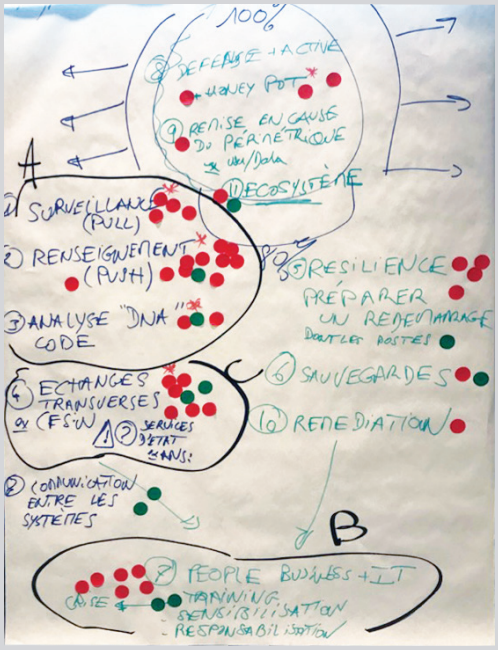
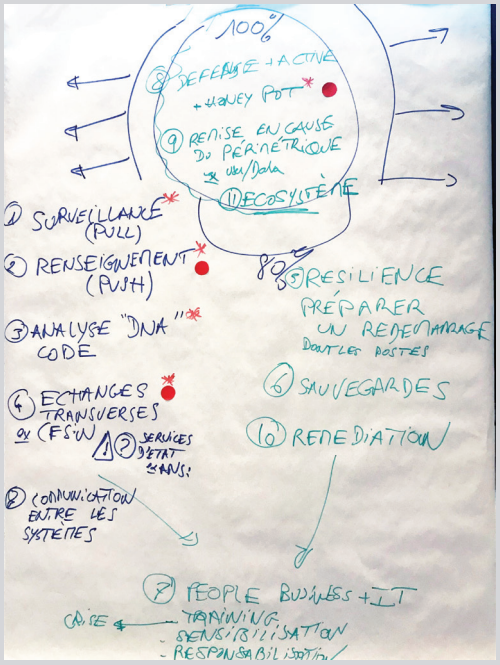
FICHE #4

CyberSécurité : soyons pro-actifs avec de nouvelles pratiques telles que le darkweb, darknet et autres…





ANIMATEUR
Patrice VALADEAU
(SUEZ GROUPE)

ASSESSEUR
Hervé LIOTAUD
(SAILPOINT)

1er sujet : **Anticipation « la guerre se gagne par le renseignement »**

Détecter les tentatives d'attaque :

- Aller rechercher dans les bases de données contenant les comptes,
- Scroller le darknet avec les mots-clés des assets (site web, adresse IP, point d'ancrage centraux),
- Utilisation des marqueurs pour la surveillance ciblée
  - Distinguer les attaques opportunistes et les attaques ciblées
- Les équipes vont voir sur le dark web les versions les plus piratées pour orienter l'achat de hardware. Cela peut devenir un réflexe.

Développement d'un véritable marché souterrain du dark web :

- Notation des meilleurs vendeurs, meilleurs pirates de base => Apparition d'une Blockchain des bases
- Les hackers ont copié le système mafia, qui protège les cibles
- Utilisation d'équipes externes, notamment pour les zones grises (RGPD)

Honey pot :

- Préventif pour détecter les mouvements
- Exemple : test de loyauté des administrateurs (Canary Tools)

FINAKI

2e sujet : **People : tout l'écosystème doit être adressé**

On parle des :

- Ressources internes :
  - IT dont les comptes à privilèges et les développeurs
  - Business
  - VIP
  - VAP (very attacked people)
- Ressources externes :
  - Contractants
  - Freelance
- Ecosystème :
  - Fournisseurs
  - Clients

Actions :

- Sensibilisation
  - Utiliser l'axe personnel pour renforcer l'impact
  - Exemples : Campagnes de Phishing, Journée des enfants pour les parents collaborateurs « passe ton permis web »
  - VIP : compréhension des enjeux et devoir d'exemplarité
- Formation
  - Exemples des groupes imposant une formation obligatoire régulière,
  - Exemple de plateformes : Cybermalveillance.gouv.fr
  - Responsabilisation pour rendre les employés ambassadeurs
- Entraînement et simulation
- Objectif : renforcer la capacité de réaction en période de forte tension
- 80 % doit devenir du réflexe/procédure, 20 % d'adaptation

3e sujet : **Échanges et transversalité**

- Communication publique sur les attaques
- Communauté et clubs ; exemples CESIN, CERCLE de la Sécurité
- Verticaux business : aérospace, retail, agro…
- Échanges entre états : ex ANSSI, BSI (Ger)
- Plateforme dédiée : pharos
- Vigilance renforcée sur les pays sensibles

Conclusion : « Où est la police ? »

- Le foisonnement des menaces et l'explosion des surfaces vulnérables sont une réalité.
- Des efforts d'anticipation et sur la résilience doivent compléter les approches historiques
- Le renforcement des protections doit aider à renforcer la confiance des citoyens et pérenniser le développement de l'économie numérique.
- Néanmoins, malgré leurs efforts les entreprises restent livrées à elle-même : il manque une véritable police du numérique. Il faut une prise de conscience et une véritable volonté politique.

FINAKI