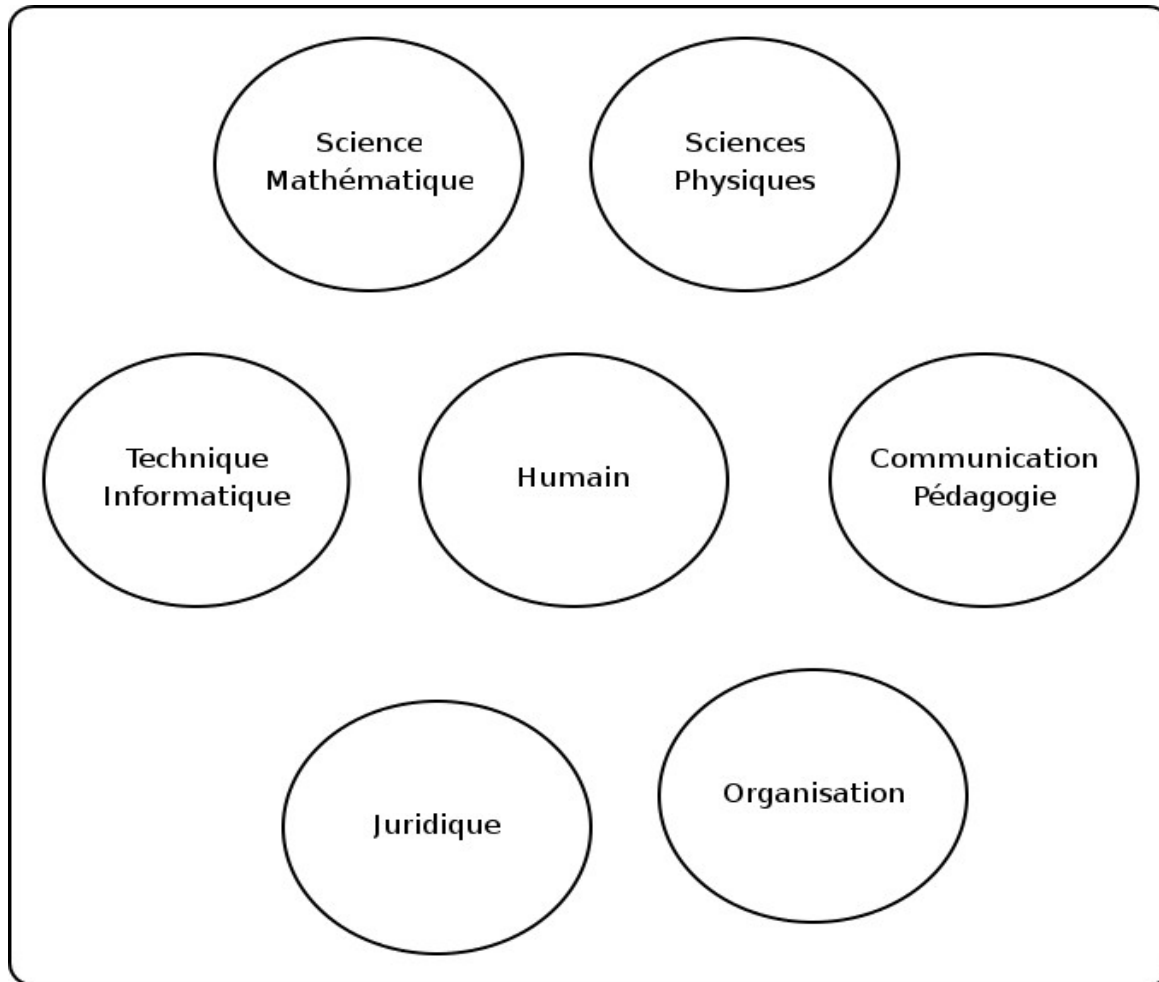


Présentation Paysage

UNIV-PAU / LP

Sécurité des Systèmes d'Information (SSI)
Présentation du paysage

Description du paysage



- Les mathématiques sont impeccables, les ordinateurs faillibles, les réseaux médiocres et les gens pire que tout.
Bruce Schneier
- La technique est impuissante pour répondre à tous les objectifs de sécurité du Système d'information.
- Le sujet est vaste et doit être abordé globalement

