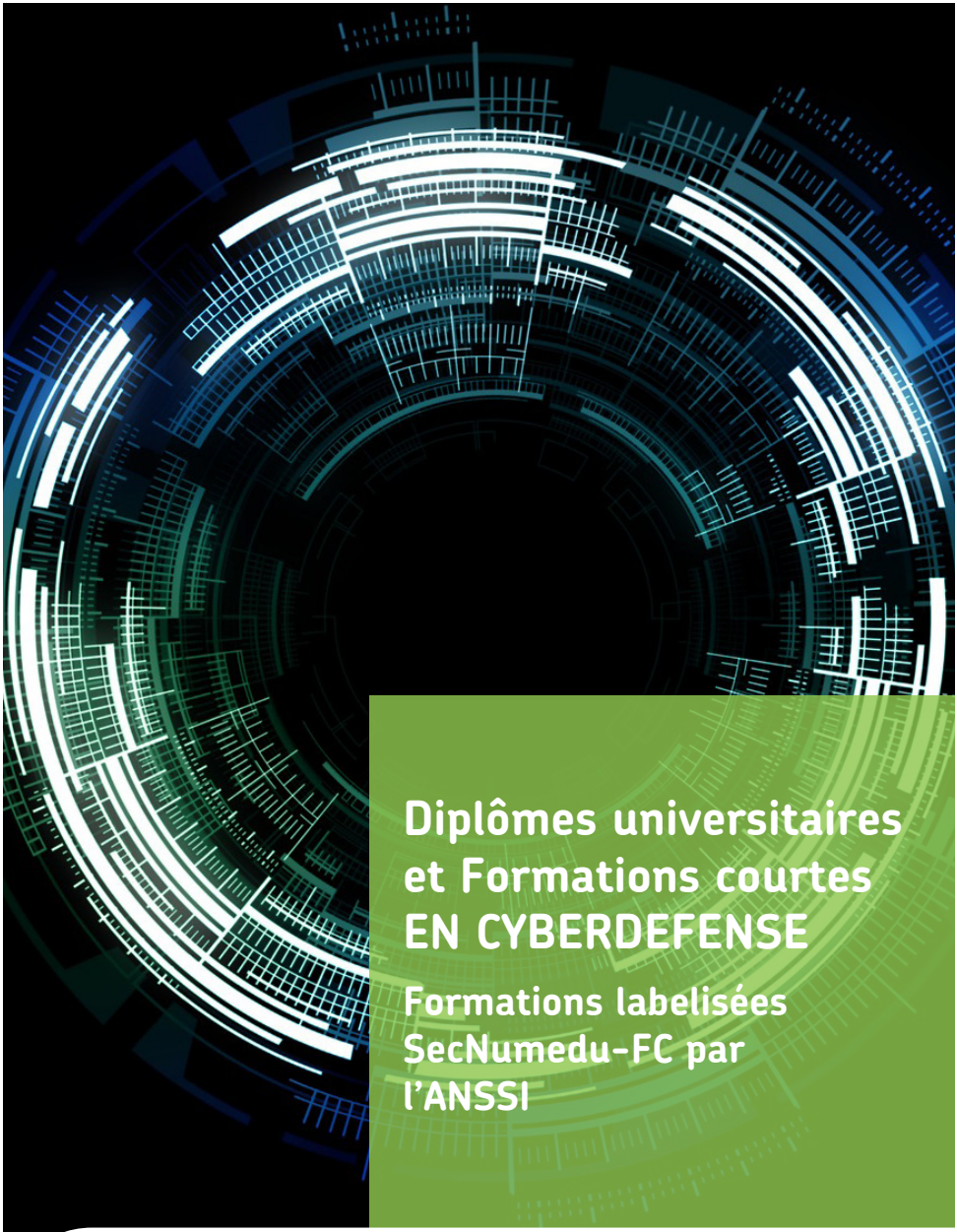

Diplômes universitaires et Formations courtes EN CYBERDEFENSE

Formations labelisées SecNumedu-FC par l'ANSSI

École d'ingénieurs
ensibs
Université Bretagne Sud

www.ensibs.fr

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

Formation Diplômante

Objectif

L'objectif de la formation est de faire du participant un référent cyberdéfense interne sur l'organisation de la Cyberdéfense 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

