SEC102 - Menaces informatiques et codes malveillants : analyse et lutte

Mis à jour le 17-12-2018

Code : SEC102

Unité d'enseignement de type cours

6 crédits

Volume horaire de référence (+/- 10%) : **50 heures**

Responsabilité nationale :
EPN05 - Informatique / 1

Contact national :

EPN05 - Informatique

2 rue Conté
75003 Paris
01 40 27 22 58
Swathi RANGANADIN RAJASELVAM
swathi.ranganadin@lecnam.net

Présentation

Prérequis

Informaticiens en poste dans les entreprises mais aussi publics en recherche de double compétence ou en reconversion.
Bac+ 2 en scientifique, technique ou informatique ou expérience professionnelle significative dans les métiers de l'informatique

Objectifs pédagogiques

Etre capable de faire de la remédiation adaptée aux contextes de menace.

Compétences

Phase de veille : comprendre les modes d'action pour prévoir les effets
Phase d'alerte : Détecter les effets des codes malveillants
Phase de réponse : minimiser, stopper ou réduire l'impact du code malveillant

Programme

Contenu

Typologies des codes et des effets : Virus, worm, botnet, etc.
Etudes des modes d'action des codes malveillants : analyse intrinsèque des codes malveillants, anatomies d'attaques type, à partir d'exemples réels.
Lutte contre le code malveillant- veille, alertes, détection des effets des codes, identification de la menace.
Caractérisation des effets, Impacts techniques, économiques, fonctionnels.
Réduction des effets, limitation des impacts techniques et fonctionnels.
Analyse postmortem (forensic)
Méthodologies de réponses à incidents
Audits

Description des modalités de validation

Contrôle continu : TP et mémoire portant sur un sujet lié aux codes malveillants (modélisation, anatomie, rétro-conception d'un malware...)