Formation sécurité opérationnelle

Troisième module : La détection et l'analyse

20 mai 2020

Antoine SURMONNE

École pour l'informatique et les techniques avancées
Majeure Systèmes, Réseaux et Sécurité
SOC

Sommaire

Correction TP1

De bonnes idées :

- parallèle entre les risques identifiés et les mesures de détection appropriées ;
- identification du critère disponibilité prioritaire par rapport aux autres.
- priorisation des chantiers
- Échelle d'évaluation des impacts **quantifiable**
- Identifiants sur la mire de login
- sauvegardes

Quelques oublis :

- menace interne ;
- menaces principalement logiques/système et destructives ;
- matrices d'aversion ;
- Une trop faible prise en compte de l'inertie des entreprises
- des "scénarii"

De bonnes idées :

- tester le système après l'avoir mis en place
- Défense en profondeur
- gestion des règles dans le temps

De bonnes idées, mais risquées :

- WAF

Quelques oublis

- Principalement des mesures de prévention
- "Error : blocked by toto", attention aux signatures d'équipements de défense

De bonnes idées :

- présenter le niveau de criticité des alarmes
- Mode d'emploi des outils

Quelques oublis

- bonjour ?
- contexte, risques identifiés
- que faire d'une alerte ?
- procédure d'escalade

De bonnes idées :

- **Évolution dans le temps**
- Volumétrie d'incidents vs chantiers
- Feuille de route, Gantt

Quelques oublis

- coût des incidents
- dashboard gouvernance trop techniques avec des IPs et des protocoles
- dashboard gouvernance trop "corporate" avec du coloriage
- Satisfaction des employés ? Nombre de produits vendus ?
- "Ces outils doivent être gérés par des professionnels de la sécurité informatique étant donné qu'ils sont compliqués à prendre en main."

Rappels sur le module 2 : la détection et la qualification

Rappels sur le module 2 : la détection et la qualification

Des signaux à pondérer par le temps

précurseur

indicateur

Rappels sur le module 2 : la détection et la qualification

Des signaux à pondérer par le temps

Les éléments suivants sont des signaux précurseurs :

- Un scan de ports
- Une remontée antivirale
- La publication d'une CVE

Les éléments suivants sont des indicateurs de compromission informatique :

- Modification du codensant d'un fichier
- Une remontée antivirale
- La publication d'un dump d'informations

Rappels sur le module 2 : la détection et la qualification

Des signaux à pondérer par le temps

Les éléments suivants sont des signaux précurseurs :

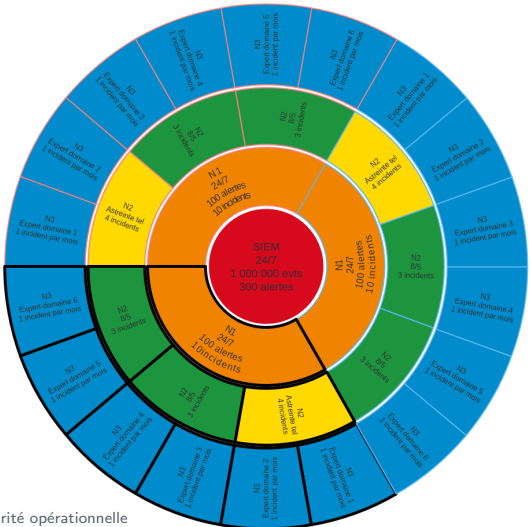
- Un scan de ports ✔
- Une remontée antivirale ✗
- La publication d'une CVE ✔

Les éléments suivants sont des indicateurs de compromission **informatique** :

- Modification du codensant d'un fichier ✔
- Une remontée antivirale ✔
- La publication d'informations internes dans la presse ✗

Rappels sur le module 2 : la détection et la qualification

Structure N1, N2, N3



Dans une organisation N-tiers, les rôles sont les suivants :

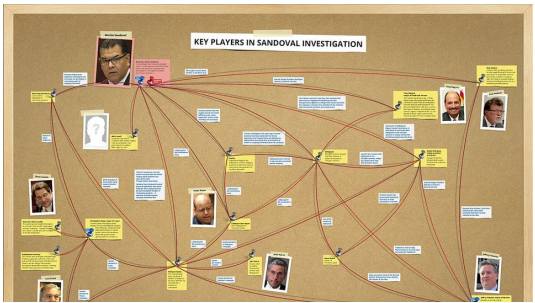
- Le N1 doit prendre en compte l'exhaustivité des alertes
- Le N1 doit finaliser chacune des investigations commencées
- Le N2 peut décider d'arrêter les investigations.
- Le N2 est un expert de la sécurité
- Le N3 est un membre senior du SOC

Dans une organisation N-tiers, les rôles sont les suivants :

- Le N1 doit prendre en compte l'exhaustivité des alertes ✔
- Le N1 doit finaliser chacune des investigations commencées ✗
- Le N2 peut décider d'arrêter les investigations. ✔
- Le N2 est un expert de la sécurité ✗
- Le N3 est un membre senior du SOC ✗

