

LSE ÉQUIPE SÉCURITÉ
Une seule adresse email:
lsesecurite@protonmail.com

RECRUTEMENT 2018-2019

Décembre 2018 — Janvier 2019

- ➊ Présentation de l'équipe "Sécurité"
- ➋ Recrutement parallèle ?
- ➌ Quand ?
- ➍ Quoi ? Étape 1
- ➎ Quoi: Étape 2
- ➏ Quoi: Étape 3
- ➐ La fin: Étape 4

❶ Présentation de l'équipe "Sécurité"

❷ Recrutement parallèle ?

❸ Quand ?

❹ Quoi ? Étape 1

❺ Quoi: Étape 2

❻ Quoi: Étape 3

❼ La fin: Étape 4

Équipe "Sécurité"

- Analyse, Comparaison et Clusterisation/Classification de malware [à grande échelle]
- Algorithmes de la sécurité [génération automatique de règles Yara, cryptanalyse etc.]
- Projet de recherche DGA: sondes de détection d'intrusions sur réseaux d'opérateurs → Machine Learning + Sécurité
- + Projets personnels [à valider par équipe]
- + ANSSI (à négocier).

Profils

- Nous cherchons des "profils" sachant programmer, curieux des problèmes de sécurité (voire d'IA appliquée à la sécurité)
- et surtout désireux d'apprendre par des projets.

LSE 2018 @EPITA

LSE ÉQUIPE
SÉCURITÉ

Présentation de
l'équipe "Sécurité"

Recrutement
parallèle ?

Quand ?

Quoi ? Étape 1

Quoi: Étape 2

Quoi: Étape 3

La fin: Étape 4

① Présentation de l'équipe "Sécurité"

② Recrutement parallèle ?

③ Quand ?

④ Quoi ? Étape 1

⑤ Quoi: Étape 2

⑥ Quoi: Étape 3

⑦ La fin: Étape 4

LSE 2018: Dernière nouvelle

- Vous voulez intégrer l'équipe sécurité
- mais vous voulez faire le projet "équipe IA" en entier
- Faisable: à condition de
 - Faire les deux (petits) challenges
 - Faire le projet IA en entier
- Et donc: vous serez déchargés du projet bitorrent.

➊ Présentation de l'équipe "Sécurité"

➋ Recrutement parallèle ?

➌ Quand ?

➍ Quoi ? Étape 1

➎ Quoi: Étape 2

➏ Quoi: Étape 3

➐ La fin: Étape 4

LSE 2018: Dates importantes

- Présentation: jeudi 6 Décembre
- Recrutement en 4 étapes
- Sujet en ligne: vendredi 7 décembre
- Soutenances: semaine du 7 au 12 Janvier
- Entretiens individuels: du 14 au 19 Janvier
- Accueil des étudiants à partir du 28 Janvier (après l'atelier C++)
- Semaine de formation : 28 Janvier au 2 Février (avec les autres étudiants)
- Remarques: nous serons peut-être amenés à modifier les dates en fonctions des contraintes de type révisions/examens.

- ① Présentation de l'équipe "Sécurité"
- ② Recrutement parallèle ?
- ③ Quand ?
- ④ Quoi ? Étape 1
- ⑤ Quoi: Étape 2
- ⑥ Quoi: Étape 3
- ⑦ La fin: Étape 4

LSE 2018 @EPITA

LSE ÉQUIPE
SÉCURITÉ

Présentation de
l'équipe "Sécurité"

Recrutement
parallèle ?

Quand ?

Quoi ? Étape 1

Quoi: Étape 2

Quoi: Étape 3

La fin: Étape 4

Étape 1

- Projet(s) (ne remplaçant pas MyBittorrent):
- Une seule adresse email:
lsesecurite@protonmail.com
- Une "lettre" de motivation **avant dimanche soir 9 décembre 2018:**
 - 1 Nom, prénom, email (ce n'est pas un cv)
 - 2 Une unique page A4 maximum (tout format mais elle doit être lisible: 11pt minimum)
 - 3 Et surtout: cette "lettre" doit dire ce que voulez vous faire au LSE en 2 ans et demi.
 - 4 Objectifs: en clair ? Vous devez nous convaincre!

- ① Présentation de l'équipe "Sécurité"
- ② Recrutement parallèle ?
- ③ Quand ?
- ④ Quoi ? Étape 1
- ⑤ Quoi: Étape 2**
- ⑥ Quoi: Étape 3
- ⑦ La fin: Étape 4

LSE 2018 @EPITA

LSE ÉQUIPE
SÉCURITÉ

Présentation de
l'équipe "Sécurité"

Recrutement
parallèle ?

Quand ?

Quoi ? Étape 1

Quoi: Étape 2

Quoi: Étape 3

La fin: Étape 4

Étape 2: Challenges

- 0. Site: <http://51.15.4.122/>
- 1. Résolution d'un (petit) challenge "analyse de malware": le but est de trouver le code qui débloque l'application. Fichier: **chall_re.txt**
- 2. Résolution d'un challenge "Forensic": No Comment Fichier: **chall_forensic.zip**

- ➊ Présentation de l'équipe "Sécurité"
- ➋ Recrutement parallèle ?
- ➌ Quand ?
- ➍ Quoi ? Étape 1
- ➎ Quoi: Étape 2
- ➏ Quoi: Étape 3
- ➐ La fin: Étape 4

LSE 2018 @EPITA

LSE ÉQUIPE
SÉCURITÉ

Présentation de
l'équipe "Sécurité"

Recrutement
parallèle ?

Quand ?

Quoi ? Étape 1

Quoi: Étape 2

Quoi: Étape 3

La fin: Étape 4

Étape 3: Challenges

- Un projet "programmation C" (cf première partie du projet équipe "IA")
- Version courte: optimiser un code en C (fourni) qui implémente l'algorithme K-means
- Données: une matrice) de vecteurs de caractéristiques (*features vectors*) de 900 000 malware (EMBER). Chaque vecteur faisant plus de 2300 composantes. Attention: les matrices en jeu sont très grandes ! Utilisez les versions binaires.
- Votre code sera exécuté sur la machine de l'équipe IA [voir recrutement Équipe IA].
- Tout sur <http://ie.dehak.org> (bientôt en ligne)

- ① Présentation de l'équipe "Sécurité"
- ② Recrutement parallèle ?
- ③ Quand ?
- ④ Quoi ? Étape 1
- ⑤ Quoi: Étape 2
- ⑥ Quoi: Étape 3
- ⑦ La fin: Étape 4

LSE 2018 @EPITA

LSE ÉQUIPE
SÉCURITÉ

Présentation de
l'équipe "Sécurité"

Recrutement
parallèle ?

Quand ?

Quoi ? Étape 1

Quoi: Étape 2

Quoi: Étape 3

La fin: Étape 4

Étape 4: Résultats et date limite

- La date limite sera communiquée une fois celle-ci fixée en fonction des contraintes des ING1 mais ce sera début janvier . . . et au plus tard la même date limite que pour l'équipe IA
- Vous devrez envoyer en une seule fois (lsesecurite@protonmail.com)
 - 1 Un petit dossier présentant vos résultats [2 challenges (avec explications) + résultats au CTF]
 - 2 Votre code en C (qui sera en plus normalement sur le compte qui vous aura été attribué sur la machine de l'équipe IA).
- Et venir si et quand vous serez convoqués ou convoquées.