Description du paysage

- Ce n'est pas une affaire de
 - mathématiciens
 - physiciens
 - Juristes
 - Techniciens en Informatique
 - Gestionnaires
 - Utilisateurs
- C'est tout en même temps

Description du paysage

- Le processus SSI englobe de nombreux domaines
 - Une approche globale est indispensable
- Les métiers
 - Les compétences
 - Les qualités

Les compétences

- Techniques de sécurisation informatique
- Méthodologie / Normalisation / Organisation / Gestion
- Communication / pédagogie
- Juridiques
- Mathématiques

Les qualités

- La curiosité
 - Le "hacker" dans le bon sens du terme
 - L'avenir est aux curieux de profession
- Modestie / Bon sens
 - Attention à la complexité
 - Connaître son niveau (maturité SSI)
- Rapidité / lenteur
- Communication

Le métier

- Le responsable sécurité idéal
 - Avoir toutes les qualités et compétences citées précédemment !
- Dans la pratique malheureusement, il existe souvent un fossé entre
 - Les aspects techniques et
 - Les aspects gestion / organisation / méthodologie

Les acteurs

- Dans l'entreprise
 - Organisation de la SSI
 - Toute la hiérarchie de la société est concernée
 - Importance de l'implication de la direction
 - Une défaillance en un point suffit
- A l'extérieur (nous ne sommes pas seuls)
 - Associations (OSSIR, CLUSIF)
 - ANSSI
 - FIRST et CERT
 - Sociétés spécialisées
 - Organismes de certification

Le rôle d'un CERT

- CERT : Computer Emergency Response Team
 - Création du premier CERT en 1988 aux USA suite à l'apparition du premier ver Internet ;
 - centralisation des demandes d'assistance suite aux incidents de sécurité (attaques) sur les réseaux et les systèmes d'informations : réception des demandes, analyse des symptômes et éventuelle corrélation des incidents ;
 - traitement des alertes et réaction aux attaques informatiques : analyse technique, échange d'informations avec d'autres CERT, contribution à des études techniques spécifiques ;
 - établissement et maintenance d'une base de données des vulnérabilités ;

Le rôle d'un CERT

- prévention par diffusion d'informations sur les précautions à prendre pour minimiser les risques d'incident ou au pire leurs conséquences ;
- coordination éventuelle avec les autres entités (hors du domaine d'action) : centres de compétence réseaux, opérateurs et fournisseurs d'accès à Internet CERT nationaux et internationaux.

Liste des CERT

- le CERTA est le CERT dédié au secteur de l'administration française.
- le CERT-IST est le CERT dédié au secteur de l'Industrie, des Services et du Tertiaire (IST). Il a été créé à la fin de l'année 1998 par quatre partenaires : ALCATEL, le CNES, ELF et France Télécom.
- le CERT-RENATER est le CERT dédié à la communauté des membres du GIP RENATER (Réseau National de télécommunications pour la Technologie, l'Enseignement et la Recherche).
- **Autres** : CERT-LEXSI, CSIRT BNP Paribas, CERT SG CERT Société Générale, ISIRT INTERPOL INFORMATION SECURITY INCIDENT RESPONSE, Orange-CERT-CC Orange-CERT Coordination Center

Le FIRST

- Organisme mondial
- Coordination des CERT
- Favoriser le partage des connaissances
- Favoriser la diffusion de l'information
- Aider les CERT dans le domaine de la recherche

Quelques rendez-vous annuels

- JSSI / OSSIR
- CLUSIR
- SSTIC
- Salon de la sécurité