INSTITUT UNIVERSITAIRE FORMATION CONTINUE
UNIVERSITÉ SAVOIE MONT BLANC

Formation CONTINUE

R&T
RÉSEAUX INFORMATIQUES ET TELECOMS

IUT ANNECY
UNIVERSITÉ SAVOIE MONT BLANC

CYBER SÉCURITÉ

Selon une étude Gartner, la moitié des entreprises mondiales seront dans l'obligation d'ici 2020 de recourir aux services d'un professionnel pour gérer le risque informatique.
L'explosion du nombre d'objets connectés au sein de l'entreprise (BYOD) met en évidence un grand nombre de failles de sécurité qui s'ajoute à un nombre croissant de cyber-attaques sur des SI d'entreprises ou même privés. La mise en œuvre du RGPD (règlement européen sur la protection des données), en obligeant les entreprises à sécuriser leurs données, va également provoquer une demande encore accrue d'experts en sécurité.

Objectifs de la formation

- Maîtriser les méthodes et outils permettant de lutter contre la cybercriminalité
- Identifier et réparer les failles des systèmes d'information
- Apprendre à traiter les problèmes liés aux domaines de la sécurité numérique
- Auditer et concevoir des SI sécurisés
- Elaborer et superviser un système d'information sécurité
- Définir une stratégie et une politique de gestion des risques

Atouts

- **Inscription libre au module ou au cycle complet,**
- **Rythme de la formation spécialement aménagé afin de permettre la poursuite de l'activité professionnelle,**
- **Pédagogie active, alternant les apports théoriques et les mises en situation pratiques,**
- **Complémentarité des profils au sein de la promotion et richesse des échanges,**
- **Reconnaissance professionnelle délivrée par Stormshield (Certified Stormshield Network Administrator, CSNA) aux candidats obtenant un score supérieur à 70% à l'examen CSNA (dans le cadre du module 5).**
- **Module de formation labellisée SecNumEdu-FC par l'ANSSI (Agence nationale de la sécurité des systèmes d'information).**

Publics

Cette formation s'adresse à tout public, salarié ou demandeur d'emploi, titulaire d'une licence ou équivalent.

Directeurs/chefs de projet SI, managers des systèmes d'information, RSI, ingénieurs R&D, consultants techniques, consultants sécurité, …

Admissions

- Bac + 3 secteur Informatique ou expérience significative en infra réseaux et systèmes
- CV + lettre expliquant les motivations du candidat l'amenant à s'inscrire à ce DU cyber sécurité

Débouchés

- Selon formation initiale : DSI, responsable informatique, responsable sécurité

Rythme

- De janvier à décembre la formation de 175 heures est organisée sur 25 jours à raison de 1 à 3 jours par mois répartis sur l'année civile.
- Le DU comprend 8 modules qui peuvent se faire sur une ou 2 années.

www.iut-acy.univ-smb.fr

Cybersecurite
Pentesting
Forensic
RGPD
Audit de sécurité
Firewalling

FINANCEMENT

Plusieurs possibilités de financement pour les salariés et demandeurs d'emplois : Plan de formation, Période de professionnalisation, Congé Individuel de Formation, Aide individuelle à la formation...

CONTACTS

Responsables de la formation :
Eric CHOTIN
eric.chotin@univ-smb.fr
Maxime BOURBON
maxime.bourbon@univ-smb.fr

Renseignements et candidatures :
formation.continue@univ-smb.fr
04 50 09 22 51

Service Alternance et Formation Continue
9 rue de l'Arc-en-Ciel - BP 240
74942 Annecy-le-Vieux cedex
Tél. 04 50 09 22 45 / www.univ-smb.fr

www.iut-acy.univ-smb.fr

Modalités d'obtention du DU

• Evaluation du projet en fin de DU : présentation de la mise en place d'une infrastructure technique sécurisée (en lien avec un cas concret d'entreprise)

• L'attribution du diplôme est donc conditionnée par le suivi complet du cursus de formation et par une moyenne générale au moins égale à 10/20 (capitalisation possible des modules pour une validation en deux ans).

