ypsi.fr

Yes we learn

OBJECTIFS

Objectif général : À l'issue de la demi-journée, le dirigeant sera capable d'assumer son rôle de décideur au sein d'une cellule de crise cyber, d'arbitrer sous pression entre enjeux opérationnels, financiers, juridiques et réputationnels, et d'identifier les actions prioritaires à engager dans son organisation pour renforcer sa résilience.

Objectifs opérationnels :

- Reconnaître les signaux caractéristiques d'une crise cyber majeure et en mesurer les impacts business
- Structurer et animer une cellule de crise en clarifiant les rôles, les circuits de décision et les modes de communication interne
- Prendre des décisions stratégiques en environnement incertain et sous contrainte temporelle (paiement de rançon, arrêt d'activité, mobilisation des ressources)
- Arbitrer entre des priorités concurrentes : continuité d'activité, protection des données, conformité réglementaire, image de marque
- Construire et délivrer une communication de crise différenciée selon les parties prenantes (collaborateurs, clients, partenaires, autorités, médias)
- Identifier ses obligations légales et réglementaires immédiates (notification CNIL sous 72h, NIS2 le cas échéant, dépôt de plainte, déclaration assurance cyber)
- Évaluer la maturité de son propre dispositif de gestion de crise et formaliser un plan d'actions correctives transposable dans son organisation

YPSI CYBERSÉCURITÉ

PROGRAMME DE LA FORMATION

- **Séquence 1 :** Cadrage et briefing (30 min)
  Accueil, tour de table, présentation du dispositif Krisium, rappel du cadre de l'exercice et des règles du jeu, distribution des rôles et du contexte fictif de l'organisation simulée.
- **Séquence 2 :** Exercice de simulation sur plateforme Krisium (2h00)
  Mise en situation immersive avec injection d'événements en temps réel : emails, appels téléphoniques, sollicitations médias, messages internes, communiqués partenaires, alertes techniques. Les participants doivent prendre des décisions, communiquer et arbitrer collectivement face à un scénario cyber évolutif. L'animateur pilote les injects et fait monter la pression progressivement.
- **Séquence 3 :** Débriefing à chaud et RETEX (1h00)
  Restitution chronologique des décisions prises, analyse des écarts entre actions menées et bonnes pratiques, identification des points forts et axes d'amélioration. Échange entre pairs sur la transposition dans chaque organisation représentée.

MODALITÉS D'ÉVALUATION

Validation des compétences et des réflexes d'organisation encadrée par le consultant au travers de la mise en situation immersive et validée lors de la phase de débriefing de fin de session.

MOYENS PÉDAGOGIQUES

Utilisation de l'outil Krisium, une plateforme de simulation technologique hautement immersive qui reproduit fidèlement la tension et l'environnement chaotique d'une attaque informatique.

Accessibilité Handicap : Notre processus pédagogique est adaptable. Nous vous invitons à contacter nos équipes en amont de la session pour étudier les aménagements nécessaires à l'accueil de tout participant en situation de handicap.