TP du 19 mars 2020

Objectif :

Utiliser & produire de la Cyber 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 sur une campagne en cours : Banacry.

Sur la base de ce compte rendu, vous mènerez une investigation et produirez, le cas échéant, un rapport d'analyse.

Modalités :

Vous bénéficiez d'un accès au SIEM du SOC (instance Splunk) jusqu'au 19 mars 23h59.

Les comptes doivent être répartis sur l'ensemble de la promotion à l'aide du google sheet.

Splunk peut s'utiliser en effectuant des recherches simples.

Livrable :

Production d'un rapport d'incident (noté) présentant :

- ✓ Le résumé de l'attaque et sa chronologie ;
- ✓ Le détail de l'analyse ;
- ✓ Une annexe contenant les IOC confirmés et les nouveaux IOC identifiés.

Rapport d'incident au format .pdf à envoyer à nicolas.pierson@for-cyb.com avant le **26 mars 2020 23h59.**