3IF1120 - Détection d'intrusion

Responsables : **Pierre-François GIMENEZ**

Langues d'enseignement : **FRANCAIS**

Campus où le cours est proposé : **CAMPUS DE RENNES**

Nombre d'heures d'études élèves (HEE) : **35**

Nombre d'heures présentielles d'enseignement (HPE) : **18**

Année académique : **2024-2025**

Niveau avancé : **non**

Présentation, objectifs généraux du cours :

Les approches de sécurité classiques sont des approches préventives qui visent à empêcher les violations de la politique de sécurité. Si les approches préventives sont indispensables, elles ne sont cependant pas suffisantes. En effet, des failles permettent de contourner les mécanismes préventifs. La sécurité réactive s'intéresse en conséquence à des techniques permettant de détecter les tentatives de violation de la politique de sécurité et de superviser la sécurité des systèmes d'information. L'objectif final est de pouvoir réagir, parfois automatiquement, afin de ramener le système surveiller dans un état sain, en appliquant des contre-mesures. Le cours aborde les différentes approches de détection des intrusions via les sondes IDS (Intrusion Detection Systems), de corrélation des alertes produites par ces sondes, réalisée typiquement au sein des SIEM (Security Information and Event Manager), et d'échange de données de sécurité (Cyber Threat Intelligence). Il présente également les architectures de supervision qui utilisent ces composants afin de constituer des SOC (Security Operationnal Center).

Période(s) du cours (n° de séquence ou hors séquence) :

SM10

Prérequis :

- Programmation en Python (cours SIP)
- Réseau informatique (électif réseau et sécurité)

Plan détaillé du cours (contenu) :

- De la supervision de sécurité à la réponse à incidents (CM, 3h)
- Sonde IDS : Snort (TP, 3h)
- Cyber Threat Intelligence (CM, 3h)
- Utilisation de l'apprentissage automatique pour la détection d'intrusions (CM, 3h)
- Cas d'étude (CM, 1h30)
- Corrélation d'alerte (CM, 1h30)
- SIEM (TP, 3h)

Déroulement, organisation du cours :

- Cours magistraux (10h30)
- TP (6h)
- Etude de cas (1h30)

Organisation de l'évaluation :

Evaluation des TP

Moyens :

- les TP sont réalisés à l'aide de VirtualBox et s'appuient sur des logiciels open-source (Snort, Suricata, Prelude)

Acquis d'apprentissage visés dans le cours :

- Déployer et configuer une sonde de détection d'intrusions afin de détecter des intrusions
- Déployer et configuer un SIEM afin de corréler des alertes

Description des compétences acquises à l'issue du cours :

- C2.1 Thoroughly master a domain or discipline based on the fundamental sciences or the engineering sciences.

Bibliographie :

- Kruegel C., Valeur F., Vigna G. Intrusion detection and correlation: Challenges and solutions. Springer Advances in Information Security, Vol. 14, ISBN: 978-0-387-23398-7, 2005
- PDIS, Référentiel d'exigences, https://www.ssi.gouv.fr/uploads/2014/12/pdis_referentiel_v2.0.pdf
- Chris Sanders and Jason Smith. 2013. Applied Network Security Monitoring: Collection, Detection, and Analysis (1st. ed.). Syngress Publishing.