



ÉCOLE
SUPÉRIEURE
DE LA SÛRETÉ
DES ENTREPRISES

CERTIFICAT GESTION DE CRISE CYBER



VERS UNE NOUVELLE CULTURE DE LA SÛRETÉ



E.S.S.E.



FAIRE FACE À UNE CRISE CYBER : REAGIR, PILOTER, NEGOCIER

Le certificat Gestion de crise cyber de l'ESSE est la première formation à proposer un spectre de réponses complet pour faire face aux conséquences d'une crise cyber.

Désormais devenue une réalité dans toutes les organisations, une cyberattaque requiert une réponse multidimensionnelle : à la fois dans la gestion des parties prenantes de l'organisation visée qui travaillent souvent en silos, dans l'interaction avec l'attaquant, dans la communication de crise interne et externe, et dans la compréhension technique de la situation et des données impactées.

En combinant la méthode de gestion de crise de l'ESSE, mise en application au sein de grands groupes français, avec l'expertise et les techniques de négociation spécifiques à une cyberattaque, la certification permet de mettre en place un système de pilotage adapté et de faire face à l'ensemble des défis d'une crise cyber.



UNE MÉTHODOLOGIE MISE EN ŒUVRE AU SEIN DE GRANDS GROUPES

Cœur du certificat, la méthodologie SOLACE est aujourd'hui déployée et mise en application au quotidien dans plusieurs grands groupes français sous différentes appellations. Cette méthode, nourrie en permanence par les retours d'expérience de nos clients, permet le déploiement d'un système complet de gestion de crise.



UN MODULE SPÉCIFIQUE DE NÉGOCIATION ET DE COMMUNICATION DE CRISE

Les attaques par rançongiciel reproduisent les mêmes étapes qu'une prise d'otage. Qui dit demande de rançon, dit négociation de crise. Qui dit négociation de crise, dit confidentialité. La mobilisation de techniques de négociation et de communication de crise adaptées est essentielle pour gérer la pression de l'attaquant et, si nécessaire, les éventuelles conséquences d'une divulgation des données..

ERIUM

UN PARTENAIRE TECHNIQUE DE PREMIER PLAN : ERIUM

Erium est une société française de cybersécurité, membre du Campus Cyber et du Pôle d'Excellence Cyber (PEC), reconnue pour son expertise dans les domaines de la sécurité opérationnelle : réponse à incident, gestion de crise, CSIRT/CERT, SOC. Ses experts fournissent une veille quotidienne de référence pour plus de 1000 RSSI en France (CESIN) et en Europe (ECSO). Erium développe des solutions de sécurité notamment CyberInvestigation (plateforme de formation et acculturation aux risques cyber) et BlackNoise (première solution européenne de simulation d'attaque #BAS permettant d'évaluer les dispositifs de sécurité en conditions réelles).

Public visé

Le certificat s'adresse à toute personne intéressée par la thématique gestion de crise ou impliquée dans une cellule de crise.

En particulier :

- Responsable de SOC/CERT/CSIRT
- Directeur/Responsable de la sécurité des systèmes d'information
- Directeur de PME/TPE
- Directeur sûreté
- Risk manager
- Responsable de la communication
- Négociateur

Lieu

École Supérieure de la Sûreté des Entreprises
204 boulevard Raspail
75014 PARIS

Prix individuel

2500 euros H.T./3000 euros TTC

Prix entreprise

4500 euros H.T./5400 euros TTC

Durée et rythme

12 jours (84h)

Fréquence

2 sessions par an

Prérequis

- 3 ans d'expérience professionnelle minimum dans une fonction d'encadrement
- Être titulaire d'un bac +3

Conditions d'admission

- Admission sur dossier
- Entretien individuel

Contact

📧 contact@ess-e.fr

☎ 01 79 97 37 37

🌐 www.ess-e.fr

OBJECTIFS

- Mettre en place un système de gestion de crise spécifique à la menace cyber
- Coordonner et piloter les cellules décisionnelles et opérationnelles
- Appréhender les phases techniques de la crise
- Intégrer les principes de résilience opérationnelle propres à une crise cyber
- Mettre en œuvre une négociation et une communication de crise
- Concevoir, préparer et piloter un exercice de crise cyber

PROGRAMME

PILIER 1 – LE PILOTAGE DE LA CELLULE DE CRISE (3 jours)

- Le changement de posture et la gestion du stress
- Les quatre piliers de la gestion de crise (organisation, processus, méthodologie, supports)
- Les attendus et la composition de la cellule de crise
- Le processus de pilotage de la cellule
- La communication et la coordination inter-cellules

PILIER 2 – LES FONDAMENTAUX DE LA CYBERSECURITE EN PERIODE DE CRISE (2 jours)

- La spécificité et les types de crise cyber
- Les événements déclencheurs
- La chronologie type de la crise cyber
- Les phases de détection et de réaction
- La communication dans le séquençage de la crise
- Les pièges à éviter
- Faire face à la crise : le point mort et les trois composants de la préparation
- Le plan de continuité d'activité cyber et la résilience opérationnelle

PILIER 3 – LA NEGOCIATION ET LA COMMUNICATION DE CRISE (2 jours)

- La formation et le rôle du négociateur
- La négociation avec l'attaquant
- Les fondamentaux de la communication de crise
- La définition des éléments de langage
- Le communiqué de presse

PILIER 4 – LA PREPARATION ET LA REALISATION D'UN EXERCICE DE CRISE CYBER (5 jours)

- La conception de l'exercice
- La préparation du dossier d'exercice
- La réalisation et l'animation de l'exercice
- L'organisation du débriefing

Epreuves opérationnelles et examen final :

- **Epreuve collective** : La formation se conclut par la préparation et l'organisation d'un exercice de gestion de crise de grande ampleur qui permet d'intégrer et d'appliquer l'ensemble des méthodes et techniques délivrées pendant la formation
- **Epreuve individuelle** (0,5 jour) : La certification est sanctionnée par un questionnaire à choix multiples



“

« Qu'elle soit probable ou effective, la survenue d'une crise cyber est maintenant une réalité pour toutes les organisations. La gestion d'une crise cyber nécessite des moyens, des capacités opérationnelles et des mécanismes de décision spécifiques. Ce sont ces bonnes pratiques, nourries par les retours d'expérience des crises que nous avons été amenés à gérer, que nous partageons dans cette certification. »

Arnaud Le Men,
Fondateur et DG d'Erium

”



“

« Cette formation est une première car elle permet de s'imprégner de l'ensemble des fondamentaux à connaître pour gérer avec méthode une gestion de crise cyber. Première aussi car elle associe l'expertise méthodologique en gestion de crise de SOLACE et de l'ESSE à celle d'ERIUM dans le domaine de la cybersécurité. Première enfin car la certification introduit un pilier de négociation qui est essentiel à la gestion d'une crise impliquant une fuite de données. »

Lilian Laugerat,
directeur de Solace et directeur
pédagogique du certificat

”



✉ contact@ess-e.fr

☎ 01 79 97 37 37

WWW.ESS-E.FR

204 BOULEVARD RASPAIL
75014 PARIS

