



Paris, le 15 Janvier 2019

Challenge Forensic du FIC 2019, des investigations numériques inédites sur fond d'actualité

Mercredi 23 janvier, étudiants et professionnels tenteront de résoudre les Challenges Forensic lors du FIC 2019, organisés avec le parrainage du Commandement de la Cyberdéfense du ministère des Armées. De multiples enquêtes à résoudre suite à des cyberattaques ont été conçues par les étudiants de la majeure Système, Réseau et Sécurité de l'EPITA, avec de nombreux clin d'œil aux actualités 2018 et aux enjeux à venir en matière de cybersécurité.

Un air de déjà-vu et pourtant des challenges uniques

Notpetya : juin 2017, une attaque à des fins de sabotage touche de nombreuses victimes européennes dont des grands industriels du CAC40. **Coinhive** : des codes malveillants s'infiltrèrent et colonisent l'internet pour générer de la monnaie virtuelle à votre insu. **Objets connectés** : et si votre enceinte connectée se retournait contre vous ?

Prolifération d'outils d'attaques sophistiqués, cyberattaques aux effets destructeurs par compromission d'éditeurs ou de prestataires informatiques, le challenge Forensic 2019 du [FIC, Forum International de la Cybersécurité](#), conçu pendant l'année 2018 s'inspire de cyberattaques passées, telles que Notpetya, et des nouvelles tendances en cybersécurité, telles que les coinhives et celles liées aux objets connectés par exemple.

L'ambition de ce challenge est de faire découvrir les métiers liés à l'investigation numérique et à la lutte informatique défensive, ainsi que de promouvoir des talents. Quel est le mode opératoire employé par l'adversaire ? Comment identifier les vulnérabilités exploitées par un attaquant ? Quels sont les effets finaux recherchés par les attaquants ? Autant de questions que devront se poser les participants de ce challenge conçu depuis 2014 par l'EPITA.

« Le parrainage par le Commandement de la Cyberdéfense du [ministère des Armées](#), offre l'opportunité aux étudiants de travailler sur un projet exigeant » détaille Sébastien Bombal, responsable de la [majeure Système Réseau Sécurité de l'EPITA](#).

Des enquêtes bien ficelées par les étudiants et testées par des réservistes opérationnels de cyberdéfense

Début mai 2018, quelques mois après avoir intégré la majeure Système Réseau Sécurité, les étudiants en quatrième année d'ingénieur de l'EPITA se sont démenés pour concevoir et préparer de multiples enquêtes numériques. Ce projet est mené en trois temps précis :

1. Création d'un contexte et d'un réseau d'entreprise.
2. Réalisation de scénarios d'attaques crédibles, en créant des conditions de vulnérabilité et la réalisation de la cyberattaque étape après étape.
3. Montage de l'énigme avec la sélection d'indices initiaux et de ceux à découvrir pendant le challenge.

Le 8 décembre 2018, des [réservistes opérationnels de cybersécurité](#) se sont prêtés à titre d'entraînement à la résolution du challenge ([cf. image en ligne](#)). Leur retour : l'intérêt et l'approbation de son niveau de difficulté graduel et de la qualité des scénarios. **Êtes-vous prêt à relever vous aussi le défi ?**

L'EPITA, grand acteur de la sécurité numérique

Le [Challenge Forensic](#) se déroulera le 2^e jour du FIC, le mercredi 23 janvier de 11h30 à 15h30. Plus de 140 participants sont attendus, étudiants comme professionnels, pour tenter de résoudre ces enquêtes et de remporter des prix tech et une formation en sécurité. Pour bien se préparer, l'EPITA met à disposition [en ligne](#) les scénarios des challenges des années précédentes et apporte la démonstration en vidéo de résolution d'exercices sur la [chaîne YouTube de l'EPITA](#).

[SECUSPHERE by EPITA](#), le centre de formation professionnelle de l'EPITA destiné aux salariés, cadres et dirigeants des entreprises, participera aussi à cette édition du FIC 2019 pour présenter ses modules de formations qui couvrent aussi bien la sensibilisation que l'approfondissement technique et organisationnel. Depuis 2015, ce sont plus de mille collaborateurs qui ont participé aux formations et ainsi acquis les compétences en sécurité numérique adaptées à leurs métiers.

Contacts médias

Florence Moreau

Directrice Communication EPITA & Concours Advance - 01 84 07 43 82 - florence.moreau@epita.fr

Géraldine Seuleusian

Responsable des relations médias - 01 44 54 33 15 - geraldine.seuleusian@ionis-group.com

Anaëlle Sacco

Responsable des relations presse - 01 84 07 43 76 - anaelle.sacco@epita.fr

À propos de l'EPITA

Créée il y a 34 ans, l'EPITA est l'école d'ingénieurs qui forme celles et ceux qui imaginent et créent le monde numérique de demain. Dans sa démarche d'innovation permanente, l'EPITA développe une approche pédagogique numérique inédite et associe avec excellence enseignement et recherche. L'EPITA apporte, par sa présence sur cinq grands campus en France, ses laboratoires et son startup studio, des réponses innovantes aux grands défis technologiques, industriels, économiques et sociaux. Avec ses 7500 diplômés présents dans plus de 2000 entreprises, l'EPITA offre des opportunités de carrière sans frontières.

www.epita.fr

À propos de SECURESPHERE

Pour faire face aux demandes croissantes des entreprises dans le domaine de la sécurité informatique, l'EPITA a créé « SECURESPHERE by EPITA », une offre de formation continue dédiée à la cybersécurité. Cette offre transversale conçue pour les salariés, les cadres et les dirigeants des entreprises couvre aussi bien la sensibilisation que l'approfondissement technique, juridique et organisationnel. Les formations se déclinent en présentiel et en enseignement à distance grâce à la collaboration avec IONIS.

www.securesphere.fr