Rappels sur le module 2 : la détection et la qualification

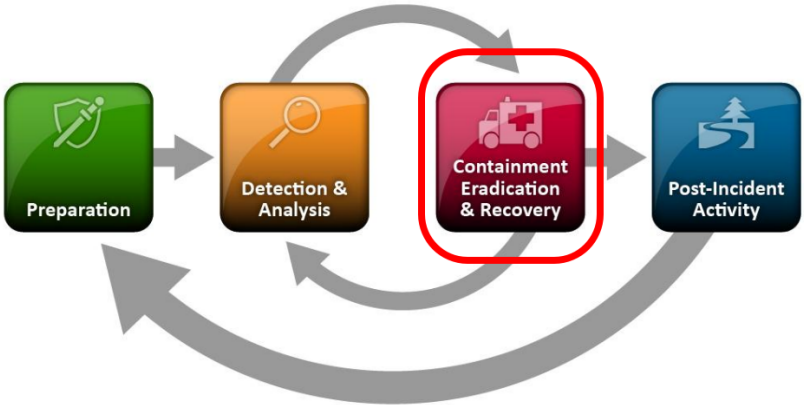
Analyse : raffiner et corréler

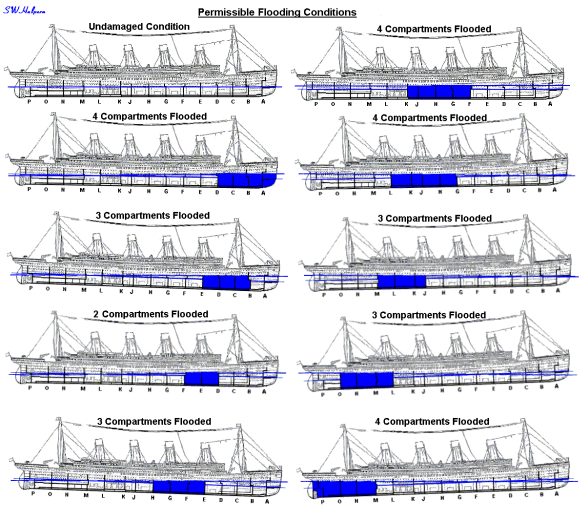


Lors de l'analyse il est prioritaire de :

- Travailler en temps réel ✗
- Synchroniser les sources de temps ✔
- Éviter les inférences ✔
- Sauter sur des conclusions ✗
- Réévaluer les précédentes conclusions à la lumière de nouveaux éléments ✔
- Nommer un coupable ✗
- S'agiter et organiser de nombreuses réunions et mails pour montrer qu'on est sur le pont ✗

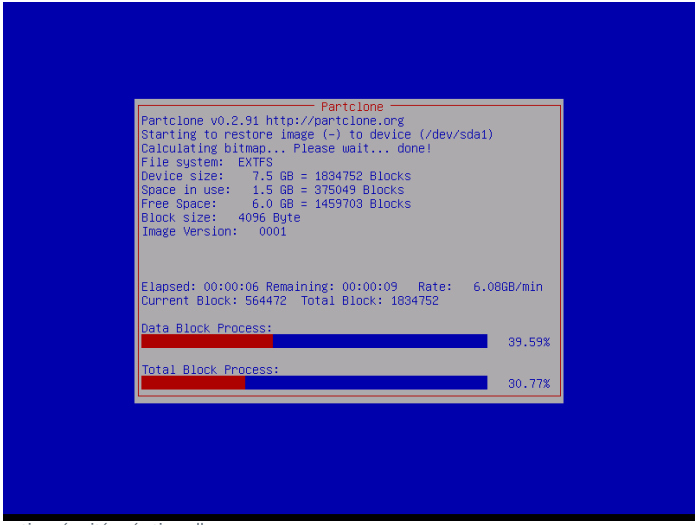
Module 3 : La réponse


Preparation
Detection & Analysis
Containment Eradication & Recovery
Post-Incident Activity


Permissible Flooding Conditions
Undamaged Condition
4 Compartments Flooded
4 Compartments Flooded
4 Compartments Flooded
3 Compartments Flooded
3 Compartments Flooded
2 Compartments Flooded
3 Compartments Flooded
3 Compartments Flooded
4 Compartments Flooded


SCELLÉ NE PAS OUVRIR
500
500
500
SCELLÉ NE PAS OUVRIR
500
500
500


KILL IT WITH FIRE!


Partclone
Partclone v0.2.91 http://partclone.org
Starting to restore image (-) to device (/dev/sda1)
Calculating bitmap... Please wait... done!
File system: EXTFS
Device size: 7.5 GB = 1834752 Blocks
Space in use: 1.5 GB = 375049 Blocks
Free Space: 6.0 GB = 1459703 Blocks
Block size: 4096 Byte
Image Version: 0001
Elapsed: 00:00:06 Remaining: 00:00:09 Rate: 6.08GB/min
Current Block: 564472 Total Block: 1834752
Data Block Process:
39.59%
Total Block Process:
30.77%


You hear someone smash open the door
Panik
It your roommate
Kalm
You have no roommate
Panik

Questions ?