GS21 - Session automne 2015 - Examen final -
Consignes : notes de cours autorisées

Nom et prénom : _____

Signature de l'étudiant : _____

I- Questions générales (8 points)

1. (1 point) Qu'est-ce que la recherche en source ouverte ? Citez deux exemples d'institutions qui la pratiquent ?
2. (1 point) Qu'est-ce qu'un CERT ? Quelles sont ses tâches prioritaires ?
3. (1 point) Quel est le rôle de TRACFIN ? Qui le sollicite ? Cet organisme a-t-il un pouvoir d'enquête judiciaire ?
4. (1 point) Le code monétaire et financier s'applique-t-il à toute entreprise ? Si non à qui ?
5. (1 point) Quel est le rôle d'un expert judiciaire ?
6. (1 point) Donnez un exemple d'infraction SSI de type a)délictuel, b)contraventionnel. Y en a-t-il de niveau criminel ?
7. (1 point) Quel est le principe du blanchiment d'argent ? De quel code juridique relève-t-il ? Quelles sont les organismes impliqués sur les aspects détection ?
8. (1 point) La CNIL a-t-elle un droit de

-	Oui	Non
Perquisition		
Visite		
Réquisition		

TABLE 1 – Pouvoirs de la CNIL

II- Traitement post-incident (12 points)

Une entreprise de production industrielle avec un département R&D, dans un secteur fortement concurrentiel, est victime d'une tentative d'intrusion. Cette entreprise a un contrat avec un CERT. L'entreprise a des échanges avec le SI d'autres partenaires, fournisseurs, sous-traitants, distributeurs.

1. (1 point) Citez trois exemples de signes de compromission détectables par un usager
2. (1 point) Quelles sont les premières mesures " réflexe " à appliquer, et celles qu'il faut éviter
3. (1 point) L'usager qui constate une anomalie doit prévenir qui et comment ?
4. (1 point) Si l'entreprise constitue une cellule de gestion de crise, comment proposez-vous de la constituer ?
5. (1 point) Quelles seront les différentes phases à gérer par cette cellule de crise ?

6. (1 point) Si l'entreprise décide de porter plainte, qui le fait, et qui peut-il contacter ?
7. (1 point) Quelles sont les techniques d'analyse utilisées par l'enquêteur à chaque étape de son enquête. Commenter.
8. (1 point) 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 ?
9. (1 point) Quelle est la différence entre extraction physique et logique sur un terminal ?
10. (1 point) En cas de dégât à des tiers, quelle est le risque pour l'entreprise ?
11. (1 point) Quels sont les pouvoirs accordés aux enquêteurs officiers de police judiciaire (OPJ)

-	Oui	Non
Perquisition		
Réquisition		
Mise en examen		
Audition		
Garde à vue		
Instruction		
Communication		

TABLE 2 – Pouvoir des OPJ