CAS en Cyber Security

Préambule

Cette formation vous permet de comprendre les enjeux de la sécurité informatique sous l'angle des techniques et de la stratégie et d'appréhender les différentes lois y relatives.

Le CAS en Cyber Security est décliné en 4 modules, suivis d'un travail pratique.

Contenu

Module 1 : Sécurité Opérationnelle – 78 périodes

Thématique

Ce module de sécurité opérationnelle a pour but de comprendre et de mettre en place la sécurité tant sous l'angle des techniques de protection d'une infrastructure réseau (firewall, proxy, vpn) que logiciel ou base de données.

Dans un second temps, une fois les protections en place en suivant divers guides de bonnes pratiques, une batterie de tests d'intrusion (hacking, social engineering, sécurité du code, forensic) est entreprise afin d'évaluer le niveau de protection réalisé en amont.

Finalement, les nouveaux paradigmes en sécurité (Blockchain, IAM, Utilisation des logs, Cloud) sont également présentés pour garantir une vision large de la sécurité.

Module 2 : Sécurité Stratégique – 32 périodes

Thématique

Ce module de sécurité stratégique a pour but de considérer l'ensemble de l'IT sous l'angle de la sécurité et plus précisément comme Système de Gestion de la Sécurité de l'Information (SMSI).

La mise en place de la sécurité opérationnelle est une étape capitale, mais sans analyse préalable, il n'est pas judicieux de se lancer dans des implémentations architecturales et dans l'achat de diverses solutions.

La sécurité stratégique, par le biais de Standards comme ISO 27000 ou COBIT, permet de prendre du recul en termes de sécurité des technologies de l'information. En commençant par une analyse de risque, le RSSI va pouvoir déceler les actifs informationnels importants pour l'entreprise et ainsi mettre en place tout un plan visant à appliquer un niveau de sécurité adéquat.

Module 3 : Règlement et lois dans le cadre de la protection des données – 22 périodes

Thématiques

Ce module consiste à prendre en compte les différentes lois actuelles (GDPR, P-LPD, LIPDA, Convention 108, Privacy Shield) en ce qui concerne la protection des données et par conséquent la sécurité IT dans son ensemble.

L'organisation de la protection des données et les différents principes juridiques à appliquer sur la sécurité d'une infrastructure informatique sont analysés selon les différentes lois applicables.

Module 4 : Gouvernance – 8 périodes

Thématiques

Aucune entreprise ne peut donner une ligne directrice claire au niveau du métier sans Gouvernance. Il en est de même pour l'informatique. La gouvernance du Système d'Information revêt un aspect capital.

La sécurité d'un SI doit s'intégrer dans des notions plus larges telles la Gouvernance d'entreprise ou la Gouvernance du système d'information. Ces concepts sont abordés pour garantir une compréhension sur l'ensemble des éléments influençant la mise en place d'une sécurité stratégique.

Ce module présente, sous l'angle de certains standards (ISO 20'000, COBIT), les aspects importants d'une gouvernance du SI afin de s'aligner sur la gouvernance d'entreprise en général et de répondre en termes d'objectifs aux besoins actuels.

Travail pratique

- Travail personnel intégrant les modules suivis
- Rapport écrit
- Défense orale

Prérequis

Avoir un bachelor en informatique ou diplôme équivalent ou pouvoir prouver d'une activité professionnelle dans le domaine de l'informatique.

***** Aucun prérequis pour la participation aux modules sans certification finale.

Titre obtenu

Certificat CAS HES-SO (Certificate of Advanded Studies) – 15 crédits ECTS

Lieu

Les cours sont donnés dans nos salles de classe de Bellevue ou de TechnoPôle, à Sierre.

Prix

CHF 6'900.- (finance examen comprise)