UNIVERSITÉ SAVOIE MONT BLANC

SCIENCES, TECHNOLOGIES, SANTÉ

CU R&T : Cybersécurité pour l'administration d'un système d'information

Présentation

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 systèmes d'information 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, provoque également une demande accrue d'experts en sécurité.

Organisation : Se déroulant de septembre à mai, la formation de 175 heures est organisée sur 25 jours à raison de 1 à 3 jours par mois. Inscription libre au module ou au cycle diplômant complet.

Objectifs

- Maîtriser les méthodes et outils permettant de lutter contre la cybercriminalité
- Identifier et réparer les failles des systèmes d'information (SI)
- 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 sécurisé
- Définir une stratégie et une politique de gestion des risques

Les atouts de la formation

- Pédagogie active, alternant apports théoriques et mises en situations pratiques
- Rythme de la formation aménagée afin de permettre la poursuite de l'activité professionnelle
- Complémentarité des intervenants : enseignants chercheurs experts cybersécurité du monde de l'entreprise.
- 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)

Admission

A qui s'adresse la formation ?

PUBLICS :
Cette formation s'adresse à tout public, salarié ou demandeur d'emploi, titulaire d'un BAC+2 ou équivalent en informatique. Directeurs/chefs de projet SI, managers des systèmes d'information, RSI, ingénieurs R&D, consultants techniques, consultants sécurité…

PROCEDURE DE CANDIDATURE :
Dossier de candidature (CV et lettre de motivation) soumis à l'appréciation du conseil pédagogique (adéquation profil et projet professionnel) + questionnaire .

DÉLAIS D'ADMISSION :
Envoi de la candidature 15 jours avant le début de la formation.

PASSERELLE VAPP :
En cas d'absence du diplôme requis les candidats ont la possibilité d'accéder à la formation par l'intermédiaire de la

MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR, DE LA RECHERCHE ET DE L'INNOVATION
Liberté
Égalité
Fraternité

Validation des Acquis Personnels et Professionnels (VAPP) :
vapp@univ-smb.fr

ACCESSIBILITE :
Cette formation est accessible aux personnes en situation de handicap. La référente handicap est disponible pour répondre à toutes les questions. Les locaux sont accessibles aux personnes à mobilité réduite.

TARIFS ET FINANCEMENT :
Cycle diplômant complet (175h)
4200 € soit 24€/ heure.(Tarif conventionné)
Financement individuel : nous consulter.
Eligible au CPF
Module à la carte : tarif sur demande.

Infos pratiques

Contacts

Responsable pédagogique

Eric Chotin
+33 4 50 09 23 92
Eric.Chotin@univ-savoie.fr

Secrétariat pédagogique

Audrey Lacordaire
+33 4 50 09 22 67
Audrey.Lacordaire@univ-savoie.fr

Gestionnaire administratif

Christelle Dopler
+33 4 50 09 22 51
Christelle.Dopler@univ-savoie.fr

Campus

Annecy / campus d'Annecy-le-Vieux

En savoir plus

Page web et formulaire de contact CU Cybersécurité
https://www.univ-smb.fr/formation-continue/formation-certificat-universitaire-cybersecurite-securite-informatique-annecy-renseignements-informations/

Plaquette PDF CU Cybersécurité
https://www.univ-smb.fr/formation-continue/wp-content/uploads/sites/8/2019/10/formation-cybersecurite-informatique-annecy-diplome-universitaire-cyber-securite-universite-savoie-mont-blanc-formation-continue-securite-des-systemes-dinformation.pdf

Planning prévisionnel CU Cybersécurité 2026-2027
https://www.univ-smb.fr/formation-continue/wp-content/uploads/sites/8/2026/01/planning_previsionnel_cu_cybersecurite_-2026-2027-usmb.pdf

Programme

Organisation

MODULE 1 Les enjeux de la sécurité des systèmes d'information – 7 h
Comprendre les motivations et le besoin de sécurité des systèmes d'information (SI).
MODULE 2 : Attaques et rapports d'investigation : typologie, analyse, investigation et mise en œuvre (pentesting / forensic) – 35 h
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
MODULE 3 : Audit de sécurité – 21 h
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
MODULE 4 Systèmes cryptographiques, infrastructures de confiance et mise en œuvre – 21 h
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 Linux
MODULE 5 Sécurité des infrastructures et passage de la certification professionnelle Stormshield CSNA – 24 h
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)
MODULE 6 Sécurité des systèmes – 35 h
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

MODULE 7 Communication et aspects juridiques de la cyber sécurité, formation et règlementation – 17,5 h

Appréhender et se mettre en conformité avec les obligations légales en matière de protection des données et de sécurisation des systèmes d'information (Loi de Programmation Militaire, Loi pour la Confiance dans l'Economie Numérique, directive Network and Information Security, Règlement Général sur la Protection des Données)
Reconnaître les différentes infractions en matière de cyber sécurité
Mettre en place des mesures et bonnes pratiques pour prévenir et faire face aux cyberattaques.
Projet de fin d'études- environ 40h (26h de travail personnel et 14h de travail encadré)
Mise en place d'un projet de fin d'études.
Soutenance individuelle