



Lutte Informatique Défensive

SOC, CERT et CTI

Georges Bossert - SEKOIA
Fredéric Guihéry - AMOSSYS

6 novembre 2018 - Université Rennes 1



Lutte Informatique Défensive

Abréviation : LID

Domaine : INFORMATIQUE - DÉFENSE

Définition : Ensemble coordonné d'actions menées par un État, qui consistent à détecter, à analyser et à prévenir des cyberattaques, et à y réagir le cas échéant.

JORF n°0219 du 19 sept. 2017 (texte 45)

Organisation du module

—



Un programme en trois chapitres

- Cyber Threat Intelligence (1x2h cours, 1x4h TP)
 - *Analyse et anticipation des menaces*
- SOC (2x2h cours, 1x4h TP)
 - *Supervision et détection des intrusions*
- CERT (2x2h cours, 1x4h TP)
 - *Réponse et remédiation en cas d'incident*



Évaluation des connaissances

- Tous les TPs sont notés
- Épreuve écrite un fin de module



Quelques rappels

Pas de pause sur 2h de cours

- Co-responsabilité
- Les interruptions sont les bienvenues
 - georges.bossert@sekoia.fr
 - frederic.guihery@amossys.fr
- Bienveillance, écoute et respect
- Téléphone éteint