Objectif :

Utiliser & produire de la Threat Intelligence

Scénario :

Vous êtes analystes au sein d'un SOC du ministère des armées.
Le centre d'analyse et de lutte informatique défensive vous a envoyé par mail un rapport d'analyse (joint) sur une campagne en cours : Banacry.
Sur la base de ce compte rendu, vous mènerez une investigation et produirez un rapport d'analyse.

Modalités pratiques :

- Accès au SIEM du SOC (liste des comptes en annexe) jusqu'au 28 mars à 23h59
- Par binôme
- **Production d'un rapport d'incident (noté)**
  - ✓ **Résumé de l'attaque**
  - ✓ **Détail de l'analyse**
  - ✓ **Annexe contenant les IOC identifiés**
- Échéance pour le rapport : 4 avril 2018
- À nicolas.pierson@for-cyb.com

Données disponibles :

```
Bluecoat : Proxy web
cisco:esa  : Passerelle Mail
fgt_traffic : Firewall réseau
linuxsecure : Infos d'authentification Linux
portcontrol : Branchement support amovible
streammysql : Ecoute réseau et interprétation protocolaire de
SQL
winhostmon : Infos de création de processus Windows
```

Annexe : Liste des comptes par binôme

N° de binome	URL	Login	Mot de passe
1	http://ec2-34-241-196-221.eu-west-1.compute.amazonaws.com	user1	lpy(JCj|N4
	http://ec2-34-241-196-221.eu-west-1.compute.amazonaws.com	user2	lpy(JCj|N4
2	http://ec2-34-241-196-221.eu-west-1.compute.amazonaws.com	user3	lpy(JCj|N4
	http://ec2-34-241-196-221.eu-west-1.compute.amazonaws.com	user4	lpy(JCj|N4
3	http://ec2-34-241-196-221.eu-west-1.compute.amazonaws.com	user1	lpy(JCj|N4
	http://ec2-34-241-196-221.eu-west-1.compute.amazonaws.com	user2	lpy(JCj|N4
4	http://ec2-34-241-196-221.eu-west-1.compute.amazonaws.com	user3	lpy(JCj|N4
	http://ec2-34-241-196-221.eu-west-1.compute.amazonaws.com	user4	lpy(JCj|N4
5	http://ec2-34-244-78-43.eu-west-1.compute.amazonaws.com	user1	lpy(JCj|N4
	http://ec2-34-244-78-43.eu-west-1.compute.amazonaws.com	user2	lpy(JCj|N4
6	http://ec2-34-244-78-43.eu-west-1.compute.amazonaws.com	user3	lpy(JCj|N4
	http://ec2-34-244-78-43.eu-west-1.compute.amazonaws.com	user4	lpy(JCj|N4
7	http://ec2-34-241-155-158.eu-west-1.compute.amazonaws.com	user1	lpy(JCj|N4
	http://ec2-34-241-155-158.eu-west-1.compute.amazonaws.com	user2	lpy(JCj|N4
8	http://ec2-34-241-155-158.eu-west-1.compute.amazonaws.com	user3	lpy(JCj|N4
	http://ec2-34-241-155-158.eu-west-1.compute.amazonaws.com	user4	lpy(JCj|N4
9	http://ec2-34-253-68-150.eu-west-1.compute.amazonaws.com	user1	lpy(JCj|N4
	http://ec2-34-253-68-150.eu-west-1.compute.amazonaws.com	user2	lpy(JCj|N4
10	http://ec2-34-253-68-150.eu-west-1.compute.amazonaws.com	user3	lpy(JCj|N4
	http://ec2-34-253-68-150.eu-west-1.compute.amazonaws.com	user4	lpy(JCj|N4
11	http://ec2-34-243-34-136.eu-west-1.compute.amazonaws.com	user1	lpy(JCj|N4
	http://ec2-34-243-34-136.eu-west-1.compute.amazonaws.com	user2	lpy(JCj|N4
12	http://ec2-34-243-34-136.eu-west-1.compute.amazonaws.com	user3	lpy(JCj|N4
