

Organiser la cybersécurité des TPE, PME, organismes publics et privés

Objectif

L'objectif de la formation est de faire du participant un référent cybersécurité interne sur l'organisation de la cybersécurité au sein de l'entité et/ou des métiers.

Personnes concernées

Dirigeants, Responsables des Systèmes d'Information (RSI/DSI), Responsables de la Sécurité des Systèmes d'Information (RSSI), responsables métiers avec forte dépendance cyber

Prérequis

Sensibilisation à la SSI via <https://secnumacademie.gouv.fr/>

Compétences à l'issue de la formation

- Identifier et classer une donnée stratégique ou sensible pour mettre en place des mesures de sécurité Adaptées
- Appréhender les dangers de son écosystème (risques et menaces)
- Interagir avec les structures de sécurité numérique française
- Analyser les risques cyber (définir le cadrage fonctionnel et réglementaire du risque à évaluer ; évaluer la menace les parties prenantes pour décrire la vraisemblance des scénarios stratégiques et opérationnels des attaquants ; proposer et prioriser les mesures organisationnelles et techniques permettant de remédier au niveau de risque)
- Protéger juridiquement l'entreprise ou l'organisme (définir cadre juridique, réaliser des notifications d'incidents, évaluer l'assurance en cybersécurité, analyser le contenu des contrats)
- Organiser la gouvernance et la conformité cyber de l'entreprise ou organisme (analyser, définir et organiser la sécurité des systèmes d'information et le traitement des incidents et des crises)

Organisation

- Session 8 : 05/11/24 – 14/2/25 (S52/1 non travaillées)
- Ou session 9 : 11/3/25 – 6/6/25
- 1ers et derniers jours en présentiel (de préférence)

Formation à distance

Utilisant tous les outils collaboratifs

Office 365/teams tout le long de la formation :

- 7h de travail (asynchrone) par semaine en autonomie et en groupe avec tuteurs disponibles (dont 2 à 3 classes virtuelles synchrones d'échanges avec les experts)
- 13 semaines

Évaluation de la formation

- Évaluation qualitative de la participation et des productions donnant droit à la délivrance d'un diplôme universitaire et d'une certification suite à jury
- Évaluation de la qualité (certification-Qualiopt)

Méthodes pédagogiques actives

- utilisation d'outils de travail en groupe synchrone (visio, chat, partage d'écrans, tableaux, pads, ...) et asynchrones
- Tuteurs affectés aux participants pour les suivre dans le travail en autonomie

Responsable et intervenants

- siham.bouchelaghem@univ-ubs.fr, responsable opérationnelle de la formation
- julien.breyault@univ-ubs.fr, responsable de la formation professionnelle cybersécurité
- Intervenants : professionnels et issus du milieu universitaire

Tarifs

4600€ individuel et nous consulter pour les groupes (12 mini par session)

Organiser la cybersécurité des TPE, PME, organismes publics et privés

PROGRAMME

Public	Organisation de la formation
<ul style="list-style-type: none">- Dirigeants- Responsables des Systèmes d'Information (RSI/DSI),- Responsables de la Sécurité des Systèmes d'Information (RSSI)- Responsables métiers avec forte dépendance cyber	<p>Gouvernance et Conformité (34h)</p> <ul style="list-style-type: none">- Mettre en place une démarche de sécurité (4h)- Mettre en place une PSSI (Politique de Sécurité des Systèmes d'Information) (12h)- Mettre en place un PCA (Plan de Continuité d'Activité) (5h)- Mettre en place un PRA (Plan de Reprise d'Activité) (5h)- Organiser la gestion de crise (4h)- Viser la certification ISO27001 (4h)
	<p>Analyser les risques cyber : mise en œuvre (20h)</p> <ul style="list-style-type: none">- Formation certifiante respectant le référentiel secnumedu-fc- Trois études de cas pratiques en utilisant la méthode EBIOS-RM de l'ANSSI
	<p>Protéger les SI (20h)</p> <ul style="list-style-type: none">- Comprendre les enjeux économiques et organisationnels d'une entreprise liés à leurs informations classifiées (2h)- Comprendre la typologie et motivations des acteurs de l'insécurité et de la sécurité économique (3h)- Utiliser les renseignements de sources opérationnelles, techniques humaines : méthodologies et protections (OSINT, ...) (3h)- Mettre en place des moyens de protections contre les techniques de manipulation (6h)- Comprendre et interagir avec les structures de sécurité française (ANSSI, Gendarmerie, renseignement, ...) (2h)- Exercice de synthèse (4h)
	<p>Intégrer les obligations et responsabilités juridiques de la cybersécurité (16h) :</p> <ul style="list-style-type: none">- Comprendre et agir dans un contexte de droit international complexe (4h)- Se mettre en conformité avec le RGPD : principes fondamentaux, cas pratiques, rédaction d'un registre de traitement de données, contrats et clauses contractuelles, ... (8h)- Anticiper les conséquences juridiques d'une cyberattaque, assurance cyber (4h)