- Analyser les risques cyber
- Mettre en place une politique de sécurité des systèmes d'information,
- Mettre en place des plans de continuité et de reprise d'activité associés,
- Comprendre les enjeux économiques, juridiques et organisationnels liés aux types d'informations traitées
- Comprendre les menaces
- Interagir avec les structures de sécurité étatiques (ANSSI, gendarmerie, cybermalveillance,…)

SecNumedu
Formation continue
ANSSI

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

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

Tarifs

4500€ individuel
et nous consulter pour les groupes 8mini/18max par session

Organisation

- **Session 1 : 15/11/21 – 11/2/22 (S52 non travaillée)**
- **Ou session 2 : 14/3/22 – 2/6/22**
- **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)**
- **12 semaines**

Évaluation de la formation

- **Évaluation qualitative de la participation et des productions donnant doit à la délivrance d'un diplôme universitaire et d'une certification suite à jury**
- **Évaluation de la qualité (certification FCU depuis 2021, et Qualiopi en cours)**

Cybersécurité des installations industrielles

Formation certifiante

Objectif

- Comprendre les enjeux liés à la sécurité des systèmes d'information, liés à la cybersécurité des systèmes industriels, leurs particularités.
- Aborder les concepts normatifs, tant sur les plans de l'organisation et du management que sur les plans techniques.
- Identifier les points faibles, développer les règles d'hygiène numérique adaptées aux systèmes industriels.

Personnes concernées

- Toute personne en charge de la conception, du développement, de l'intégration ou de l'exploitation et de la maintenance des systèmes industriels.
- Personnes amenées à réaliser des audits ou à accompagner des clients dans leurs projets de renforcement de la cybersécurité des systèmes industriels

Prérequis

Connaissances niveau technicien supérieur en informatique, automatismes et réseaux.

SecNumedu
Formation continue
ANSSI

Méthodes pédagogiques actives

- **à distance** : utilisation d'outils de travail en groupe synchrone (visio, chat, partage d'écrans, tableaux, pads, ...)
- **TP en présentiel** : face-à-face pédagogique, cas pratiques, mises en situations en groupes.

Responsable et intervenants

- eric.martin@univ-ubs.fr, responsable pédagogique de la formation et intervenant
- thomas.toublanc@univ-ubs.fr, responsable de la partie TP
- Intervenants : professionnels et issus du milieu universitaire
- julien.breyault@univ-ubs.fr, responsable de la formation professionnelle cyber

Tarifs

1750€ individuel
et nous consulter pour les groupes 8mini/18max par session
(+ 150€ si 2nd passage de la certification
necessaire suite aux tests)

Organisation

2 sessions par an : la première au printemps et la seconde à l'automne

- **3h de travail asynchrone en autonomie à distance sur 4 semaines (avec travail en groupe, classes virtuelles intermédiaires, témoignages d'experts)**
- **TP sur 2 j en présentiel à Lorient**

Évaluation de la formation

- **Évaluation qualitative de la participation et des productions donnant doit à la délivrance d'un diplôme universitaire et d'une certification suite à jury**
- **Évaluation de la qualité (certification FCU depuis 2021, et Qualiopi en cours)**

EBIOS-RM : mise en pratique de la méthode et des outils

Formation certifiante

Objectif

L'objectif est de pouvoir mettre en œuvre la méthode et/ou être moteur au sein de son organisation afin que la prise de conscience, la prise en compte et l'acceptation des risques SI soit la plus partagée possible et optimise le service rendu.

Personnes concernées

RSSI, risk-manageurs, personnels en charge de l'homologation des SI, consultants SSI, auditeurs SSI, assureurs, DSI, officiers de la SSI, chef d'entreprise/projet SSI...

Prérequis

Sensibilisation à la SSI
https://secnumacademie.gouv.fr/ devra avoir été suivi avant la formation (partie à distance dans tous les cas)

Compétences à l'issue de la formation

Mettre en place un management des risques de cybersécurité utilisant la méthode EBIOS Risk Manager
- en étant efficace plutôt qu'exhaustif
- en prenant en compte l'écosystème
- en organisant selon les objectifs ateliers et participants
- associant conformité et scénarios de risque
- alternant entre point de vue de l'organisation et de l'attaquant
- en utilisant les outils et méthode recommandés par l'ANSSI

Programme

- Accueil, recueil des attentes/contextes, modalités
- Rappels sur le contexte de la gestion du risque SI (ISO 27k,...)
- 1er cas pratique étudié tous ensemble : cadrage et socle de sécurité, sources de risques, scénarios stratégiques, scénarios opérationnels, mesures correctives
- Seconde étude de cas pratique en groupe, utilisation d'un logiciel d'aide à l'analyse

Méthodes pédagogiques actives

Formation à distance : utilisation d'outils de travail en groupe synchrone et asynchrone (visio, chat de groupe, partage d'écrans,...)

