Formation sécurité opérationnelle

Premier module : La préparation

6 mai 2020

Antoine SURMONNE

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

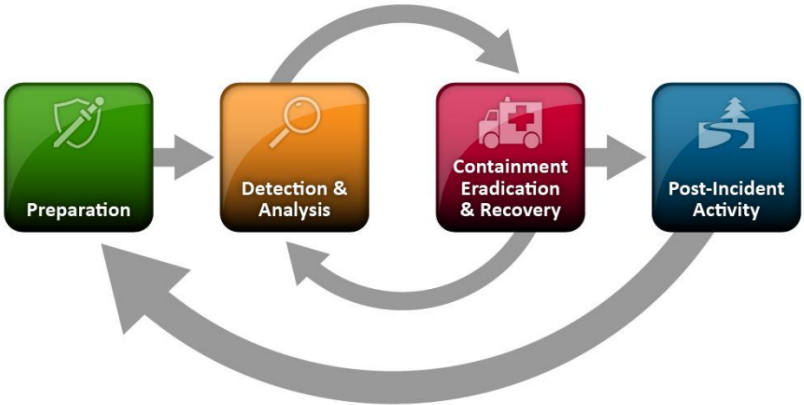
Objectifs

Objectifs de ce module

- connaître le cycle de vie de la cyber-défense ;
- mettre en place une posture de défense.

Sommaire

Le cycle de vie de la gestion d'incidents



Préparer la gestion de l'incident

Moyens de communication

- points de contact : numéros de téléphone, emails, clés de chiffrement, procédures de vérification d'identité ;
- canaux de communications : téléphone portable, messagerie chiffrée ;
- salle de crise : moyens logistiques, montée en puissance des équipes, stockage de scellés ;
- cellule communication : gestion des badauds et des médias.

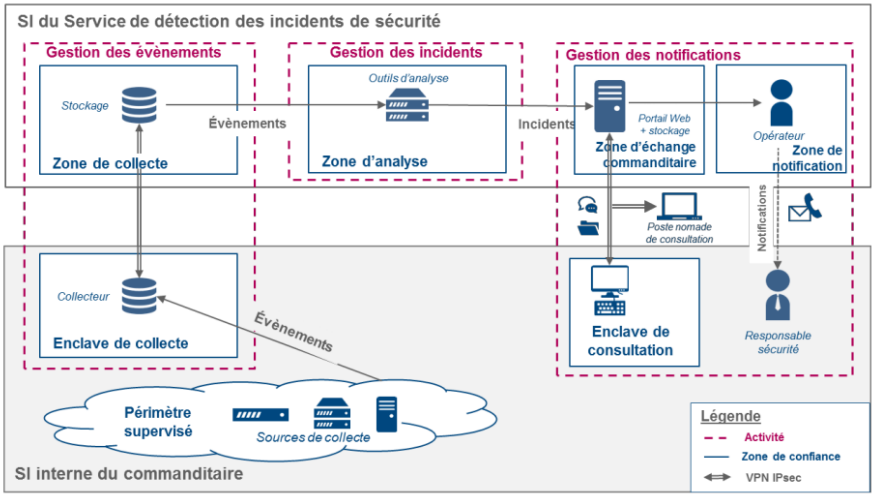
Moyens matériels

- environnement de travail sain ;
- points de capture.

Moyens logiciels

- licences ;
- volumétrie.

Préparer la gestion de l'incident
Logistique



Préparer la gestion de l'incident
Procédures

Documentation

- cartographie réseau ;
- cartographie des points de "valeur" ;
- documentation technique format hors ligne ;
- correctement indexée ;
- empreintes cryptographiques.

Reflexes

- fiches réflexes ;
- organisation, structure et hiérarchie ;
- échelles de qualification.

- collecteur de journaux ;
- NIDS ;
- HIDS.

- simulation ;
- red team ;
- formation.

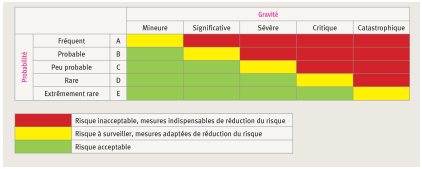
Indicateurs techniques

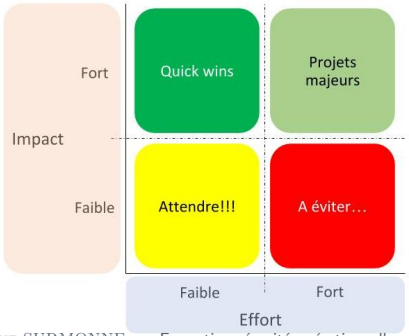
- vision instantanée ;
- écrans de supervision.

Indicateurs gouvernance

- évolution dans le temps ;
- tableaux de bord de suivi.

Préparer la gestion de l'incident
Analyses de risque





Les objectifs d'une analyse de risque bien réalisée

- identification des vulnérabilités ;
- identification des scénarios redoutés ;
- priorisation des contre mesures ;
- itérations. **régulières**

Prévenir les incidents

Garder le flux d'incidents à un volume raisonnable

- sensibilisation des personnels sur les bonnes pratiques ;
- campagnes de fishing factices ;
- durcissement système ;
- tests d'intrusion.

Questions ?