Programme

MODULES 1 : Les enjeux de la sécurité des SI – 1 jour

- Comprendre les motivations et le besoin de sécurité des systèmes d'information (SI)

MODULES 2 : Sécurité des systèmes (Sauvegarde/antivirus/cloud/serveur de mise à jour/ etc.) – 5 jours

- Connaître les techniques de sécurisation d'un SI, partiellement ou intégralement externalisé
- Mise en place d'un plan de sauvegarde (externalisation de backups), notions de DRP, RPO RTO
- Mise en place d'un WSUS pour maintenir les serveurs et postes de travail à jour (valider les mises à jour avant le déploiement)
- Mise en place de système antivirus avec update on prem et cloud
- Solutions cloud / sécurité stockage et authentification MFA pour accès cloud et prem
- Connaître les enjeux des applications SAAS PAAS
- Comment bien choisir son prestataire de services

MODULES 3 : Systèmes cryptographiques, infrastructures de confiance et mise en œuvre – 3 jours

- Chiffrer/déchiffrer, signer électroniquement un fichier
- Installer, configurer, maintenir une PKI dans un environnement Windows
- Installer des certificats sur un serveur Web ou un client/serveur VPN en environnement Unix.

MODULES 4 : Communication et aspects juridiques de la cyber sécurité, formation et règlementation (LPM, LCEN, NIS, RGPD, OIV, OSE, charte, pédagogie, sensibilisation interne, Bonne pratiques, etc.) – 2,5 jours

- Appréhender et se mettre en conformité avec les obligations légales en matière de protection des données et de sécurisation des systèmes d'information (**L**oi de **P**rogrammation **M**ilitaire, **L**oi pour la **C**onfiance dans l'**E**conomie **N**umérique, directive **N**etwork and **I**nformation **S**ecurity, **R**èglement **G**énéral sur la **P**rotection des **D**onnées)
- Reconnaitre les différentes infractions en matière de cyber sécurité
- Mettre en place des mesures et bonnes pratiques pour prévenir et faire face aux cyberattaques

MODULES 5 : Sécurité des infrastructures et passage de la certification professionnelle Stormshield CSNA inclue dans le module. 3,5 jours

La certification Stomshield est recensée à l'Inventaire de la Commission Nationale de la Certification Professionnelle (fiche 2870 : http://inventaire.cncp.gouv.fr/fiches/2870/).
La CSNA stormshield est labéllisée SecNumEdu-FC par l'ANSSI».

- Prendre en main un firewall SNS et connaître son fonctionnement
- Configurer un firewall dans un réseau
- Définir et mettre en œuvre des politiques de filtrage et de routage
- Configurer des proxys
- Configurer des politiques d'authentification
- Mettre en place différents types de réseaux privés virtuels (VPN IPSec et VPN SSL)
- Sécuriser les accès nomades et lié au BYOD (Bring your Own Devices)

MODULES 6 : Attaques et rapports d'investigation ; typologie, analyse, investigation et mise en œuvre (pentesting / forensic) – 5 jours

- Définir un test d'intrusion
- Maîtriser les différents types d'attaques
- Sélectionner un type de test d'intrusion en fonction du besoin
- Scanner les vulnérabilités d'un système informatique
- Réaliser un test d'intrusion
- Utiliser les outils de test d'intrusion
- Proposer des solutions correctives
- Rédiger et présenter un rapport de test d'intrusion

MODULES 7 : Audit de sécurité – 3 jours

- Connaitre les principales normes ISO du domaine de la sécurité (ISO 27.001, ISO 27.002)
- Connaitre les méthodes d'analyse de risques ISO 27.005, EBIOS
- Connaitre une méthodologie d'audit sécurité du SI basé sur la norme ISO 19.011
- Identifier les principaux risques de sécurité d'une organisation
- Formaliser des constats et recommandations

MODULES 8 : Projet de fin d'études – 2 jours

- Mise en place d'un projet de fin d'étude
- Soutenance individuelle

Coût

Cycle diplômant complet (175 heures) : 4200 € (soit 24 €/heure -tarif avec financement)
Financement individuel : nous consulter
Lieu de la formation : Annecy-le-Vieux