Étude de cas – Posinc

Instructions générales

Situation : Vous travaillez pour InvNum Inc et vous participez à la perquisition qui vous sera assignée sous peu par courriel. Ce courriel vous assignera aussi l'analyse d'un média précis ainsi qu'un mode de cueillette dont vous devrez justifier la raisonnabilité.

Mission : Vous devez faire une analyse R-OCICE relativement à la raisonnabilité du mode de cueillette des preuves contenues dans un média. Le média qui vous est assigné ainsi que le mode de cueillette que vous devrez justifier vous seront communiqués sous peu. Vous devez répondre en utilisant le formulaire qui vous est transmis via le site web du cours. Les faits découlant de la phase préliminaire de l'investigation seront divulgués dans le document « Étude de cas – Briefing » via le site web du cours. Les faits observés et les actions posées sur le site opérationnels seront divulgués un peu plus tard dans le document « Étude de cas – Actions et observations » via le site web du cours.

Approche : Les instances investigatrices employant InvNum ont décidé d'adopter l'approche « Fouille-Saisie-Examen ».

Décision à justifier : Vos motifs **doivent** aboutir à la conclusion que le mode de cueillette le plus raisonnable est celui qui vous aura été indiqué dans le courriel d'assignation.

Précisions : Pour avoir vos points, il ne suffit pas de citer un passage tiré des « Notes d'investigation numérique ». Il ne suffit pas, non plus, de mentionner des éléments cités dans les documents relatifs à la présente étude de cas. Vous devez clairement relier un passage des « Notes d'investigation numérique » à un élément de la présente étude de cas ou à un élément déduit d'un élément de la présente étude de cas (un « mash-up » similaire à ce qui est enseigné pour les cas de droit). Par exemple : Si vous répondez « Relatifs aux données – Perte éventuelle d'information » à la rubrique « Faits et circonstances » ça vous vaudra **zéro point**. Si vous écrivez « Le suspect coopère pleinement à la perquisition et nous a fourni les mots de passe administrateur du serveur Novell » ça vous vaudra aussi zéro point. En revanche, si vous répondez « Perte éventuelle d'information car le système Novell comporte 12 types de permissions et les données sont copiées sur média formaté NTFS qui ne comporte que 7 permissions. L'utilisation du compte administrateur Novell est donc utile mais ne nous livre tout de même pas l'intégralité de l'information », ça vous vaudra tous vos points.

Exécution : L'assignation vous fournira les renseignements suivants :

- Lieu de perquisition
- Média pour lequel vous devez livrer l'analyse R-OCICE
- Qui est le propriétaire ou l'utilisateur du média en question
- Mode de cueillette que vous devez justifier

Les quatre documents utiles pour réaliser la présente étude de cas seront disponibles sur le site web du cours :

- Instructions générales (la présente page);
- Briefing (donnant le contexte de l'enquête);
- Actions et observations (donnant l'information sur l'exécution de la perquisition);
- Formulaire de réponse.

Le cinquième document est l'assignation de mission qui vous parviendra par le moyen indiqué par le chargé de cours.