SOC – Fondamentaux | Projet de fin de module

Le projet de fin de module vise à mettre en pratique les connaissances que vous avez acquises lors du cours, et surtout, de vous mettre en condition réelle.

Il n'est bien sûr pas attendu de vous la réalisation d'une investigation de niveau professionnelle, mais surtout d'être curieux, de justifier intelligemment vos raisonnements, et de détailler vos observations. Il est encouragé d'inclure le maximum de captures d'écrans & annexes lors de votre restitution.

Le projet se déroulera en groupes de 3 à 4 étudiant·es.

Contexte :

Vous avez la charge de la rédaction d'un rapport d'incident - d'investigations, après qu'une structure aie subit une compromission.

Les seules informations que l'on a pu vous transmettre sont les suivantes :

- Le contrôleur de domaine a été chiffré par le ou les attaquants, qui demandent une rançon
- Il semblerait que le périmètre se cantonne à un VLAN dans lequel se situaient 3 machines : le DC (192.168.206.49), un serveur applicatif (192.168.206.50), et le PC d'un développeur (192.168.206.51)
- Juste après le chiffrement du DC, le développeur, bloqué, a pu extraire les journaux Windows des 3 machines avant qu'elles soient éteintes. Ces journaux sont à récupérer en parallèle du sujet
- Nous utilisons habituellement le logiciel Anydesk pour administration des machines. Celui-ci est d'ailleurs poussé sur les machines du domaine automatiquement.

Votre objectif est donc la **rédaction d'un rapport**, basé sur les principes abordés en cours, qui vous semble assez complet pour présenter à un client final. L'utilisation d'Hayabusa & Timeline Explorer est recommandée, mais pas obligatoire. Attention, les règles de bases ne suffiront pas, il est recommandé de créer vos propres règles et de parser les logs en fonction de ce que vous recherchez.

Les critères de notation sont :

- Respect des consignes (15%)
- Clarté du rapport, mise en forme & rédaction (15%)
- Présence des différentes actions réalisées par l'attaquant (50%)
- Raisonnement / explication des résultats (20%)

Aparté sur l'utilisation de l'IA : l'utilisation d'agents IA en ligne pour ingestion de logs, et / ou pour la rédaction du livrable est strictement interdite. En cas de non-respect de cette consigne, rattrapage systématique.