Master STIC / SSI

UV GS21 Cyber enquête en entreprises

Session automne 2014

Examen final

1 - Décomposez le processus d'analyse post-incident en quelques tâches élémentaires. Les commenter. 1 point

2- Quelle est la différence entre analyse « live » et analyse post-mortem ? Quelles sont les données concernées dans les deux cas ? Qu'est-ce que cela implique en termes d'outils ? 1 point

3 – Quelle est la différence entre extraction physique et logique ? 1 point

4 - Quel intérêt peut avoir l'ordinateur d'un suspect, lorsqu'on souhaite analyser son appareil iOS? 2 points

5- Qu'est-ce qu'un CERT ? 1 point

6- Quel est le rôle de TRACFIN ? Statuts ? Périmètres ? Pouvoir ? 1 point

7- Quelles sont les ressources internet surveillées par Cyberdouane? Quels sont les moyens techniques de ce service ? 1 point

8- A partir des données recueillies, quelles sont les hypothèses plus particulièrement surveillées par Cyberdouane? 1 point

9- Quand Cyberdouane mène une enquête sur un site de vente en ligne de médicaments, quelles sont les techniques d'enquête utilisées ? 1 point

10- Quel est le rôle d'un expert judiciaire ? 1 point

11- Donnez un exemple de cas (et de service) où une enquête est de type : a)criminel, b)délictuel, c)contraventionnel. 1 point

12 - Quels sont d'une manière générale les pouvoirs et les obligations des enquêteurs? 1 point

13- Entre intervention post-incident et dossier d'enquête, quel est le cheminement de la preuve ?

1 point

14- Cas d'étude (6 points)

Une entreprise de 2000 salariés travaille dans un secteur industriel fortement concurrentiel. Elle pratique des marges serrées. La maison mère comprend le département R&D, la production (800 personnes), l'administration (650 personnes). Elle dispose de 100 points de vente en France (400 personnes) et 25 dans 25 pays du monde (150 personnes).

L'entreprise est concernée par les incidents suivants:

Cas 1 - L'entreprise constate que le prix de ses produits a été modifié sur son site internet.

Cas 2 – L'entreprise constate que deux ordinateurs ont été volés dans son département R&D

Cas 3 – L'entreprise constate des pics d'activité inhabituels pendant la nuit.

Dans chacun de ces cas :

1) Décrire la réaction attendue de l'entreprise
   a) au niveau technique (vous vous placerez dans le rôle du RSSI)
   b) au niveau judiciaire.
2) Quels sont les interlocuteurs de l'entreprise concernés vis-à-vis d'un service d'enquête ?