	http://ec2-34-243-34-136.eu-west-1.compute.amazonaws.com	user4	lpy(JCj|N4
13	http://ec2-52-50-105-228.eu-west-1.compute.amazonaws.com	user1	lpy(JCj|N4
	http://ec2-52-50-105-228.eu-west-1.compute.amazonaws.com	user2	lpy(JCj|N4
14	http://ec2-52-50-105-228.eu-west-1.compute.amazonaws.com	user3	lpy(JCj|N4
	http://ec2-52-50-105-228.eu-west-1.compute.amazonaws.com	user4	lpy(JCj|N4
15	http://ec2-52-211-216-72.eu-west-1.compute.amazonaws.com	user1	lpy(JCj|N4
	http://ec2-52-211-216-72.eu-west-1.compute.amazonaws.com	user2	lpy(JCj|N4
16	http://ec2-52-211-216-72.eu-west-1.compute.amazonaws.com	user3	lpy(JCj|N4
	http://ec2-52-211-216-72.eu-west-1.compute.amazonaws.com	user4	lpy(JCj|N4
17	http://ec2-34-244-21-65.eu-west-1.compute.amazonaws.com	user1	lpy(JCj|N4
	http://ec2-34-244-21-65.eu-west-1.compute.amazonaws.com	user2	lpy(JCj|N4
18	http://ec2-34-244-21-65.eu-west-1.compute.amazonaws.com	user3	lpy(JCj|N4
	http://ec2-34-244-21-65.eu-west-1.compute.amazonaws.com	user4	lpy(JCj|N4
19	http://ec2-34-249-190-202.eu-west-1.compute.amazonaws.com	user1	lpy(JCj|N4
	http://ec2-34-249-190-202.eu-west-1.compute.amazonaws.com	user2	lpy(JCj|N4
20	http://ec2-34-249-190-202.eu-west-1.compute.amazonaws.com	user3	lpy(JCj|N4
	http://ec2-34-249-190-202.eu-west-1.compute.amazonaws.com	user4	lpy(JCj|N4
21	http://ec2-52-212-77-94.eu-west-1.compute.amazonaws.com	user1	lpy(JCj|N4
	http://ec2-52-212-77-94.eu-west-1.compute.amazonaws.com	user2	lpy(JCj|N4
22	http://ec2-52-212-77-94.eu-west-1.compute.amazonaws.com	user3	lpy(JCj|N4
	http://ec2-52-212-77-94.eu-west-1.compute.amazonaws.com	user4	lpy(JCj|N4
23	http://ec2-52-211-140-242.eu-west-1.compute.amazonaws.com	user1	lpy(JCj|N4
	http://ec2-52-211-140-242.eu-west-1.compute.amazonaws.com	user2	lpy(JCj|N4
24	http://ec2-52-211-140-242.eu-west-1.compute.amazonaws.com	user3	lpy(JCj|N4
	http://ec2-52-211-140-242.eu-west-1.compute.amazonaws.com	user4	lpy(JCj|N4
25	http://ec2-54-154-206-102.eu-west-1.compute.amazonaws.com	user1	lpy(JCj|N4
	http://ec2-54-154-206-102.eu-west-1.compute.amazonaws.com	user2	lpy(JCj|N4
26	http://ec2-54-154-206-102.eu-west-1.compute.amazonaws.com	user3	lpy(JCj|N4
	http://ec2-54-154-206-102.eu-west-1.compute.amazonaws.com	user4	lpy(JCj|N4
27	http://ec2-34-242-152-135.eu-west-1.compute.amazonaws.com	user1	lpy(JCj|N4
	http://ec2-34-242-152-135.eu-west-1.compute.amazonaws.com	user2	lpy(JCj|N4
28	http://ec2-34-242-152-135.eu-west-1.compute.amazonaws.com	user3	lpy(JCj|N4
	http://ec2-34-242-152-135.eu-west-1.compute.amazonaws.com	user4	lpy(JCj|N4
29	http://ec2-52-30-245-225.eu-west-1.compute.amazonaws.com	user1	lpy(JCj|N4
	http://ec2-52-30-245-225.eu-west-1.compute.amazonaws.com	user2	lpy(JCj|N4
30	http://ec2-52-30-245-225.eu-west-1.compute.amazonaws.com	user3	lpy(JCj|N4
	http://ec2-52-30-245-225.eu-west-1.compute.amazonaws.com	user4	lpy(JCj|N4