Responsable et intervenants

- Julien BREYAULT, enseignant en cyberdéfense à l'ENSIBS formé à EBIOS-RM par le CFSSI de l'ANSSI - julien.breyault@univ-ubs.fr
- Logan FERNANDEZ, CISO, certifié ISO27001 Lead auditor & ISO27005 Lead Risk manager.

Renseignements et inscription

Benoît GAUDICHEAU
benoit.gaudicheau@univ-ubs.fr
tél. +33 (0)2 97 01 72 70

Organisation

Durée : 16 heures à distance sur 2 semaines
Dates : 11-22 octobre 2021 et 15-26 mars 2022
+sessions à la demande
(présentiel possible)

Formation à distance

- **Outils collaboratifs**
- **Office365/teams**
- **8h de travail (asynchrone) /semaine en autonomie et en groupe avec tuteurs (dont 2 à 3 classes virtuelles synchrones d'échanges avec les experts)**
- **2 semaines**

Évaluation de la formation

- **Évaluation qualitative de la participation et des productions donnant doit à la délivrance d'une attestation de participation**
- **Évaluation de la qualité (certification Qualiopi en cours)**

Formation courte de sensibilisation :
My Ludik' Cyber

Objectif
My Ludik' conçoit des « serious games » qui s'adaptent à chaque domaine d'activité.
Avec les équipes My Ludik' et la société MGDIS, l'ENSIBS a développé My Ludik' Cyber pour sensibiliser et former les collaborateurs à la Cybersécurité.

La plateforme My Ludik' favorise l'ancrage réel et le développement des compétences par une méthode ludique et innovante qui permet de transmettre et d'y prendre du plaisir. Le caractère ludique permet d'impliquer davantage les participants en formation.

L'objectif de la formation est de de sensibiliser les participants aux enjeux de la cybersécurité dans leur organisation et d'acquérir les premiers bons réflexes face à des situations issues d'expériences vécues décrites par le support ou les participants.

Personnes concernées
Tous collaborateurs exposés au risque cyber (déjà sensibilisé ou non).

Prérequis
Aucun

Compétences à l'issue de la formation
- Acquérir des bonnes pratiques face aux menaces cyber et les bons réflexes lorsd'attaques
- Connaître la législation spécifique aux risques cyber, à la protection des données
- Identifier les acteurs et interlocuteurs cyber
- Choisir une solution répondant à un besoin en prenant en compte des critères liés au risque cyber
- Analyser les risques cyber

Méthodes pédagogiques actives
- Jeu avec quatre types de questions
- Vrai/Faux et Quizz : pour valider ses connaissances
- Explik' : pour mettre ses compétences en perspective et échanger autour d'un cas pratique
- Déf : pour confronter ses idées avec les adversaires

Responsable et intervenants
- Benoit Gaudicheau, contact administratif et formateur ENSIBS du jeu My Ludik'Cyber
- Camille Barbarin-Renvoisé, Emilie Fromont, Lilian Cizeron, Fabien Levy, apprentis ingénieurs ENSIBS, concepteurs et animateurs du jeu My Ludik'Cyber
- Yoann Prioux, Elian Privat et Philippe Charton, formateurs ENSIBS du jeu My Ludik'Cyber

Tarifs
sur devis

Organisation
Chaque partie dure environ 2h
Plus de 100 questions réparties en 5 catégories : Bonnes pratiques, Gouvernance, Incidents, Protection des données et Solutions sécurisées.
Jusqu'à 4 équipes de 2 à 4 personnes

Renseignements et inscription
Benoît GAUDICHEAU
benoit.gaudicheau@univ-ubs.fr
tél. +33 (0)2 97 01 72 70
07 64 78 37 08

CONTACT ENSIBS

Benoit GAUDICHEAU
chargé de développement de la formation professionnelle et de l'alternance

benoit.gaudicheau@univ-ubs.fr
tél. +33 (0)2 97 01 72 70
tél portable 07 64 78 37 08